Palo Alto WildFire

Table of Contents

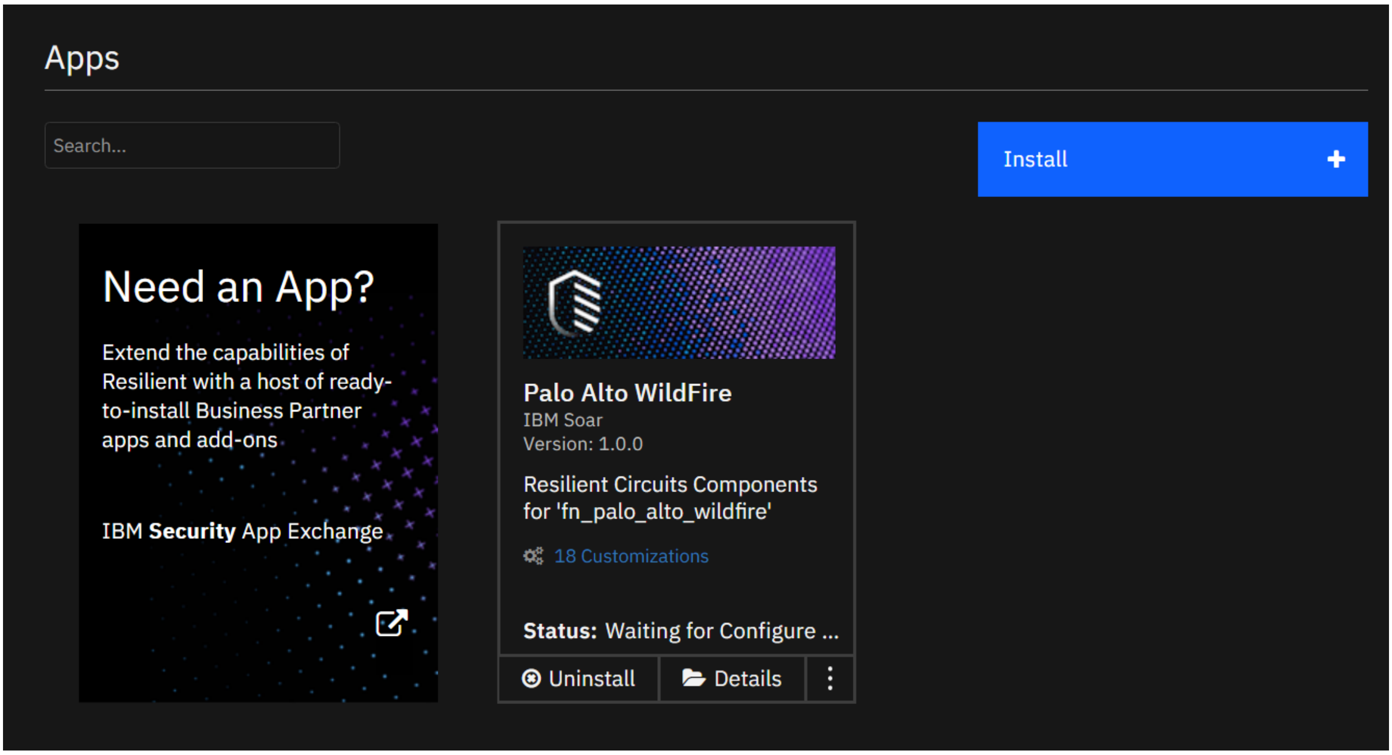
Release Notes

Version	Date	Notes
1.0.0	02/2022	Initial Release
1.0.1	08/2022	Release with functionality update for 'Get Report' function

Overview

The Palo Alto WildFire API provides malware detection capabilities through a RESTful XML-based API. Using the API allows you to obtain file analysis from WildFire and query for information uploaded to WildFire.

Resilient Circuits Components for 'fn_palo_alto_wildfire'


Apps
Search...
Install +
Need an App?
Extend the capabilities of Resilient with a host of ready-to-install Business Partner apps and add-ons
IBM Security App Exchange
Palo Alto WildFire
IBM Soar
Version: 1.0.0
Resilient Circuits Components for 'fn_palo_alto_wildfire'
18 Customizations
Status: Waiting for Configure ...
Uninstall
Details

Resilient Circuits Components for 'fn_palo_alto_wildfire'

Key Features

- Get Verdict
- Get Report
- Get Verdicts
- Get URL Web Artifacts
- Upload File
- Upload File URL
- Upload URL

Requirements

This app supports the IBM Resilient SOAR Platform and the IBM Cloud Pak for Security. You must obtain a Palo Alto WildFire Subscription in order to use this app.

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 >= `40.0.6554`.
- 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 >= `40.0.6554`.
- 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>=42.0.0`.
- If using an API key account, make sure the account provides the following minimum 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/soar-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.

Python Environment

Python 3.6 is supported. Additional package dependencies may exist for each of these packages:

- markupsafe==2.0.1
- resilient-circuits>=42.0.0

Endpoint Developed With

This app has been implemented using:

Product Name	Product Version	API URL	API Version
Palo Alto WildFire	1.0.0	WildFire API	N/A

Prerequisites

- Obtain and activate a Palo Alto WildFire Subscription to get an API Key.

Configuration

- Provide your API Key inside the Configuration file (app.config).

Permissions

- Get info from WildFire
- Upload files and URLs to WildFire

Installation

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at ibm.biz/soar-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
palo_alto_wildfire_api_key	Yes	`<api_key>`	API Key assocaited with an active Palo Alto WildFire Subscription.

Function - PALO ALTO WILDFIRE: Get Report

Get a report for a specified sample hash value or web page URL. If specifiying a web page URL, the report will only be a JSON response. If using a hash, the `format` parameter can be used to return reports in XML or PDF format. When "pdf" reports are returned the response will be an octet-stream from the API which will be returned as a base64 encoded string.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_report_url`	`text`	No	`http://example.com`	(Required for URL-based requests) The URL of the web page.
`palo_alto_wildfire_hash`	`text`	No	`afe6b95ad95bc689c356f34ec8d9094c495e4af57c932ac413b65ef132063acc`	MD5 or SHA-256 hash value of the sample.
`palo_alto_wildfire_report_format`	`select`	No	`xml | pdf`	(Applicable to sample reports only) Report format.

▶ Outputs:

Response for URL input:

```
results =  {
    'version': 2.0,
    'success': True,
    'reason': None,
    'content': {
        'success': True,
        'result': '<report object>'
    },
    'raw': None,
    'inputs': {
        'palo_alto_wildfire_report_url': 'http://google.com',
        'palo_alto_wildfire_report_format': 'xml',
    },
    'metrics': {
        'version': '1.0',
        'package': 'fn-palo-alto-wildfire',
        'package_version': '1.0.0',
        'host': 'localhost',
        'execution_time_ms': 878,
        'timestamp': '2022-02-28 19:06:12',
    }
}
```

Response for hash input with XML report format:

```
results =  {
    'version': 2.0,
    'success': True,
    'reason': None,
    'content': {
        'success': True,
        'result': '''<wildfire>
            <version>2.0</version>
            <file_info>
                <file_signer>None</file_signer>
                <malware>yes</malware>
                <sha1></sha1>
                <filetype>Microsoft Excel 97 - 2003 Document</filetype>
                <sha256>175aee5f236d464b3b825edc8cb71b47828f248356c36759a641d7da0db95323</sha256>
                <md5>dca86121cc7427e375fd24fe5871d727</md5>
                <size>13825</size>
            </file_info>
```

```
          <task_info>
          ...'''
      },
      'raw': None,
      "inputs":{
        'palo_alto_wildfire_hash':'dca86121cc7427e375fd24fe5871d727',
        'palo_alto_wildfire_report_format': 'xml'
      },
      'metrics': {
          'version': '1.0',
          'package': 'fn-palo-alto-wildfire',
          'package_version': '1.0.0',
          'host': 'localhost',
          'execution_time_ms': 878,
          'timestamp': '2022-02-28 19:06:12',
      }
  }
```

Response for hash input with PDF report format:

```
results =  {
    'version': 2.0,
    'success': True,
    'reason': None,
    'content': {
        'success': True,
        'result':
'JVBERi0xLjQKMSAwIG9iago8PAovVGl0bGUgKP7/KQovQ3JlYXRvciAo/v8AdwBrAGgAdABtAGwAdABvAHAAZABmACAAMAAuADEAMgAuADUpCi9Qcm9kdWNlci
Ao/v8AUQB0ACAANAAuADgALgA3KQovQ3JlYXRpb25EYXRlIChEOjIwMjIwNzEzMTk1NTQzWikKPj4KZW5kb2JqCjMgMCBvYmoKPDwKL1R5cGUgL0V4dEdTdGF0Z
QovU0EgdHJ1ZQovU00gMC4wMgovY2EgMS4wCi9DQSAxLjAKL0FJUyBmYWxzZQovU01hc2sgL05vbmU+PgplbmRvYmoKNCAwIG9iagpbL1BhdHRlcm4gL0Rldmlj
Z...'
    },
    'raw': None,
    "inputs":{
      'palo_alto_wildfire_hash':'dca86121cc7427e375fd24fe5871d727',
      'palo_alto_wildfire_report_format': 'pdf'
    },
    'metrics': {
        'version': '1.0',
        'package': 'fn-palo-alto-wildfire',
        'package_version': '1.0.0',
        'host': 'localhost',
        'execution_time_ms': 878,
        'timestamp': '2022-02-28 19:06:12',
    }
}
```

Function - PALO ALTO WILDFIRE: Get URL Web Artifacts

Get the web artifacts found during analysis of the specified web page URL.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_types`	`text`	No	`download_files`	Whether to download web artifacts as screenshots or as downloadable files. if not specified, both will be downloaded. Possible values are: download_files, screenshot. Default is all. The following values can be specified in a comma-separated list.
`palo_alto_wildfire_url`	`text`	Yes	`http://google.com`	URL of the webpage. Supports HTTP and HTTPS URLs.

▶ Outputs:

```
results = {
  'version': 2.0,
  'success': True,
  'reason': None,
  'content': {
    'artifacts':
'H4sIAAAAAAAA/+zVTYsjRRgH8H8niy/r7JiefSEMCsEXmIub6pfqrpYYh8SdMb6sa3TZmXVh6O6qTpQkHTtZdveuNw9evQ1evHrSq4c9eFMQRFcP4icQQa8t3S
NkksEsZpkM4vODpB6eLrqq+mmelvGtQS/25V70bk+NcCwYY8zlPB8ZY7NjHhu2yVzTME3DBTMs17FR4ceznWk3R2M/AWNJHI/nzbvf9dnD/UdM17/qu5ESlgodO
whMSwWmYB7jnpCBJQ3HUdITipvK8qThR0EQSdcOuetxbkWepWx18erlV7Pf1Br3rb/tTtffdEyTo7KUh/g/r3+tO+736rWu8mW9Vj0Ygljeqdeqfw/5hJPeJjkm
ozBRajDqzn+5H8wC/d/gjPr/MkzqX5VhKFnI7chyuBcFhuAeN7gVKjcQ0lI2i7i0hS9twR0lXFu4POJCGNwyI5/7dt773xuqzuwa8+tvurYz2/+5ZVvU/5ch/SH
9BaVXtlpb0DRAgwakvxY2Ws3m3pX2G1ut1y7lFwrlbHahBPQH46S93ajs7F6vHL6TH46GcxbSgD+/z/6B755bYKOPSjUKAfwGYJzs7F4HNAngXOcgvp3FwUH8UR
Ynb7ebgLYPYKNzKA4OxbfGwzGgfZ3ND4dJFv+cfRT7vZvhZN9YUYOrbwHYAfAERmhjG40FzjDX5HnGnwLiD6D48SQXfAJ8+SFQvjfJPbMPPP4B8MU3Qz/x89Spr
EhRBPz+GXBmFzj7LXD6naNrTGrxD2et5GfdRowYHfSgUEELA4S4iApMMBhw0p/QROmxldWV06XVM6treulseWO9fOFC2Xj62Sc3nrdeqHmWcDdfvnF586Vrl1xx
pf/mtb2g0+3UX3//zlDevqE6YXYTTV9bK58vV9fXq2FDNMJ/Lf0K+iOnPn9os6g9hYKuFXUtvYvz+bs75eH0Ls6VZrPIskfm5ln9aPYeVooaCnpRx4vYX7TghBB
CCCGEEEIIIYQQQgghhBBCCCGEEEIIIYSQZUh/POkdEELIA/srAAD//6P3M/EAPgAA'
  },
  'raw': None,
  'inputs': {
    'palo_alto_wildfire_url': 'http://google.com'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 797,
    'timestamp': '2022-02-28 18:29:34'
  }
}
```

Function - PALO ALTO WILDFIRE: Get Verdict

Get a WildFire verdict for a sample based on the MD5 or SHA-256 hash or a web page based on the URL. A hash or URL must be provided not both.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_hash`	`text`	No	`afe6b95ad95bc689c356f34ec8d9094c495e4af57c932ac413b65ef132063acc`	MD5 or SHA-256 hash value of the sample.
`palo_alto_wildfire_url_optional`	`text`	No	`http://google.com`	URL of the webpage. Supports HTTP and HTTPS URLs.

▶ Outputs:

```
results = {
  'version': 2.0,
  'success': True,
  'reason': None,
  'content': '<?xml version="1.0" encoding="UTF-8"?>\n<wildfire>\n\t<get-verdict-
info>\n\t\t<url>http://google.com</url>\n\t\t<verdict>0</verdict>\n\t\t<analysis_time>2022-02-
28T17:46:52Z</analysis_time>\n\t\t<valid>Yes</valid>\n\t</get-verdict-info>\n</wildfire>\n', 'raw': None,
  'inputs': {
    'palo_alto_wildfire_url_optional': 'http://google.com'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 321,
    'timestamp': '2022-02-28 18:31:43'
  }
}
```

Function - PALO ALTO WILDFIRE: Get Verdicts

Get multiple WildFire verdicts based on a text file that contains multiple hashes. You can include up to 500 hash values in a single file, with each hash value being on a separate line.

▶ Inputs:

Name	Type	Required	Example	Tooltip

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_hash_list`	`text`	Yes	`@c:\hashlist.txt`	Local path to file containing up to 500 hash values (MD5 or SHA-256).

▶ Outputs:

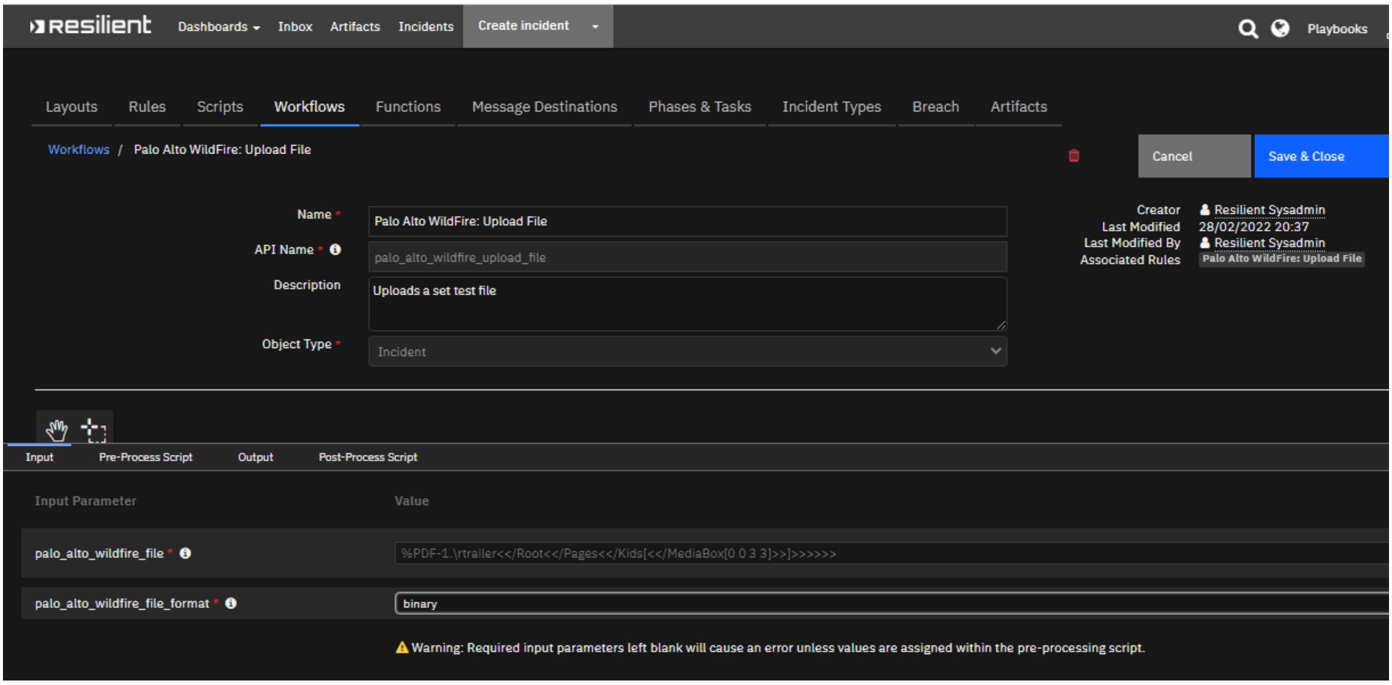
```
results = {
  'version': 2.0,
  'success': True,
  'reason': None,
  'content': '<?xml version="1.0" encoding="UTF-8">\n<wildfire>\n\t<get-verdict-
info>\n\t\t<sha256>9739eb4207fe251d40f05187cbfd16081f97b246ebcc6010660244a84a9391b0</sha256>\n\t\t<verdict>0</verdict>\n\t\
t<md5>481e625e50211efcaf6edb8f54f8cf83</md5>\n\t</get-verdict-info>\n\t<get-verdict-
info>\n\t\t<sha256>e9039e873b59574762afb0d15bdcaf9fee9b163c81d239458b95b4087167f86e</sha256>\n\t\t<verdict>0</verdict>\n\t\
t<md5>b8624d8d267ba2c8e2f91d90eb1a5c9b</md5>\n\t</get-verdict-info>\n</wildfire>\n',
  'raw': None,
  'inputs': {

'palo_alto_wildfire_hash_list':'9739eb4207fe251d40f05187cbfd16081f97b246ebcc6010660244a84a9391b0,e9039e873b59574762afb0d15b
dcaf9fee9b163c81d239458b95b4087167f86e'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 267,
    'timestamp': '2022-02-28 18:34:29'
  }
}
```

Function - PALO ALTO WILDFIRE: Upload File

Upload a local file to WildFire for analysis by using Pre-Process Script option in workflow.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_file`	`text`	Yes	`%PDF-1.\rtrailer<</Root<</Pages<</Kids[<</MediaBox[0 0 3 3]>>]>>>>>>`	File contents, either as a base64 encoded string or a binary string. Need to be mapped using Pre-Process Script option in workflow.
`palo_alto_wildfire_file_format`	`text`	Yes	`binary`	The format of the file content being submitted.



Workflows / Palo Alto WildFire: Upload File

Name * Palo Alto WildFire: Upload File

API Name * palo_alto_wildfire_upload_file

Description Uploads a set test file

Object Type * Incident

Creator Resilient Sysadmin
Last Modified 28/02/2022 20:37
Last Modified By Resilient Sysadmin
Associated Rules Palo Alto WildFire: Upload File

Input Parameter	Value
palo_alto_wildfire_file *	%PDF-1.\rtrailer<</Root<</Pages<</Kids[<</MediaBox[0 0 3 3]>>]>>>>>>
palo_alto_wildfire_file_format *	binary

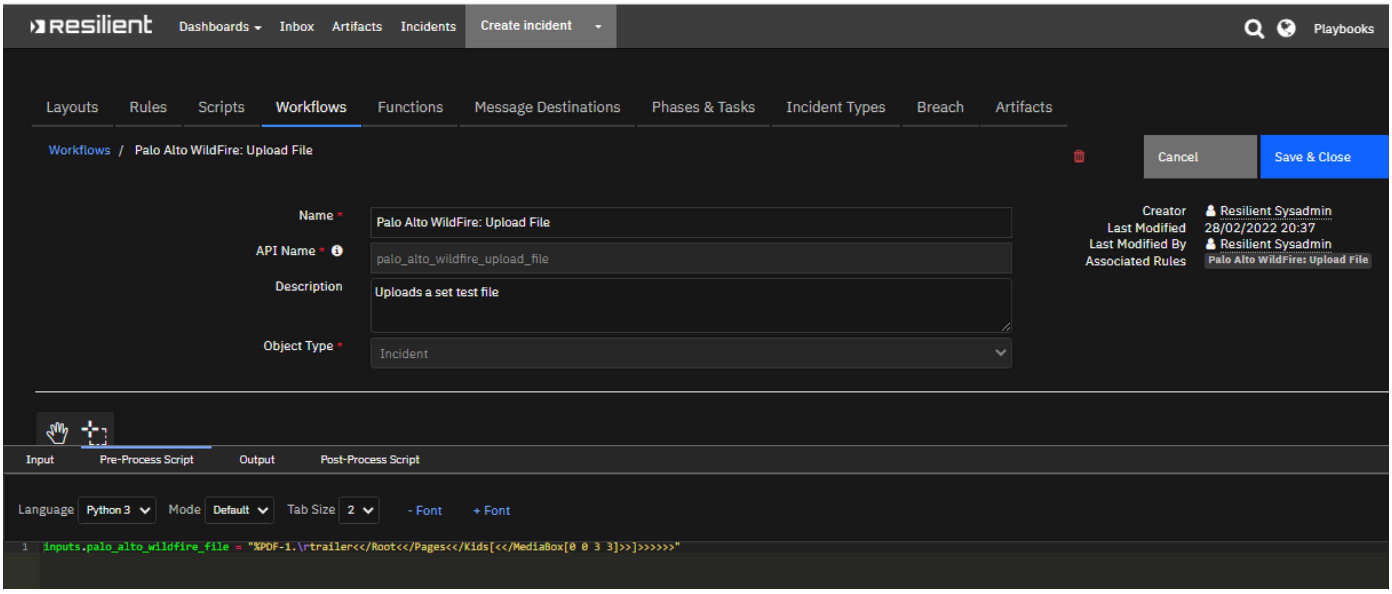
⚠ Warning: Required input parameters left blank will cause an error unless values are assigned within the pre-processing script.

▶ Outputs:

```
results = {
  'version': 2.0,
  'success': True,
  'reason': None,
  'content': {
    'wildfire': '<?xml version="1.0" encoding="UTF-8"?>\n<wildfire>\n    <upload-file-info>\n        <url></url>\n
<filetype>Adobe PDF document</filetype>\n<filename></filename>\n
<sha256>2cf383cdd942aba7fa4dff07118d5f5d415818b1ff09dba4ef1fc247f260e577</sha256>\n
<md5>65b881bb85599a4e9c42cbc3fd67c916</md5>\n        <size>56174</size>\n    </upload-file-info>\n</wildfire>'
  },
  'raw': None,
  'inputs': {
    'palo_alto_wildfire_file': '%PDF-1.\rtrailer<</Root<</Pages<</Kids[<</MediaBox[0 0 3 3]>>]>>>>>>',
    'palo_alto_wildfire_file_format': 'binary'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 497,
    'timestamp': '2022-02-28 18:35:38'
  }
}
```

▶ Example Pre-Process Script:

```
inputs.palo_alto_wildfire_file = "%PDF-1.\rtrailer<</Root<</Pages<</Kids[<</MediaBox[0 0 3 3]>>]>>>>>>"
```



Workflows / Palo Alto WildFire: Upload File

Name * Palo Alto WildFire: Upload File

API Name * palo_alto_wildfire_upload_file

Description Uploads a set test file

Object Type * Incident

Creator Resilient Sysadmin
Last Modified 28/02/2022 20:37
Last Modified By Resilient Sysadmin
Associated Rules Palo Alto WildFire: Upload File

Language Python 3 Mode Default Tab Size 2

```
inputs.palo_alto_wildfire_file = "%PDF-1.\rtrailer<</Root<</Pages<</Kids[<</MediaBox[0 0 3 3]>>]>>>>>>"
```

Function - PALO ALTO WILDFIRE: Upload File URL

Upload a remote files URL to WildFire for analysis.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_context`	`text`	No	`test.sh`	(Required for script submissions) Specify the filename of the sample.
`palo_alto_wildfire_file_url`	`text`	Yes	`http://example.com/file.txt`	Remote file URL path.

▶ Outputs:

```
results = {
  'version': 2.0,
  'success': True,
  'reason': None,
  'content': {
    'wildfire': '<?xml version="1.0" encoding="UTF-8"?>\n<wildfire>\n    <upload-file-info>\n
<url>https://www.americanexpress.com/content/dam/amex/us/staticassets/pdf/GCO/Test_PDF.pdf</url>\n        <filetype>Adobe
PDF document</filetype>\n        <filename></filename>\n
<sha256>e06ca773eca3657851415a5d64d226f81a9604cab75430b91d33ee1574b076b2</sha256>\n<md5>f72d72e0433edd25a1b888128646ee23</m
d5>\n        <size>14812</size>\n<upload-file-info>\n</wildfire>'},
  'raw': None,
  'inputs': {
    'palo_alto_wildfire_file_url': 'https://www.americanexpress.com/content/dam/amex/us/staticassets/pdf/GCO/Test_PDF.pdf'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 607,
    'timestamp': '2022-02-28 18:36:41'
  }
}
```

Function - PALO ALTO WILDFIRE: Upload URL

Upload a webpage's URL to WildFire for analysis.

▶ Inputs:

Name	Type	Required	Example	Tooltip
`palo_alto_wildfire_url`	`text`	Yes	`http://google.com`	URL of the webpage. Supports HTTP and HTTPS URLs.

▶ Outputs:

```
results = {
  'version': 2,
  'success': True,
  'reason': None,
  'content': {
    'wildfire': '<?xml version="1.0" encoding="UTF-8"?>\n<wildre>\n    <submit-link-info>\n
<url>http://google.com</url>\n        <sha256>aa2239c17609b21eba03464af878f3eec8ce83ed0f2768597d2bc2fd4e4da5</sha256>\n
<md5>c7b920f57e553df2bb68272f61570210</md5>\
   </submit-link-info>\n</wildfire>'
  },
  'raw': None,
  'inputs': {
    'palo_alto_wildfire_url': 'http://google.com'
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-palo-alto-wildfire',
    'package_version': '1.0.0',
    'host': 'localhost',
    'execution_time_ms': 539,
    'timestamp': '2022-02-28 18:42:57'
  }
}
```

Troubleshooting & Support

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

For Support

This is an IBM supported app. Please search https://ibm.com/mysupport for assistance.