

# fn-proofpoint-trap Functions for IBM Resilient

---

- [Release Notes](#)
  - [Overview](#)
  - [Requirements](#)
  - [Installation](#)
  - [Uninstall](#)
  - [Troubleshooting](#)
  - [Support](#)
- 

## Release Notes

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  $\geq$  **v30.0.3476**
  - An Integration Server running **resilient\_circuits**  $\geq$  **30.0.0**
    - To set up an Integration Server see: [ibm.biz/res-int-server-guide](https://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
<b>base_url</b>	Yes	https://192.168.1.1/api	<i>Base URL of Proofpoint TRAP API</i>
<b>api_key</b>	Yes	abcd1234-a123-123a-123a-123456abcdef	<i>API Key for Proofpoint TRAP</i>
<b>polling_interval</b>	Yes	2	<i>Interval to poll TRAP in Minutes</i>
<b>startup_interval</b>	Yes	60	<i>Initial Import Look-back Interval in minutes (default: 1 hour)</i>
<b>state</b>	Yes	open	<i>State of Incidents to Query</i>
<b>host_categories</b>	Yes	attacker,cnc,forensics,url	<i>Comma separated list of 'host' categories to check for artifacts. The default is forensics.</i>
<b>cafile</b>	No	cafile=~/.resilient/trap/cert.cer	<i>Optional setting to use a ca certificate to access Proofpoint TRAP</i>
<b>http_proxy</b> or <b>https_proxy</b>	No	https://proxyhost:8080	<i>Optional settings for access to Proofpoint TRAP via a proxy</i>

- **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:

**Fields** ⓘ Add Field

Q

✎

**Data Tables** ⓘ Add Table

✎

✎

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

Customization Settings

The screenshot shows the 'Layouts' tab in the Customization Settings. On the left, under 'Incident Tabs', the 'Artifacts' tab is selected. The main panel, titled 'Incident: Artifacts', contains a list of widgets: 'Artifacts Widget', 'Proofpoint TRAP Events', and 'Proofpoint TRAP List Members'. A 'Save' button is located in the top right corner.

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

Customization Settings

The screenshot shows the 'Layouts' tab in the Customization Settings. On the left, under 'Incident Tabs', the 'Details' tab is selected. The main panel, titled 'Incident: Details', contains a list of fields organized into sections: 'Basic Details' (Name, Description, Incident Type, NIST Attack Vectors, Incident Disposition, Phase, Resolution, Resolution Summary, Owner, Creator, proofpoint\_trap\_incident\_id) and 'Date and Location' (Create Date). A 'Save' button is located in the top right corner.

## 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 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

- 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	1.0.0	IBM Resilient Support	support@resilient-systems.com