The Sentinel JIRA® Cloud Plugin

Synopsys

2023-11-15: TW-PUB-SH-0018-1.1

Table of Contents

Chapter 1. The Sentinel JIRA® Cloud Plugin

The WhiteHat Sentinel Cloud Plugin for **JIRA®** is a plugin designed to integrate the WhiteHat Portal with **JIRA®**. The plugin provides a seamless interface within **JIRA®** that will sync vulnerabilities from Sentinel to your **JIRA®** application.

As vulnerabilities are discovered and added to the WhiteHat Portal, they are pulled into **JIRA®** and issues are created to get these vulnerabilities into the hands of the individuals responsible for remediation. The vulnerability can be retested and developers can use the WhiteHat Portal's **Ask A Question** feature directly from the issue in **JIRA®** as though they were in the WhiteHat Portal.

1.1. Requirements

- The Jira Project must be a **Company Managed Project**. A **Team Managed Project** will not function correctly.
- You must be logged in as a **JIRA®** Administrator with global permissions in order to install or configure the plugin.

Chapter 2. Installing the Sentinel JIRA® Cloud Plugin

2.1. Downloading the Plugin

The plugin is available from:

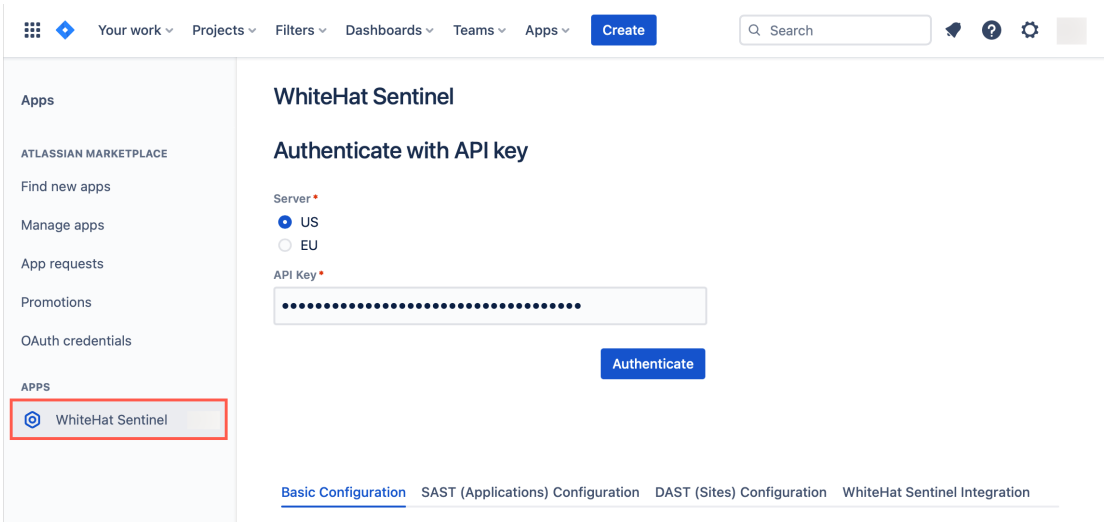
- The Atlassian Marketplace

2.1.1. Install from within JIRA®

To install the plugin, perform the following steps:

1. Log into your JIRA® instance as an admin.
2. Click the admin dropdown and choose **Add-ons**.
3. Click **Find new apps** or **Find new add-ons** from the left-hand side of the page.
4. Locate **WhiteHat Dynamic** via search.
5. Click **Install** to download and install the app.
6. When prompted, grant the app permission to access Atlassian products on your behalf.

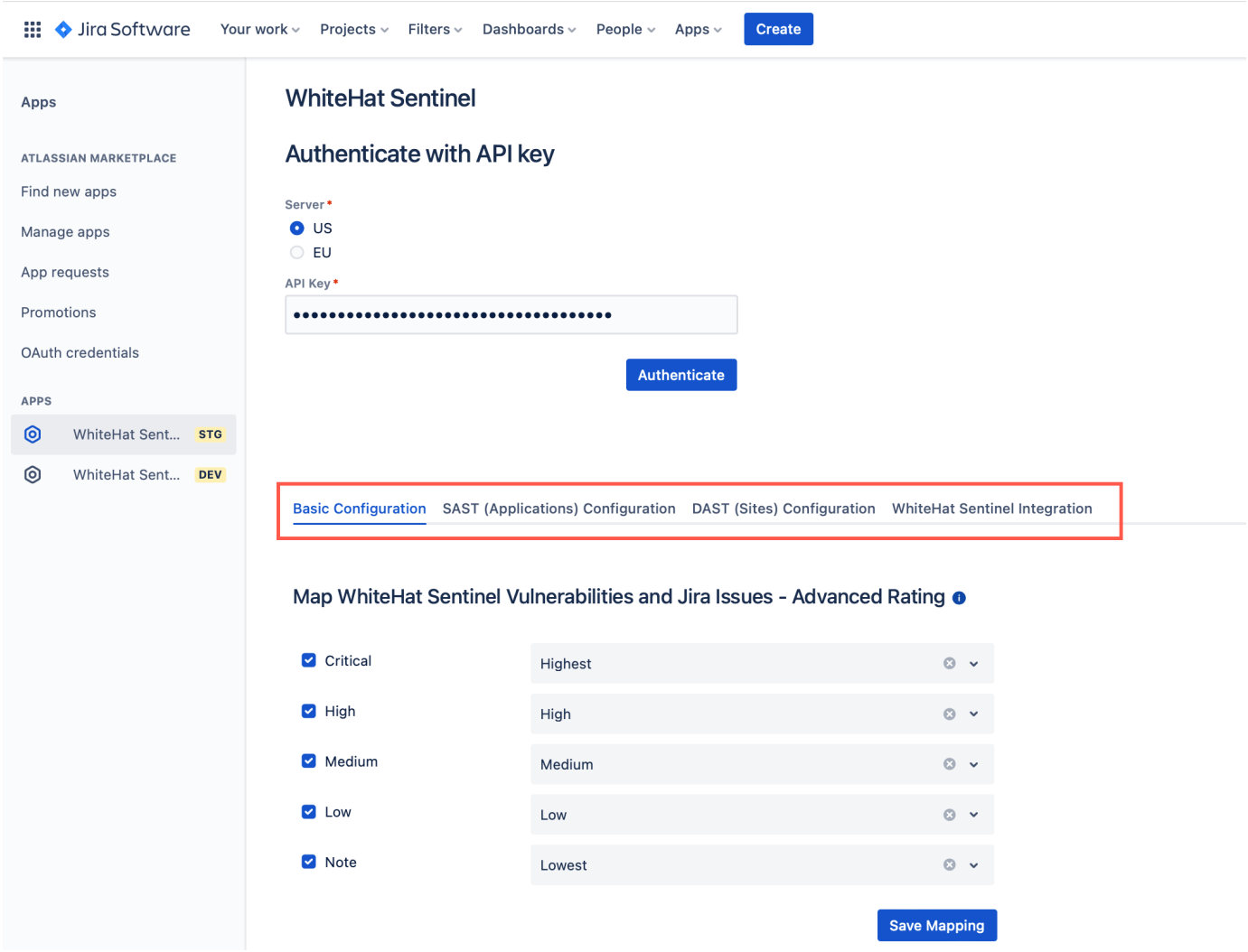
The plugin should now be displayed in the **Manage Apps** section.



Once the add-on is installed, you will need to configure it. Please see Configuring the WhiteHat Sentinel JIRA® Cloud Plugin for more information.

Chapter 3. Configuring the WhiteHat Sentinel JIRA® Cloud Plugin

After a successful API Key authentication to the **WhiteHat Sentinel Cloud Plugin**, the new configuration options are displayed below. Refreshing the **Apps** page may be necessary.



- Basic Configuration: Configure the connections between the plugin and Sentinel. Map WhiteHat Sentinel Vulnerabilities with Jira Issues, Configuration of Jira Tickets, Vulnerability Content, Scheduling Integration, Disable/Enable SAST/DAST integration.
- SAST (Applications) Configuration: Configure the SAST interactions between the plugin and SAST Sentinel services.
- DAST (Sites) Configuration: Configure the interactions between the plugin and DAST Sentinel services.
- WhiteHat Sentinel Integration: Start and stop integration, or redirect to a Developer Console to monitor the plugin.

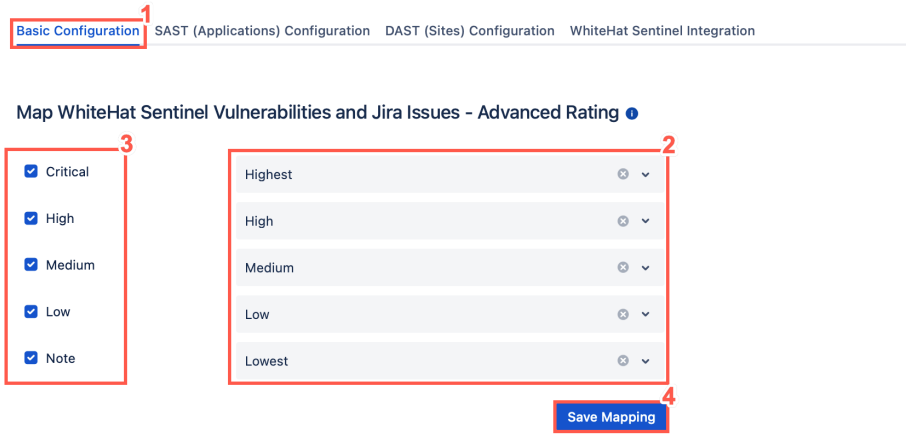
Chapter 4. Basic Configuration

4.1. Mapping Vulnerability Ratings to JIRA® Priorities

Vulnerability ratings will automatically use the **WhiteHat Advanced Rating Methodology**, which is based on **OWASP** ratings.

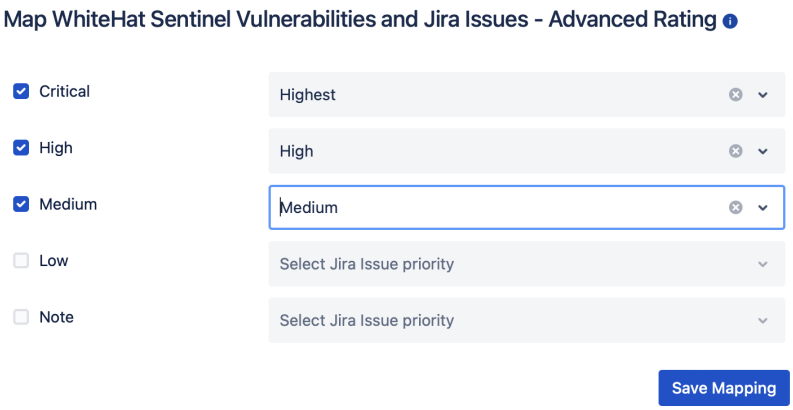
To configure the WhiteHat Sentinel Cloud Plugin for **JIRA®** perform the following steps:

1. Click the **Basic Configuration** tab.
2. The default mapping will associate the most severe rating with the highest **JIRA®** priority. You can change this mapping using the drop-down lists.



NOTE For more information on choosing Legacy Ratings or Advanced Ratings, see Understanding the Rating Methodology.

3. Select the vulnerability ratings that should (checked) or should not (unchecked) be used to create **JIRA®** tickets.



JIRA® tickets will now be created for vulnerabilities rated **Critical**, **High**, or **Medium**. **Critical** vulnerabilities will receive the **Highest JIRA®** priority, **High** risk vulnerabilities will receive a **JIRA®** priority of **High**, and **Medium** risk vulnerabilities will receive a **JIRA®** priority of **Medium**. **JIRA®** tickets will not be created for vulnerabilities with a rating of **Low** or **Note**. In addition it is also possible to limit vulnerabilities that will result in **JIRA®** tickets based on the Sentinel tags associated to the vulnerability.

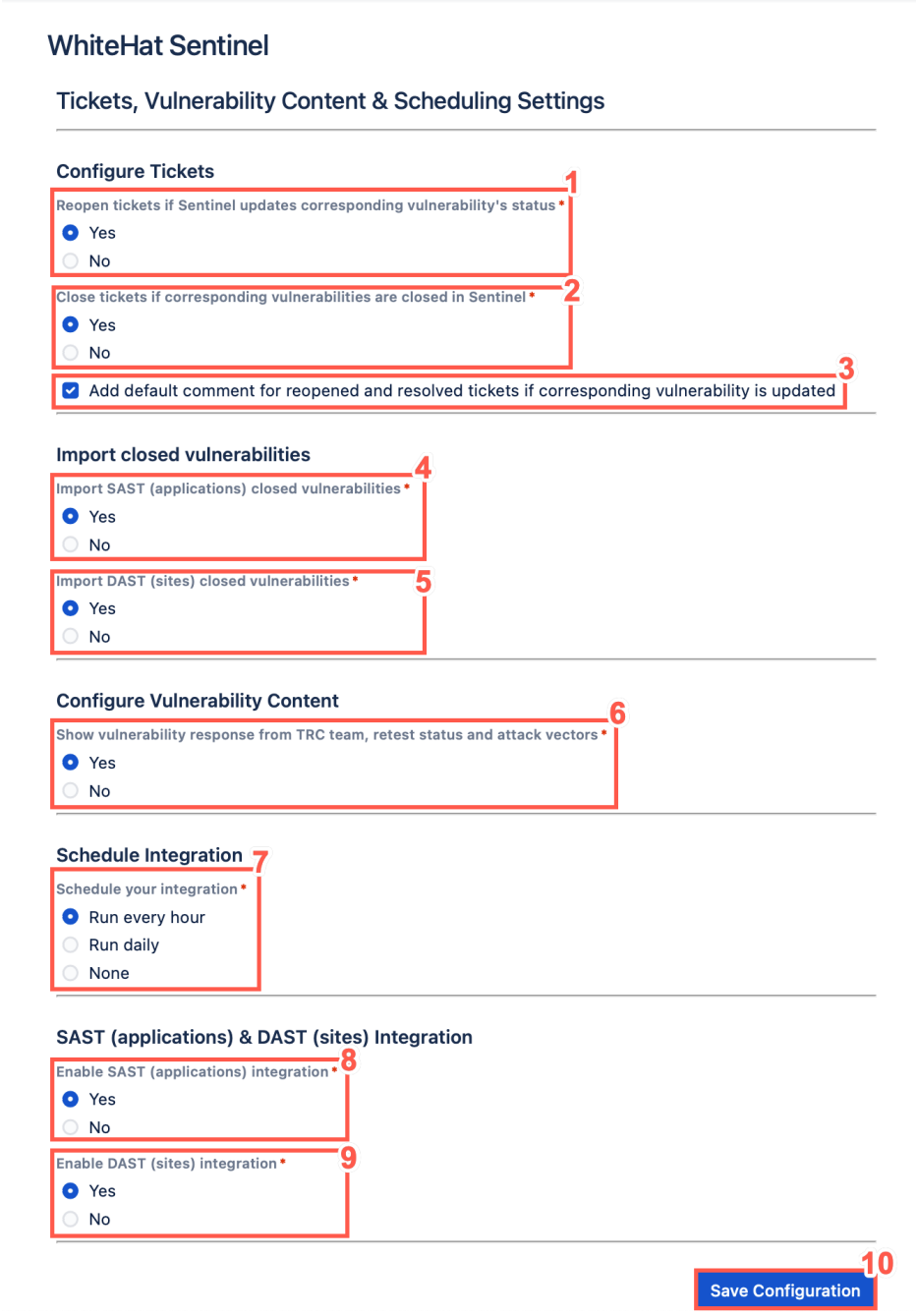
4. When you have completed mapping vulnerability ratings to **JIRA®** priorities according to your preferences, click **Save**.

NOTE	If you select any tags to be used to create **JIRA®** tickets, only vulnerabilities that have at least one of the listed tags in the WhiteHat Portal will be used to create **JIRA®** issues.

4.2. Tickets, Vulnerability Content & Scheduling Settings

Select the relevant radio buttons to configure default updates for your tickets.

1. Select to reopen closed tickets whenever a vulnerability's status is updated in the WhiteHat Portal.



2. Select to close your existing tickets automatically if corresponding vulnerabilities are closed in the WhiteHat Portal.
3. Optionally, click the **check box** to Add default comments for reopened and resolved tickets if the corresponding vulnerability is updated.
4. Optionally, configure the **Import SAST (applications) closed vulnerabilities**. Select the relevant radio button to import closed SAST vulnerabilities.
5. Optionally, configure the **Import DAST (applications) closed vulnerabilities**. Select the relevant radio button to import closed DAST vulnerabilities.
6. Optionally, configure the **Vulnerability Content**. Select the relevant radio button to show responses from the TRC team, vulnerability retest status and attack vectors.

7. Schedule your Integration, the default value is **Run Daily** select from:
    - **Run every hour**,
    - **Run Daily** or
    - **None**.

NOTE	If you choose to run your integration daily, you must select the exact hour when integration should run every day.

8. To **Enable SAST (Applications) Integration** select **Yes**.
9. To **Enable DAST (Sites) Integration** select **Yes**.
10. Click **Save Configuration** to keep your changes.

Chapter 5. SAST (Applications) Configuration

Select Configure SAST Settings to set your default reporter and assignee, map assets or groups to JIRA® projects, and map ticket priority to Sentinel ratings. The settings for each are broadly comparable, but some specifics will be called out where relevant.

To configure the WhiteHat Sentinel Cloud Plugin for **JIRA®** perform the following steps:

1. Click **SAST (Applications) Configuration**.

2. Set the default **JIRA®** assignee for a given asset (site or application) and associated **JIRA®** project. (This will map these assets to the **JIRA®** project(s) in question.) To set default assignees by group rather than asset, select the Sentinel Groups radio button. In this case, all assets in a group will be associated to the **JIRA®** project selected.

5.1. Mapping Configuration

1. Select an asset from the list of SAST Assets.

2. Select a project from the **Projects** list to assign.

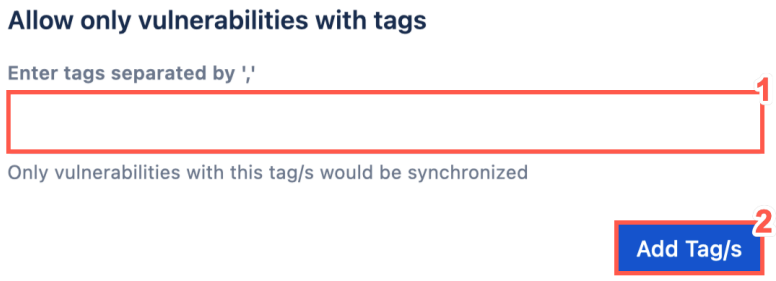
> **NOTE** The autocomplete for some fields might not populate until you enter an exact match. This is due to an Atlassian limitation.

3. Type the username of your **Jira User Reporter** in the search bar provided and then select them from the list.

4. Type the username of your **Jira User to assign** in the search bar provided and then select them from the list.
5. Select the **Jira Issue Type** from the drop down list.
6. **Jira Issue Status for OPEN Issues** this value is automatically set, based on the Jira project workflow. This Select box is disabled and manual change is not possible.
7. Select a **Jira Issue Transition For Closed Issues**, in this select box you can choose the status of Jira Tickets when the plugin closes the Jira Ticket. (Done, In Review, Closed) These values can be different, depending on the selected Jira Issue Type.
8. You can create **Custom Issue Labels**, which apply to each Jira Issue in the selected Jira Project.
9. If you wish to remove **Mapping Configuration** click **Remove Mapping Configuration**. It is now possible to remove or save the first **Mapping Configuration**. In case you don't want SAST integration to run simply disable SAST integration in the **Basic Configuration** tab.
10. If you want to map your SAST assets to multiple Jira Projects you can add another **Mapping Configuration** by clicking the **Add Mapping Configuration** button. To configure another **Mapping Configuration** follow previous steps (1-8).
11. After finishing your configuration, adding or removing **Mapping Configurations** save this configuration by clicking **Save All Mapping Configurations**. If saving was successful message will appear. If the message does not appear refer to the Monitoring/Debugging section.

5.2. Allow only vulnerabilities with tags

1. Type in the text box, you can define tag/s. Only SAST vulnerabilities including defined tag/s will be processed by the plugin.

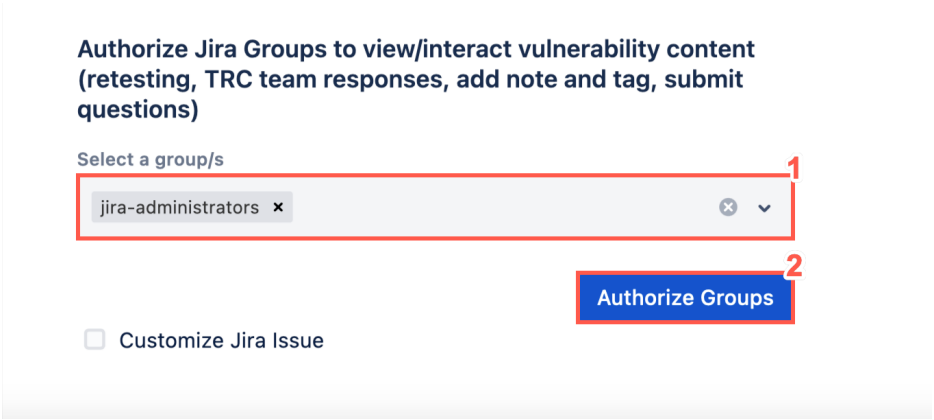


NOTE	If the input is empty and does not contain any tag/s all selected SAST assets will be a process.

2. To save changes click the **Add Tag/s**. If saving the successful message should appear. If the message does not appear refer to the Monitoring/Debugging section.

5.3. Authorize Jira Groups to View/Interact Vulnerability Content (Retesting, TRC Team Responses, Add note and tag, and Submit Questions)

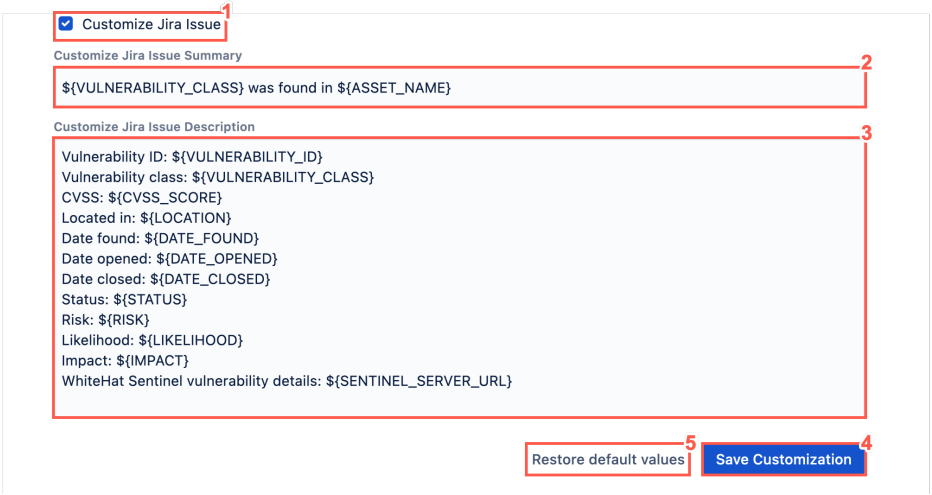
1. Select one or multiple **Jira User Groups** which will be authorized to view retesting status of asset/vulnerability, and TRC team responses. This group is authorized to Add Notes and Tag/s and Submit questions related to specific vulnerability opened in Jira Issue view.



2. After adding/removing groups to save changes click **Authorize Groups**. If saving the successful message should appear. If the message does not appear refer to the Monitoring/Debugging section.

5.4. Customize Jira Issue

1. Click **Customize Jira Issue**.



2. Edit the **Customize Jira Issue Summary** text field.
3. Edit the **Customize Jira Issue Description** text field.
4. When you have completed configuration for SAST (Applications) according to your preferences, click **Save Customization**.

5. To restore the default values, click **Restore default values**.

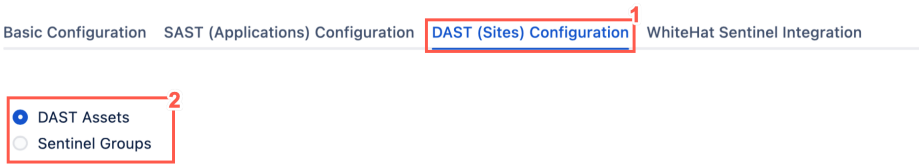
NOTE	You must click **Save Customization** after selecting **Restore default values** to keep the default values.

Chapter 6. DAST (Sites) Configuration

Select Configure DAST Settings to set your default reporter and assignee, map assets or groups to JIRA® projects, and map ticket priority to Sentinel ratings. The settings for each are broadly comparable, but some specifics will be called out where relevant.

To configure the WhiteHat Sentinel Cloud Plugin for **JIRA®** perform the following steps:

1. Click **DAST (Sites) Configuration**.



2. Set the default **JIRA®** assignee for a given asset (site or application) and associated **JIRA®** project. (This will map these assets to the **JIRA®** project(s) in question.) To set default assignees by group rather than asset, select the Sentinel Groups radio button. In this case, all assets in a group will be associated to the **JIRA®** project selected.

6.1. Mapping Configuration

1. Select an asset from the list of DAST Assets.

2. Select a project from the **Projects** list to assign.

NOTE	The autocomplete for some fields might not populate until you enter an exact match. This is due to an Atlassian limitation.

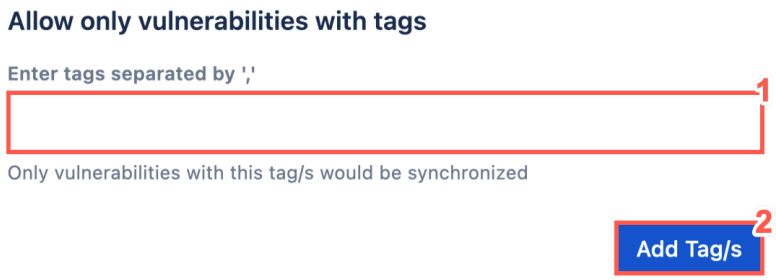
3. Type the name or email of your **Jira User Reporter** in the search bar provided and then select them from the list.
4. Type the name or email of your **Jira User to assign** in the search bar provided and then select

them from the list.

5. Select the **Jira Issue Type** from the drop down list.
6. The value of **Jira Issue Status for OPEN Issues** is automatically set, based on the Jira project workflow. This Select box is disabled and manual change is not possible.
7. Set **Jira Issue Transition For Closed Issues** to the status you want Jira Tickets to have when the plugin closes them (for example, Done, In Review, or Closed). These values can be different, depending on the selected Jira Issue Type.
8. You can create **Custom Issue Labels**, which apply to each Jira Issue in the selected Jira Project.
9. If you want to map your DAST assets to multiple Jira Projects you can add another **Mapping Configuration** by clicking the **Add Mapping Configuration**“ button. To configure another **Mapping Configuration** follow previous steps (1-8).
10. If you wish to remove **Mapping Configuration** click **Remove Mapping Configuration**. It is not possible to remove the first **Mapping Configuration**. In case you don’t want DAST integration to run simply disable DAST integration in the **Basic Configuration** tab.
11. Click **Save All Mapping Configurations**. If saving was successful, a message will appear. If the message does not appear, refer to the Monitoring/Debugging section.

6.2. Allow only vulnerabilities with tags

1. Type in the text box, you can define tag/s. Only DAST assets including defined tag/s will be processed by the plugin.

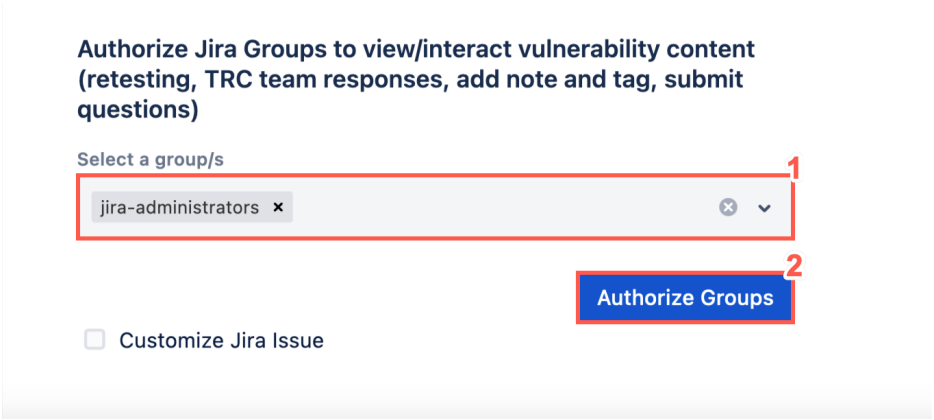


NOTE	If the input is empty and does not contain any tag/s, all selected DAST assets will be processed.

2. To save changes click the **Add Tag/s**. If saving the successful message should appear. If the message does not appear refer to the Monitoring/Debugging section.

6.3. Authorize Jira Groups to View/Interact Vulnerability Content (Retesting, TRC Team Responses, Add note and tag, and Submit Questions)

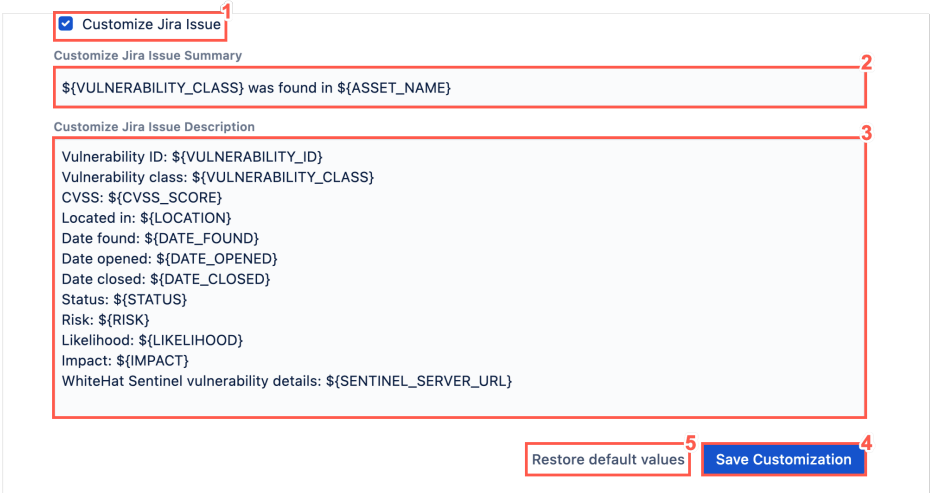
1. Select one or multiple **Jira User Groups** which will be authorized to view retesting status of asset/vulnerability, and TRC team responses. This group is authorized to Add Notes and Tag/s and Submit questions related to specific vulnerability opened in Jira Issue view.



2. Click **Authorize Groups**. If saving was successful, a message will appear. If the message does not appear, refer to the Monitoring/Debugging section.

6.4. Customize Jira Issue

1. Click **Customize Jira Issue**.



2. Edit the **Customize Jira Issue Summary** text field.
3. Edit the **Customize Jira Issue Description** text field.
4. When you have completed configuration for DAST (Sites) according to your preferences, click **Save Customization**.

5. To restore the default values, click **Restore default values**.

NOTE	You must click **Save Customization** after selecting **Restore default values** to keep the default values.

Chapter 7. WhiteHat Sentinel Integration

This page allows an admin user to start and stop integration or view the plugin log files. Once all fields are populated correctly and the previous settings are saved, integration can begin.

NOTE	If any changes to the settings of the Plugin are made while integration is running, you will need to stop the integration and re-start it to reflect the changed values.

To begin the initial integration process, perform the following steps:

1. Click the **WhiteHat Sentinel Integration** tab.

2. Click **Start Integration** to begin WhiteHat Portal data syncing to **JIRA®**. This runs on the interval specified by the user.
3. Click **Jira Admin** to view the plugin logs.

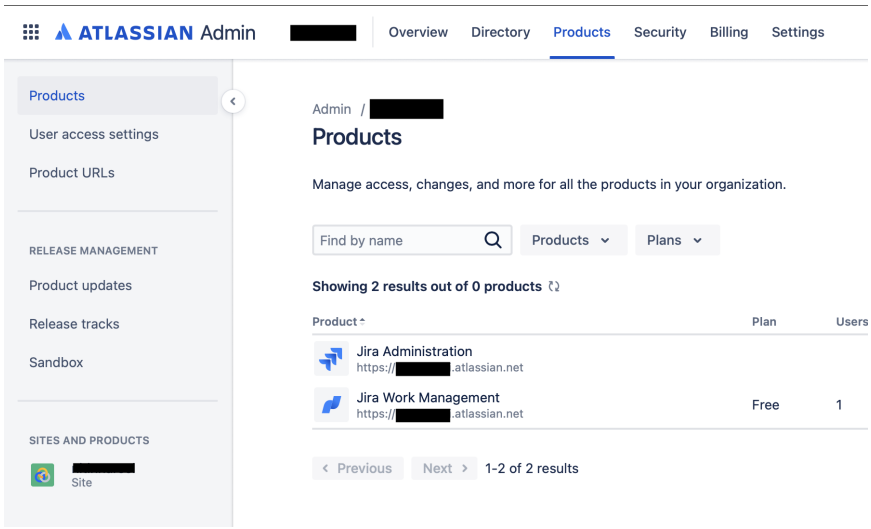
Chapter 8. Troubleshooting the WhiteHat Sentinel JIRA® Cloud Plugin

The most common issue is that no **Issues** are generated after starting the integration. In most cases this is due to the selected **Assignee** not having adequate privileges to create that issue. One way to verify this is to create a dummy issue within the Project, manually in **JIRA®**. If there are other issues, the plugin has been set up to generate verbose debug logging.

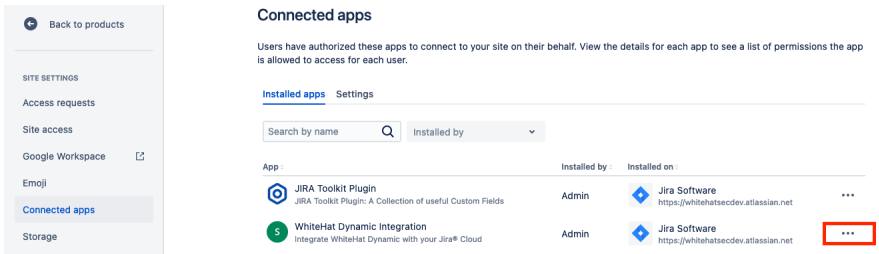
8.1. Viewing Log Files

To view the plugin log files, perform the following steps:

1. Log in with **Admin** level permissions.
2. If you have more than one organization, select the organization which has the site you want to download logs for.
3. Select the site's name and URL to open the **Admin** for that site. Or, if you have an improved user management experience, select **Products** and then select the site from the left-hand side, under **Sites and Products**.



4. Select **Connected apps** in the left menu.
5. On the Connected apps page, select ••• next to the app for which you want to download logs.



6. From the dropdown, select **Download** logs.

NOTE	Plugin log files are stored for sixty days.