# ElasticSearch Functions for IBM SOAR

## Table of Contents



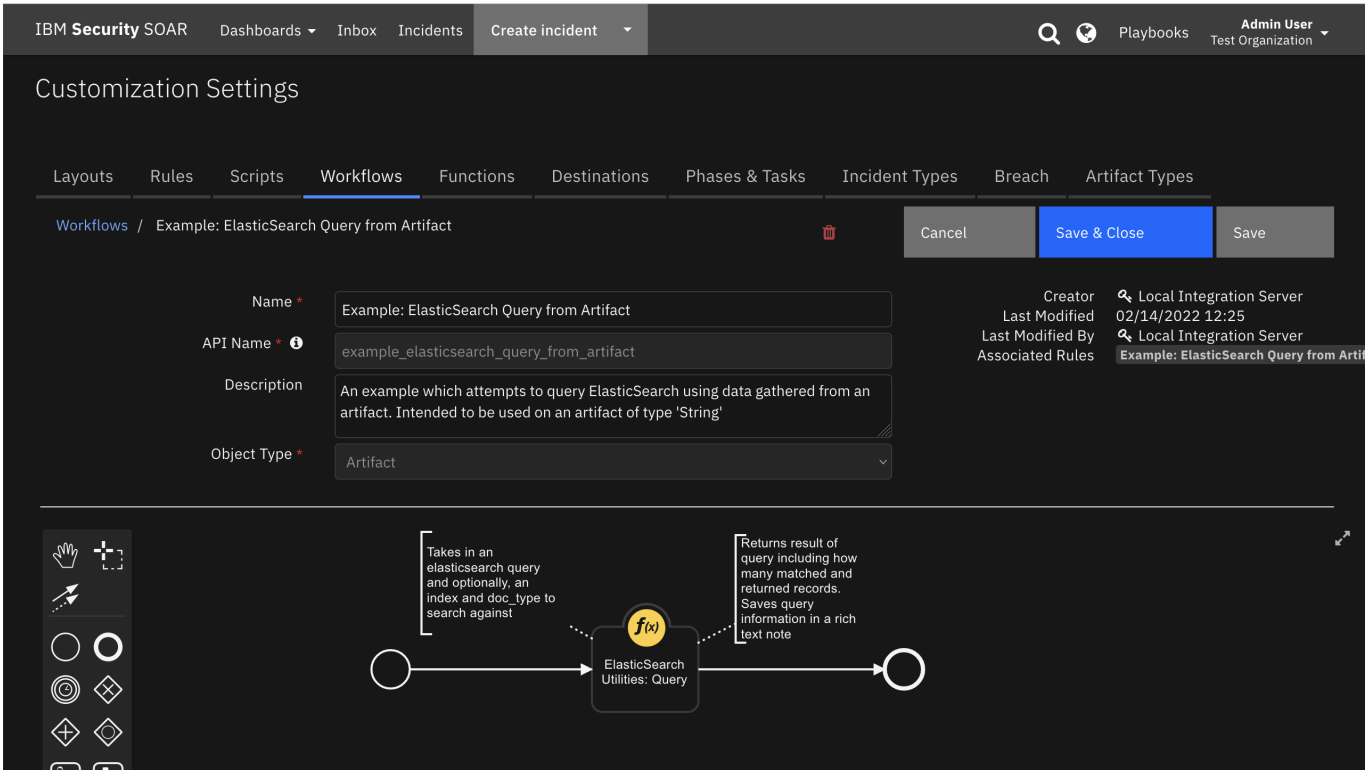
## Release Notes

| Version | Date | Notes |
|---|---|---|
| 1.0.9 | 06/2022 | Added support for disabling SSL Certificate verification |
| 1.0.8 | | Pinned dependency `elasticsearch~=7.17` |
| 1.0.7 | | Add support for AppHost |
| 1.0.6 | | Add resilient-lib dependency to setup.py |
| 1.0.5 | | Added logic to conditionally use doc_type depending on the major version of ElasticSearch and Updated documentation |
| 1.0.4 | | Customer hotfix related to breaking version changes to ElasticSearch library |
| 1.0.3 | | Bugfix http |

| Version | Date | Notes |
| --- | --- | --- |
| 1.0.2 | | Updated documentation and Added a selftest capability, to enable users to test their Elasticsearch connection before starting the integration server |

# Overview

**The app queries Elasticsearch using SOAR incident or artifact data.**




Allows users of the SOAR to connect to and query an ElasticSearch database. Users can specify the location of a remote ElasticSearch instance and query this instance for data within SOAR.

Queries provided to the function must be properly formed to work. Please review the ElasticSearch documentation for examples on how to form your query. A number of example queries are available when setting up the function in a workflow.

**Important caveat: Your ElasticSearch library version must match the major ElasticSearch version since changes might be introduced with each release. This app supports the recent version changes.**

Two options are available for connection, HTTP connection to localhost or remote HTTPS connection with username and password authentication.

## Key Features

- Perform queries on an elasticsearch instance

# Requirements

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

## SOAR platform

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

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

- SOAR platform >= `45.0.7899`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

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

- SOAR platform >= `45.0.7899`.
- 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>=43.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

| Name | Permissions |
|---|---|
| Org Data | Read |
| Function | Read |

The following SOAR 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 Documentation website at ibm.biz/soar-docs. On this web page, select your SOAR platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **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 IBM Documentation table of contents, select Case Management and Orchestration & Automation > **System administrator**.

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

### Proxy Server

The app **does** support a proxy server.

### Python Environment

Both Python 2.7 and Python 3.6 are supported. Additional package dependencies may exist for each of these packages:

- elasticsearch~=7.17
- resilient_circuits>=43.0.0
- resilient_lib>=43.0.0

### Endpoint Information

This app has been implemented using:

| Product Name | Product Version | API URL | API Version |
|---|---|---|---|
| Elastic Search | 8.2.3 | https://www.elastic.co/guide/en/cloud/current/index.html | |

## Installation

### Install

- To install or uninstall an App or Integration on the *SOAR 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

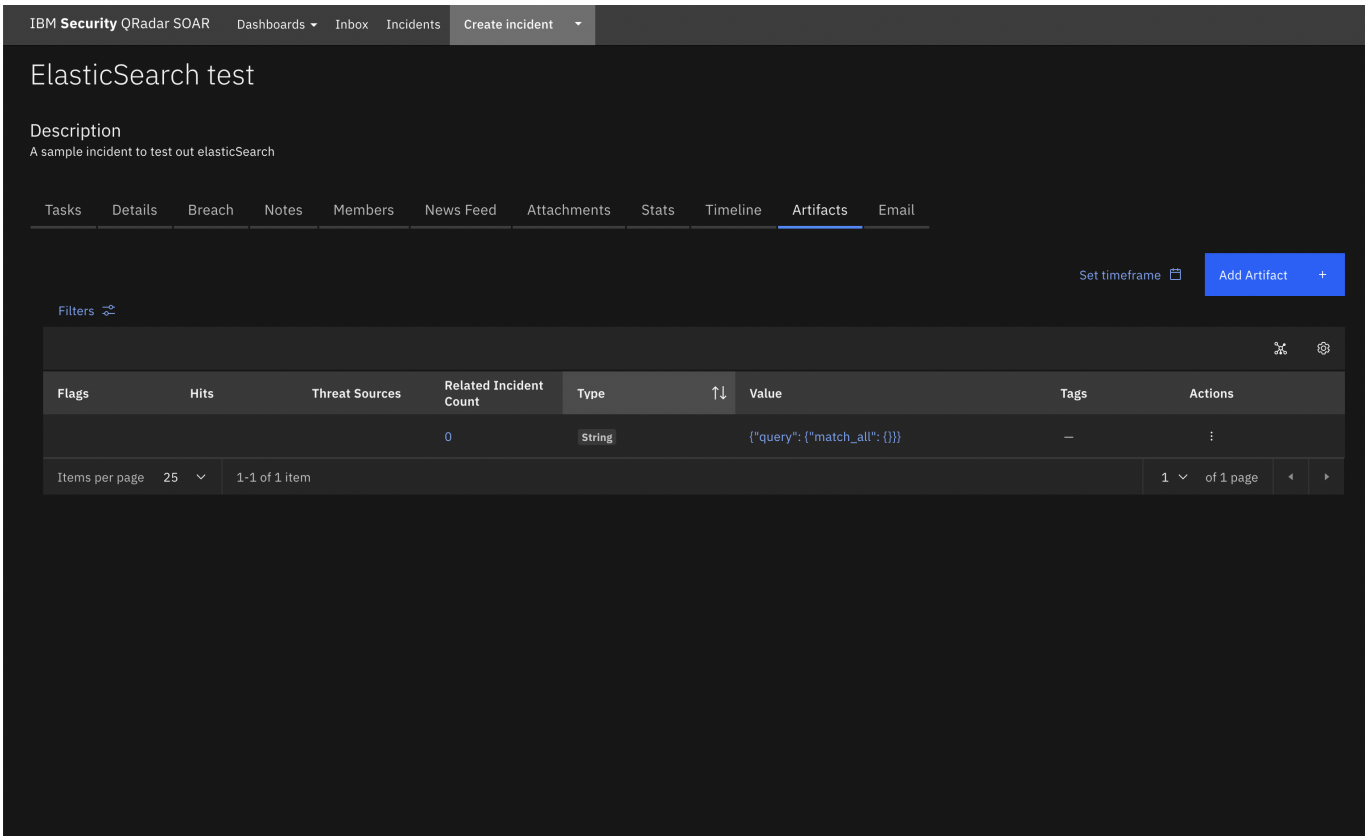
The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

| Config | Required | Example | Description |
|---|---|---|---|
| **es_auth_username** | Yes | `<ELASTICSEARCH_USERNAME>` | *Username of the elastic instance* |
| **es_auth_password** | Yes | `<ELASTICSEARCH_PASSWORD>` | *Password of the elastic instance* |

| Config | Required | Example | Description |
|---|---|---|---|
| **es_cafile** | No | `<CA_FILE_TO_BE_USED>` | *Location of the certificate file if using HTTPS* |
| **es_verify_certs** | No | `<True OR False>` | *Enable or disable SSL certificate verification* |
| **es_datastore_scheme** | Yes | `<HTTPS OR HTTP>` | *If HTTPS is provided, an SSL Context is configured for the connection* |
| **es_datastore_url** | Yes | `<ELASTICSEARCH_URL>` | *URL of the elastic instance* |
| **es_use_http** | Yes | `<True OR False>` | *If true, connection to the elastic instance uses HTTP. Set to False if the es_veryify_certs is True.* |

## Function - ElasticSearch Utilities: Query

A function that allows a user to query a specified ElasticSearch datastore for data.




▶ Inputs:

| Name | Type | Required | Example | Tooltip |
|---|---|---|---|---|
| `es_doc_type` | `text` | No | – | Document type to search. |

| Name | Type | Required | Example | Tooltip |
| --- | --- | --- | --- | --- |
| es_index | text | No | – | Index to search for data. If left blank, all indices are searched. |
| es_query | textarea | Yes | – | Query that is submitted to ElasticSearch. |

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.


```
results = {
  "inputs": {
    "es_doc_type": null,
    "es_index": null,
    "es_query": "{\"query\": {\"match_all\": {}}}"
  },
  "matched_records": {
    "relation": "gte",
    "value": 10000
  },
  "query_results": [
    {
      "_id": "kS_ekIEBTwR1htd9OD_f",
      "_index": ".ds-logs-app_search.analytics-default-2022.06.23-000001",
      "_score": 1.0,
      "_source": {
        "@timestamp": "2022-06-23T14:01:30.224Z",
        "agent": {
          "ephemeral_id": "1ac55df2-51a2-4756-b50e-a4fa638ab155",
          "hostname": "9ee8fac8927c",
          "id": "19cfd1c7-99c3-461b-97e2-fd1a1e9e50fa",
          "name": "9ee8fac8927c",
          "type": "filebeat",
          "version": "7.15.1"
        },
        "data_stream": {
          "dataset": "app_search.analytics",
          "namespace": "default",
          "type": "logs"
        },
        "ecs": {
          "version": "1.7.0"
        },
        "event": {
          "action": "loco_moco_search",
          "category": "app-search-analytics",
          "created": "2022-06-23T14:01:30Z",
          "dataset": "app-search-analytics",
          "document_ids": [
            "park_rocky-mountain"
```

```
            ],
            "loco_moco_search_request_id": "6sHMDt44SGG_V-p11TXUyw",
            "query_string": "rocky",
            "tags": []
          },
          "host": {
            "name": "9ee8fac8927c"
          },
          "input": {
            "type": "log"
          },
          "labels": {
            "engine_id": "62b326c9d0164ee8e257b729",
            "index_date": "2022.06.23",
            "lm_account_id": "62b2f277d0164e239457b719"
          },
          "log": {
            "file": {
              "path": "/app/logs/filebeat.log"
            },
            "offset": 58011
          },
          "related": {
            "ip": "129.41.46.6"
          }
        }
      },
      {
        "_id": "DJXekIEBhfwfcOFNGY18",
        "_index": ".ds-logs-app_search.analytics-default-2022.06.23-000001",
        "_score": 1.0,
        "_source": {
          "@timestamp": "2022-06-23T14:01:21.239Z",
          "agent": {
            "ephemeral_id": "1ac55df2-51a2-4756-b50e-a4fa638ab155",
            "hostname": "9ee8fac8927c",
            "id": "19cfd1c7-99c3-461b-97e2-fd1a1e9e50fa",
            "name": "9ee8fac8927c",
            "type": "filebeat",
            "version": "7.15.1"
          },
          "data_stream": {
            "dataset": "app_search.analytics",
            "namespace": "default",
            "type": "logs"
          },
          "ecs": {
            "version": "1.7.0"
          },
          "event": {
            "action": "loco_moco_search",
            "category": "app-search-analytics",
            "created": "2022-06-23T14:01:21Z",
            "dataset": "app-search-analytics",
```

```
            "document_ids": [
              "park_rocky-mountain"
            ],
            "loco_moco_search_request_id": "f7z0me0oSeGuUArcVdl9xw",
            "query_string": "1075.6",
            "tags": []
          },
          "host": {
            "name": "9ee8fac8927c"
          },
          "input": {
            "type": "log"
          },
          "labels": {
            "engine_id": "62b326c9d0164ee8e257b729",
            "index_date": "2022.06.23",
            "lm_account_id": "62b2f277d0164e239457b719"
          },
          "log": {
            "file": {
              "path": "/app/logs/filebeat.log"
            },
            "offset": 51948
          },
          "related": {
            "ip": "129.41.46.6"
          }
        }
      },
    ],
    "returned_records": 10,
    "success": true
}
```


▶ Workflows

```
if artifact.value is not None:
  inputs.es_query = artifact.value
```

▶ Example Post-Process Script:

```
"""
# An Example of the result object
    results = {
        "inputs": {
          "es_query": { "query": { "match_all": {} } },
          "es_doc_type": logs,
          "es_index" : my_logstore
        },
```

```
        "query_results": [
          <elasticsearch-record>,
        "success": True / False,
        "matched_records": 1000,
        "returned_records": 100
    }
    Note: The schema of elasticsearch-record; outlined above, will reflect
the structure of your data in Elastic itself
"""

if results.matched_records:
  noteText = """<b>ElasticSearch Query status</b>
               <br> Query supplied: <b>{0}</b>
               <br> Total matched records :<b>{1}
</b>""".format(results.inputs["es_query"], results.matched_records)

  if results.returned_records != 0:
    noteText += """<br> Total returned records : <b>{0}
</b>""".format(results.returned_records)
  incident.addNote(helper.createRichText(noteText))
```

## Rules

| Rule Name | Object | Workflow Triggered |
|---|---|---|
| Example: ElasticSearch Query from Artifact | artifact | `example_elasticsearch_query_from_artifact` |
| Example: ElasticSearch Query from Incident | incident | `example_elasticsearch_query_from_incident` |

## Troubleshooting & Support

If using the app with an App Host, see the SOAR System Administrator Guide and the App Host Deployment Guide for troubleshooting procedures. You can find these guides on the IBM Knowledge Center, where you can select which version of the SOAR platform you are using. Refer to the documentation listed in the Requirements section for troubleshooting information.

If using the app with an integration server, see the Integration Server Guide

### For Support

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