fn-proofpoint-trap Functions for IBM Resilient

- Release Notes
- Overview
- Requirements
- Installation
- Uninstall
- Troubleshooting
- Support

Release Notes

v1.0.3

- Fixed bug where incident summary is unavailable.
- Fixed bug where incidents not not being filtered by state.
- Fixed bug with Resilient incident severity codes.

v1.0.2

- Fix bug in workflow 'Proofpoint TRAP Update List Member'.

v1.0.1

- Fix url concatenation issue.

v1.0.0

- Initial Release

Overview

Proofpoint Threat Response Auto-Pull (TRAP) enables messaging and security administrators to analyze emails and move malicious or unwanted emails to quarantine, after delivery. It follows forwarded mail and distribution lists, and creates an auditable activity trail.

The ProofPoint TRAP function package provides the following features:

- Poll a Proofpoint TRAP server for incidents and create corresponding incidents in the Resilient platform.
- Get Proofpoint TRAP incident details.
- Get a Proofpoint TRAP list member or members.
- Add a member to a Proofpoint TRAP list for artifacts of type host, IP address, or URL.
- Update a member of a Proofpoint TRAP list.
- Delete a member from a Proofpoint TRAP list.

Requirements

- Resilient platform >= `v32`
- An Integration Server running `resilient_circuits>=33.0.192`
  - To set up an Integration Server see: ibm.biz/res-int-server-guide

---

Installation

- Download the `fn_proofpoint_trap-x.x.x.zip` from the app exchange.
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_proofpoint_trap-x.x.x.zip
```

- **Install** the package:

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

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u -l fn-proofpoint-trap
```

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

```
$ resilient-circuits customize -y -l fn-proofpoint-trap
```

- Open the config file, scroll to the bottom and edit your fn_proofpoint_trap configurations:

```
$ nano ~/.resilient/app.config
```

Config	Required	Example	Description
base_url	Yes	https://192.168.1.1/api	*Base URL of Proofpoint TRAP API.*
api_key	Yes	abcd1234-a123-123a-123a-123456abcdef	*API Key for Proofpoint TRAP.*

Config	Required	Example	Description
polling_interval	Yes	2	*Interval to poll Proofpoint TRAP in Minutes, 0 to turn off.*
startup_interval	Yes	60	*Initial Import Look-back Interval in minutes (default: 1 hour).*
state	Yes	open	*State of Incidents to Query*
host_categories	Yes	attacker,cnc,forensics,url	*Comma separated list of 'host' categories to check for artifacts. The default is forensics.*
cafile	No	cafile=~/.resilient/trap/cert.cer	*Optional setting to use a ca certificate to access Proofpoint TRAP.*
http_proxy or **https_proxy**	No	https://proxyhost:8080	*Optional settings for access to Proofpoint TRAP via a proxy.*

- **Save** and **Close** the app.config file.
- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-proofpoint-trap
```

- **Run** resilient-circuits as follows, or restart the resilient-circuits service:

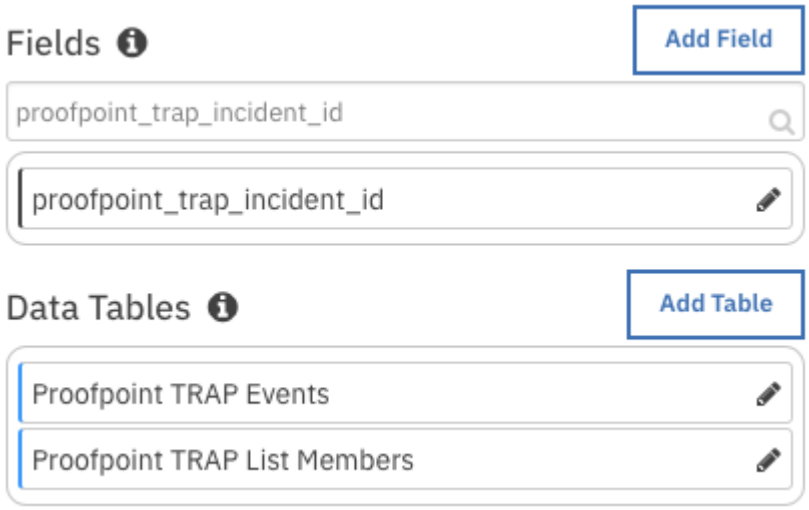
```
$ resilient-circuits run
```

- **Run** resilient-circuits with extra logging:

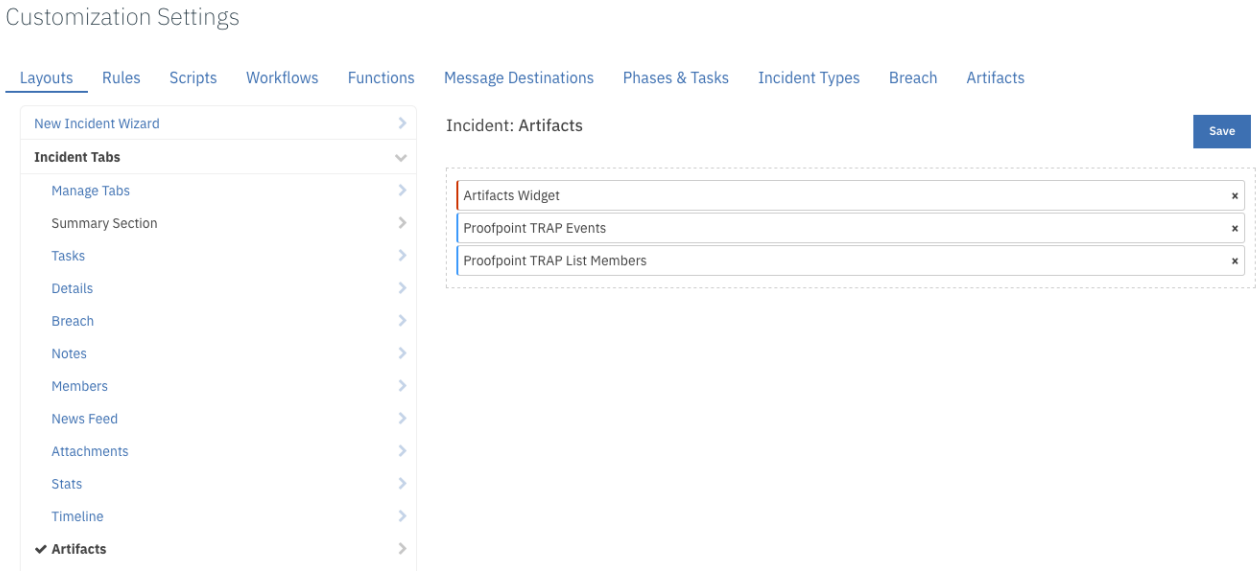
```
$ resilient-circuits run --loglevel=DEBUG
```

Custom Layouts

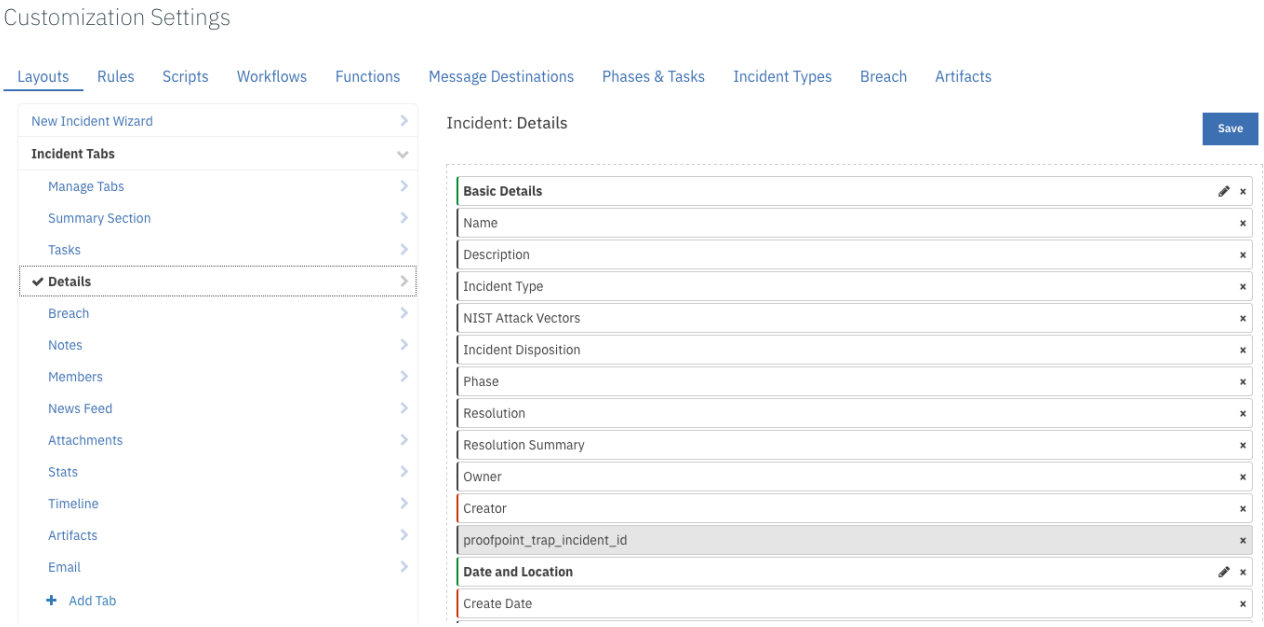
- The package customizations includes the following custom field and data tables:



- In the Layouts tab, add the data table to the Artifacts tab and save:



- In the Layouts tab, add the custom field to the Details tab and save:



Uninstall

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

```
$ pip uninstall fn-proofpoint-trap
```

- Open the config file, scroll to the [fn_proofpoint_trap] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

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 a®lso 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

- 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_proofpoint_trap	1.0.1	IBM Resilient Support	support@resilientsystems.com