IBM Resilient

Incident Response Platform Integrations

Jira Function V1.0.0

Release Date: April 2018

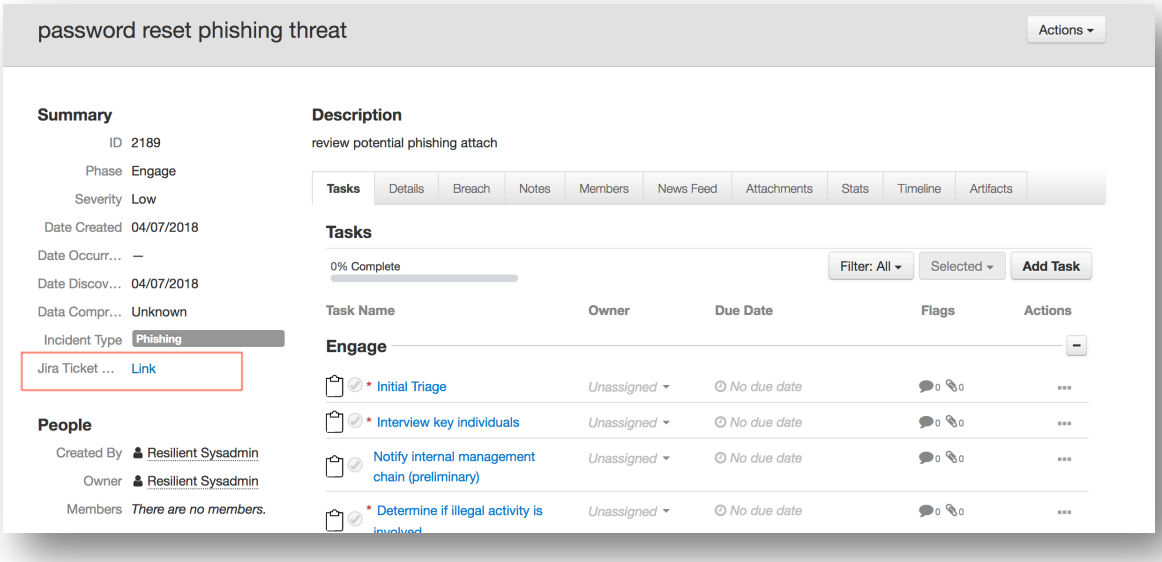
Resilient Functions simplify development of the integrations by sending data from the Resilient platform to a remote program that performs an activity then returns the results to the function. The results can be acted upon by a script and the result of that becomes a decision point in the Resilient workflow.

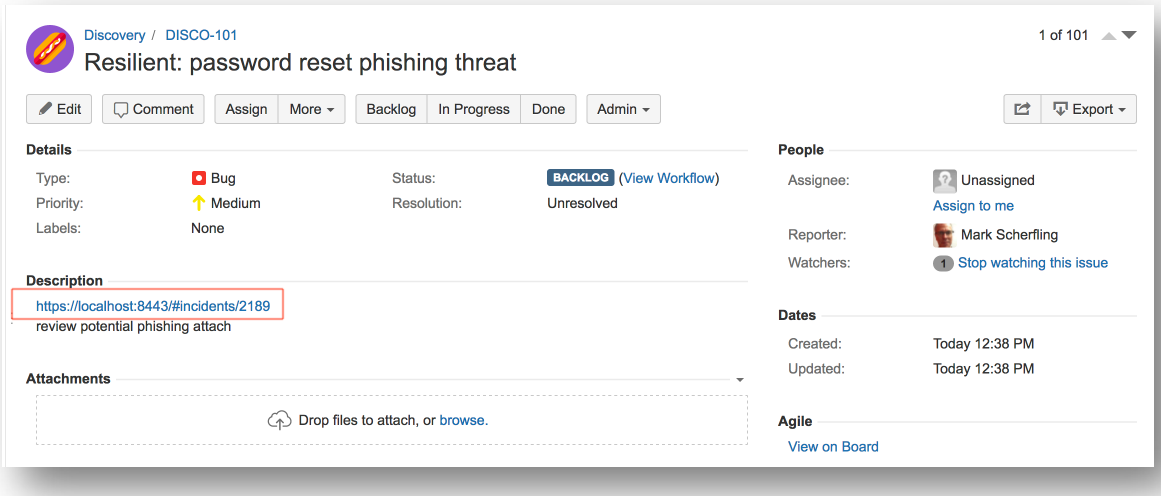
This guide describes the Jira Function.

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.





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 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>
verifyFlag=[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.

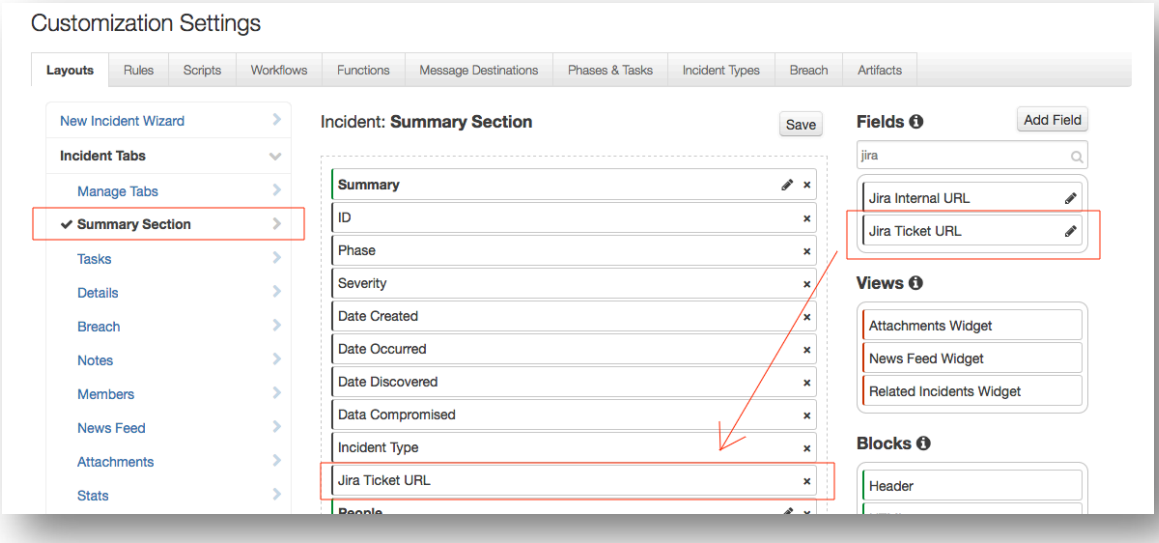
- Functions
  - **Jira Create Issue**. Creates a Jira issue including an incident's title, description and severity level. A custom Incident field provides a link back to Jira. See the corresponding workflow which defines which issue project and issue type to use.
  - **Jira Create Comment**. Creates 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.
    - **Jira Open Issue**. Edit the Jira Open Issue function for the specific **jira_project** and **jira_issuetype** fields for your Jira use.
    - **Jira Create Comment**.
    - **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.
- Rules. Operate on an incident 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.
    - Jira Open Issue
    - Jira Create Comment
    - Jira Close Issue

Layout

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



Operation

The default operation is to automatically create a Jira issue when a Resilient incident is created. You can change this behavior as indicated in the Configuration section above. Furthermore, you can add conditions to restrict the type of Incidents which trigger Jira issue creation.

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, contact support@resilientsystems.com.

Including relevant information from the log files will help us resolve your issue.