

fn-proofpoint-trap Functions for IBM Resilient

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

Release Notes

v1.0.0

- Initial Release
-

Overview

Resilient integration for Proofpoint TRAP

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 Resilient.
 - 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 to a list.
 - Update a member of a Proofpoint Trap list.
 - Delete a member from of a Proofpoint Trap list.
-

Requirements

- Resilient platform >= **v30.0.3476**
 - An Integration Server running **resilient_circuits>=30.0.0**
 - 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
polling_interval	Yes	2	Interval to poll TRAP in Minutes
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.

Config	Required	Example	Description
cafile	No	cafile=~/.resilient/trap/cert.cer	<i>Optional setting to use a ca certificate to access Proofpoint TRAP</i>
http_proxy or https_proxy	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 or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

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

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

Custom Layouts

- The package customizations includes the following Data Table and Custom Field:

Fields ⓘ

Add Field

proofpoint_trap_incident_id

proofpoint_trap_incident_id

Data Tables ⓘ

Add Table

Proofpoint TRAP Events

Proofpoint TRAP List Members

- Add the data table to the Incident->Artifacts tab and save:

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

New Incident Wizard

Incident Tabs

- Manage Tabs
- Summary Section
- Tasks
- Details
- Breach
- Notes
- Members
- News Feed
- Attachments
- Stats
- Timeline
- ✓ Artifacts

Incident: Artifacts

Save

- Artifacts Widget
- Proofpoint TRAP Events
- Proofpoint TRAP List Members

- Add the custom field to the Incident->Details tab and save:

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

New Incident Wizard

Incident Tabs

- Manage Tabs
- Summary Section
- Tasks
- ✓ Details
- Breach
- Notes
- Members
- News Feed
- Attachments
- Stats
- Timeline
- Artifacts
- Email
- + Add Tab

Incident: Details

Save

Basic Details

- Name
- Description
- Incident Type
- NIST Attack Vectors
- Incident Disposition
- Phase
- Resolution
- Resolution Summary
- Owner
- Creator
- proofpoint_trap_incident_id

Date and Location

- Create Date

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

- 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_proofpoint_trap	1.0.0	IBM Resilient Support	support@resilientsystems.com