IBM Resilient

resilient

# Incident Response Platform Integrations

## LDAP Search Function V1.0.0

Release Date: June 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 LDAP Search Function.

## Overview

The Lightweight Directory Access Protocol or LDAP is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. It is used to connect to, search, and modify internet directories.

The LDAP search integration with the IBM Resilient platform allows an LDAP search to be initiated from the Resilient platform to an external LDAP server. The returned results can be used to make customized updates to the Resilient platform such as updating incidents, artifacts, data tables and so on.

There is one function supplied in the Resilient function package for LDAP search. The function runs a query against an LDAP server. There are 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 function, how to configure example custom workflows, and any additional customization options.

# Installation

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

- The Resilient platform must be 30 or later.
- You must have 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 must  know the account username and password.
- You must 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 you are 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.)

## LDAP server configuration

Access to the LDAP server is based on user and password. The user is in the form of a cn or common name.

The LDAP search Function currently supports the following possible authentication types for connection to an LDAP server:

```
ANONYMOUS

SIMPLE

NTLM
```

The LDAP Search function defaults to ANONYMOUS login if there are no credentials provided.

## Install the Python components

The functions package contains Python components that are 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.

Complete the following steps to install the Python components:

1. Ensure that the environment is up to date, as follows:

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

2. Run the following command to install the package:

```
sudo pip install --upgrade fn_ldap_search-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.

Complete the following to configure and run the integration:

1. Using sudo, switch to the integration user, as follows:

   ```
   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, as follows:

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

   b. In the `[fn_ldap_search]` section, edit the settings as follows: (Note: The default credentials are for an on-line test server.)

   ```
   # LDAP server ip or fully qualified hostname
   server=ldap.forumsys.com
   port=389
   # The domain setting must be set to a valid Windows domain if using NTLM
   authentication.
   #domain=WORKGROUP
   user=cn=read-only-admin,dc=example,dc=com
   password=password
   auth=SIMPLE
   use_ssl=False
   ```

   c. For an Active Directory, the following are both valid configuration settings formats.

   ```
   # Active Directory example 1.
   server=adserver
   port=389
   user=mydomain\myuser
   password=mypass
   auth=SIMPLE
   use_ssl=False
   connect_timeout=10


   # Active Directory example 2.

   server=adserver
   port=389
   domain=mydomain
   user=myuser
   password=mypass
   auth=NTLM
   use_ssl=False
   connect_timeout=10
   ```

## 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.

Complete the following steps to deploy customizations:

1. Use the following command to deploy these customizations to the Resilient platform:

   ```
   resilient-circuits customize
   ```

2. Respond to 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, using 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.

## Configure resilient-circuits for restart

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

1. The unit file must be named `resilient_circuits.service`. To create the file, enter the following command:

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

2. Add the following contents to the file and change 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
   ```

3. Ensure that the service unit file has the correct permissions:

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

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

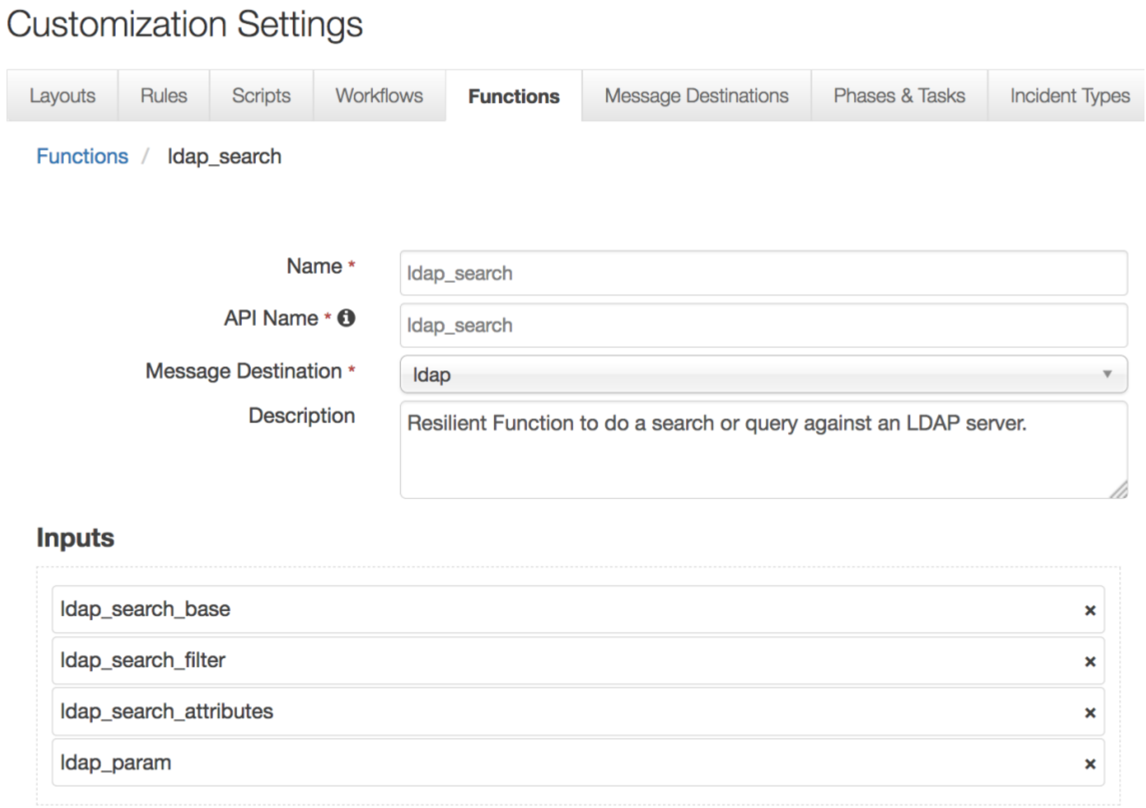
   ```
   sudo systemctl resilient_circuits [start|stop|restart|status]
   ```

You can view log files for `systemd` and the `resilient-circuits` service using the `journalctl` command:

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

# Function Description

Once the function package deploys the function, ldap_search, you can view it in the Resilient platform Functions tab, as shown below. The package also includes an example workflow, rule and data table that show how the function can be used. You can copy and modify these items for your own needs.



Name * ldap_search

API Name * ldap_search

Message Destination * ldap

Description Resilient Function to do a search or query against an LDAP server.

Inputs

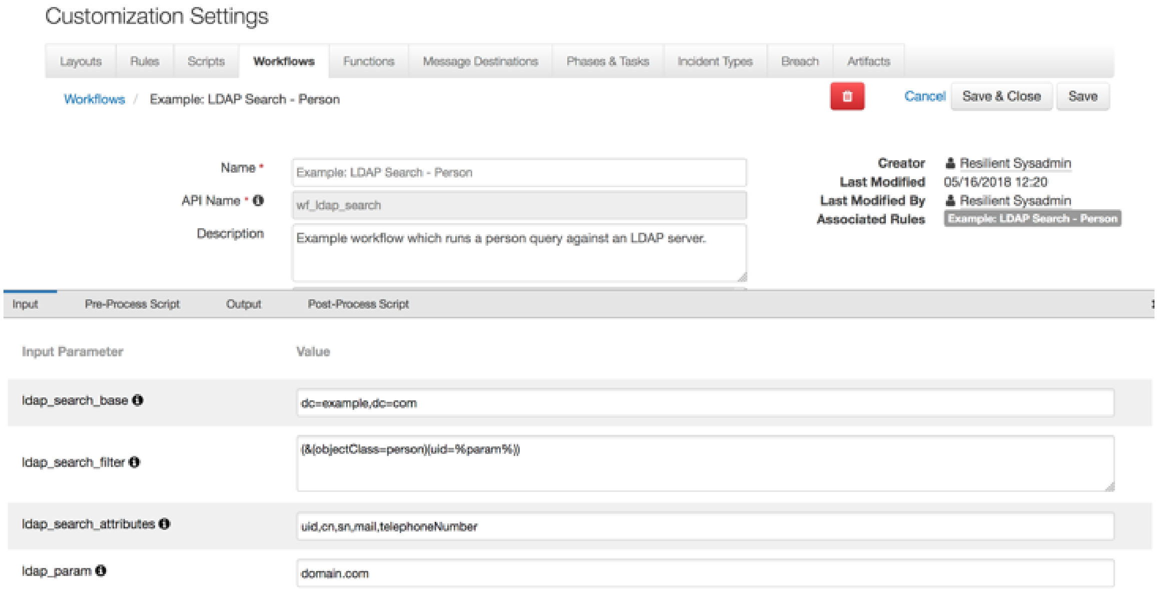
- ldap_search_base
- ldap_search_filter
- ldap_search_attributes
- ldap_param

This function takes the following input fields. Refer to LDAP documentation on the use of LDAP search arguments.

- ldap_search_base
- ldap_search_filter
- ldap_search_attributes
- ldap_param

# Workflow

The **Example: LDAP Search – Person** workflow is available in the Workflows tab, as shown below. The rule Object Type is Artifact.



Name *: Example: LDAP Search - Person

API Name *: wf_ldap_search

Description: Example workflow which runs a person query against an LDAP server.

Creator: Resilient Sysadmin

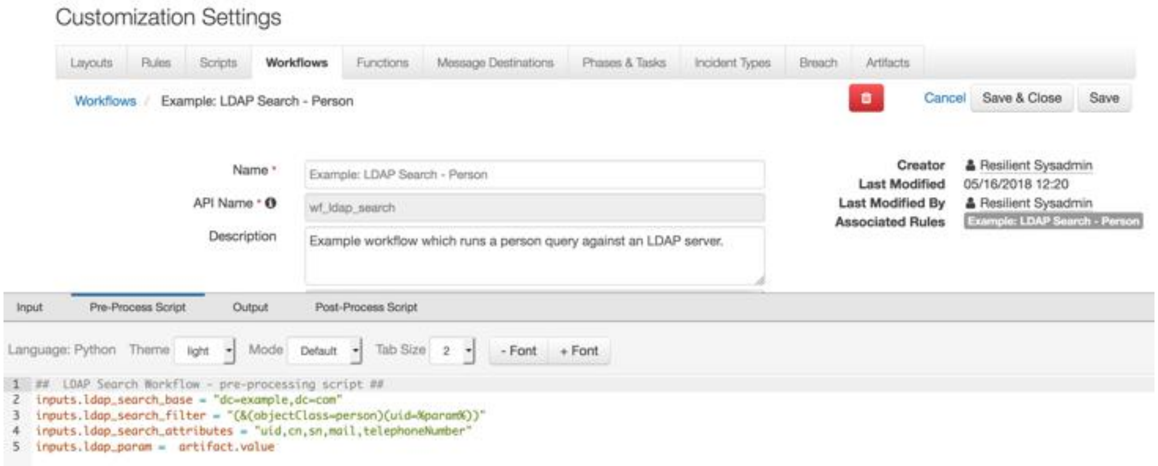
Last Modified: 05/16/2018 12:20

Last Modified By: Resilient Sysadmin

Associated Rules: Example: LDAP Search - Person

| Input Parameter | Value |
|---|---|
| ldap_search_base | dc=example,dc=com |
| ldap_search_filter | (&(objectClass=person)(uid=%param%)) |
| ldap_search_attributes | uid,cn,sn,mail,telephoneNumber |
| ldap_param | domain.com |

The package includes predefined parameter values. Users should change these values to match their environment either in the Input tab or the Pre-Process Script as shown in the following figure.



Name *: Example: LDAP Search - Person

API Name *: wf_ldap_search

Description: Example workflow which runs a person query against an LDAP server.

Creator: Resilient Sysadmin

Last Modified: 05/16/2018 12:20

Last Modified By: Resilient Sysadmin

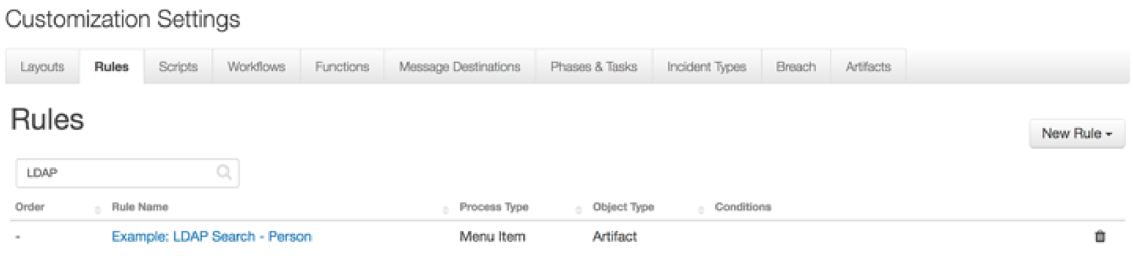
Associated Rules: Example: LDAP Search - Person

Language: Python Theme: light Mode: Default Tab Size: 2

```
##  LDAP Search Workflow - pre-processing script ##
inputs.ldap_search_base = "dc=example,dc=com"
inputs.ldap_search_filter = "(&(objectClass=person)(uid=%param%))"
inputs.ldap_search_attributes = "uid,cn,sn,mail,telephoneNumber"
inputs.ldap_param =  artifact.value
```

# Rule

You can view the example rule in the Rules tab. The rule is a Menu Item rule that is selectable in the Actions button when viewing the Artifacts tab of an incident. When selected, the rule calls the provided workflow.

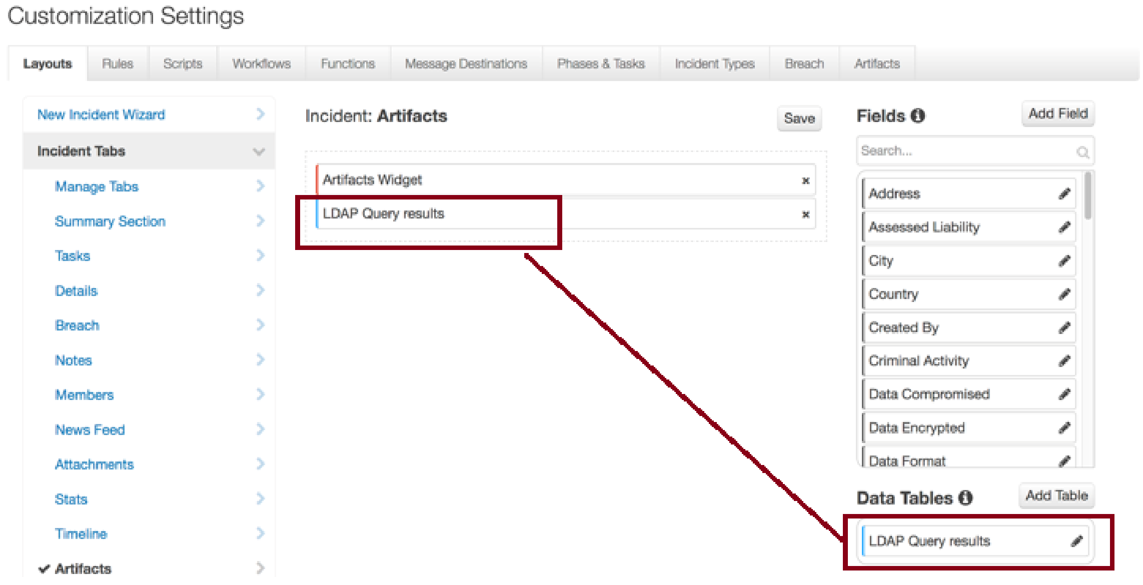


| Order | Rule Name | Process Type | Object Type | Conditions |
|---|---|---|---|---|
| - | Example: LDAP Search - Person | Menu Item | Artifact | |

# Resilient Platform Configuration

To display query results, users need to manually add the “LDAP Query results” data table to the Artifacts tab.

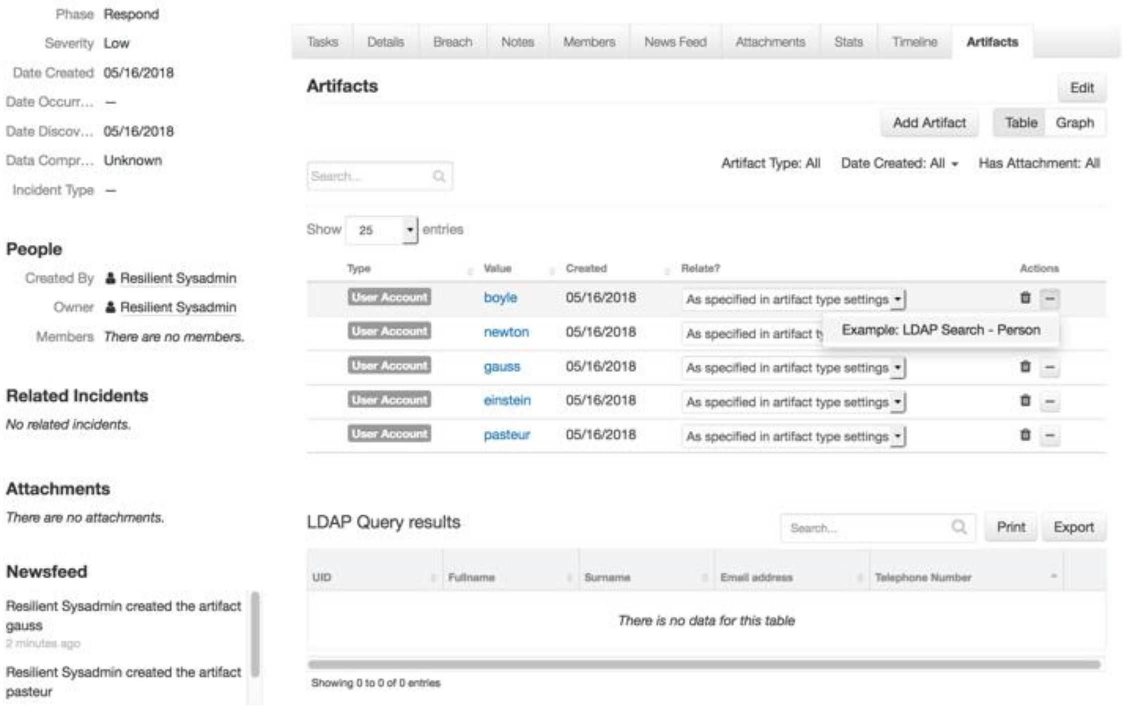
1. Navigate to the Customization Settings and select the Layouts tab.
2. Select Artifacts.
3. Drag the “LDAP Query results” data table to your Artifacts tab.
4. Click Save.



To run an LDAP search query:

1. Go to the Artifacts tab of an incident.
2. Click the **Actions** icon for an artifact.
3. Select **Example: LDAP Search – Person**.

This executes the corresponding workflow against that particular artifact. In the following example, the corresponding data table is updated, where the artifact values are User Accounts.



|  |  |
|---|---|
| Phase | Respond |
| Severity | Low |
| Date Created | 05/16/2018 |
| Date Occurr… | — |
| Date Discov… | 05/16/2018 |
| 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 created the artifact gauss
2 minutes ago

Resilient Sysadmin created the artifact pasteur

**Artifacts**

Artifact Type: All   Date Created: All   Has Attachment: All

Show 25 entries

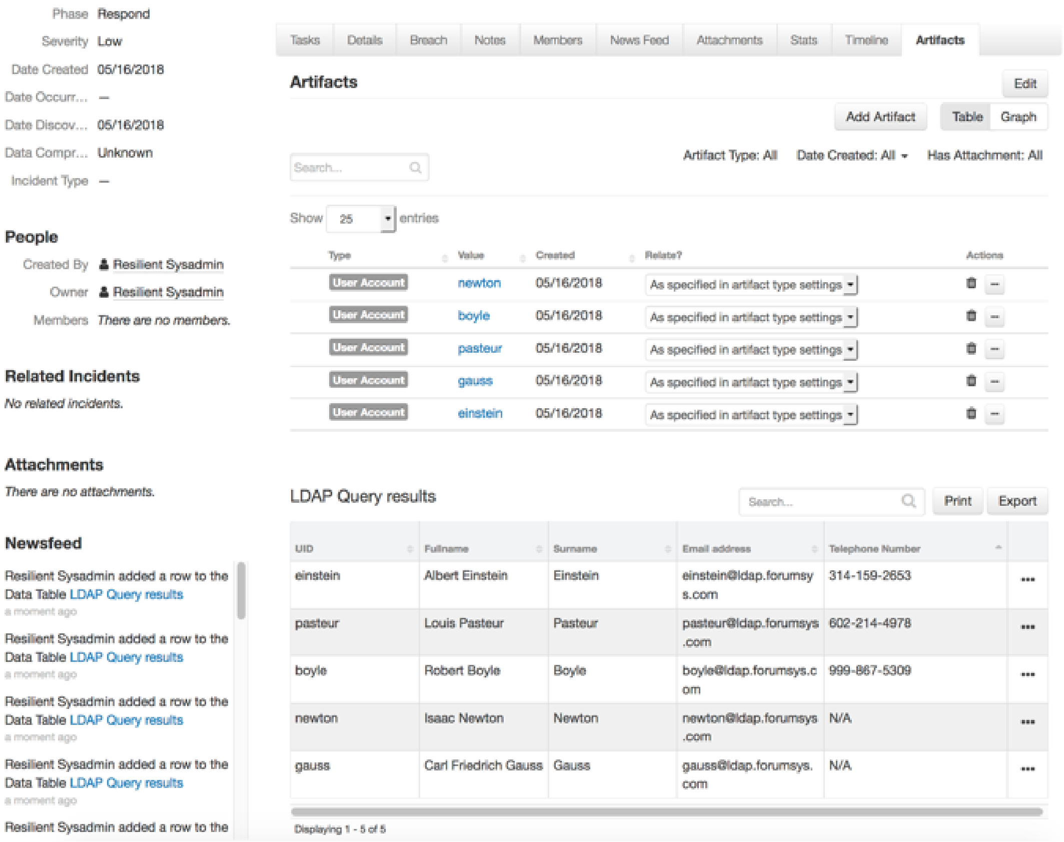
| Type | Value | Created | Relate? | Actions |
|---|---|---|---|---|
| User Account | boyle | 05/16/2018 | As specified in artifact type settings | |
| User Account | newton | 05/16/2018 | As specified in artifact t | Example: LDAP Search - Person |
| User Account | gauss | 05/16/2018 | As specified in artifact type settings | |
| User Account | einstein | 05/16/2018 | As specified in artifact type settings | |
| User Account | pasteur | 05/16/2018 | As specified in artifact type settings | |

LDAP Query results

| UID | Fullname | Surname | Email address | Telephone Number |
|---|---|---|---|---|
| *There is no data for this table* | | | | |

Showing 0 to 0 of 0 entries

Users can update the LDAP Query results data table with an entry for each user name by running the LDAP search action.



|  |  |
|---|---|
| Phase | Respond |
| Severity | Low |
| Date Created | 05/16/2018 |
| Date Occurr… | — |
| Date Discov… | 05/16/2018 |
| 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 added a row to the Data Table LDAP Query results
a moment ago

Resilient Sysadmin added a row to the Data Table LDAP Query results
a moment ago

Resilient Sysadmin added a row to the Data Table LDAP Query results
a moment ago

Resilient Sysadmin added a row to the Data Table LDAP Query results
a moment ago

Resilient Sysadmin added a row to the

**Artifacts**

Artifact Type: All   Date Created: All   Has Attachment: All

Show 25 entries

| Type | Value | Created | Relate? | Actions |
|---|---|---|---|---|
| User Account | newton | 05/16/2018 | As specified in artifact type settings | |
| User Account | boyle | 05/16/2018 | As specified in artifact type settings | |
| User Account | pasteur | 05/16/2018 | As specified in artifact type settings | |
| User Account | gauss | 05/16/2018 | As specified in artifact type settings | |
| User Account | einstein | 05/16/2018 | As specified in artifact type settings | |

LDAP Query results

| UID | Fullname | Surname | Email address | Telephone Number | |
|---|---|---|---|---|---|
| einstein | Albert Einstein | Einstein | einstein@ldap.forumsys.com | 314-159-2653 | ••• |
| pasteur | Louis Pasteur | Pasteur | pasteur@ldap.forumsys.com | 602-214-4978 | ••• |
| boyle | Robert Boyle | Boyle | boyle@ldap.forumsys.com | 999-867-5309 | ••• |
| newton | Isaac Newton | Newton | newton@ldap.forumsys.com | N/A | ••• |
| gauss | Carl Friedrich Gauss | Gauss | gauss@ldap.forumsys.com | N/A | ••• |

Displaying 1 - 5 of 5

# 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.