fn-incident-utils Functions for IBM Resilient

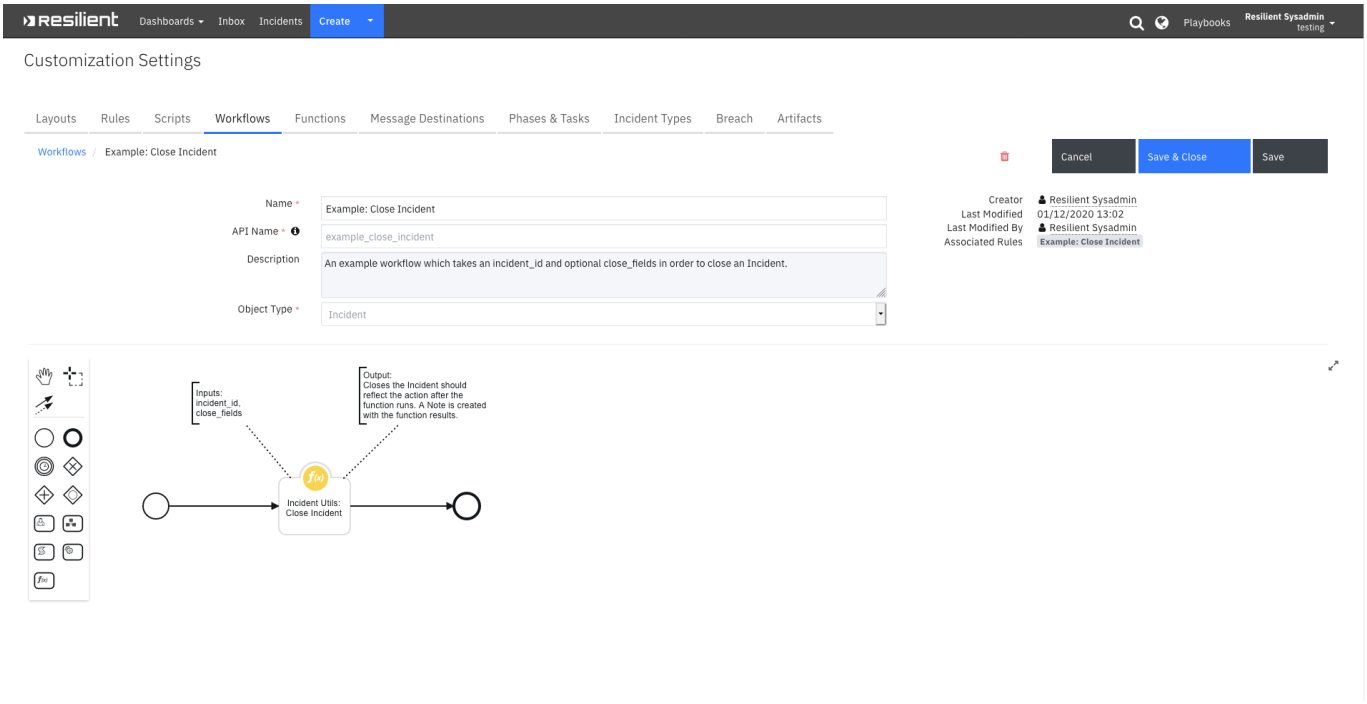
Release Notes

v1.0.0

- Initial Release

Overview

Close Incident Function for IBM Resilient



Close Incident Function takes an incident_id and a JSON String of field_name and field_value pairs to close an Incident.

Requirements

- Resilient platform >= `v36.0.5634`
- An Integration Server running `resilient_circuits>=30.0.0`

- To set up an Integration Server see: ibm.biz/res-int-server-guide
- If using API Keys, minimum required permissions are:
  - Org Data: Read, Edit
  - Function: Read

Installation

- Download the `fn_incident_utils.zip`.
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_incident_utils-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_incident_utils-x.x.x
```

- **Install** the package:

```
$ pip install fn_incident_utils-x.x.x.tar.gz
```

- Import the fn_incident_utils **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-incident-utils
```

- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-incident-utils
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-incident-utils
```

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 will create progress information.
- Failures will show up as errors and may contain python trace statements.

Support

Name	Version	Author	Support URL
fn_incident_utils	1.0.0	IBM Resilient	http://ibm.biz/resilientcommunity