The Continuous Dynamic Plugin for Jira® Cloud

Black Duck Software, Inc.

2025-05-12

Table of Contents

Chapter 1. Continuous Dynamic Plugin for Jira Cloud

The Black Duck® Continuous Dynamic™ Plugin for Jira Cloud is designed to integrate the Black Duck Continuous Dynamic Portal with Jira® Cloud. The Plugin provides a seamless interface within Jira that syncs vulnerabilities from Continuous Dynamic to your Jira instance.

As new vulnerabilities are discovered and added to the Portal, they are automatically pulled into Jira where issues are created. This gets vulnerabilities into the hands of developers, the individuals responsible for remediation. The vulnerability can be retested and, if needed, developers can use the Portal's **Ask A Question** feature directly from the issue in Jira.

1.1. Prerequisites

To install and configure the Plugin:

- The Jira project must be a **Company Managed Project**.

  NOTE A **Team Managed Project** will not function correctly with the Plugin.

- You must be logged in as a Jira admin with global permissions.

Chapter 2. Installing the Continuous Dynamic Plugin for Jira Cloud

2.1. Atlassian Marketplace

The Continuous Dynamic Plugin for Jira Cloud is available to install from the Atlassian Marketplace. Alternatively, install the Plugin from within Jira, as described in the next task.

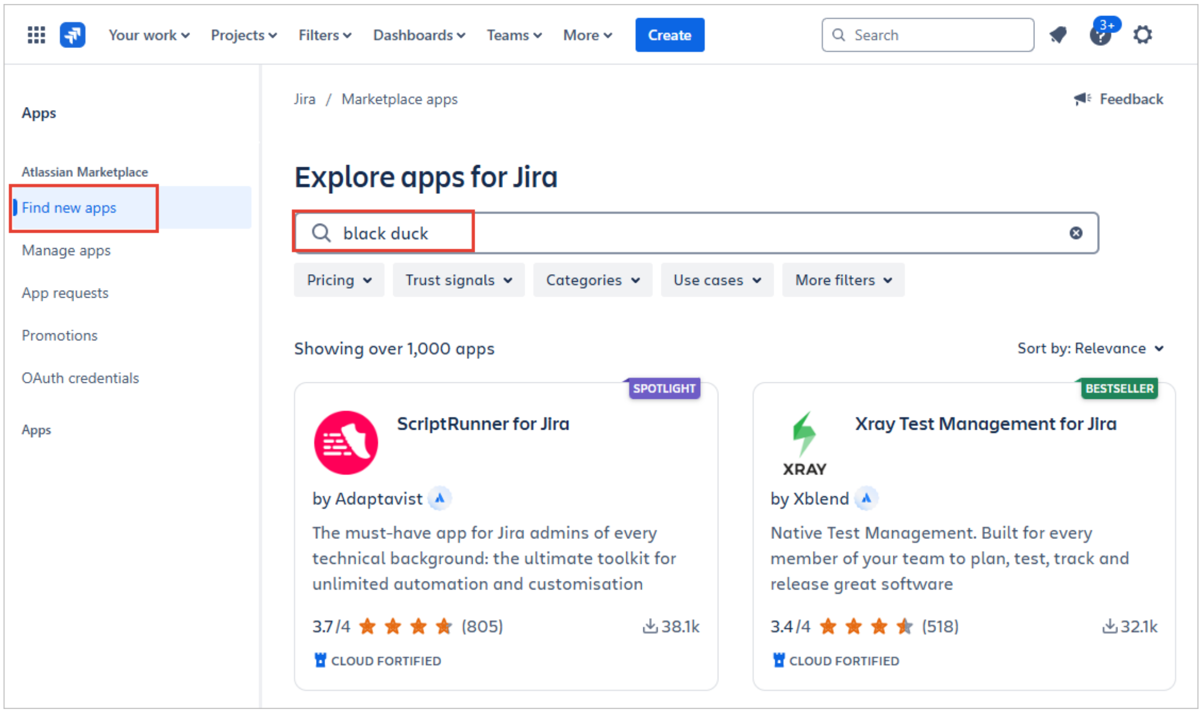
2.2. Install the Jira Cloud Plugin from within Jira

To install the Plugin, perform the following steps as a Jira admin:

1. Log in to your Jira instance.
2. Select **Settings** at the top right and then select **Apps** from the drop down menu.

   The **Find new apps** page is displayed.

3. Search for the **Black Duck Continuous Dynamic Plugin**:



Explore apps for Jira

black duck

Showing over 1,000 apps

ScriptRunner for Jira

by Adaptavist

The must-have app for Jira admins of every technical background: the ultimate toolkit for unlimited automation and customisation

3.7/4 ★★★★ (805) 38.1k

Xray Test Management for Jira

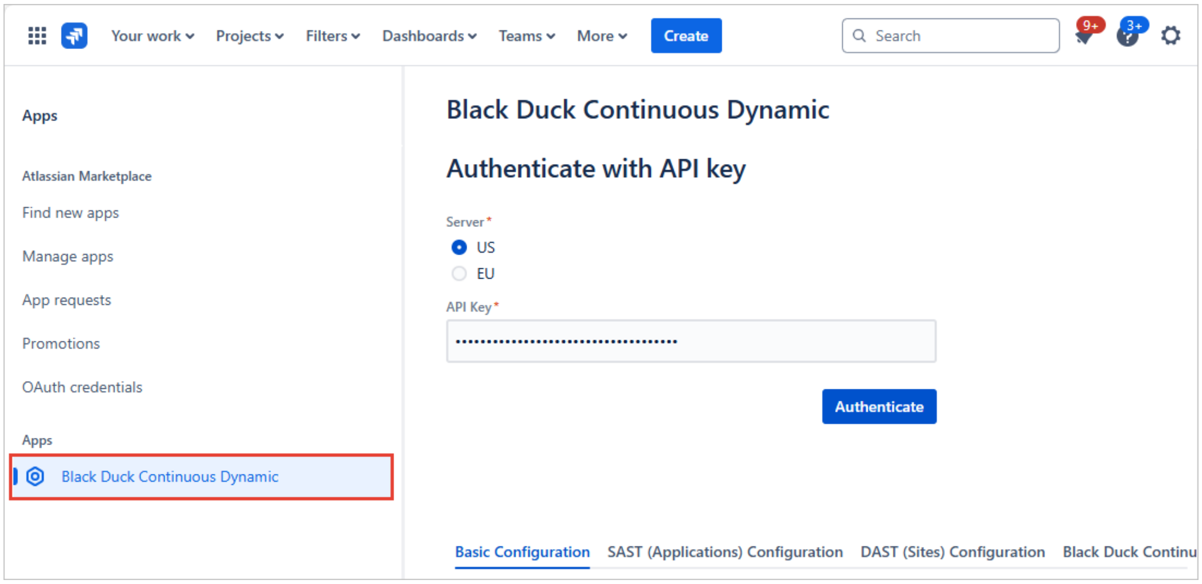
by Xblend

Native Test Management. Built for every member of your team to plan, test, track and release great software

3.4/4 ★★★★ (518) 32.1k

4. Select the **Black Duck Continuous Dynamic Plugin** app.
5. Click **Install**.
6. When prompted, grant the app permission to access Atlassian products on your behalf.

   The Plugin is now available under **Apps** in the left menu:



Black Duck Continuous Dynamic

Authenticate with API key

Server*

● US

○ EU

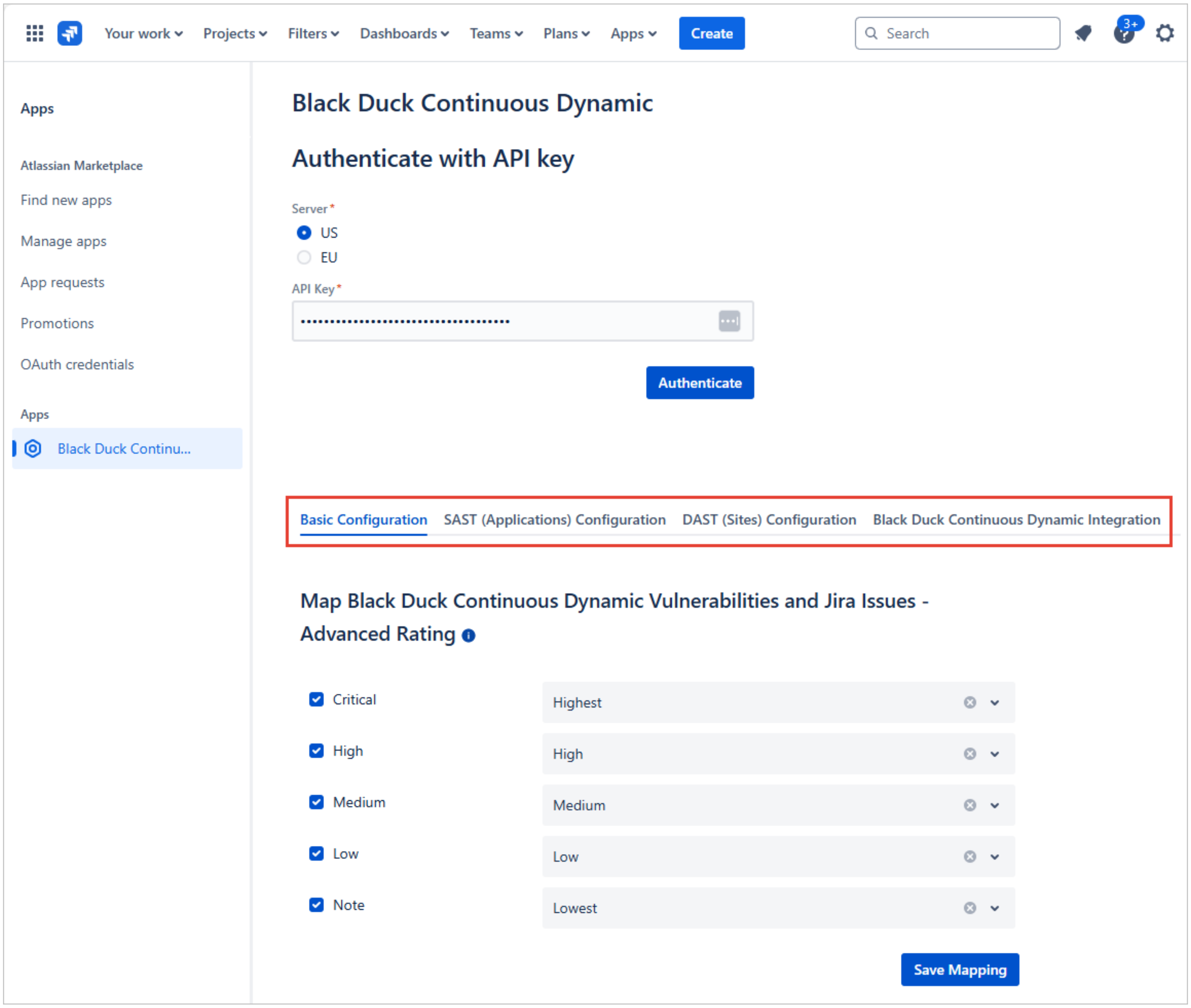
API Key*

••••••••••••••••••••••••••••••••••••

Now that the Plugin is installed, you need to configure it as described in Configuring the Continuous Dynamic Plugin for Jira Cloud.

Chapter 3. Configuring the Continuous Dynamic Plugin for Jira Cloud

After successfully authenticating your API Key, the following configuration tabs are displayed. You might need to refresh the **Apps** page to see the new options.



Black Duck Continuous Dynamic

Authenticate with API key

Server*
● US
○ EU

API Key*
••••••••••••••••••••••••••••••••••••

Map Black Duck Continuous Dynamic Vulnerabilities and Jira Issues - Advanced Rating

☑ Critical	Highest
☑ High	High
☑ Medium	Medium
☑ Low	Low
☑ Note	Lowest

- Basic Configuration: Configure the connections between the Plugin and Continuous Dynamic; Map vulnerabilities to Jira Issues; Configuration of Jira Tickets; Vulnerability Content; Scheduling Integration; Disable/Enable SAST/DAST integration.
- SAST (Applications) Configuration: Configure the interactions between the Plugin and Sentinel Source (SAST) services.
- DAST (Sites) Configuration: Configure the interactions between the Plugin and Continuous Dynamic DAST services.
- Continuous Dynamic Integration: Start and stop the integration, or redirect to a Developer Console

to monitor the Plugin.

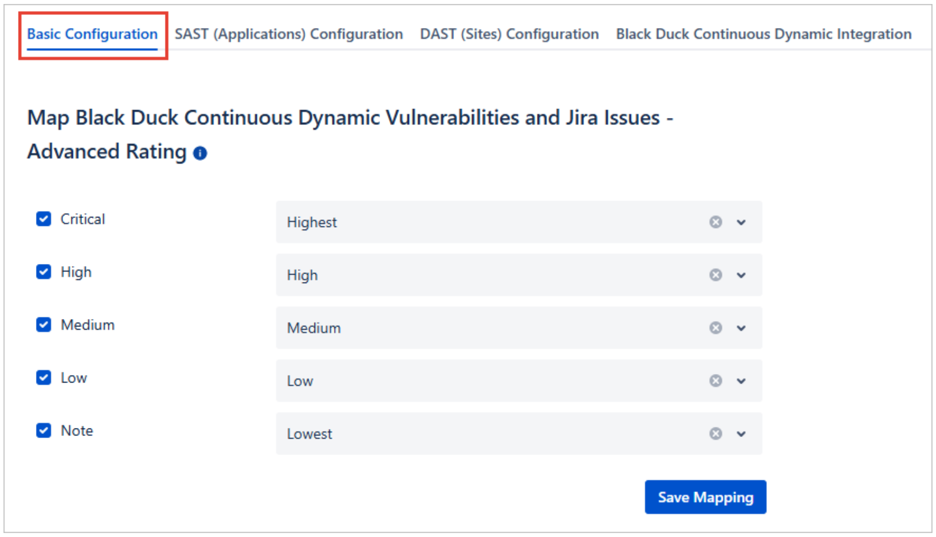
Chapter 4. Basic Configuration

4.1. Mapping Vulnerability Ratings to Jira Priorities

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

To map vulnerability ratings to Jira priorities, perform the following steps:

1. On the app page, select the **Basic Configuration** tab.
2. The default mapping associates the most severe vuln rating with the highest Jira priority. You can change this mapping using the drop-down lists.

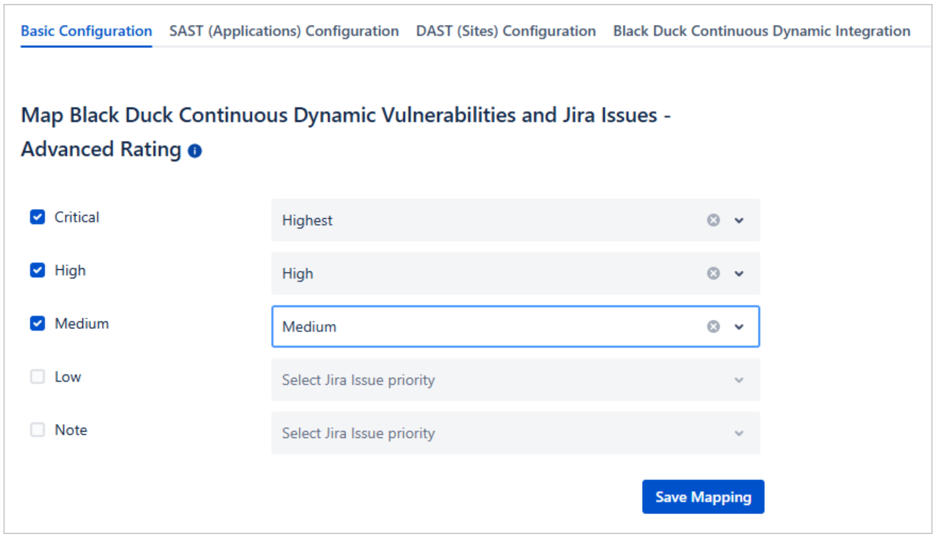

Basic Configuration
SAST (Applications) Configuration
DAST (Sites) Configuration
Black Duck Continuous Dynamic Integration
Save Mapping

Map Black Duck Continuous Dynamic Vulnerabilities and Jira Issues - Advanced Rating

☑ Critical	Highest
☑ High	High
☑ Medium	Medium
☑ Low	Low
☑ Note	Lowest

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.


Basic Configuration
SAST (Applications) Configuration
DAST (Sites) Configuration
Black Duck Continuous Dynamic Integration
Save Mapping

Map Black Duck Continuous Dynamic Vulnerabilities and Jira Issues - Advanced Rating

☑ Critical	Highest
☑ High	High
☑ Medium	Medium
□ Low	Select Jira Issue priority
□ Note	Select Jira Issue priority

NOTE

In the above example, Jira tickets will 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, you can limit vulnerabilities that will result in Jira tickets based on the Continuous Dynamic tags associated with the vulnerability.

4. When you have completed mapping vulnerability ratings to Jira priorities, click **Save Mapping**.

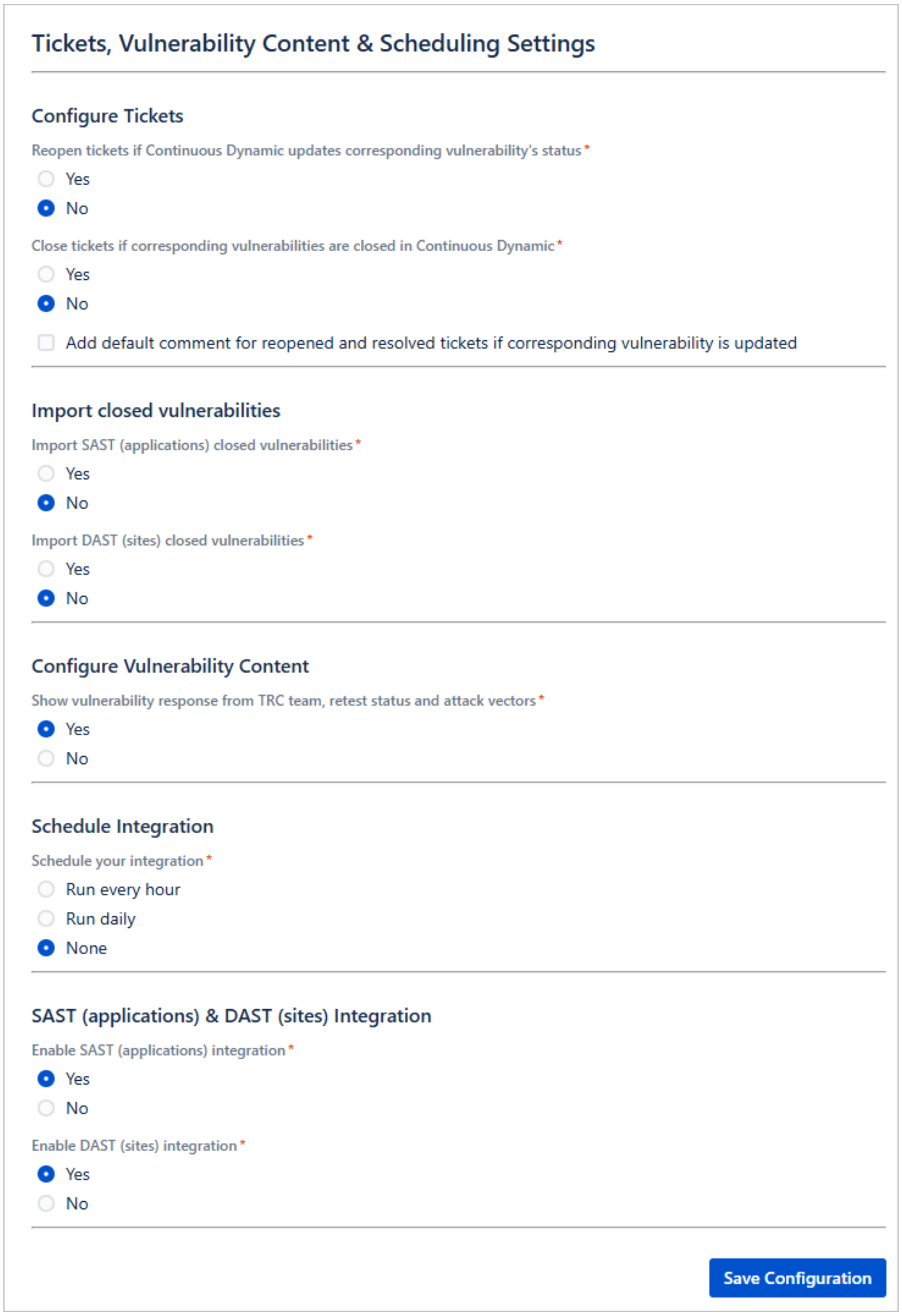
NOTE

If you selected any tags to be used to create Jira tickets, only vulnerabilities that have *at least one* of the listed tags in the Continuous Dynamic Portal will be used to create Jira issues.

4.2. Tickets, Vulnerability Content & Scheduling Settings

In the **Tickets, Vulnerability Content & Scheduling Settings** section, you can configure default updates for your tickets.

1. Choose whether to reopen closed Jira tickets whenever a vulnerability’s status is updated in the Portal.



Tickets, Vulnerability Content & Scheduling Settings

Configure Tickets

Reopen tickets if Continuous Dynamic updates corresponding vulnerability's status*

○ Yes
● No

Close tickets if corresponding vulnerabilities are closed in Continuous Dynamic*

○ Yes
● No

□ Add default comment for reopened and resolved tickets if corresponding vulnerability is updated

Import closed vulnerabilities

Import SAST (applications) closed vulnerabilities*

○ Yes
● No

Import DAST (sites) closed vulnerabilities*

○ Yes
● No

Configure Vulnerability Content

Show vulnerability response from TRC team, retest status and attack vectors*

● Yes
○ No

Schedule Integration

Schedule your integration*

○ Run every hour
○ Run daily
● None

SAST (applications) & DAST (sites) Integration

Enable SAST (applications) integration*

● Yes
○ No

Enable DAST (sites) integration*

● Yes
○ No

2. Choose whether to close your existing Jira tickets automatically if corresponding vulnerabilities are closed in the Portal.
3. Optionally, select the check box to **Add default comment for reopened and resolved tickets if corresponding vulnerability is updated**.
4. Optionally, configure the **Import SAST (applications) closed vulnerabilities**. Select the relevant option to import closed SAST vulnerabilities.
5. Optionally, configure the **Import DAST (applications) closed vulnerabilities**. Select the relevant option to import closed DAST vulnerabilities.
6. Optionally, configure the vulnerability content that will be displayed on Jira tickets. Select the relevant option to show responses from the Threat Research Center (TRC) team, the vulnerability

retest status, and the attack vectors.

7. Schedule your integration with Continuous Dynamic. You can select from the following schedules:
   - **Run every hour**
   - **Run Daily** (default)
   - **None**

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

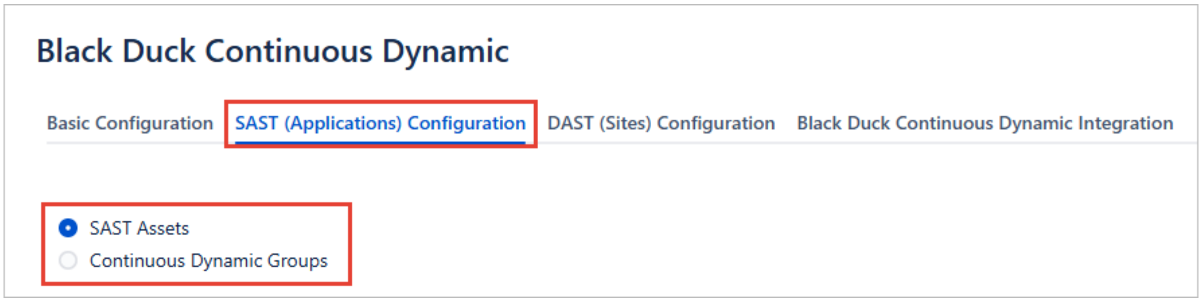
8. To **Enable SAST (Applications) Integration** select **Yes**.
9. To **Enable DAST (Sites) Integration** select **Yes**.
10. Click **Save Configuration**.

Chapter 5. SAST (Applications) Configuration

Select the **SAST (Applications) Configuration** tab to set the default reporter and assignee, map assets or groups to Jira projects, and map ticket priority to Continuous Dynamic ratings.

To configure the Continuous Dynamic Plugin for Jira Cloud, perform the following steps:

1. On the app page, select the **SAST (Applications) Configuration** tab.



Black Duck Continuous Dynamic

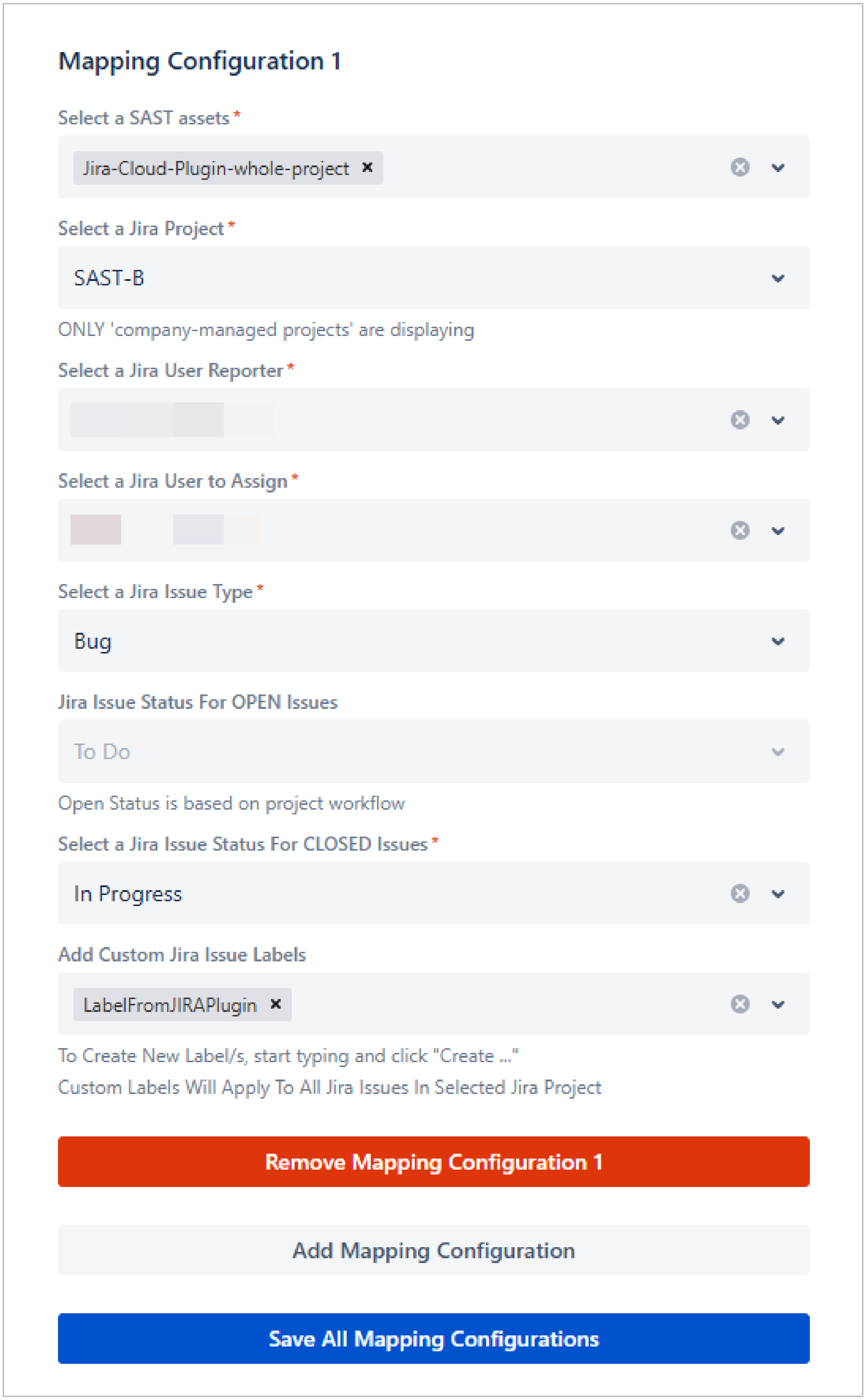
Basic Configuration
SAST (Applications) Configuration
DAST (Sites) Configuration
Black Duck Continuous Dynamic Integration

● SAST Assets
○ Continuous Dynamic Groups

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 **Continuous Dynamic 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.



Mapping Configuration 1

Select a SAST assets *

Jira-Cloud-Plugin-whole-project ×

Select a Jira Project *

SAST-B

ONLY 'company-managed projects' are displaying

Select a Jira User Reporter *

[redacted]

Select a Jira User to Assign *

[redacted]

Select a Jira Issue Type *

Bug

Jira Issue Status For OPEN Issues

To Do

Open Status is based on project workflow

Select a Jira Issue Status For CLOSED Issues *

In Progress

Add Custom Jira Issue Labels

LabelFromJIRAPlugin ×

To Create New Label/s, start typing and click "Create ..."

Custom Labels Will Apply To All Jira Issues In Selected Jira Project

Remove Mapping Configuration 1
Add Mapping Configuration
Save All Mapping Configurations

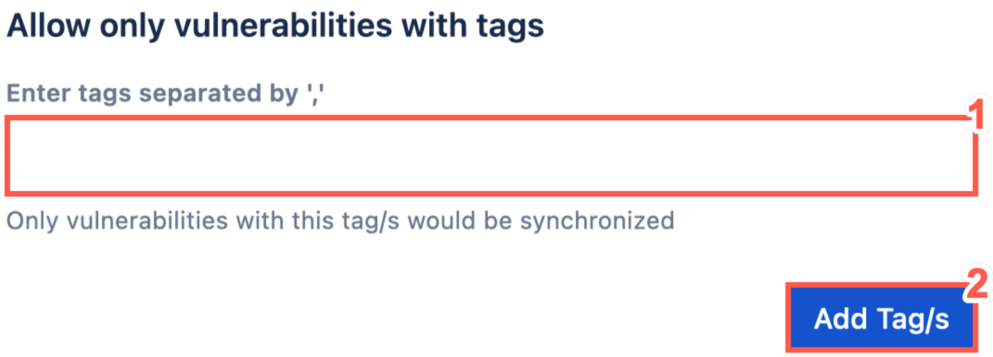
2. Select a Jira project from the **Projects** list.

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

3. Enter the username of your **Jira User Reporter** in the search bar provided, then select them from the list.
4. Enter the username of your **Jira User to assign** in the search bar provided, then select them from the list.
5. Select the **Jira Issue Type** from the drop down list.
6. The **Jira Issue Status for OPEN Issues** value is automatically set based on the Jira project workflow. The drop-down menu is disabled and manual change is not possible.
7. Select a **Jira Issue Transition For Closed Issues**. In this menu, you can choose the status of Jira tickets that are closed by the Plugin: Done, In Review, or Closed. These values can differ 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 possible to remove or save the first **Mapping Configuration**. If you do not 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 **Add Mapping Configuration**. To configure another **Mapping Configuration** follow previous steps.
11. After finishing your configuration and adding or removing **Mapping Configurations**, save this configuration by clicking **Save All Mapping Configurations**. A success message should appear. If the message does not appear, refer to the Troubleshooting section.

5.2. Allow only vulnerabilities with tags

1. In the **Allow only vulnerabilities with tags** text box, you can define one or more tags. Only SAST vulnerabilities which include the defined tag(s) will be processed by the Plugin.



Allow only vulnerabilities with tags

Enter tags separated by ','

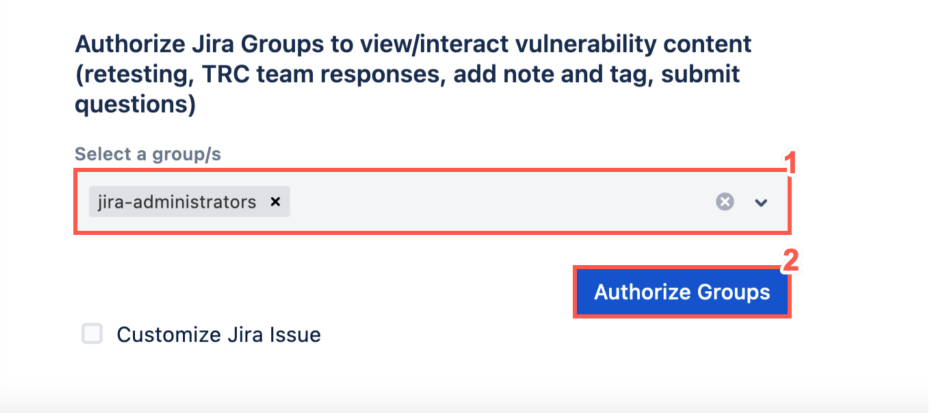
Only vulnerabilities with this tag/s would be synchronized

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

2. Click **Add Tag/s** to save your changes. The success message should appear. If the message does not appear, refer to the Troubleshooting 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 more **Jira User Groups** that will be authorized to view the retesting status of asset/vulnerability, and TRC team responses. Members of this group are authorized to **Add Notes** and **Tag/s** and **Submit questions** related to a specific vulnerability opened in Jira Issue view.



Authorize Jira Groups to view/interact vulnerability content (retesting, TRC team responses, add note and tag, submit questions)

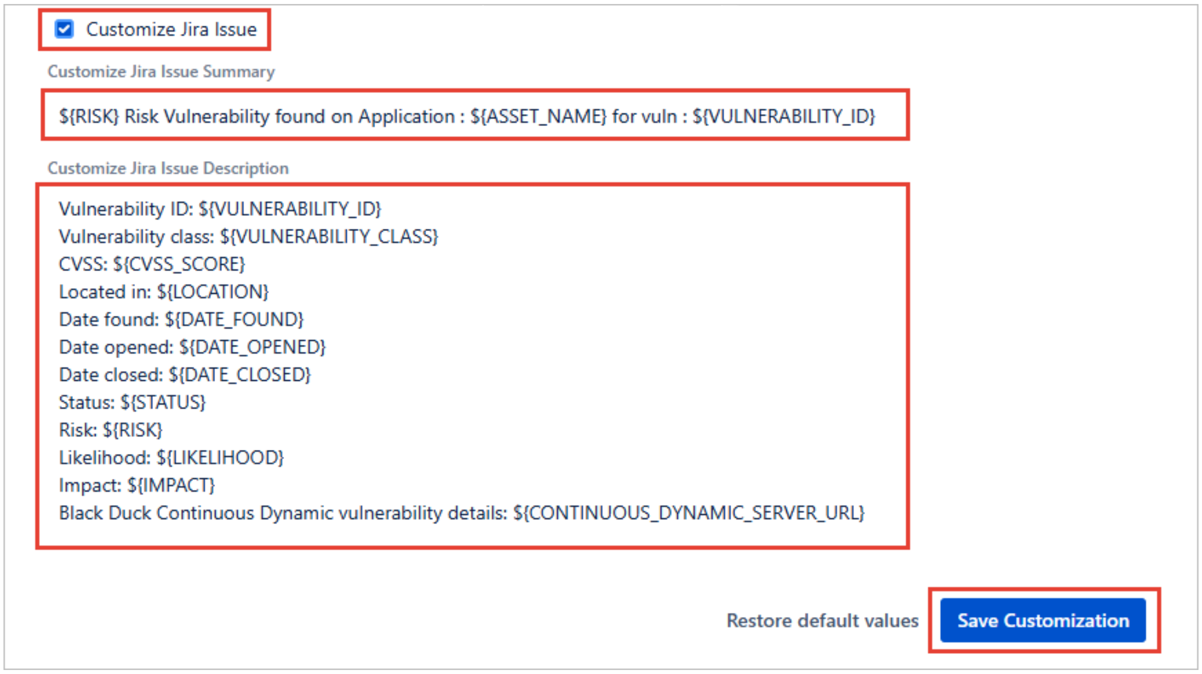
Select a group/s: jira-administrators ×

□ Customize Jira Issue

2. After adding/removing groups, click **Authorize Groups** to save changes.

5.4. Customize Jira Issue

1. Select the **Customize Jira Issue** checkbox.



☑ Customize Jira Issue

Customize Jira Issue Summary

${RISK} Risk Vulnerability found on Application : ${ASSET_NAME} for vuln : ${VULNERABILITY_ID}

Customize Jira Issue Description

Vulnerability ID: ${VULNERABILITY_ID}
Vulnerability class: ${VULNERABILITY_CLASS}
CVSS: ${CVSS_SCORE}
Located in: ${LOCATION}
Date found: ${DATE_FOUND}
Date opened: ${DATE_OPENED}
Date closed: ${DATE_CLOSED}
Status: ${STATUS}
Risk: ${RISK}
Likelihood: ${LIKELIHOOD}
Impact: ${IMPACT}
Black Duck Continuous Dynamic vulnerability details: ${CONTINUOUS_DYNAMIC_SERVER_URL}

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**.

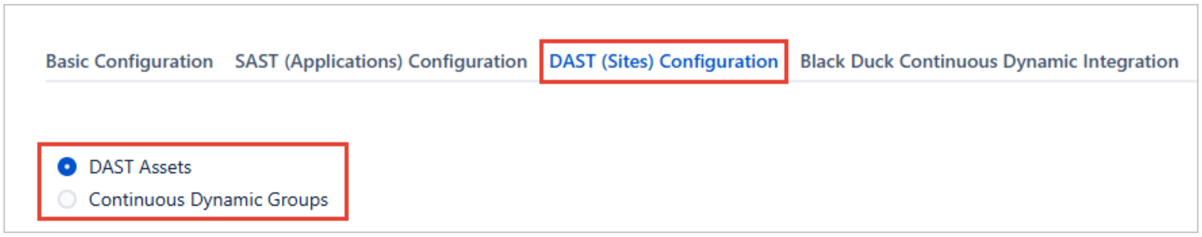
NOTE You must click **Save Customization** after selecting **Restore default values** to keep the default values.

Chapter 6. DAST (Sites) Configuration

Select the **DAST (Sites) Configuration** tab to set your default reporter and assignee, map assets or groups to Jira projects, and map ticket priority to Continuous Dynamic ratings.

To configure the Continuous Dynamic Plugin for Jira Cloud, perform the following steps:

1. On the app page, select the **DAST (Sites) Configuration** tab.

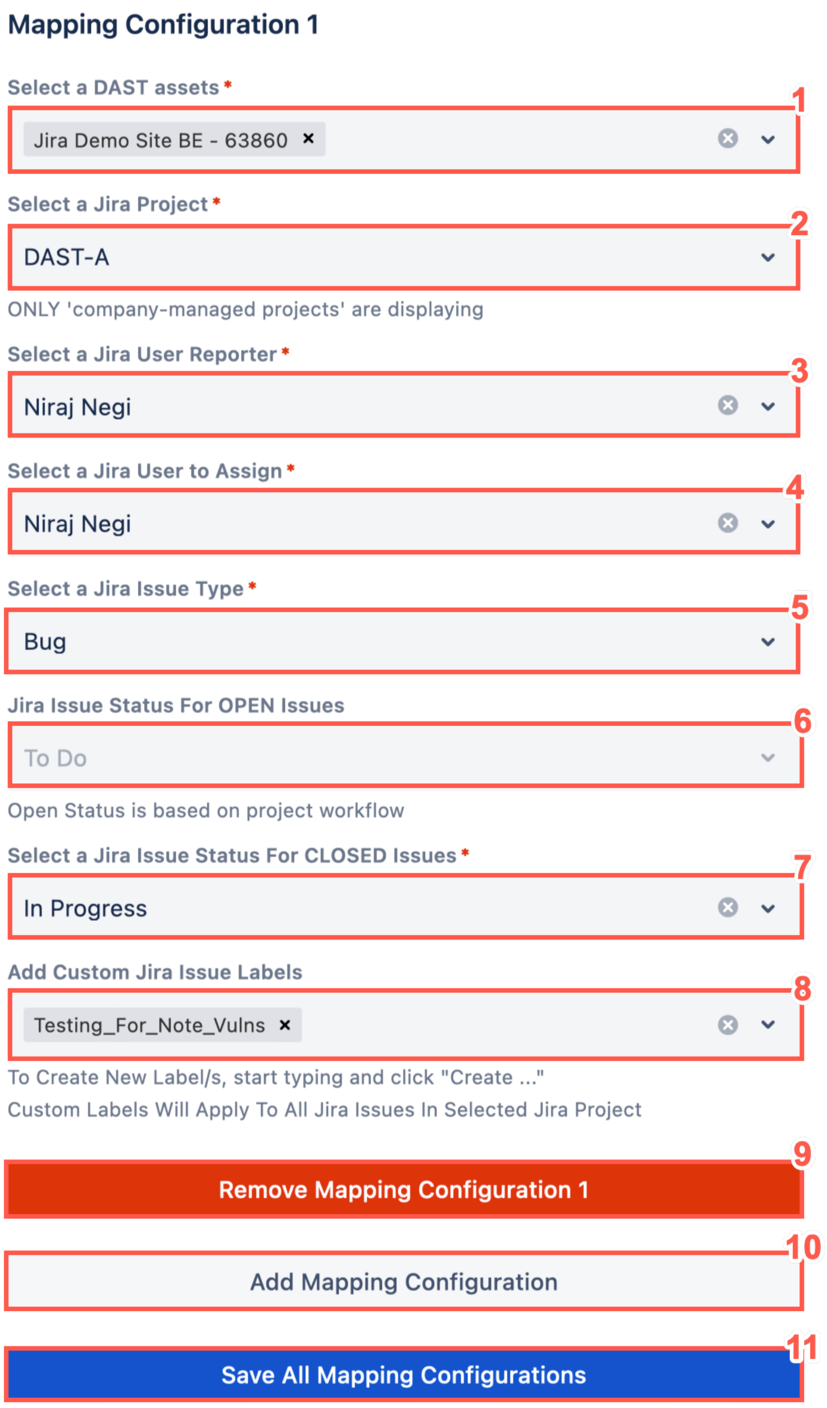

Basic Configuration
SAST (Applications) Configuration
DAST (Sites) Configuration
Black Duck Continuous Dynamic Integration

● DAST Assets
○ Continuous Dynamic Groups

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 **Continuous Dynamic 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.



Mapping Configuration 1

Select a DAST assets *

Jira Demo Site BE - 63860 ×

Select a Jira Project *

DAST-A

ONLY 'company-managed projects' are displaying

Select a Jira User Reporter *

Niraj Negi

Select a Jira User to Assign *

Niraj Negi

Select a Jira Issue Type *

Bug

Jira Issue Status For OPEN Issues

To Do

Open Status is based on project workflow

Select a Jira Issue Status For CLOSED Issues *

In Progress

Add Custom Jira Issue Labels

Testing_For_Note_Vulns ×

To Create New Label/s, start typing and click "Create ..."
Custom Labels Will Apply To All Jira Issues In Selected Jira Project

1
2
3
4
5
6
7
8
9
10
11
Remove Mapping Configuration 1
Add Mapping Configuration
Save All Mapping Configurations

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. Enter the name or email of your **Jira User Reporter** in the search bar provided and then select them from the list.

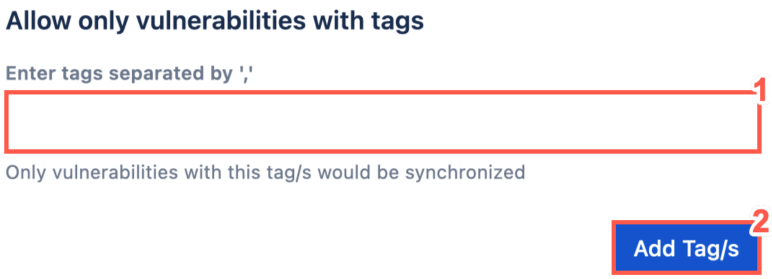
4. Enter the name or email of your **Jira User to assign** in the search bar provided and then select

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. The drop-down menu is disabled and manual change is not possible.
7. Select a **Jira Issue Transition For Closed Issues**. In this menu, you can choose the status of Jira tickets that are closed by the Plugin: Done, In Review, or Closed. These values can differ 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. In the **Allow only vulnerabilities with tags** text box, you can define one or more tags. Only DAST assets which include the defined tag(s) will be processed by the Plugin.



Allow only vulnerabilities with tags

Enter tags separated by ','

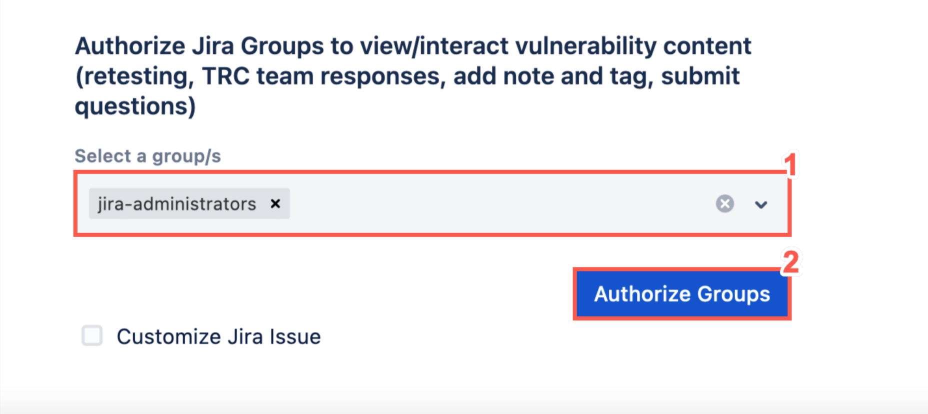
Only vulnerabilities with this tag/s would be synchronized

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

2. Click **Add Tag/s** to save your changes. The success message should appear. If the message does not appear, refer to the Troubleshooting 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 a specific vulnerability opened in Jira Issue view.



Authorize Jira Groups to view/interact vulnerability content (retesting, TRC team responses, add note and tag, submit questions)

Select a group/s

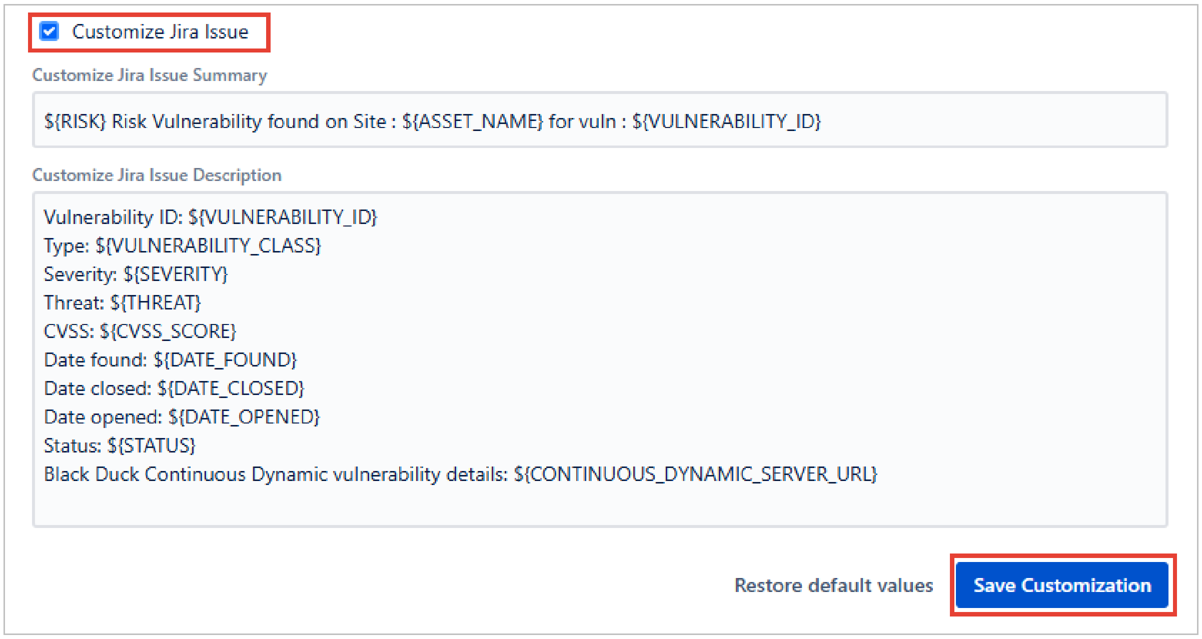
jira-administrators ×

□ Customize Jira Issue

2. Click **Authorize Groups**.

6.4. Customize Jira Issue

1. Click **Customize Jira Issue**.



☑ Customize Jira Issue

Customize Jira Issue Summary

${RISK} Risk Vulnerability found on Site : ${ASSET_NAME} for vuln : ${VULNERABILITY_ID}

Customize Jira Issue Description

Vulnerability ID: ${VULNERABILITY_ID}
Type: ${VULNERABILITY_CLASS}
Severity: ${SEVERITY}
Threat: ${THREAT}
CVSS: ${CVSS_SCORE}
Date found: ${DATE_FOUND}
Date closed: ${DATE_CLOSED}
Date opened: ${DATE_OPENED}
Status: ${STATUS}
Black Duck Continuous Dynamic vulnerability details: ${CONTINUOUS_DYNAMIC_SERVER_URL}

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. Continuous Dynamic Integration

The **Continuous Dynamic Integration** page allows a Jira admin to:

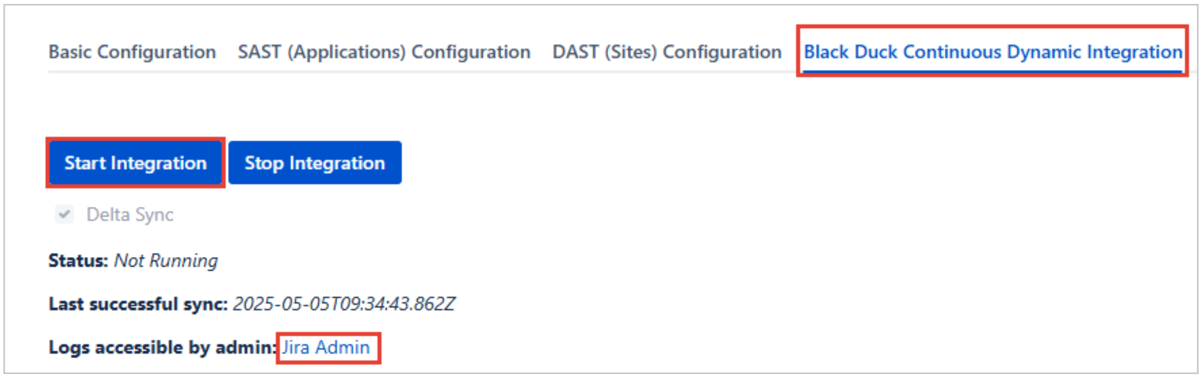
- Start and stop the integration between the Continuous Dynamic Portal and Jira Cloud.
- View the Plugin log files.

Once all fields are populated correctly and the previous settings are saved, integration can begin.

WARNING If any changes to the settings of the Plugin are made while the 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 **Black Duck® Continuous Dynamic™** tab.


Basic Configuration
SAST (Applications) Configuration
DAST (Sites) Configuration
Black Duck Continuous Dynamic Integration
Start Integration
Stop Integration

☑ Delta Sync

Status: *Not Running*

Last successful sync: *2025-05-05T09:34:43.862Z*

Logs accessible by admin: Jira Admin

2. Click **Start Integration** to begin syncing Continuous Dynamic Portal data to Jira Cloud. The sync runs on the interval that was specified by the user.
3. Click **Jira Admin** to access the Plugin logs at https://admin.atlassian.com/

Chapter 8. Troubleshooting the Continuous Dynamic Plugin for Jira Cloud

It is sometimes observed that no **Issues** are generated after starting the integration. In most cases, this is caused by the selected **Assignee** not having adequate privileges to create Jira issue(s) of the selected type(s). To verify if this is the case, try to manually create an issue in the Jira project.

To help resolve any other issues, the Plugin has been set up to generate verbose debug logging.

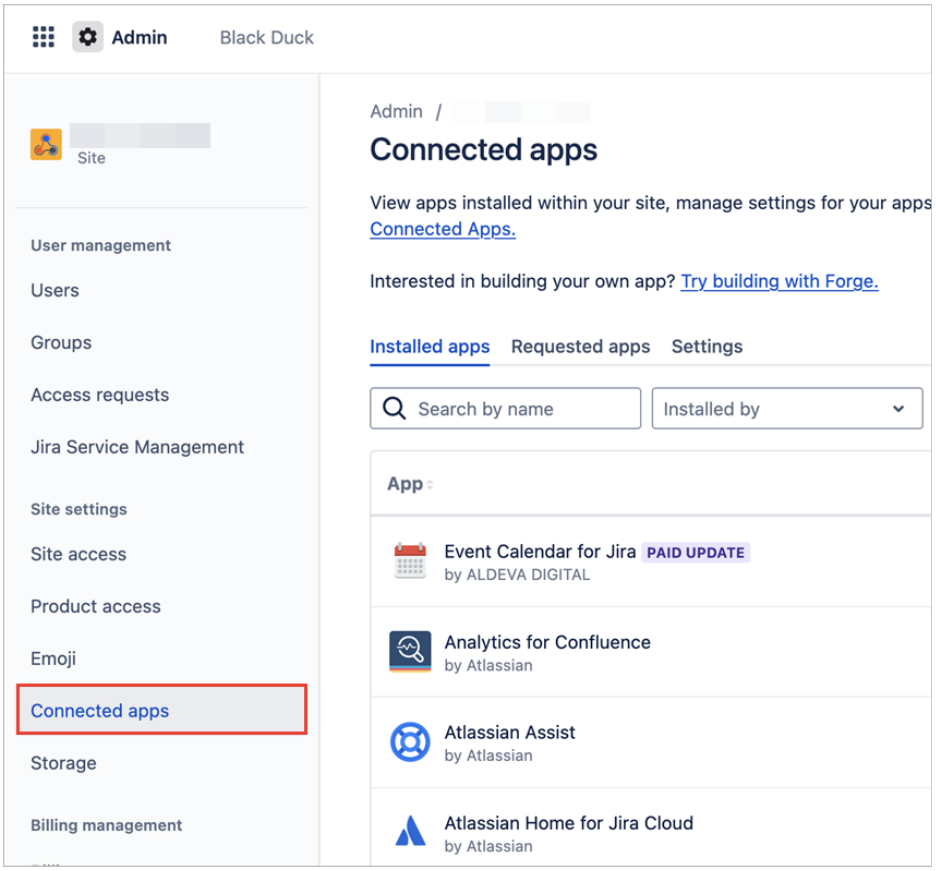
8.1. Downloading the Plugin Log Files

To download the Plugin log files for a site, perform the following steps:

1. Log in to https://admin.atlassian.com/ with **Admin** level permissions.
2. Under **Products**, select the site for which you want to download the Plugin log files. This screen is only displayed if you have more than one organization.

   The **Admin** page for the site is opened.

3. Select **Connected apps** in the left menu:



Connected apps

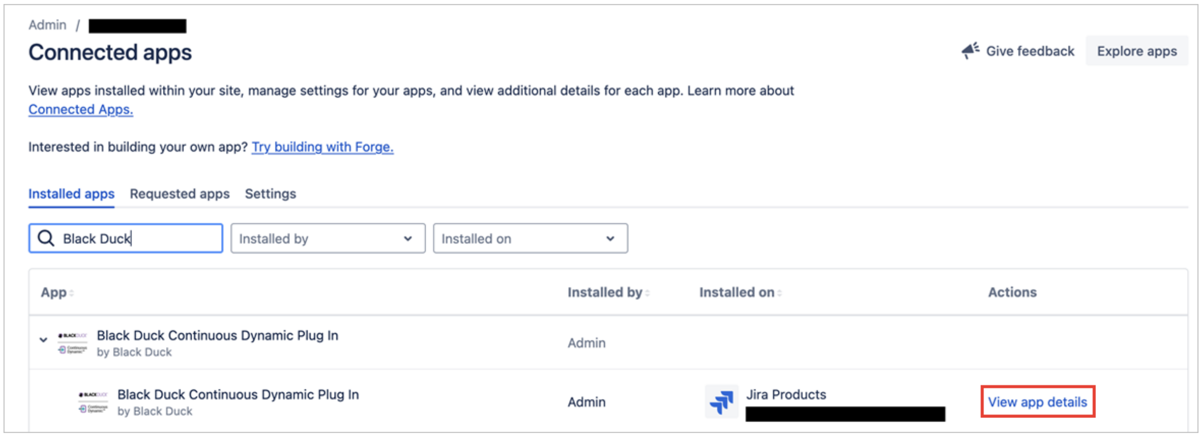
View apps installed within your site, manage settings for your apps
Connected Apps.

Interested in building your own app? Try building with Forge.

App
Event Calendar for Jira PAID UPDATE by ALDEVA DIGITAL
Analytics for Confluence by Atlassian
Atlassian Assist by Atlassian
Atlassian Home for Jira Cloud by Atlassian

4. In the search box, enter "Black Duck" to search for the **Black Duck Continuous Dynamic Plug In**,

then click the **View app details** link next to the Plugin name to view the app details page:



Admin / [redacted]

Connected apps

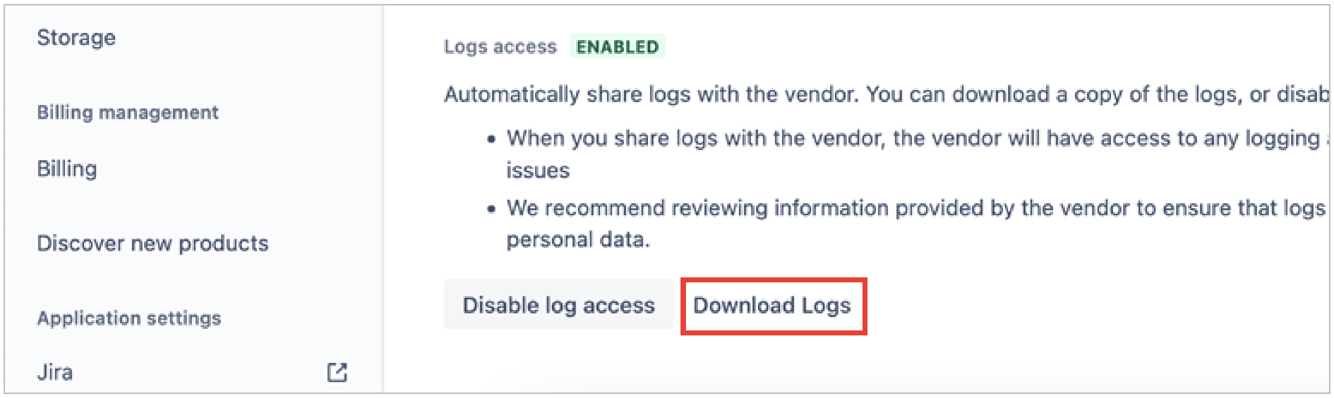
View apps installed within your site, manage settings for your apps, and view additional details for each app. Learn more about Connected Apps.

Interested in building your own app? Try building with Forge.

Black Duck

App	Installed by	Installed on	Actions
Black Duck Continuous Dynamic Plug In by Black Duck	Admin		
Black Duck Continuous Dynamic Plug In by Black Duck	Admin	Jira Products [redacted]	View app details

5. On the **Details** subtab, click **Download Logs** at the bottom of the page:



Logs access ENABLED

Automatically share logs with the vendor. You can download a copy of the logs, or disab

- When you share logs with the vendor, the vendor will have access to any logging issues
- We recommend reviewing information provided by the vendor to ensure that logs personal data.

The Plugin log files are downloaded to your local machine.

NOTE Plugin log files are stored for the past sixty days.