IBM Resilient

Incident Response Platform Integrations

Cisco Umbrella Investigate Function V1.0.0

Release Date: May 2018

Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

This guide describes the Cisco Umbrella Investigate Function.

Overview

Umbrella Investigate is the interface to the security data collated by the Cisco Umbrella Investigate research team. The Cisco Umbrella Investigate RESTful API service allows for the querying of the Umbrella DNS database to show security events and correlations in their datasets. The Investigate RESTful API opens up the power of the Investigate classification results, correlation, and history and is based on the Umbrella global network, the world's largest security network.

The Cisco Umbrella Investigate integration with IBM Resilient allows querying of the Investigate datasets using their RESTful APIs and the returned results can be used to make customized updates to a Resilient instance such as updating incidents, artifacts, data-tables etc.

There are 14 functions supplied in the Resilient Function package for Umbrella Investigate. The Functions interrogate the various RESTful APIs exposed by the Investigate service. There are also example workflows in the customizations section of the package which demonstrate usage of the Resilient Investigate Functions to update data tables.

The remainder of this document describes the included Functions, how to configure example custom workflows, and any additional customization options.

Installation

Before installing, verify that your environment meets the following prerequisites:

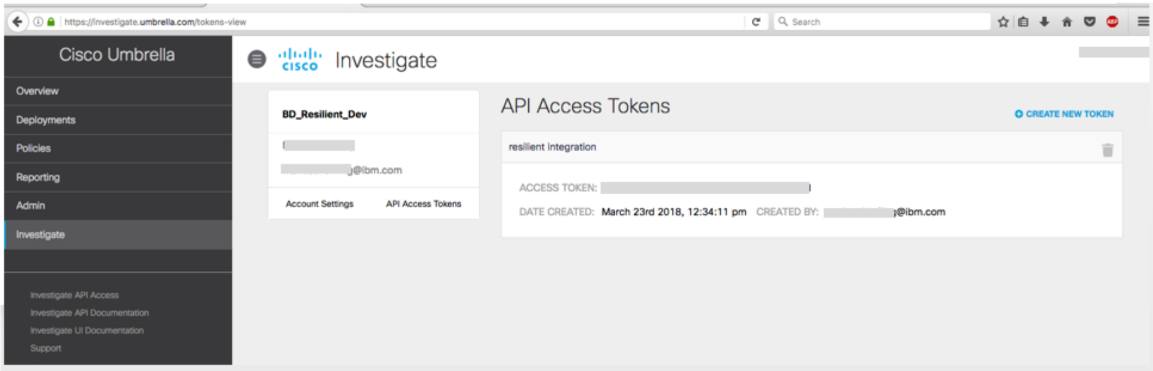
- Resilient platform is version 30 or later.
- You have a Resilient account to use for the integrations. This can be any account that has the permission to view and modify administrator and customization settings, and read and update incidents. You need to know the account username and password.
- You have access to the command line of the Resilient appliance, which hosts the Resilient platform; or to a separate integration server where you will deploy and run the functions code. If using a separate integration server, you must install Python version 2.7.10 or later, or version 3.6 or later, and “pip”. (The Resilient appliance is preconfigured with a suitable version of Python.)

Cisco Umbrella Investigate configuration

The Umbrella Investigate default base URL is **https://investigate.api.umbrella.com/** .

The base URL can be overridden by the user if required.

Access to the Cisco Umbrella Investigate RESTful API is allowed by providing an access token in the request. The access token is tied to a user account on the Umbrella platform.



BD_Resilient_Dev

[redacted]

[redacted]@ibm.com

API Access Tokens

resilient integration

ACCESS TOKEN: [redacted]

DATE CREATED: March 23rd 2018, 12:34:11 pm CREATED BY: [redacted]@ibm.com

More information can be found here https://investigate-api.readme.io/docs/about-the-api-authentication

Install the Python components

The functions package contains Python components that will be called by the Resilient platform to execute the functions during your workflows. These components run in the ‘resilient-circuits’ integration framework.

The package also includes Resilient customizations that will be imported into the platform later.

Ensure that the environment is up to date,

```
sudo pip install --upgrade pip
sudo pip install --upgrade setuptools
sudo pip install --upgrade resilient-circuits
```

To install the package:

```
sudo pip install --upgrade fn_cisco_umbrella_inv-1.0.0.tar.gz
```

Configure the Python components

The ‘resilient-circuits’ components run as an unprivileged user, typically named `integration`. If you do not already have an `integration` user configured on your appliance, create it now.

Perform the following to configure and run the integration:

1. Using sudo, become the integration user.

   ```
   sudo su - integration
   ```

2. Use one of the following commands to create or update the resilient-circuits configuration file. Use –c for new environments or –u for existing environments.

   ```
   resilient-circuits config -c
   ```

   or

   ```
   resilient-circuits config -u
   ```

3. Edit the resilient-circuits configuration file.

   a. In the [resilient] section, ensure that you provide all the information needed to connect to the Resilient platform.

   b. In the [fn_cisco_umbrella_inv] section, edit the settings as follows:

   ```
   base_url=https://investigate.api.umbrella.com/

   # The api_token will be supplied by Cisco will be in uuid format.

   api_token= abcd1234-a123-123a-123a-123456abcdef
   ```

Deploy customizations to the Resilient platform

The package contains function definitions that you can use in workflows, and includes example workflows and rules that show how to use these functions.

Deploy these customizations to the Resilient platform with the following command:

```
resilient-circuits customize
```

Answer the prompts to deploy functions, message destinations, workflows and rules.

Run the integration framework

To test the integration package before running it in a production environment, you must run the integration manually with the following command:

```
resilient-circuits run
```

The resilient-circuits command starts, loads its components, and continues to run until interrupted. If it stops immediately with an error message, check your configuration values and retry.

Configuration of resilient-circuits for restartability

For normal operation, resilient-circuits must run continuously. The recommend way to do this is to configure it to automatically run at startup. On a Red Hat appliance, this is done using a systemd unit file such as the one below. You may need to change the paths to your working directory and app.config.

The unit file should be named ‘resilient_circuits.service’:

```
sudo vi /etc/systemd/system/resilient_circuits.service
```

The contents (edit as necessary):

```
[Unit]
Description=Resilient-Circuits Service
After=resilient.service
Requires=resilient.service

[Service]
Type=simple
User=integration
WorkingDirectory=/home/integration
ExecStart=/usr/local/bin/resilient-circuits run
Restart=always
TimeoutSec=10
Environment=APP_CONFIG_FILE=/home/integration/.resilient/app.config
Environment=APP_LOCK_FILE=/home/integration/.resilient/resilient_circuits.
lock

[Install]
WantedBy=multi-user.target
```

Ensure that the service unit file is correctly permissioned:

```
sudo chmod 664 /etc/systemd/system/resilient_circuits.service
```

Use the systemctl command to manually start, stop, restart and return status on the service:

```
sudo systemctl resilient_circuits [start|stop|restart|status]
```

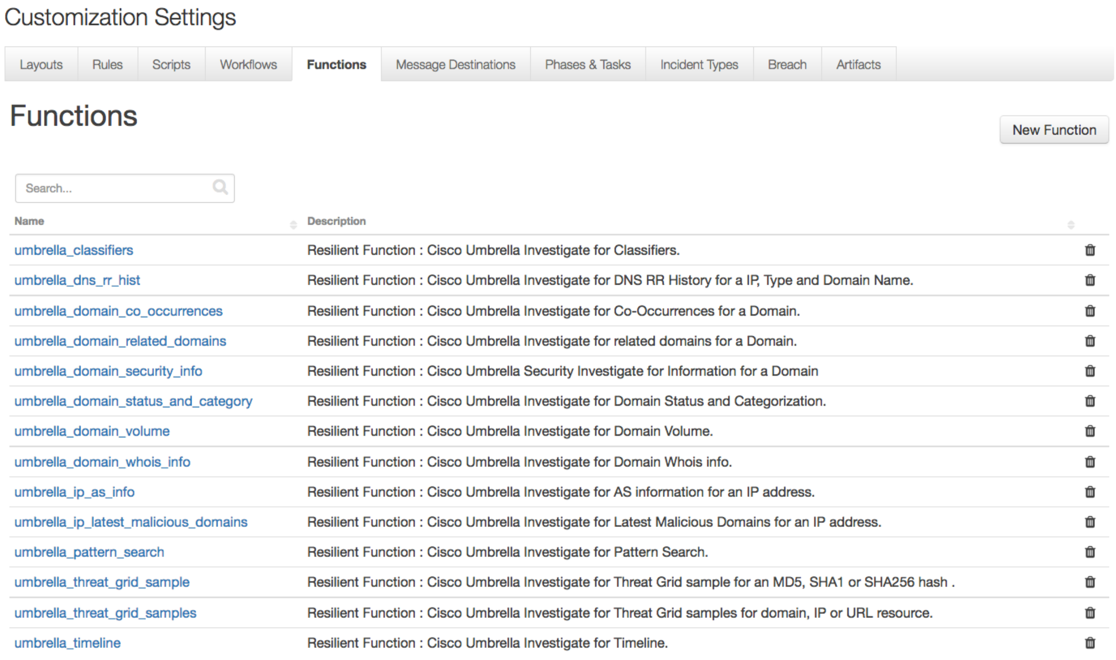
Log files for systemd and the resilient-circuits service can be viewed through the journalctl command:

```
sudo journalctl -u resilient_circuits --since "2 hours ago"
```

Function Descriptions

Once the Function package customizations are deployed to the Resilient instance, the functions can be viewed in the Resilient platform Functions tab, as shown below.

Functions

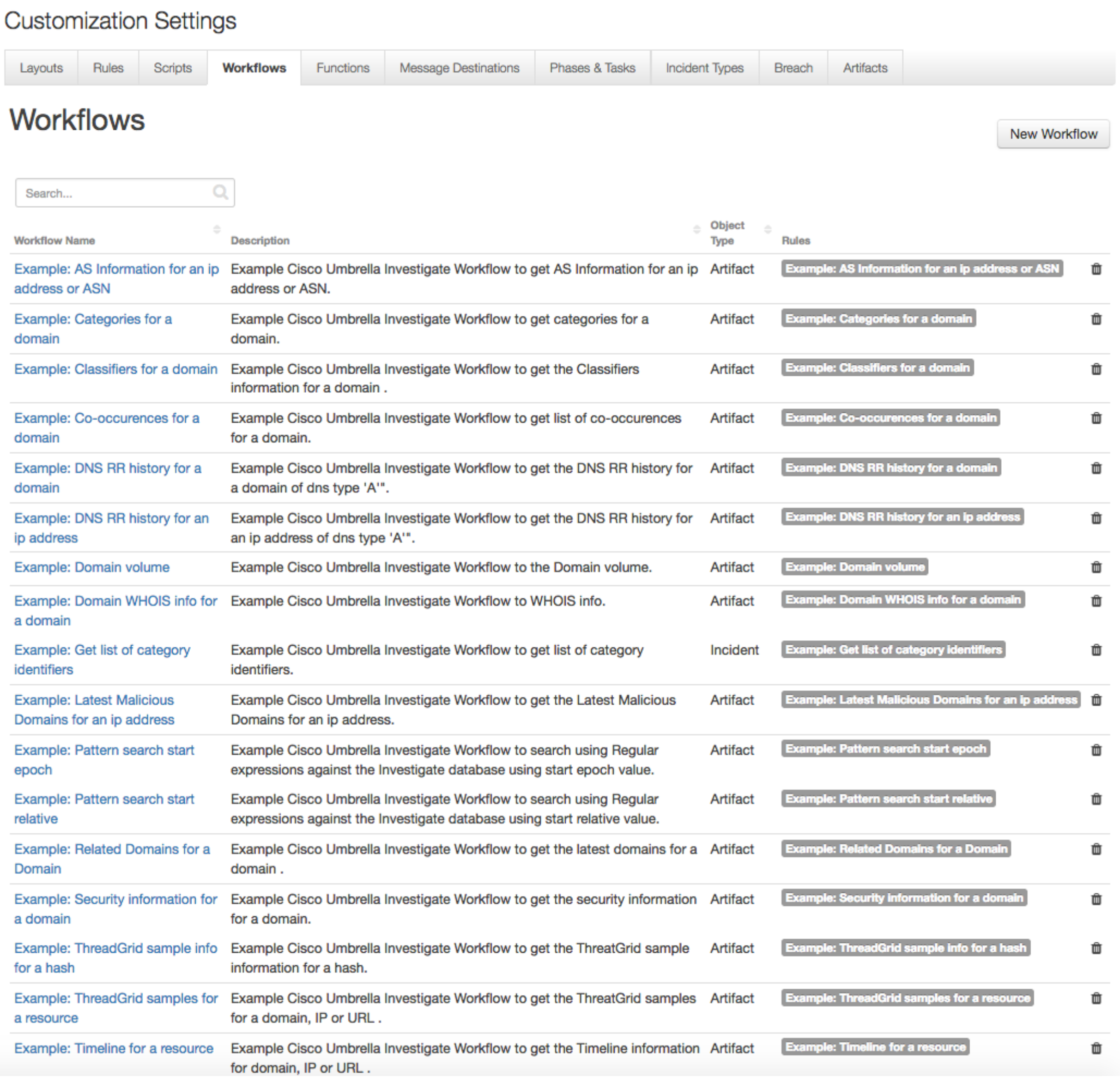


Functions

Name	Description	
umbrella_classifiers	Resilient Function : Cisco Umbrella Investigate for Classifiers.	🗑
umbrella_dns_rr_hist	Resilient Function : Cisco Umbrella Investigate for DNS RR History for a IP, Type and Domain Name.	🗑
umbrella_domain_co_occurrences	Resilient Function : Cisco Umbrella Investigate for Co-Occurences for a Domain.	🗑
umbrella_domain_related_domains	Resilient Function : Cisco Umbrella Investigate for related domains for a Domain.	🗑
umbrella_domain_security_info	Resilient Function : Cisco Umbrella Security Investigate for Information for a Domain	🗑
umbrella_domain_status_and_category	Resilient Function : Cisco Umbrella Investigate for Domain Status and Categorization.	🗑
umbrella_domain_volume	Resilient Function : Cisco Umbrella Investigate for Domain Volume.	🗑
umbrella_domain_whois_info	Resilient Function : Cisco Umbrella Investigate for Domain Whois info.	🗑
umbrella_ip_as_info	Resilient Function : Cisco Umbrella Investigate for AS information for an IP address.	🗑
umbrella_ip_latest_malicious_domains	Resilient Function : Cisco Umbrella Investigate for Latest Malicious Domains for an IP address.	🗑
umbrella_pattern_search	Resilient Function : Cisco Umbrella Investigate for Pattern Search.	🗑
umbrella_threat_grid_sample	Resilient Function : Cisco Umbrella Investigate for Threat Grid sample for an MD5, SHA1 or SHA256 hash .	🗑
umbrella_threat_grid_samples	Resilient Function : Cisco Umbrella Investigate for Threat Grid samples for domain, IP or URL resource.	🗑
umbrella_timeline	Resilient Function : Cisco Umbrella Investigate for Timeline.	🗑

The package also includes example Workflows, Rules and Data tables that show how the Functions can be used. The Resilient user can copy and modify these Resilient objects for their own needs.

Workflows

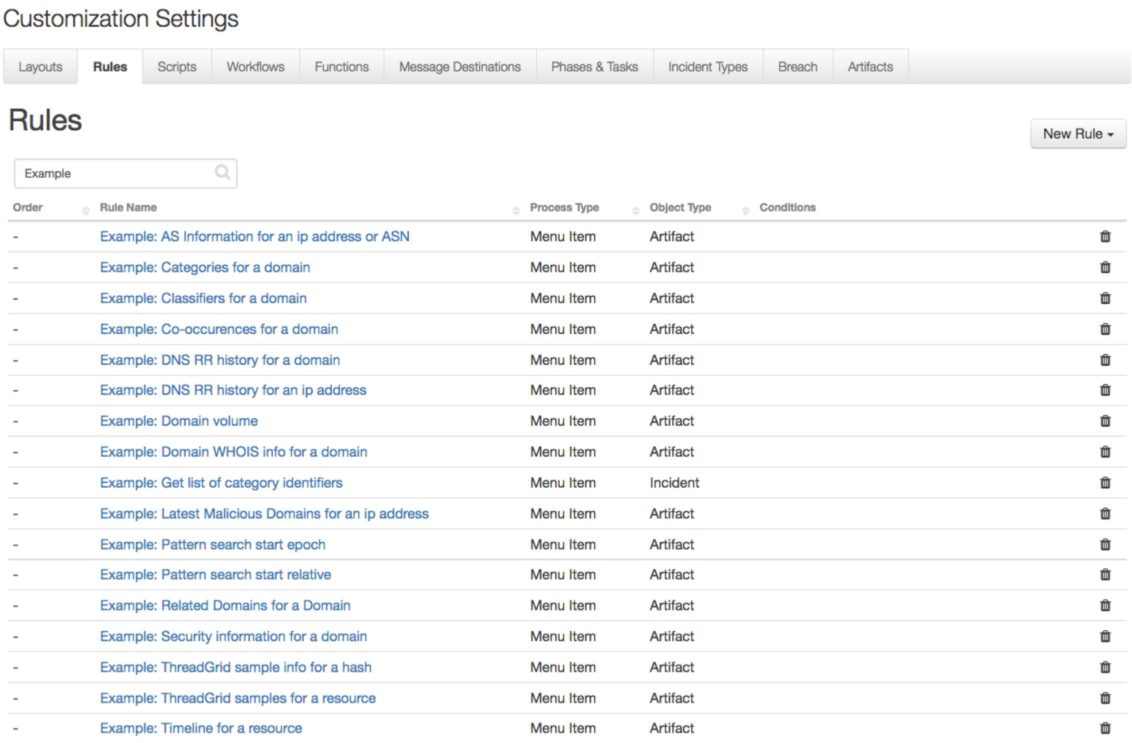


Customization Settings

Workflows

Workflow Name	Description	Object Type	Rules	
Example: AS Information for an ip address or ASN	Example Cisco Umbrella Investigate Workflow to get AS Information for an ip address or ASN.	Artifact	Example: AS Information for an ip address or ASN	🗑
Example: Categories for a domain	Example Cisco Umbrella Investigate Workflow to get categories for a domain.	Artifact	Example: Categories for a domain	🗑
Example: Classifiers for a domain	Example Cisco Umbrella Investigate Workflow to get the Classifiers information for a domain .	Artifact	Example: Classifiers for a domain	🗑
Example: Co-occurences for a domain	Example Cisco Umbrella Investigate Workflow to get list of co-occurences for a domain.	Artifact	Example: Co-occurences for a domain	🗑
Example: DNS RR history for a domain	Example Cisco Umbrella Investigate Workflow to get the DNS RR history for a domain of dns type 'A'".	Artifact	Example: DNS RR history for a domain	🗑
Example: DNS RR history for an ip address	Example Cisco Umbrella Investigate Workflow to get the DNS RR history for an ip address of dns type 'A'".	Artifact	Example: DNS RR history for an ip address	🗑
Example: Domain volume	Example Cisco Umbrella Investigate Workflow to the Domain volume.	Artifact	Example: Domain volume	🗑
Example: Domain WHOIS info for a domain	Example Cisco Umbrella Investigate Workflow to WHOIS info.	Artifact	Example: Domain WHOIS info for a domain	🗑
Example: Get list of category identifiers	Example Cisco Umbrella Investigate Workflow to get list of category identifiers.	Incident	Example: Get list of category identifiers	🗑
Example: Latest Malicious Domains for an ip address	Example Cisco Umbrella Investigate Workflow to get the Latest Malicious Domains for an ip address.	Artifact	Example: Latest Malicious Domains for an ip address	🗑
Example: Pattern search start epoch	Example Cisco Umbrella Investigate Workflow to search using Regular expressions against the Investigate database using start epoch value.	Artifact	Example: Pattern search start epoch	🗑
Example: Pattern search start relative	Example Cisco Umbrella Investigate Workflow to search using Regular expressions against the Investigate database using start relative value.	Artifact	Example: Pattern search start relative	🗑
Example: Related Domains for a Domain	Example Cisco Umbrella Investigate Workflow to get the latest domains for a domain .	Artifact	Example: Related Domains for a Domain	🗑
Example: Security information for a domain	Example Cisco Umbrella Investigate Workflow to get the security information for a domain.	Artifact	Example: Security information for a domain	🗑
Example: ThreadGrid sample info for a hash	Example Cisco Umbrella Investigate Workflow to get the ThreatGrid sample information for a hash.	Artifact	Example: ThreadGrid sample info for a hash	🗑
Example: ThreadGrid samples for a resource	Example Cisco Umbrella Investigate Workflow to get the ThreatGrid samples for a domain, IP or URL .	Artifact	Example: ThreadGrid samples for a resource	🗑
Example: Timeline for a resource	Example Cisco Umbrella Investigate Workflow to get the Timeline information for domain, IP or URL .	Artifact	Example: Timeline for a resource	🗑

Rules



Customization Settings

Layouts | Rules | Scripts | Workflows | Functions | Message Destinations | Phases & Tasks | Incident Types | Breach | Artifacts

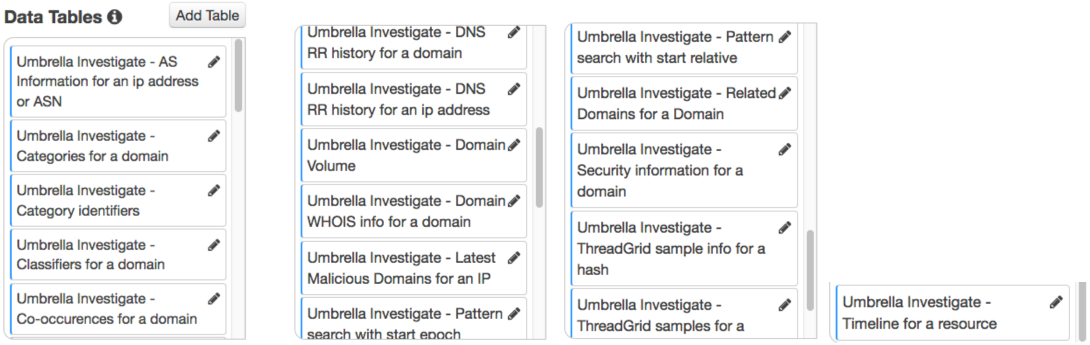
Rules

New Rule ▾

Example

Order	Rule Name	Process Type	Object Type	Conditions
-	Example: AS Information for an ip address or ASN	Menu Item	Artifact	
-	Example: Categories for a domain	Menu Item	Artifact	
-	Example: Classifiers for a domain	Menu Item	Artifact	
-	Example: Co-occurences for a domain	Menu Item	Artifact	
-	Example: DNS RR history for a domain	Menu Item	Artifact	
-	Example: DNS RR history for an ip address	Menu Item	Artifact	
-	Example: Domain volume	Menu Item	Artifact	
-	Example: Domain WHOIS info for a domain	Menu Item	Artifact	
-	Example: Get list of category identifiers	Menu Item	Incident	
-	Example: Latest Malicious Domains for an ip address	Menu Item	Artifact	
-	Example: Pattern search start epoch	Menu Item	Artifact	
-	Example: Pattern search start relative	Menu Item	Artifact	
-	Example: Related Domains for a Domain	Menu Item	Artifact	
-	Example: Security information for a domain	Menu Item	Artifact	
-	Example: ThreadGrid sample info for a hash	Menu Item	Artifact	
-	Example: ThreadGrid samples for a resource	Menu Item	Artifact	
-	Example: Timeline for a resource	Menu Item	Artifact	

Data tables



Data Tables

Add Table

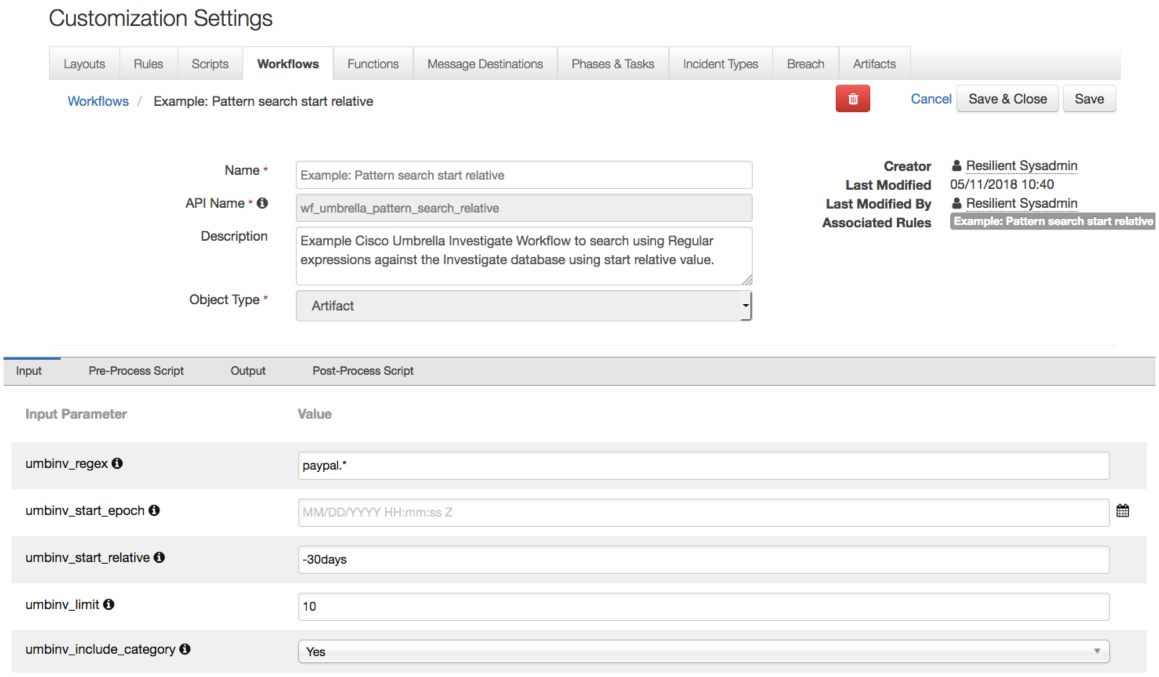
- Umbrella Investigate - AS Information for an ip address or ASN
- Umbrella Investigate - Categories for a domain
- Umbrella Investigate - Category identifiers
- Umbrella Investigate - Classifiers for a domain
- Umbrella Investigate - Co-occurences for a domain
- Umbrella Investigate - DNS RR history for a domain
- Umbrella Investigate - DNS RR history for an ip address
- Umbrella Investigate - Domain Volume
- Umbrella Investigate - Domain WHOIS info for a domain
- Umbrella Investigate - Latest Malicious Domains for an IP
- Umbrella Investigate - Pattern search with start epoch
- Umbrella Investigate - Pattern search with start relative
- Umbrella Investigate - Related Domains for a Domain
- Umbrella Investigate - Security information for a domain
- Umbrella Investigate - ThreadGrid sample info for a hash
- Umbrella Investigate - ThreadGrid samples for a
- Umbrella Investigate - Timeline for a resource

Function arguments

Refer to the Cisco Umbrella API documentation on the use of the Umbrella Investigate arguments. The Resilient Functions all use input parameters starting with "umbinv_" examples include umbinv_domains, umbinv_showlabels and umbinv_status_endpoint . These are equivalent to the parameters used in the RESTful API call. (c.f. https://investigate-api.readme.io/docs/introduction-to-cisco-investigate/).

See the Investigate Function in the workflows: Example: Pattern search start relative. Review the Input tab when editing the function within a workflow for the default settings.

Input tab



Name * Example: Pattern search start relative

API Name * wf_umbrella_pattern_search_relative

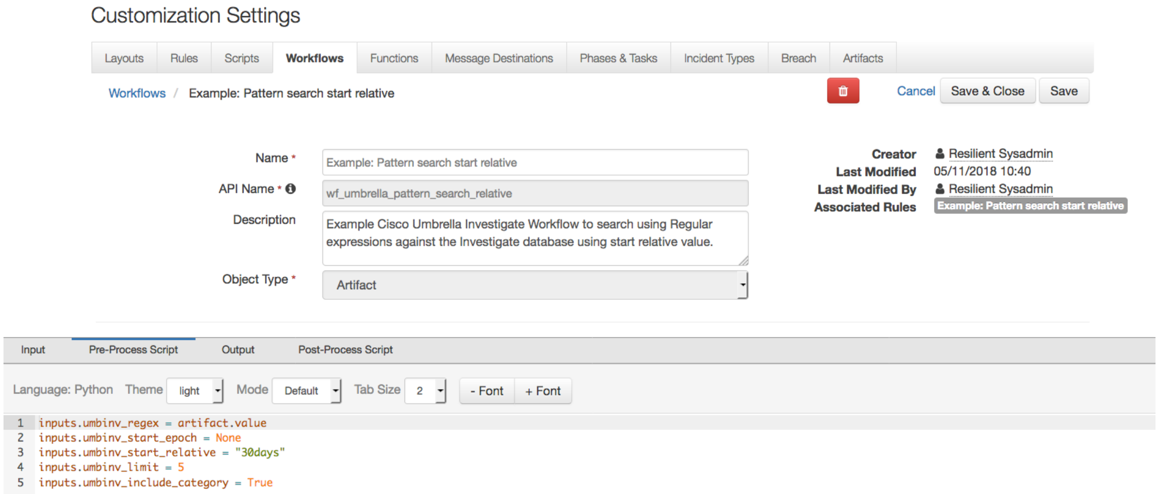
Description Example Cisco Umbrella Investigate Workflow to search using Regular expressions against the Investigate database using start relative value.

Object Type * Artifact

Creator: Resilient Sysadmin
Last Modified: 05/11/2018 10:40
Last Modified By: Resilient Sysadmin
Associated Rules: Example: Pattern search start relative

Input Parameter	Value
umbinv_regex	paypal.*
umbinv_start_epoch	MM/DD/YYYY HH:mm:ss Z
umbinv_start_relative	-30days
umbinv_limit	10
umbinv_include_category	Yes

Pre-Process Script tab



Name * Example: Pattern search start relative

API Name * wf_umbrella_pattern_search_relative

Description Example Cisco Umbrella Investigate Workflow to search using Regular expressions against the Investigate database using start relative value.

Object Type * Artifact

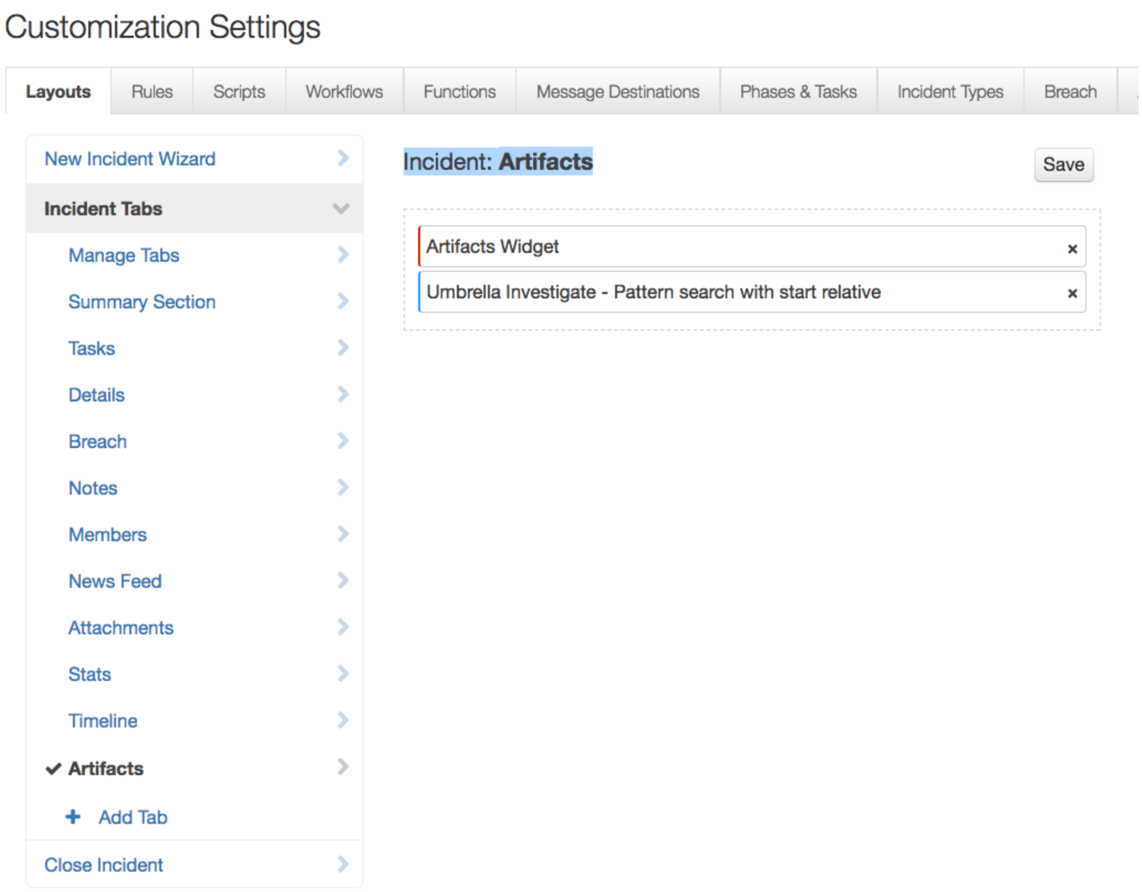
Creator: Resilient Sysadmin
Last Modified: 05/11/2018 10:40
Last Modified By: Resilient Sysadmin
Associated Rules: Example: Pattern search start relative

Language: Python Theme light Mode Default Tab Size 2

```
inputs.umbinv_regex = artifact.value
inputs.umbinv_start_epoch = None
inputs.umbinv_start_relative = "30days"
inputs.umbinv_limit = 5
inputs.umbinv_include_category = True
```

Before using a workflow

- Change the pre-defined value in either the Input or Pre-Processing Script tab for your environment (Note: Definitions in the Pre-Processing Script tab will over-ride any Input tab settings.)
- Add the required data-table to the incident artifacts tab. (Note: Most of the workflows are configured for Artifact object type with the exception of the workflow Example: Get list of category identifiers which is configured for Incident object type.)



Incident: **Artifacts**

Artifacts Widget ×

Umbrella Investigate - Pattern search with start relative ×

Relationships between Rules, Workflow Functions and data tables.

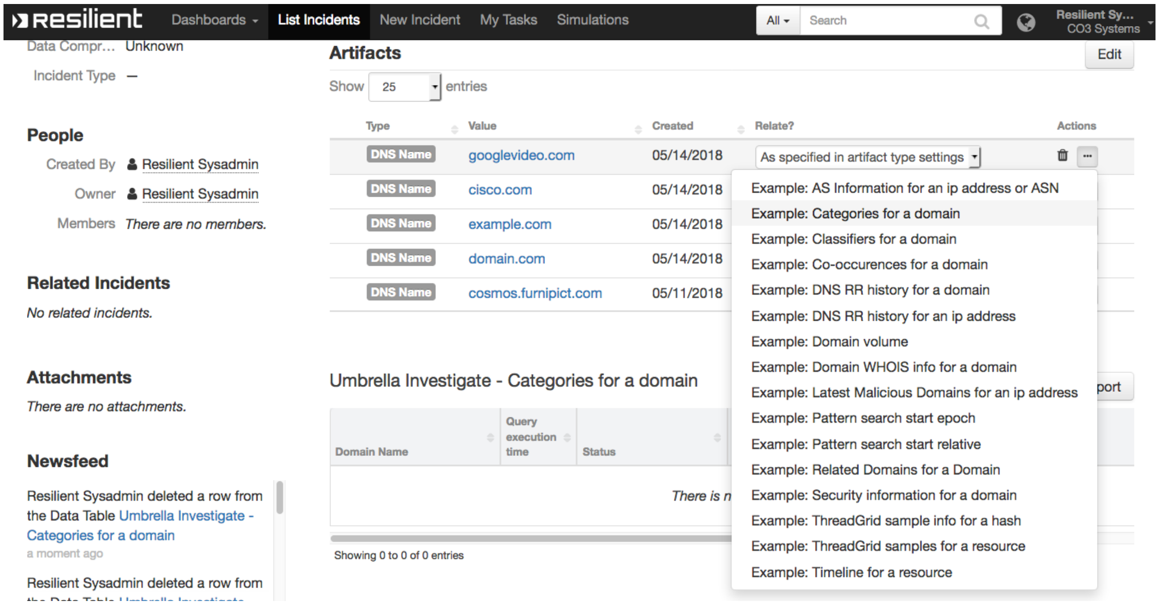
The example workflows each has a function and a data-table associated with it as shown in the following table.

Rule	Workflow (api name)_	Function	Data table (api name)
Example: AS Information for an ip address or ASN	*wf_umbrella_ip_as_info*	*umbrella_ip_as_info*	*umbinv_as_for_an_ip_or_asn*
Example: Get list of category identifiers	*wf_umbrella_domain_status_and_category_cats*	*umbrella_domain_status_and_category*	*umbinv_category_identifiers*
Example: Categories for a domain	*wf_umbrella_domain_status_and_category_dom*	*umbrella_domain_status_and_category*	*umbinv_categories_for_a_domain*
Example: Classifiers for a domain	*wf_umbrella_classifiers*	*umbrella_classifiers*	*umbinv_classifiers_for_a_domain*
Example: DNS RR history for a domain	*wf_umbrella_domain_co_occurrences*	*umbrella_domain_co_occurrences*	*umbinv_domain_co_occurrences*
Example: DNS RR history for a domain	*wf_umbrella_dns_rr_hist_domain*	*umbrella_dns_rr_hist*	*umbinv_dns_rr_history_domain*
Example: DNS RR history for an ip address	*wf_umbrella_dns_rr_hist_ip*	*umbrella_dns_rr_hist*	*umbinv_dns_rr_history_ip*
Example: Domain volume	*wf_umbrella_domain_volume*	*umbrella_domain_volume*	*umbinv_domain_volume*
Example: Domain WHOIS info for a domain	*wf_umbrella_domain_whois_info*	*umbrella_domain_whois_info*	*umbinv_domain_whois_info_domain*
Example: Latest Malicious Domains for an ip address	*wf_umbrella_ip_latest_malicious_domains*	*umbrella_ip_latest_malicious_domains*	*umbinv_latest_malicious_domains_for_an_ip*
Example: Pattern search start epoch	*wf_umbrella_pattern_search_epoch*	*umbrella_pattern_search*	*umbinv_pattern_search_start_epoch*
Example: Pattern search start relative	*wf_umbrella_pattern_search_relative*	*umbrella_pattern_search*	*umbinv_pattern_search_start_relative*
Example: Related Domains for a Domain	*wf_umbrella_domain_related_domains*	*umbrella_domain_related_domains*	*umbinv_related_domains_for_a_domain*

Rule	Workflow (api name)_	Function	Data table (api name)
Example: Security information for a domain	*wf_umbrella_domain_security_info*	*umbrella_domain_security_info*	*umbinv_domain_security_info*
Example: ThreadGrid sample info for a hash	*wf_umbrella_threat_grid_sample*	*umbrella_threat_grid_sample*	*umbinv_thread_grid_sample_info_for_a_hash_basic*
Example: ThreadGrid samples for a resource	*wf_umbrella_threat_grid_samples*	*umbrella_threat_grid_samples*	*umbinv_thread_grid_samples_for_a_resource*
Example: Timeline for a resource	*wf_umbrella_timeline*	*umbrella_timeline*	*umbinv_timeline_for_a_resource*

Workflow execution

To run a Cisco Umbrella Investigate query, right-click on the artifact and select a rule to run the corresponding workflow against that particular artifact. In the following example the user executes the rule Example: Categories for a domain and the corresponding data table will get updated as shown below, where the artifact values are domain names.


resilient
Dashboards
List Incidents
New Incident
My Tasks
Simulations
All
Search
Resilient Sy...
CO3 Systems
Edit
Example: AS Information for an ip address or ASN
Example: Categories for a domain
Example: Classifiers for a domain
Example: Co-occurences for a domain
Example: DNS RR history for a domain
Example: DNS RR history for an ip address
Example: Domain volume
Example: Domain WHOIS info for a domain
Example: Latest Malicious Domains for an ip address
Example: Pattern search start epoch
Example: Pattern search start relative
Example: Related Domains for a Domain
Example: Security information for a domain
Example: ThreadGrid sample info for a hash
Example: ThreadGrid samples for a resource
Example: Timeline for a resource
port

Data Compr... Unknown

Incident Type —

People

Created By Resilient Sysadmin

Owner Resilient Sysadmin

Members *There are no members.*

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

Resilient Sysadmin deleted a row from the Data Table Umbrella Investigate - Categories for a domain

a moment ago

Resilient Sysadmin deleted a row from

Artifacts

Show 25 entries

Type	Value	Created	Relate?	Actions
DNS Name	googlevideo.com	05/14/2018	As specified in artifact type settings	
DNS Name	cisco.com	05/14/2018		
DNS Name	example.com	05/14/2018		
DNS Name	domain.com	05/14/2018		
DNS Name	cosmos.furnipict.com	05/11/2018		

Umbrella Investigate - Categories for a domain

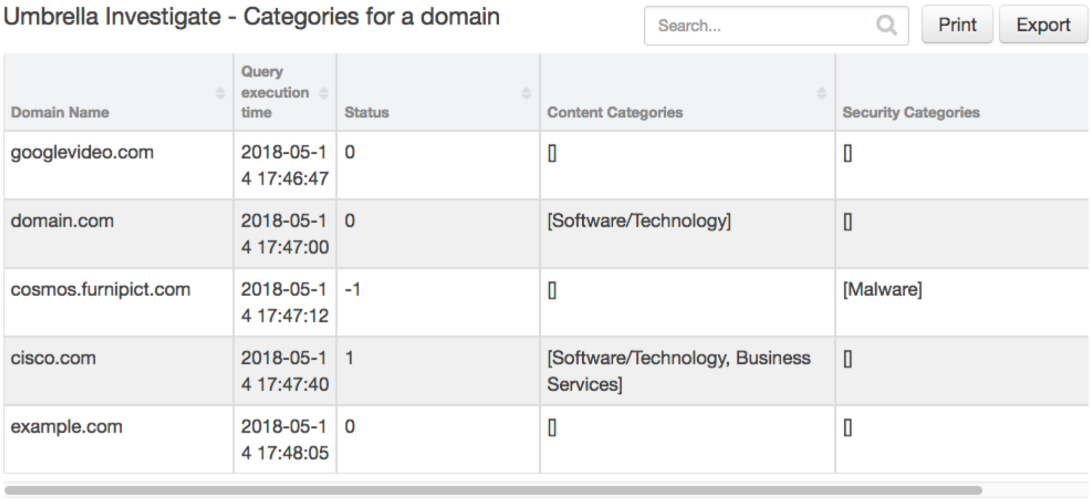
Domain Name	Query execution time	Status

There is n

Showing 0 to 0 of 0 entries

Data table Umbrella Investigate - Categories for a domain (api name umbinv_categories_for_a_domain) will get updated with an entry for each domain that the rule/workflow is run against.

Note: Some of the Workflows with add more than one row per artifact for each execution.



Umbrella Investigate - Categories for a domain

Domain Name	Query execution time	Status	Content Categories	Security Categories
googlevideo.com	2018-05-14 17:46:47	0	[]	[]
domain.com	2018-05-14 17:47:00	0	[Software/Technology]	[]
cosmos.furnipict.com	2018-05-14 17:47:12	-1	[]	[Malware]
cisco.com	2018-05-14 17:47:40	1	[Software/Technology, Business Services]	[]
example.com	2018-05-14 17:48:05	0	[]	[]

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.

Support

For additional support, contact support@resilientsystems.com.

Including relevant information from the log files will help us resolve your issue.