

IBM Resilient



Incident Response Platform Integrations

Jira Function V1.0.2

Release Date: December 2018

Resilient Functions simplify development of the integrations by sending data from the Resilient platform to a remote program that performs an activity then returns the results to the function. The results can be acted upon by a script and the result of that becomes a decision point in the Resilient workflow.

This guide describes the Jira Function Integrations.

Overview

The Jira integration with the Resilient platform allows for the tracking of Incidents as Jira Issues. Bidirectional links are saved to allow for easy navigation between the applications.

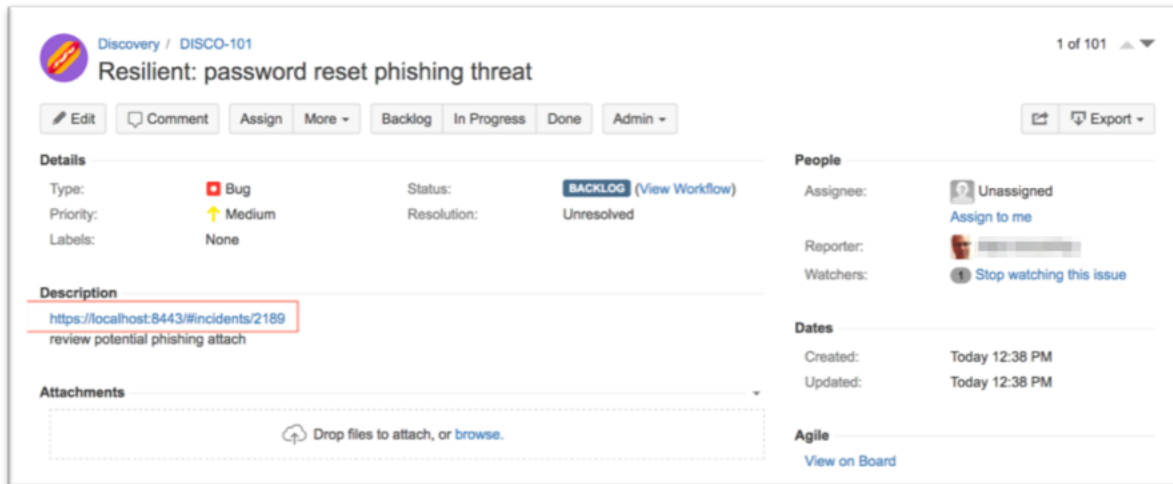
This integration allows for the creation of Jira issues, adding comments, and transitioning issues when the corresponding Incident is closed. The following screenshots show how this would appear in an incident.

The screenshot shows the IBM Resilient incident interface for an incident titled "password reset phishing threat". The interface is divided into several sections: Summary, Description, and Tasks. The Summary section on the left includes fields for ID (2189), Phase (Engage), Severity (Low), Date Created (04/07/2018), Date Occurred (—), Date Discovered (04/07/2018), Data Compromised (Unknown), Incident Type (Phishing), and a link to "Jira Ticket ...". The Description section on the right shows the incident title and a brief description: "review potential phishing attach". Below the description is a tabbed interface with tabs for Tasks, Details, Breach, Notes, Members, News Feed, Attachments, Stats, Timeline, and Artifacts. The Tasks tab is active, showing a progress bar at 0% Complete and a table of tasks. The table has columns for Task Name, Owner, Due Date, Flags, and Actions. The tasks listed are: "Initial Triage", "Interview key individuals", "Notify internal management chain (preliminary)", and "Determine if illegal activity is involved". All tasks are currently "Unassigned" and have "No due date". The "People" section at the bottom left shows the incident was created by "Resilient Sysadmin" and owned by "Resilient Sysadmin". There are no members listed.

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2018. All Rights Reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.



Setup

The following lists the system requirements:

- Python version 2.7.10 or later, or version 3.6 or later
- Resilient Circuits and Resilient Python libraries version 30.0 or later
- Resilient-Lib common package of helper utilities
- Resilient platform version 30.0 or later
- Jira version 7.4 or later

Perform the following to install and configure the function:

1. Ensure the environment is up to date:

```
sudo pip install --upgrade pip
sudo pip install --upgrade setuptools
sudo pip install --upgrade resilient-circuits
```

2. Install the required software for the function (if not already installed):

```
sudo pip install fn_jira-<version>.tar.gz
```

3. Add the function to the Resilient platform:

```
resilient-circuits customize
```

You are prompted to answer prompts to import functions, message destinations, etc.

4. From the account used for Integrations, use one of the following commands to configure the Jira settings. Use `-c` for new environments or `-u` for existing environments.

```
resilient-circuits config -c
```

OR

```
resilient-circuits config -u
```

5. Edit the `.resilient/app.config` file and section `[jira]`:

```
url=<jira url>
user=<jira access user>
password=<jira access password>
verify_cert=[True|False]
```

Use `False` for self-signed SSL certificates.

After completing the configuration steps, enter the `resilient-circuits run` command. The following is an example of the resulting messages indicating the successful connection to the Resilient platform and the loading of the Jira integration modules.

```
$ resilient-circuits run
2018-04-07 12:38:04,164 INFO [app] Configuration file:
/Users/Integration/.resilient/app.config
2018-04-07 12:38:04,165 INFO [app] Resilient server: <host>
2018-04-07 12:38:04,165 INFO [app] Resilient user: <acct>
2018-04-07 12:38:04,165 INFO [app] Resilient org: <org>
2018-04-07 12:38:04,165 INFO [app] Logging Level: INFO
...
2018-04-07 12:38:05,418 INFO [component_loader]
'fn_jira.components.jira_open_issue.FunctionComponent' loading
2018-04-07 12:38:05,419 INFO [component_loader]
'fn_jira.components.jira_create_comment.FunctionComponent' loading
2018-04-07 12:38:05,420 INFO [component_loader]
'fn_jira.components.jira_transition_issue.FunctionComponent' loading
...
2018-04-07 12:38:05,435 INFO [actions_component]
'fn_jira.components.jira_open_issue.FunctionComponent' function 'jira_open_issue'
registered to 'jira'
2018-04-07 12:38:05,436 INFO [actions_component]
'fn_jira.components.jira_create_comment.FunctionComponent' function
'jira_create_comment' registered to 'jira'
2018-04-07 12:38:05,437 INFO [actions_component]
'fn_jira.components.jira_transition_issue.FunctionComponent' function
'jira_transition_issue' registered to 'jira'
...
2018-04-07 12:38:05,729 INFO [actions_component] Subscribe to message destination
'jira'
...
2018-04-07 12:38:05,731 INFO [stomp_component] Subscribe to message destination
actions.<org id>.jira
...
```

Resilient Platform Configuration

In the Customization Settings section of the Resilient platform, you can verify that the following Jira specific functions, workflows and rules are available in the Resilient platform by clicking their respective tabs.

- **Functions**
 - **Jira Create Issue.** Creates a Jira issue including an incident's title, description and severity level. A custom Incident field provides a link back to Jira. See the corresponding workflow which defines which issue project and issue type to use.
 - **Jira Create Comment.** Creates a Jira comment based on adding a note to an incident. The note's description field is referenced.
 - **Jira Transition Issue.** Transitions a Jira issue. See the corresponding workflow which defines the transition ID to use.

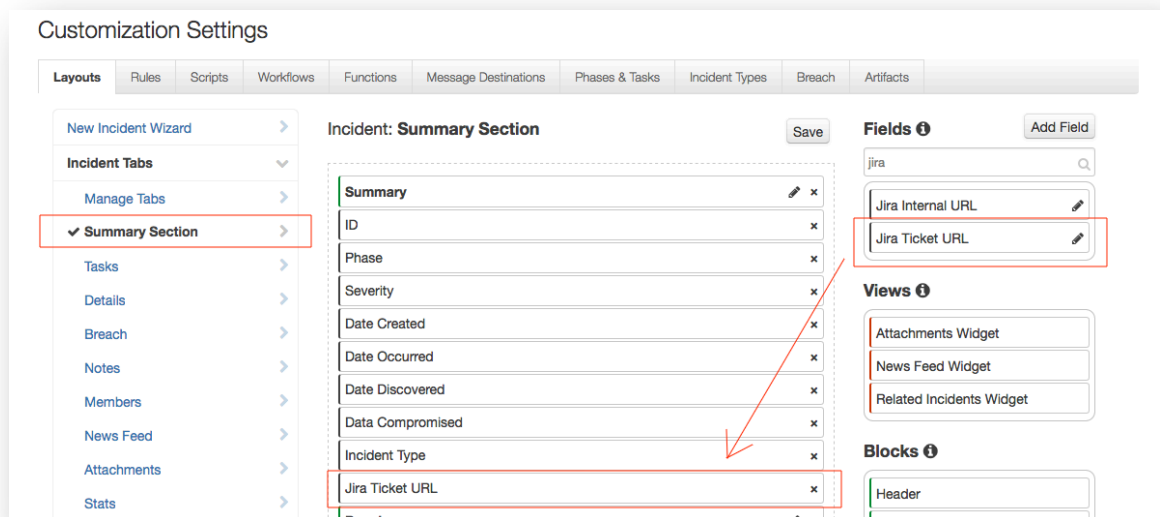
- Workflows. Some modifications are needed for your Jira environment as indicated below.
 - **Example: Jira Open Issue.** Edit the Jira Open Issue function for the specific `jira_project` and `jira_issuetype` fields for your Jira use.
 - **Example: Jira Open Issue (Task).** Similar to creating a Jira issue from an incident, but instead creates a Jira issue based on an incident task.
 - **Example: Jira Create Comment.**
 - **Example: Jira Transition Issue.** Edit the Jira Transition Issue function for the specific `jira_transition_id` required in your workflow. The default value of 41 represent the Jira close issue state.
 - **Example: Jira Transition Issue (Task):** For a task with an associated issue, transition the issue.
- Rules. Operate on an incident, task or an incident's notes. If you wish to change rules from automatic to menu item, new rules referencing the same workflows need to be created.
 - Example: Create Jira Issue
 - Example: Create Jira Issue (Task)
 - Example: Jira Create Comment
 - Example: Jira Close Issue
 - Example: Jira Close Issue (Task)

Layout

Jira Ticket URL Custom Field

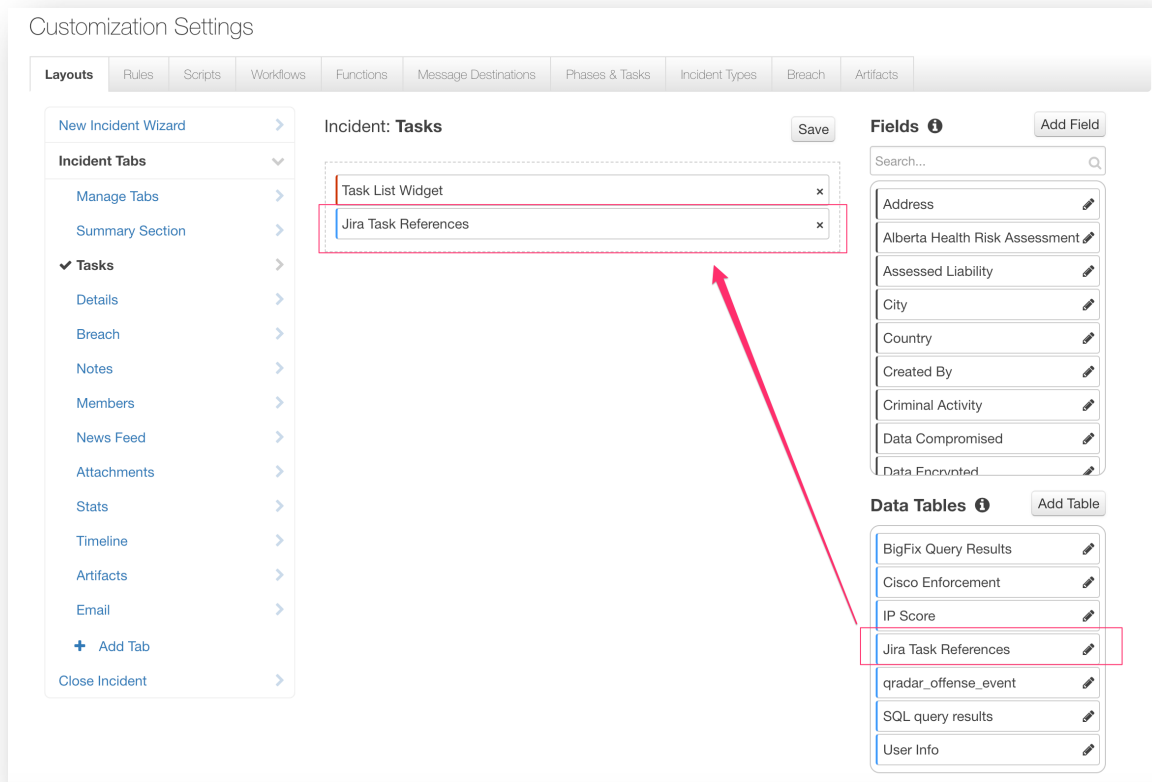
To display a link back to the Jira issue created from an incident,

- Navigate to the Customization Settings and select the Summary Section from the Layouts tab
- Search for the Jira custom fields and drag Jira Ticket URL to the Summary Section
- Click Save



Jira Task Reference Data Table

- Perform the same update operations with the Jira Task References data table on the Task layout.



Operation

There are two use cases provided in this package:

- 1) Create a Jira issue associated with a Resilient Incident
 - a. Notes are automatically pushed to Jira once the Jira Issue is created
 - b. Jira issue is closed when the Resilient Incident is closed
- 2) Create a Jira issue associated with an Incident's task
 - a. Notes are automatically pushed to Jira once the Jira Issue is created
 - b. Jira issue is closed when the data table menu rule is invoked

Modifications

Priorities

Both the Jira Open Issue and Jira Transition Issue workflows use a mapping between Resilient incident severity codes and Jira Issue priorities. If you wish to have a different mapping to Jira, modify these two workflows and their corresponding Pre-Processing Script

The screenshot displays the Jira Open Issue workflow editor. At the top, a toolbar contains various icons for workflow actions. The main canvas shows a workflow starting with a 'Start your workflow here' node, leading to a 'Jira Open Issue' node. A callout box explains: 'Choose the Jira project and issue type. Values passed to Jira include the Incident's name, description and priority'. Another callout box states: 'Output populates a URL back to the created Jira Issue and the internal Id used to add Jira comments or to close the Issue'. Below the canvas, a 'Pre-Process Script' tab is active, showing a Python script. The script maps incident severity codes to Jira priorities. A red box highlights the priority mapping dictionary.

```
1 inputs.incidentID = incident.id
2
3 inputs.jira_summary = u"Resilient: {}".format(incident.name)
4 if not incident.description is None:
5     inputs.jira_description = incident.description.content
6
7 priority = { 'Low': '3', 'Medium': '2', 'High': '1' }
8 if incident.severity_code in priority:
9     inputs.jira_priority = priority.get(incident.severity_code)
10 else:
11     inputs.jira_priority = '4'
```

Assignee

The assignee of the Jira ticket is controlled by a pre-processing script lookup relationship between Resilient users and Jira users. Edit the following line in 'Example: Jira Open Issue' workflows to match the list associated with your enterprise:

```
lookup = { "Resilient email ID": "JIRA assignee" [ "user2": "jira user2" ] }
```

Refer to the post-processing scripts for comments on the sample payload returned.

Resolution Field

Some Jira issues do not support a resolution field when closed. In these cases, edit the Jira Transition Issue and Jira Transition Issue (Task) pre-processor scripts and comment out the following line:

```
inputs.jira_resolution = lookup.get(str(incident.resolution_id).lower(),
None)
```

Transition ID

All issue types have a defined workflow of states which the issue can transition between. These states can be identified through the API using the curl command similar to the following on a given type of issue (28623).

```
curl -u admin:admin -XGET -H "Content-Type: application/json" -k  
https://localhost/rest/api/2/issue/28623/transitions
```

The returned json will identify the transition id to use in the `jira_transition_id` input field for the transition workflows:

```
{  
  "id": "231",  
  "name": "Done",  
  "to": { ... }  
}
```

Troubleshooting

There are several ways to verify the successful operation of a function.

- Resilient Action Status

When viewing an incident, use the Actions menu to view Action Status. By default, pending and errors are displayed. Modify the filter for actions to also show Completed actions. Clicking on an action displays additional information on the progress made or what error occurred.

- Resilient Scripting Log

A separate log file is available to review scripting errors. This is useful when issues occur in the pre-processing or post-processing scripts. The default location for this log file is:

```
/var/log/resilient-scripting/resilient-scripting.log
```

- Resilient Logs

By default, Resilient logs are retained at `/usr/share/co3/logs`. The `client.log` may contain additional information regarding the execution of functions.

- Resilient-Circuits

The log is controlled in the `.resilient/app.config` file under the section `[resilient]` and the property `logdir`. The default file name is `app.log`. Each function creates progress information. Failures show up as errors and may contain Python trace statements.

Support

For additional support, go to Resilient Community Forum at <https://ibm.biz/resilientcommunity>.