Phish.AI Functions for IBM Resilient

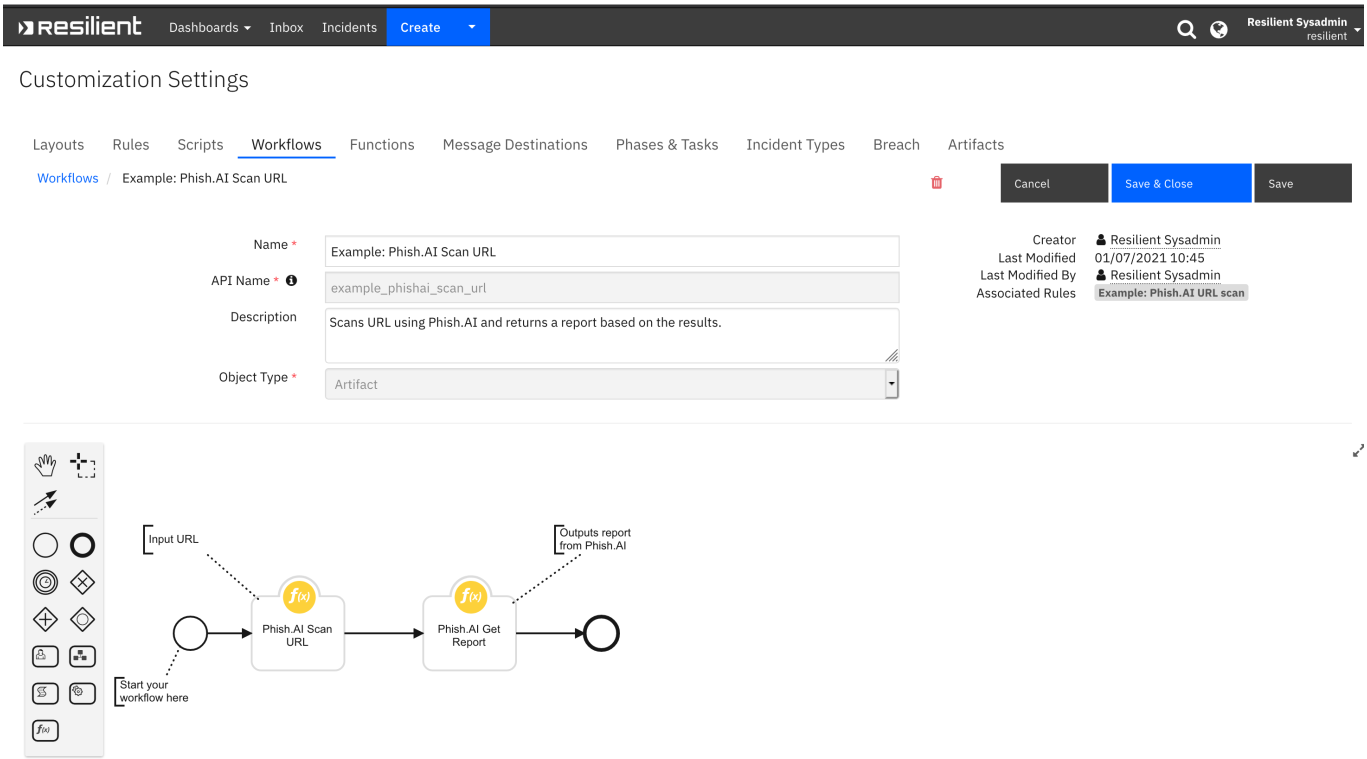
Table of Contents

Release Notes

Version	Date	Notes
1.0.0	1/2021	AppHost support
1.0.0	2/2018	Initial Release

Overview

Resilient Circuits Components for 'fn_phish_ai'



Customization Settings

Workflows / Example: Phish.AI Scan URL

Name *	Example: Phish.AI Scan URL
API Name *	example_phishai_scan_url
Description	Scans URL using Phish.AI and returns a report based on the results.
Object Type *	Artifact

Creator	Resilient Sysadmin
Last Modified	01/07/2021 10:45
Last Modified By	Resilient Sysadmin
Associated Rules	Example: Phish.AI URL scan

Resilient Circuits Components for 'fn_phish_ai'

Key Features

- This package contains two functions that scan urls and retrieve reports from Phish.AI.
- An example rule and workflow are included that show how to scan a URL artifact and write Phish.AI results to an incident note.

Requirements

This app supports the IBM Resilient SOAR Platform and the IBM Cloud Pak for Security.

Resilient platform

The Resilient platform supports two app deployment mechanisms, App Host and integration server.

If deploying to a Resilient platform with an App Host, the requirements are:

- Resilient platform >= `36.0.5634`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

If deploying to a Resilient platform with an integration server, the requirements are:

- Resilient platform >= `36.0.5634`.
- The app is in the older integration format (available from the AppExchange as a `zip` file which contains a `tar.gz` file).
- Integration server is running `resilient_circuits>=30.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions

Name	Permissions
Org Data	Read
Function	Read

The following Resilient platform guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Knowledge Center at ibm.biz/resilient-docs. On this web page, select your Resilient platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **Resilient Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= 1.4.
- Cloud Pak is configured with an App Host.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security Knowledge Center table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Knowledge Center at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific Knowledge Center page, select Case Management and Orchestration & Automation.

Proxy Server

The app does support a proxy server.

Installation

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at ibm.biz/resilient-docs.

- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

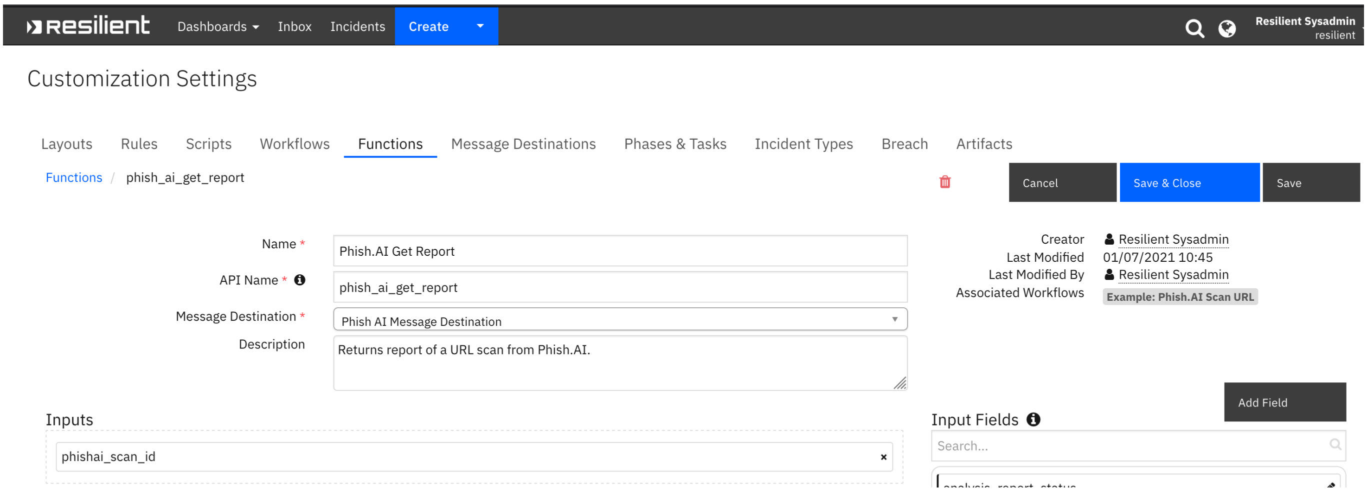
App Configuration

The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

Config	Required	Example	Description
phishai_api_key	yes	xxx	Phish.AI API Key
timeout_seconds	no	60	Time to return report in seconds

Function - Phish.AI Get Report

Returns report of a URL scan from Phish.AI.



Name * Phish.AI Get Report

API Name * phish_ai_get_report

Message Destination * Phish AI Message Destination

Description Returns report of a URL scan from Phish.AI.

Creator Resilient Sysadmin

Last Modified 01/07/2021 10:45

Last Modified By Resilient Sysadmin

Associated Workflows Example: Phish.AI Scan URL

Inputs

phishai_scan_id

▶ Inputs:

Name	Type	Required	Example	Tooltip
`phishai_scan_id`	`text`	No	`–`	-

▶ Outputs:

```
results = {
   "content":{
      "status":"completed",
      "domain":"startup417.gb.net",
      "user_agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36",
      "target":"Microsoft",
      "title":"sign_in_to_your_microsoft_account",
      "url":"https://startup417.gb.net/M3?mes1=asdf@asdf.com",
      "time":"2018-12-06T22:39:34.210Z",
      "verdict":"malicious",
      "plan":"free",
      "tld":"net",
      "iso_code":"US",
      "first_seen":"2018-12-06T19:16:20.825Z",
      "ip_address":"104.24.104.116",
      "asn":13335,
      "user_email":"api",
      "user":"free-api"
   },
   "inputs":{
      "phishai_scan_id":"gGBSaVvlN5qc5PcwvnuT"
   },
   "run_time":"0.419372797012"
}
```

▶ Example Pre-Process Script:

```
inputs.phishai_scan_id =
workflow.properties.phishai_scan_output["content"]["scan_id"]
```

▶ Example Post-Process Script:

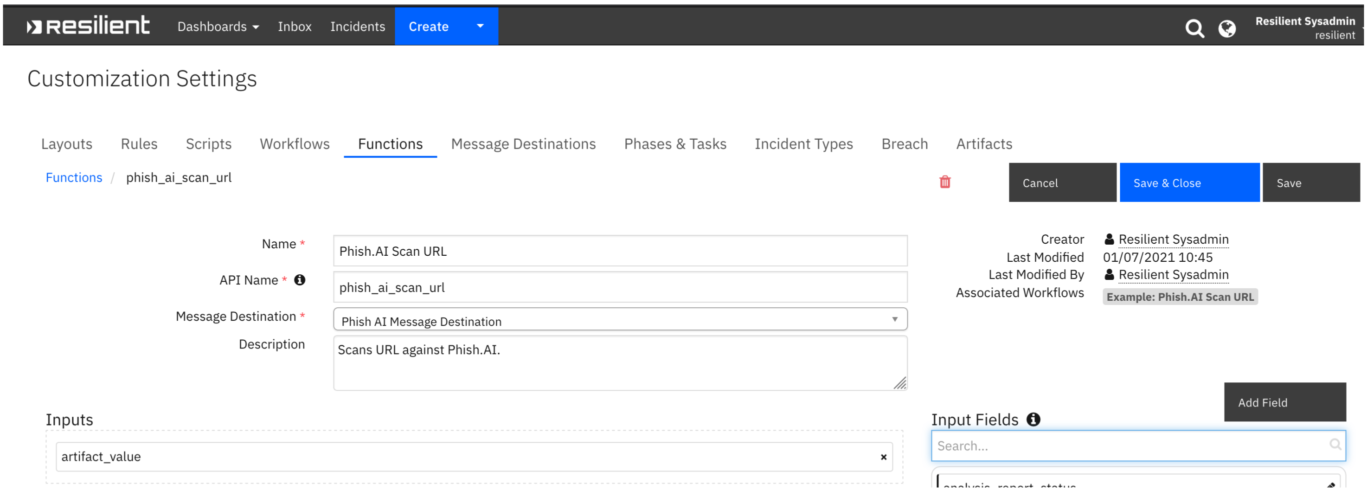
```
if results.content:
  note = "Phish.AI url: " + results.content.url
  note = note + "<br/>Phish.AI verdict: " + results.content.verdict
  note = note + "<br/><a
href=\"https://app.phish.ai/incident/{}\">Phish.AI report
link</a>".format(results.inputs.phishai_scan_id)
  incident.addNote(helper.createRichText(note))


"""
Example Response

{
   "content":{
      "status":"completed",
      "domain":"startup417.gb.net",
      "user_agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36",
      "target":"Microsoft",
      "title":"sign_in_to_your_microsoft_account",
      "url":"https://startup417.gb.net/M3?mes1=asdf@asdf.com",
      "time":"2018-12-06T22:39:34.210Z",
      "verdict":"malicious",
      "plan":"free",
      "tld":"net",
      "iso_code":"US",
      "first_seen":"2018-12-06T19:16:20.825Z",
      "ip_address":"104.24.104.116",
      "asn":13335,
      "user_email":"api",
      "user":"free-api"
   },
   "inputs":{
      "phishai_scan_id":"gGBSaVvlN5qc5PcwvnuT"
   },
   "run_time":"0.419372797012"
}
"""
```

Function - Phish.AI Scan URL

Scans URL against Phish.AI.



Customization Settings

Functions / phish_ai_scan_url

Name * Phish.AI Scan URL

API Name * phish_ai_scan_url

Message Destination * Phish AI Message Destination

Description Scans URL against Phish.AI.

Creator Resilient Sysadmin
Last Modified 01/07/2021 10:45
Last Modified By Resilient Sysadmin
Associated Workflows Example: Phish.AI Scan URL

Inputs
artifact_value

Input Fields

▶ Inputs:

Name	Type	Required	Example	Tooltip
`artifact_value`	`text`	No	`-`	-

▶ Outputs:

```
results = {
   "content":{
      "url":"https://startup417.gb.net/M3?mes1=asdf@asdf.com",
      "scan_id":"gGBSaVvlN5qc5PcwvnuT"
   },
   "inputs":{
      "artifact_value":"https://startup417.gb.net/M3?mes1=asdf@asdf.com"
   },
   "run_time":"0.446181058884"
}
```

▶ Example Pre-Process Script:

```
inputs.artifact_value = artifact.value
```

▶ Example Post-Process Script:

```
"""
Example response

{
   "content":{
      "url":"https://startup417.gb.net/M3?mes1=asdf@asdf.com",
      "scan_id":"gGBSaVvlN5qc5PcwvnuT"
   },
   "inputs":{
      "artifact_value":"https://startup417.gb.net/M3?mes1=asdf@asdf.com"
   },
   "run_time":"0.446181058884"
}
"""
```

Rules

Rule Name	Object	Workflow Triggered
Example: Phish.AI URL scan	artifact	`example_phishai_scan_url`

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is a IBM Community provided App. Please search the Community https://ibm.biz/resilientcommunity for assistance.