# 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

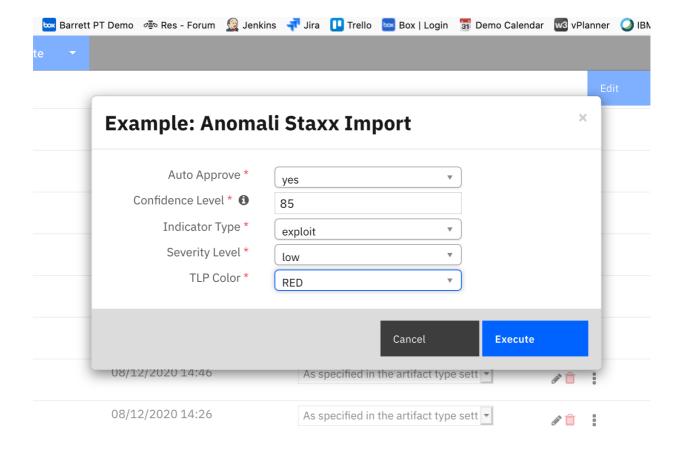
### v1.0.0

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

### Overview

'fn\_anomali\_staxx' app

2020-08-21



### **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
  - o 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

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	

### **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

2020-08-21

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

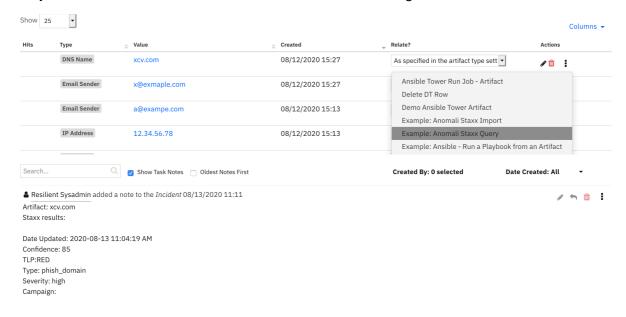
If you're upgrading from v1.0.0, please uninstall the original app (fn\_send\_to\_staxx) and reinstall as a new integration, including rerunning resilient-circuits config -u -l fn-anomali-staxx and resilient-circuits customize -l fn-anomali-staxx.

2020-08-21

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.

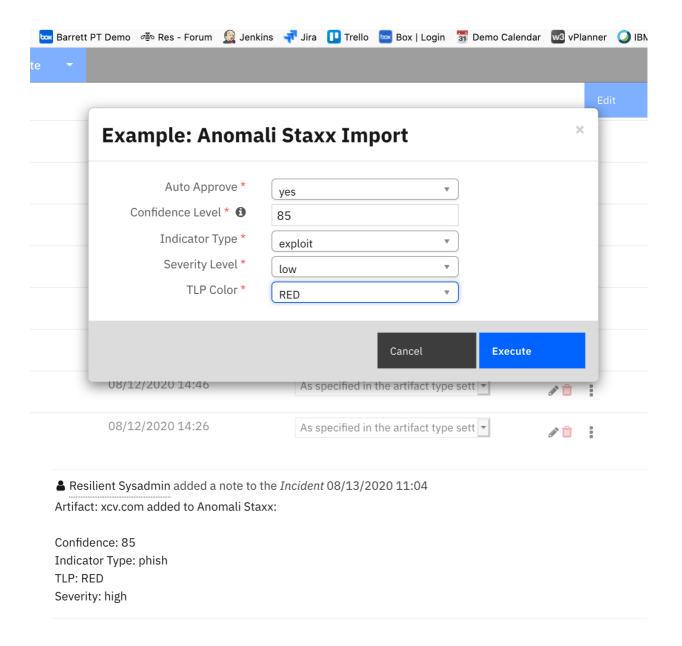


- ► Inputs:
- ► Outputs:
- ▶ Workflows

# Function - Staxx Import

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

2020-08-21



- ► 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.

2020-08-21

### **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

2020-08-21