Incident configuration

Tags: Flow

Configure incidents to help Flow provide complete DORA metric data. Once incidents and deployments are both configured, all DORA metrics will be populated in Flow. This provides you with more accurate information on how quickly you're recovering from issues and service outages.

> **Note**: You can only configure incidents from Jira integrations.

In this article

Who can use this?

Core	Plus
	✓

Before you get started

Before configuring incidents in Flow, talk to your organization about what incidents are and how you're currently tracking them. Decide which incidents you want to track in Flow, then configure those incidents in Flow.

> **Note:** To access all four DORA metrics in Flow, you must set up incident configuration and configure your deployments.

back to top

Incident data in reports

The DORA metrics Time to restore services and Change failure rate rely on Incidents configurations to have accurate data.

Incident data appears in Reports home, Retrospective, and Team health insights.

> **Note:** You can only configure incidents for Jira integrations.

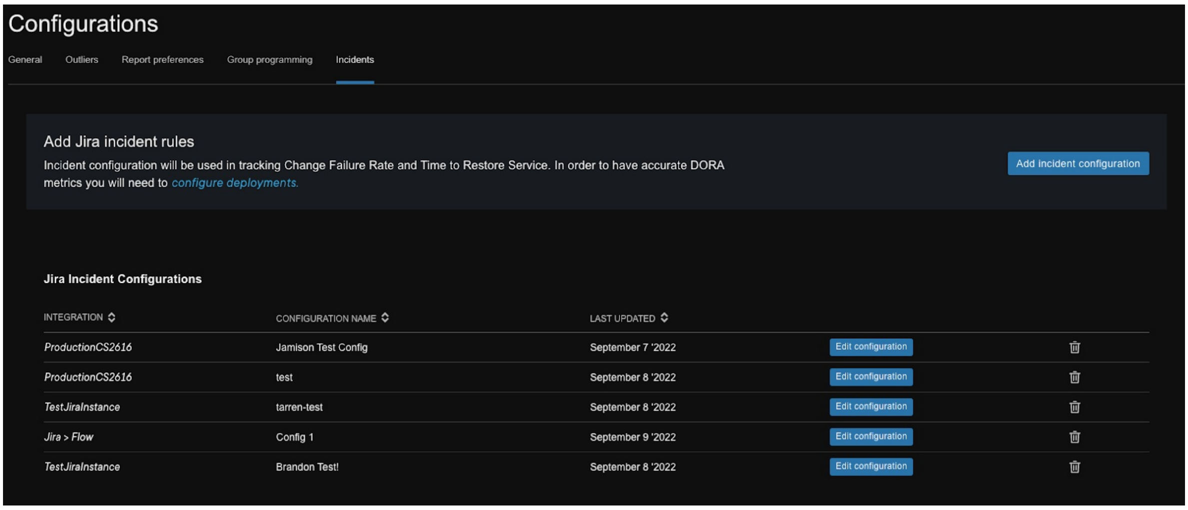
back to top

Add an incident configuration

Configuring incidents tells Flow what an incident is for you. Set incident configuration rules to apply to teams, projects, or whole integrations.

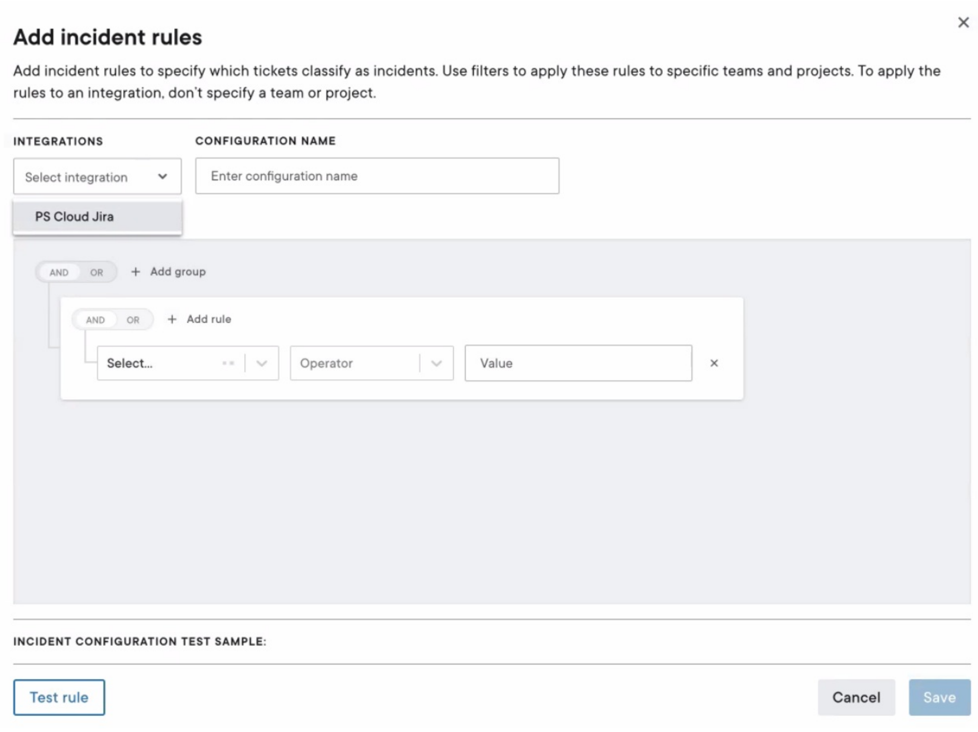
To add an incident configuration:

1. Click **Settings** in Flow's top navigation bar.
2. In the left navigation bar under **Report Settings**, click **Configurations**.
3. Click the **Incidents** tab.



4. Click **Add incident configuration**.
5. In the modal, add incident rules to indicate which tickets are incidents. Use filters to identify which tickets track incidents. Apply these rules to specific teams or projects using the ticket attributes of your integration.

   > **Note:** To apply the rules to the entire integration, don't specify a team or project.



6. Test your rule in Flow or Jira to verify your incident configuration matches the tickets you expect. Adjust your rules as needed based on the results.
7. Once you're happy with the results of the test, click **Save**.

Testing your incident configuration

Before saving your incident configuration, you should test it to make sure it returns the incidents you expect.

Tips for testing incident configurations:

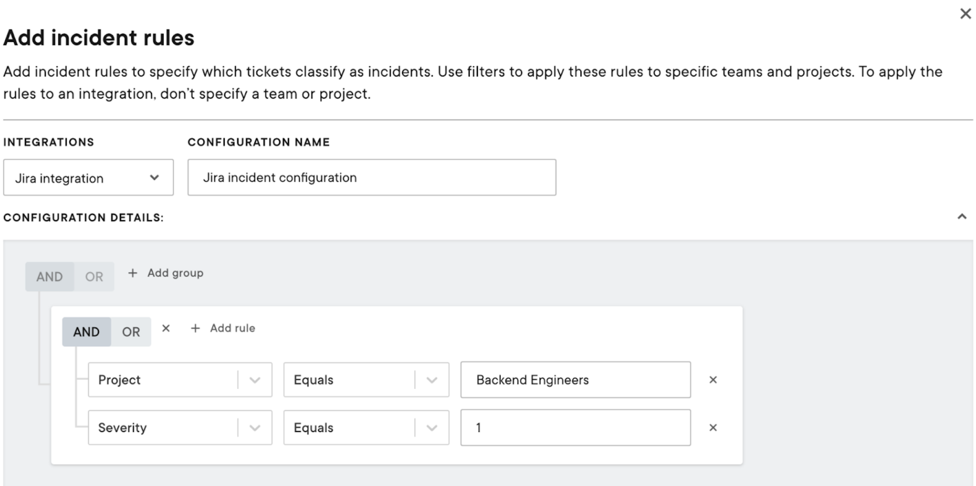
- When testing a rule in Flow, only incidents created in the last 90 days that match the configuration display.
- If you're using the **Project** field in your configuration, input the full name of the project, not the Jira short code or abbreviation. Flow must have the full project name to correctly find incidents.
- Once you've set up your configuration, Flow must process the changes before displaying the data in your DORA metrics. This can take a couple hours. Check back after this to make sure the incidents you expect are displaying.

You have two options to test your incident configuration:

1. Click **Test rule** in Flow before saving your configuration. This only displays incidents created within the last 90 days.
2. Create a JQL version of your configuration and test the configuration in JIra to see what incidents will display. This is the best option if you want to have your test display incidents created before the 90 day cutoff, or if your query returns too many incidents for Flow to display correctly.

Simple configuration example:

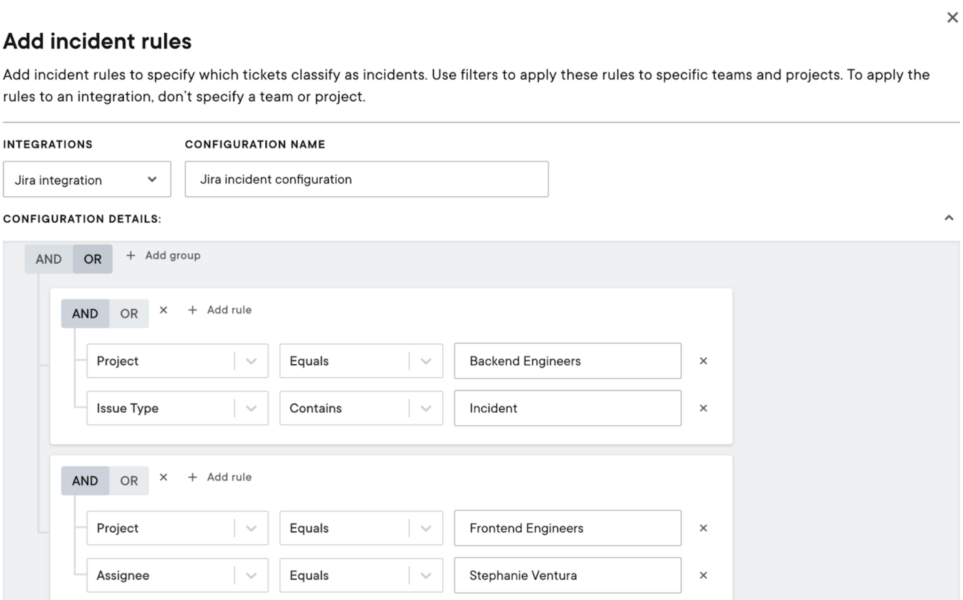
- **JQL**: `project in (BEE) AND (“Severity” = 1)`
- **Flow configuration**: `Project equals Backend Engineers AND Severity equals 1`



Tip: In this example, the project key is used in the JQL query, but the full project name must be used in Flow for the incident configuration to work properly.

Complex configuration example:

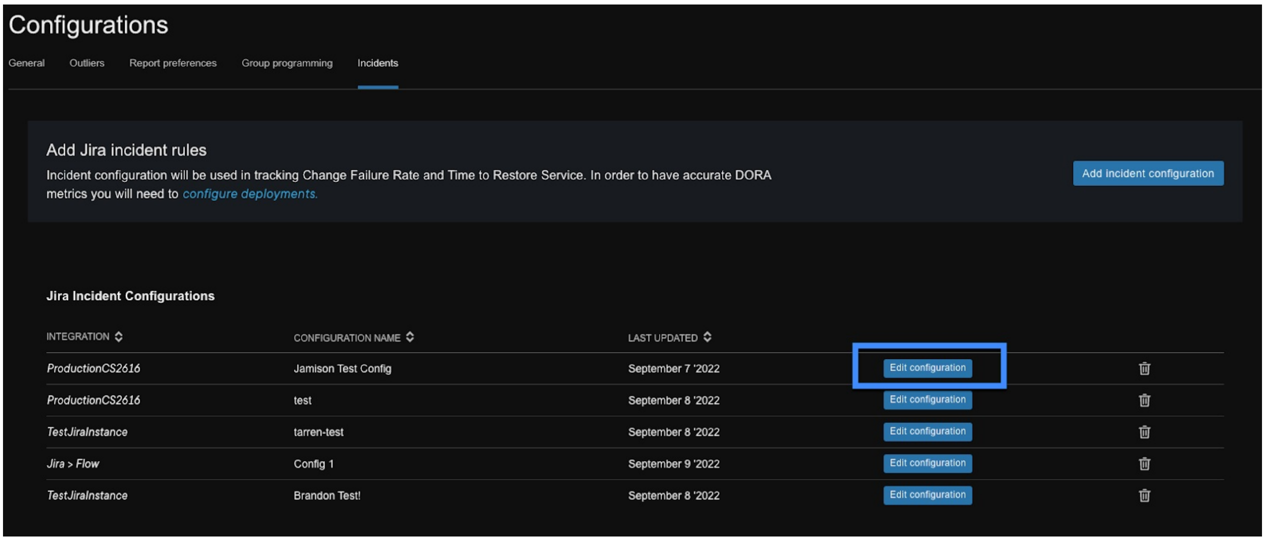
- **JQL**: (project = BEE AND issuetype in ("Potential Incident", “Confirmed Incident”)) OR (project = FEE AND assignee in ([Jira user ID]))
- **Flow configuration**: (Project equals Backend Engineers AND Issue type contains Incident) OR (Project equals Frontend Engineers AND Assignee equals Stephanie Ventura)



back to top

Edit an incident configuration

You can edit your incident configurations to change your incident settings.



To edit an incident configuration:

1. Click **Edit configuration** next to the integration you want to edit.
2. In the modal, add, remove, or edit incident rules to indicate how incidents are tracked.
3. Use the filters to apply these rules to specific teams and projects. To apply the rules to an integration, don't specify a team or project.
4. Click **Save**.

back to top

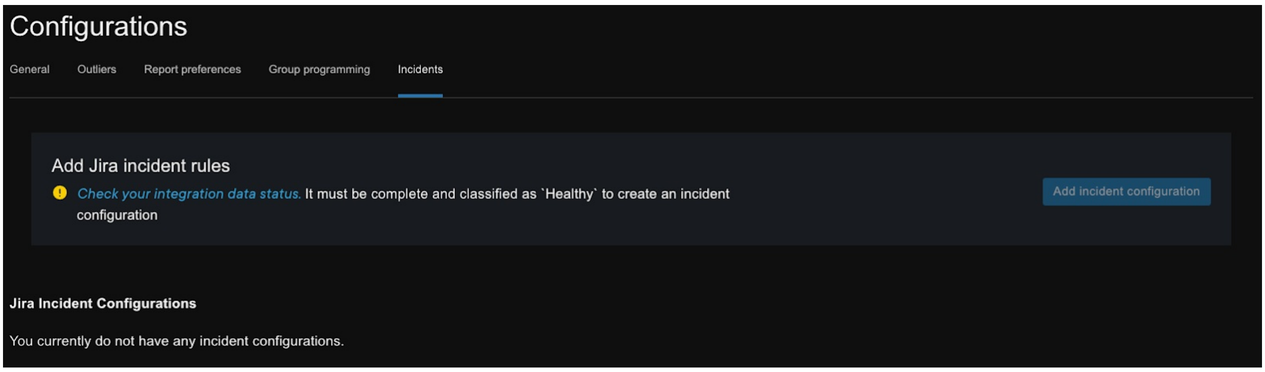
Delete an incident configuration

To delete an incident, click the **trash icon** next to the configuration you want to delete.

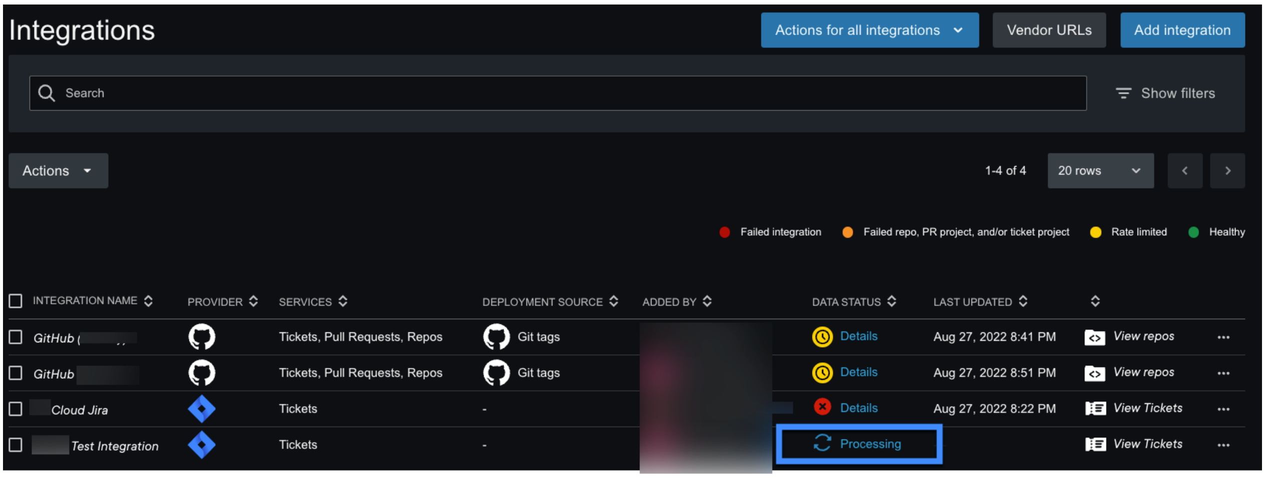
back to top

Troubleshooting

If you see an error message, your integration may not be set up completely or may not yet be fully ingested. Check the integration data status on the integrations page to see where the integration is in the process.



In this example, the integration is still processing and has not completely ingested into Flow, as indicated by the **Processing** label in the Data Status column.



If you need help, please contact Pluralsight Support.