fn-isitphishing Functions for IBM Resilient

Table of Contents

Release Notes

v1.1.0

- App Host support.
- Package name changed from fn_isitPhishing to fn_isitphishing.

NOTE Prior Installs: Edit your app.config file to change `[fn_isitPhishing]` to `[fn_isitphishing]`

v1.0.0

- Initial Release

Overview

Resilient Function that queries Vade Secure IsItPhishing Threat Detection API to analyze a URL or an HTML document

Key Features

- This package contains two functions that call the Vade Secure IsItPhishing Webservice API to analyze a URL or to analyze an HTML document.
- 3 example workflows and rules to demonstrate how to invoke and use the functions.

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 >= `37.1`.
- 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 >= `31.0.4035`.
- 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>=31.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions
Incidents	Read
Edit Incidents	Fields
Org Data	Read
Functions	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 supports 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.

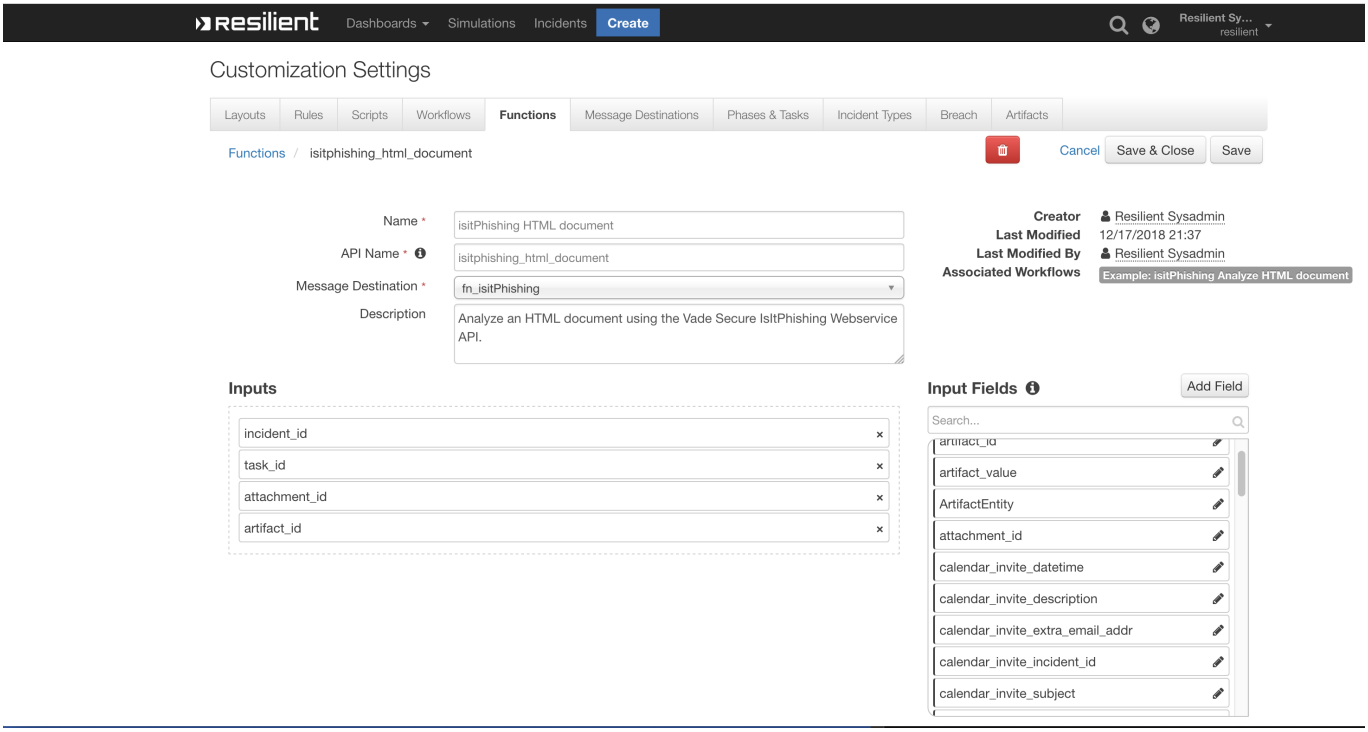
App Configuration

The following table describes the settings you need to configure in the app.config file. If using App Host, see the Resilient System Administrator Guide. If using the integration server, see the Integration Server Guide.

Config	Required	Example	Description
isitphishing_api_url	Yes	`https://ws.isitphishing.org/api/v2`	*IsItPhishing endpoint*
isitphishing_name	Yes	`name`	*username from Vade Secure*
isitphishing_license	Yes	`license from Vade Secure`	*license from Vade Secure*

Function - IsItPhishing HTML document

Analyze an HTML document using the Vade Secure IsItPhishing Webservice API.



▶ Inputs:

Name	Type	Required	Example	Tooltip
artifact_id	number	No	–	-
attachment_id	number	No	–	-
incident_id	number	Yes	–	-
task_id	number	No	–	-

▶ Outputs:

```
results = {'version': '1.0',
           'success': True,
           'reason': None,
           'content': {'result': 'unknown'},
           'raw': '{"result": "unknown"}',
           'inputs': {'incident_id': 2147,
                      'attachment_id': 259,
                      'filename': 'sample.html'},
           'metrics': {'version': '1.0', 'package': 'fn-isitphishing',
                       'package_version': '1.1.0', 'host': 'MacBook-
Pro.local',
                       'execution_time_ms': 2800, 'timestamp': '2020-11-04
16:29:44'}}
```

▶ Example Pre-Process Script:

```
# Required inputs are: incident id and artifact id.
inputs.incident_id = incident.id
```

```
inputs.artifact_id = artifact.id
```

▶ Example Post-Process Script:

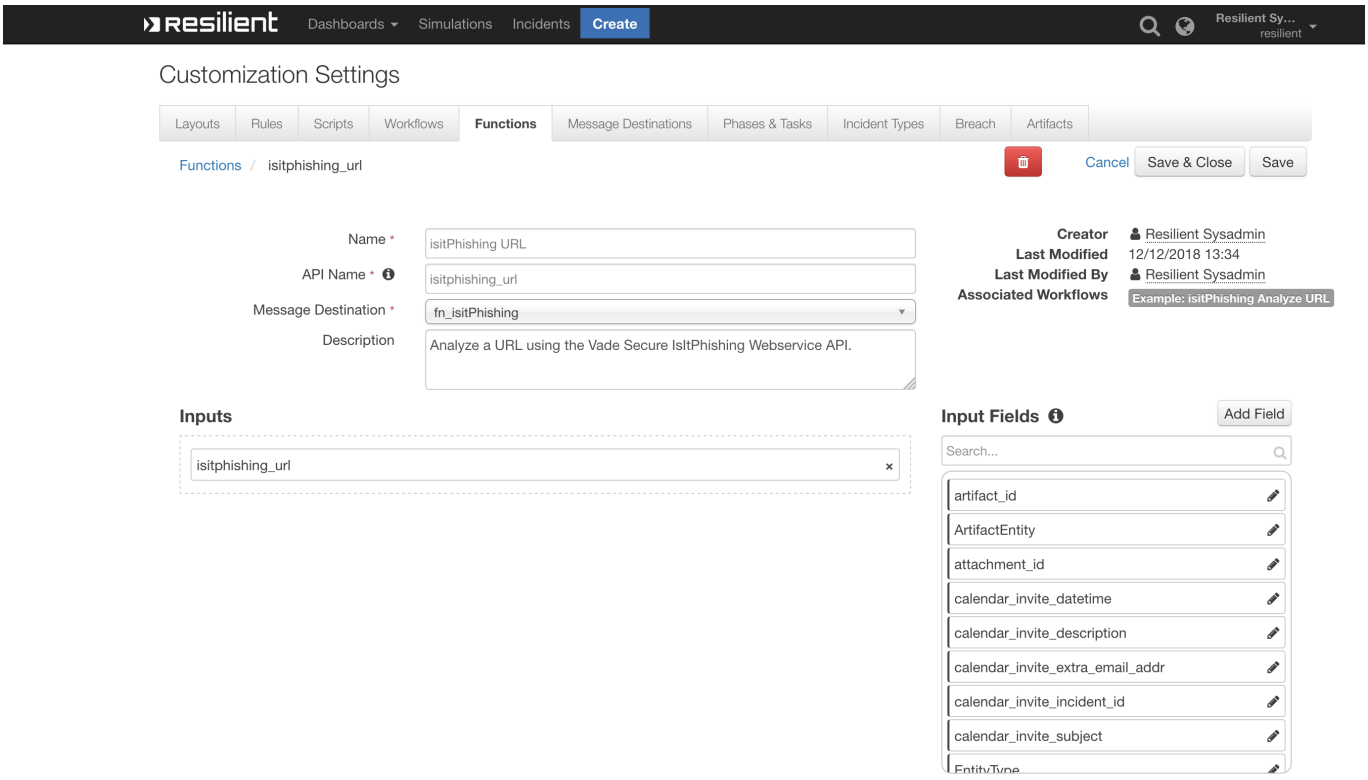
```
if results.success:
  content = u"IsItPhishing analysis of artifact document {0} :
{1}".format(results["inputs"]["filename"],results['content']['result'])
else:
  content = u"IsItPhishing analysis of artifact document {0} :
ERROR".format(results["inputs"]["filename"])

# Create a note
note = helper.createPlainText(content)

# Add note to the task or incident
if task:
  task.addNote(note)
else:
  incident.addNote(note)
```

Function - IsItPhishing URL

Analyze a URL using the Vade Secure IsItPhishing Webservice API.



▶ Inputs:

Name	Type	Required	Example	Tooltip

Name	Type	Required	Example	Tooltip
isitphishing_url	text	Yes	-	-

▶ Outputs:

```
results = {'version': '1.0',
           'success': True,
           'reason': None,
           'content': {'status': 'PHISHING'},
           'raw': '{"status": "PHISHING"}',
           'inputs': {'isitphishing_url': 'https://www.bill-
netflix.com/index.php'},
           'metrics': {'version': '1.0',
                       'package': 'fn-isitphishing',
                       'package_version': '1.1.0',
                       'host': 'MacBook-Pro.local',
                       'execution_time_ms': 5394,
                       'timestamp': '2020-11-12 17:33:23'}}

}
```

▶ Example Pre-Process Script:

```
# Get the URL from the artifact value
inputs.isitphishing_url = artifact.value
```

▶ Example Post-Process Script:

```
# Get the results and post to an incident note.
if results.success:
  content = u'IsItPhishing analysis of URL {0} :
{1}\n'.format(results['inputs']['isitphishing_url'], results['content']
['status'])
else:
  content = u'IsItPhishing analysis of URL {0} :
ERROR\n'.format(results['inputs']['isitphishing_url'])
note = helper.createPlainText(content)
incident.addNote(note)
```

Rules

Rule Name	Object	Workflow Triggered

Rule Name	Object	Workflow Triggered
Example: IsItPhishing Analyze URL	artifact	`example_isitphishing_analyze_url`
Example: IsItPhishing Analyze HTML Document: Artifact	artifact	`example_isitphishing_analyze_html_document_artifact`
Example: IsItPhishing Analyze HTML Document: Attachment	attachment	`example_isitphishing_analyze_html_document`

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.