

User Guide: fn_anomali_staxx

Table of Contents

- [Release Notes](#)
- [Overview](#)
- [Key Features](#)
- [Requirements](#)
- [Installation](#)
- [Uninstall](#)
- [Upgrades to v1.0.1](#)
- [Function - Staxx Query](#)
- [Function - Staxx Import](#)
- [Rules](#)
- [Troubleshooting](#)
- [Anomali Staxx Notes](#)
- [Support](#)

Release Notes

v1.0.1

- fn_send_to_staxx changed to fn_anomali_staxx
- Added query capability
- Updated example workflows

v1.0.0

- Initial Release (based on send-to-staxx integration)

Overview

'fn_anomali_staxx' app

te
Edit

✕

Example: Anomali Staxx Import

Auto Approve *

Confidence Level * ⓘ

Indicator Type *

Severity Level *

TLP Color *

yes

85

exploit

low

RED

Cancel

Execute

08/12/2020 14:46

08/12/2020 14:26

As specified in the artifact type sett

As specified in the artifact type sett

✎ ✖ ⋮

✎ ✖ ⋮

Key Features

- Add artifact values as indicators to Anomali Staxx
- Search Anomali Staxx for indicators matching an artifact value

Requirements

- Resilient platform >= **v35.2.32**
- An Integration Server running **resilient_circuits>=30.0.0**
 - To set up an Integration Server see: [Installation Guides](#)
 - If using API Keys, minimum required permissions are:
 - Org Data: Read, Edit
 - Function: Read

Installation

App Host

All the components for running this integration in a container already exist when using the App Host app.

To install,

- Navigate to Administrative Settings and then the Apps tab.
- Click the Install button and select the downloaded file: app-fn_anomali_staxx-x.x.x.zip.
- Go to the Configuration tab and edit the app.config file, editing the API key for Anomali Staxx and making any additional setting changes.

Config	Required	Example	Description
--------	----------	---------	-------------

2020-08-21

2/7

Config	Required	Example	Description
staxx_ip	Yes	10.10.10.10	Enter a description of the config here
staxx_port	Yes	8080	Enter a description of the config here
staxx_user	Yes	someuser	Enter a description of the config here
staxx_password	Yes	somepass	Enter a description of the config here
https_proxy	No	https://your.proxy.com / <i>https proxy for connecting to Anomali Staxx</i>	
http_proxy	No	http://your.proxy.com / <i>http proxy for connecting to Anomali Staxx</i>	

Integration Server

- Download the **app-fn_anomali_staxx-x.x.x.zip** file.
- Copy the **.zip** to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip app-fn_anomali_staxx-x.x.x.zip
```

- **Install** the package:

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

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

```
$ resilient-circuits config -u -l fn-anomali-staxx
```

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

```
$ resilient-circuits customize -y -l fn-anomali-staxx
```

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

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

Config	Required	Example	Description
staxx_ip	Yes	10.10.10.10	Enter a description of the config here
staxx_port	Yes	8080	Enter a description of the config here
staxx_user	Yes	someuser	Enter a description of the config here
staxx_password	Yes	somepass	Enter a description of the config here
https_proxy	No	https://your.proxy.com / https proxy for connecting to Anomali Staxx	
http_proxy	No	http://your.proxy.com / http proxy for connecting to Anomali Staxx	

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

```
$ resilient-circuits selftest -l fn-anomali-staxx
```

- **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-anomali-staxx
```

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

Upgrades to v1.0.1

If you're upgrading from v1.0.0, please uninstall the original app (fn_send_to_staxx) and reinstall as a new integration, including rerunning **resilient-circuits config -u -l fn-anomali-staxx** and **resilient-circuits customize -l fn-anomali-staxx**.

The app.config settings [staxx] will now become [fn_anomali_staxx] and the [staxx] settings can then be removed.

Function - Staxx Query

Query Staxx for indicators based on an artifact value. A confirming note is added to the incident.

Show 25

Columns

Hits	Type	Value	Created	Relate?	Actions
	DNS Name	xcv.com	08/12/2020 15:27	As specified in the artifact type sett	<div><div></div><div></div><div></div></div>
	Email Sender	x@exmaple.com	08/12/2020 15:27		
	Email Sender	a@exampe.com	08/12/2020 15:13		
	IP Address	12.34.56.78	08/12/2020 15:13		

Search...

☒ Show Task Notes ☐ Oldest Notes First

Created By: 0 selected

Date Created: All

Resilient Sysadmin added a note to the Incident 08/13/2020 11:11

Artifact: xcv.com

Staxx results:

Date Updated: 2020-08-13 11:04:19 AM

Confidence: 85

TLP:RED

Type: phish_domain

Severity: high

Campaign:

- Inputs:
- Outputs:
- Workflows

Function - Staxx Import

Send an observable to Anomali Staxx including categorization settings. A confirming note is added to the incident.

te
Edit

Example: Anomali Staxx Import

✕

Auto Approve *

yes

Confidence Level * ⓘ

85

Indicator Type *

exploit

Severity Level *

low

TLP Color *

RED

Cancel

Execute

08/12/2020 14:46

As specified in the artifact type sett

✎ 🗑 ⋮

08/12/2020 14:26

As specified in the artifact type sett

✎ 🗑 ⋮

👤 Resilient Sysadmin added a note to the *Incident* 08/13/2020 11:04

Artifact: xcv.com added to Anomali Staxx:

Confidence: 85
Indicator Type: phish
TLP: RED
Severity: high

- ▶ Inputs:
- ▶ Outputs:
- ▶ Workflows

Rules

Rule Name	Object	Workflow Triggered
Example: Anomali Staxx Import	artifact	example_staxx_indicator_import
Example: Anomali Staxx Query	artifact	example_staxx_indicator_search

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.

Anomali Staxx Notes

A few notes on the use of Anomali Staxx and Resilient Artifacts

- Support for Unicode characters in artifacts appears to be unsupported
- Some artifact types may not be supported, such as:
 - MAC addresses
- Windows file paths, such as: `c:\path\file.exe` are changed to `file.exe`
- Linux file paths appear to be unsupported

When in question, review the Action Status to ensure the import process succeeded correctly.

Support

Name	Version	Author	Support URL
fn_anomali_staxx	1.0.1	Resilient Labs	https://ibm.biz/resilientcommunity
fn_send_to_staxx	1.0.0	Resilient Labs	https://ibm.biz/resilientcommunity
