RSA Archer® Suite

6.9

Integration Guide

1.1

Splunk> Phantom

Contact Information
RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Revised: December 2020

Table of Contents

Release Notes

Release 1.1

New and Changed Features

- The integration now supports RSA Archer Domain Users.

Known Issues

- Shared API / login accounts can result in timing-dependent session errors or dropped connections.
- At a minimum REST API use requires the "VRM – Web Service API" role. RSA Archer's Security Incidents application also requires roles, "IM: Manager" and "System Administrator."

Chapter 1: Overview of the Splunk> Phantom Integration with RSA Archer

About Splunk> Phantom

Splunk> Phantom is a community-powered security automation and orchestration solution. The Splunk> Phantom Platform integrates existing security technologies, such as RSA Archer, forming a layer of connective tissue between separate products. Manual security-operations tasks codified into Splunk> Phantom Playbooks become software workflows that run at machine-speed to orchestrate complex interactions among RSA Archer and other Splunk> Phantom-connected security products.

Key Features and Benefits

The integration of Splunk> Phantom with RSA Archer enables Splunk> Phantom to create, list, retrieve, and update RSA Archer tickets. Splunk> Phantom Playbooks can use RSA Archer capabilities to improve efficiency and precision of ticketing, investigation, response, and reporting, so the SOC can work smarter, respond faster, and focus attention onto mission-critical decisions.

Prerequisites

Components	Recommended Software
RSA Archer Solution	RSA Archer IT Security & Risk Management
RSA Archer Use Case	RSA Archer Cyber Security and Breach Response
RSA Archer Application	Security Incidents

Uses Custom Application	No
Requires On – Demand License	No

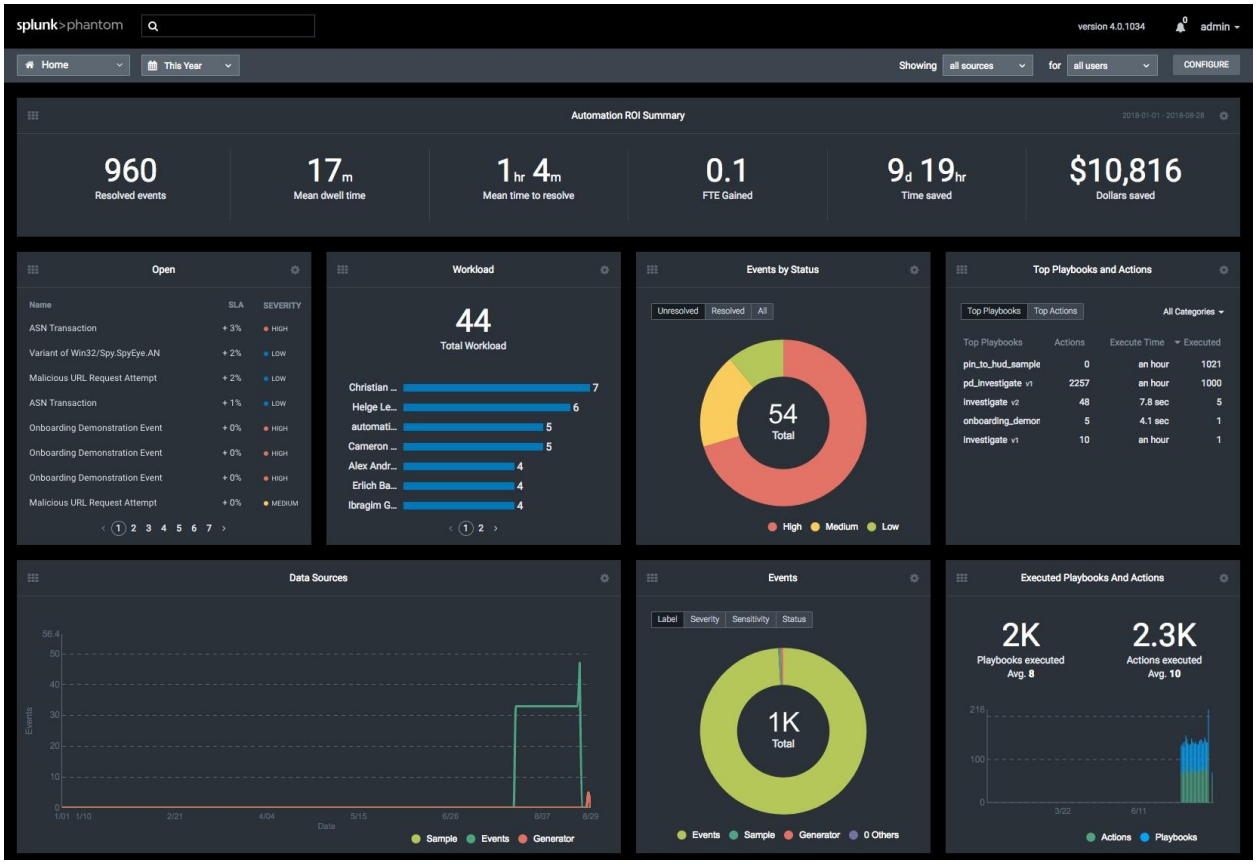
RSA Archer Applications

Application	Description
Security Incidents	The Security Incidents application provides a central location managing incidents, both those created from aggregated security alerts and those that are manually reported.

Additional Resources

The following additional resources are available for this application:

- About Splunk> Phantom: https://docs.splunk.com/Documentation/Phantom



Chapter 2: Integration Components Overview

Before You Begin

This section provides instructions for configuring the RSA Archer Application on the Splunk> Phantom Platform with RSA Archer. This document is not intended to suggest optimum installations or configurations.

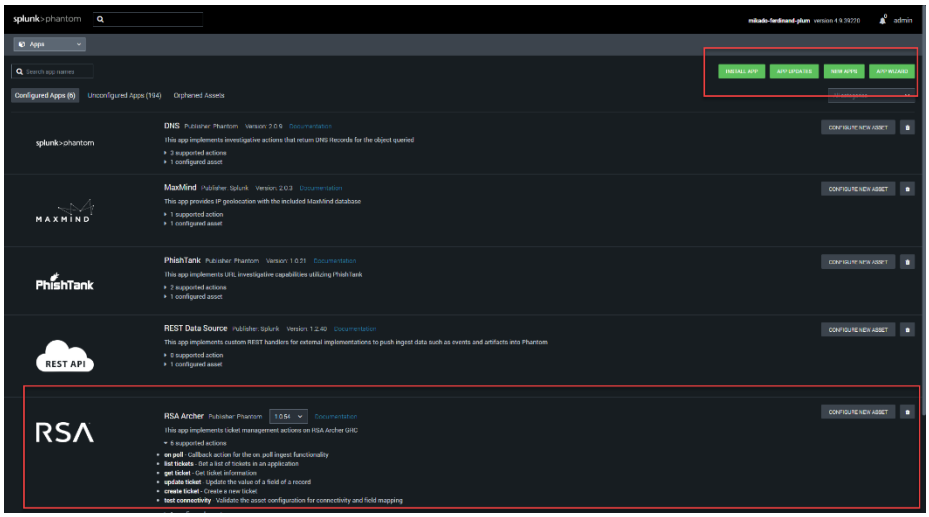
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

Prerequisites:

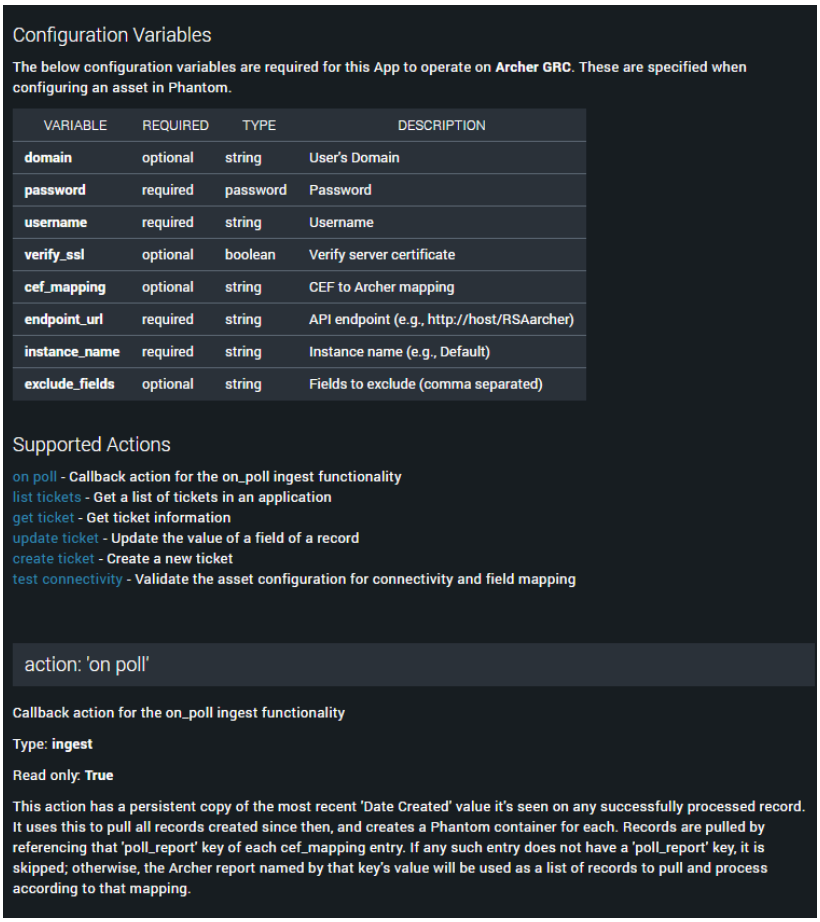
- All Splunk> Phantom and RSA Archer components must be installed and working prior to the integration
- RSA Archer Web Services must be enabled for Splunk> Phantom to use RSA Archer REST and SOAP API's; Network web-services connectivity must exist between Splunk> Phantom and RSA Archer.
- A unique RSA Archer account must be assigned to each RSA Archer Asset configured in Splunk> Phantom. The RSA Archer account(s) must have appropriate role-permissions to use the REST and SOAP API's, as well as the RSA Archer target application.
- Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Splunk> Phantom integrates with RSA Archer using the RSA Archer App on Splunk> Phantom to call RSA Archer web services (REST and SOAP) APIs. The RSA Archer App comes pre-installed and runs entirely within Splunk> Phantom — no new code needs be installed on RSA Archer. Once you enable and configure the App, RSA Archer ticketing actions are available within Splunk> Phantom.



The following diagram shows the main components of this integration:



Configuration Variables

The below configuration variables are required for this App to operate on **Archer GRC**. These are specified when configuring an asset in Phantom.

VARIABLE	REQUIRED	TYPE	DESCRIPTION
domain	optional	string	User's Domain
password	required	password	Password
username	required	string	Username
verify_ssl	optional	boolean	Verify server certificate
cef_mapping	optional	string	CEF to Archer mapping
endpoint_url	required	string	API endpoint (e.g., http://host/RSAarcher)
instance_name	required	string	Instance name (e.g., Default)
exclude_fields	optional	string	Fields to exclude (comma separated)

Supported Actions

on poll - **Callback action for the on_poll ingest functionality**
list tickets - **Get a list of tickets in an application**
get ticket - **Get ticket information**
update ticket - **Update the value of a field of a record**
create ticket - **Create a new ticket**
test connectivity - **Validate the asset configuration for connectivity and field mapping**

action: 'on poll'

Callback action for the on_poll ingest functionality

Type: **ingest**

Read only: **True**

This action has a persistent copy of the most recent 'Date Created' value it's seen on any successfully processed record. It uses this to pull all records created since then, and creates a Phantom container for each. Records are pulled by referencing that 'poll_report' key of each cef_mapping entry. If any such entry does not have a 'poll_report' key, it is skipped; otherwise, the Archer report named by that key's value will be used as a list of records to pull and process according to that mapping.

The RSA Archer App is deployed by configuring one or more Assets for the App within Splunk> Phantom. Each Asset represents a separate connection to RSA Archer, and each asset connects to a specific application within RSA Archer. Multiple assets are required to connect to different RSA Archer instances or use multiple RSA Archer applications. Each asset can specify different polling frequencies, CEF-RSA Archer mappings, or RSA Archer API access credentials.

Splunk> Phantom Apps & Assets

A Splunk> Phantom App is designed to connect with a matching point product. An Asset is a specific connection-configuration. By default, configuring an App on Splunk> Phantom involves configuring an Asset of that App. Complex deployments, such as multiple instances of a point product, may involve configuring multiple connections (i.e. multiple Assets). It is important to understand how Splunk> Phantom Apps are related to Assets:

Splunk> Phantom App	A module designed to communicate with a point product. Examples: • RSA Security Analytics App • RSA Archer App • RSA NetWitness Logs and Packets App
Splunk> Phantom Asset	A unique product-connection, using the App for that product. Multiple Assets can be configured for an App. Example multiple-asset use-cases include: • Connecting to different instances of a product (such as different sandboxes or different physical firewalls) • Connecting using different point-product accounts, each account having different permissions • Connecting on different ports, or at different polling frequencies.

In summary, an Asset is a unique-connection-configuration of an App. In some circumstances, you may choose to configure multiple Assets for an App.

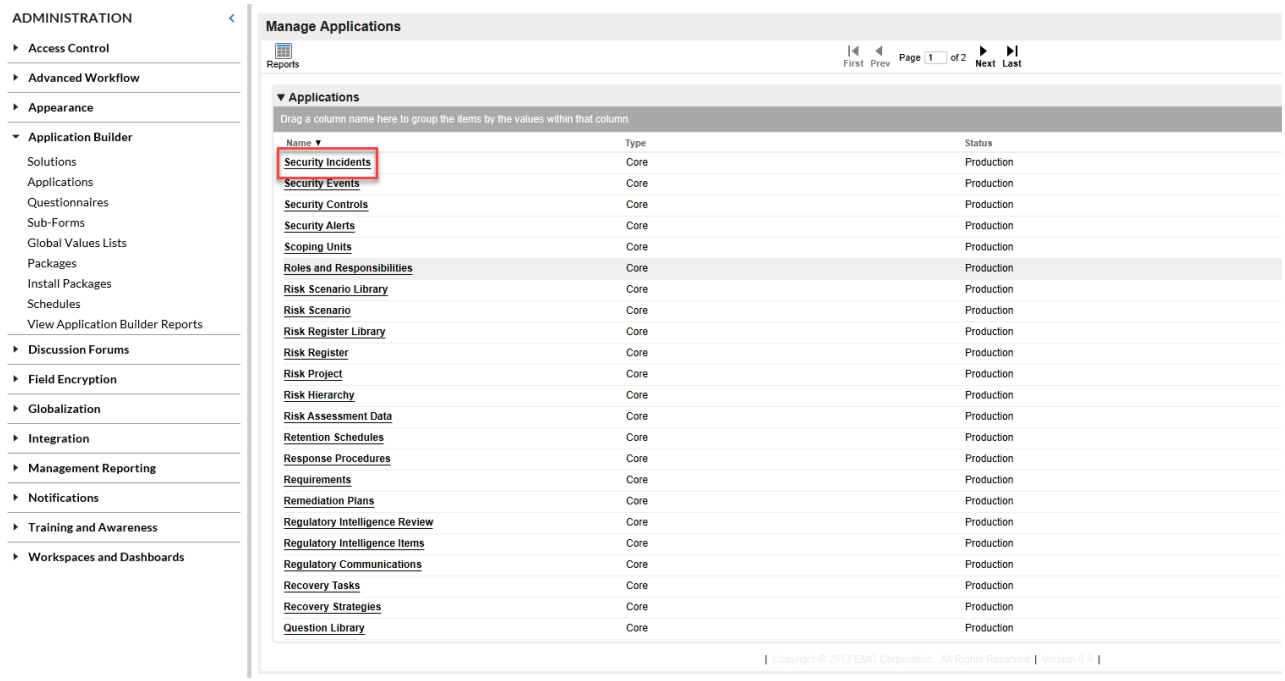
RSA Archer Applications, Fields, and Field-types

RSA Archer Solutions and Application Names

RSA Archer offers a large number of applications or solutions that can be accessed through the Splunk> Phantom integration. An example list of RSA Archer applications is shown here.

This guide references RSA Archer's **IT Security Risk Management** solution in examples, using the RSA Archer **Security Incidents application**. This type of RSA Archer application name is used during Splunk> Phantom configuration and is required by the RSA Archer API.

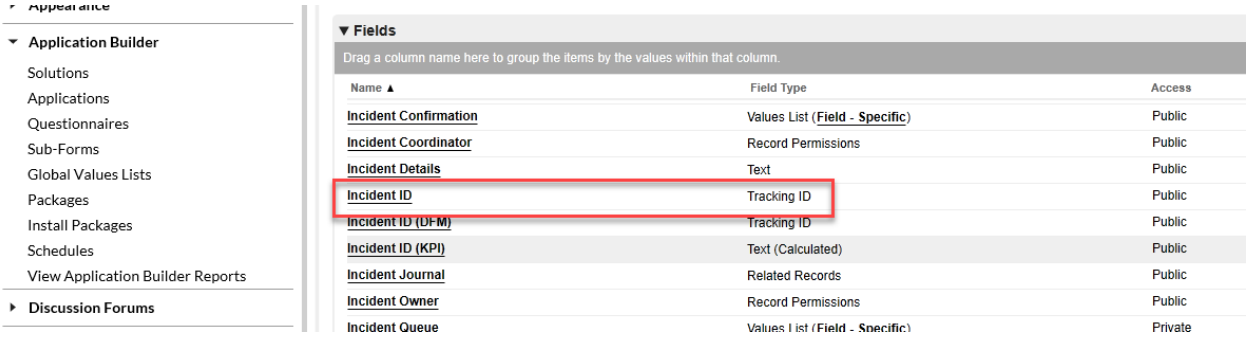
RSA Archer application names can be viewed in RSA Archer by navigating to **Administration > Application Builder > Manage Applications**, then scrolling through the **Applications** list until the specific application appears. Here, the Security Incidents application is highlighted:



RSA Archer Tracking ID Fields

Each RSA Archer application has one field defined as a tracking field, containing a unique ID for each data record. In each RSA Archer application, the tracking field is marked with the field-type **Tracking ID**.

To locate the name of the tracking field for an RSA Archer application, select the application name in the **Applications** list shown above, then select the **Fields** tab. Scroll through the Fields list to locate the one defined as field type **Tracking ID**. In the example below, the Security Incidents application uses the field **Incident ID** as the tracking field.



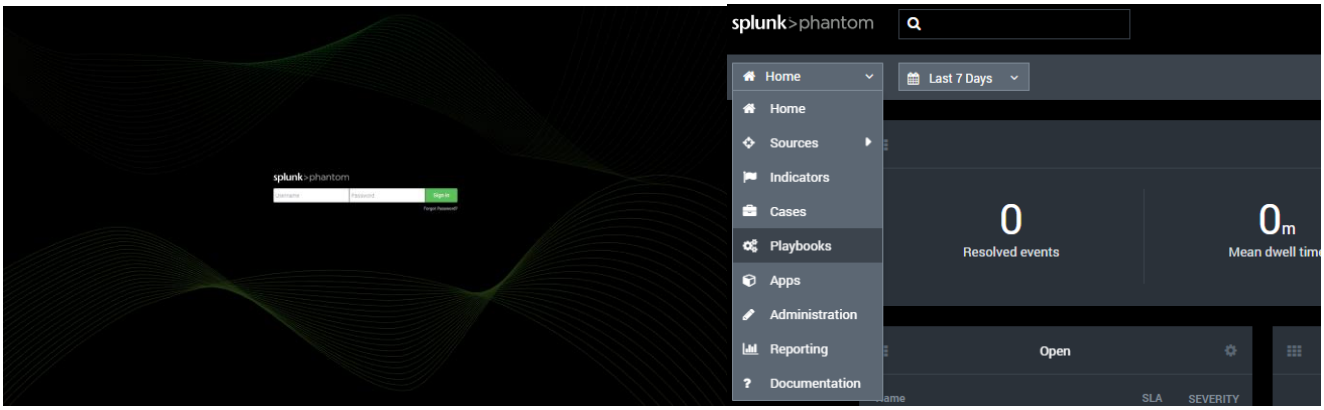
Simply Fields Versus Object Fields

Scrolling through the **Fields** list reveals certain field-types that can be considered “simple” (text, date, numeric, IP Address, etc.), and others that can be considered “objects” (sub-form, values list, user or groups list, and more). Simple fields are generally processed correctly by the Splunk> Phantom integration, even if the fields weren’t previously identified, while object fields may result in an error when reading data from RSA Archer. The names of object fields may be helpful in configuring field-exclusions, in the event that ingestion from RSA Archer encounters an object type of data that is not defined or supported in the Splunk> Phantom integration.

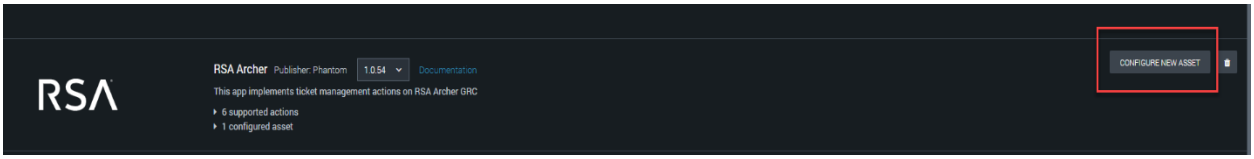
Chapter 3: Splunk> Phantom Configuration

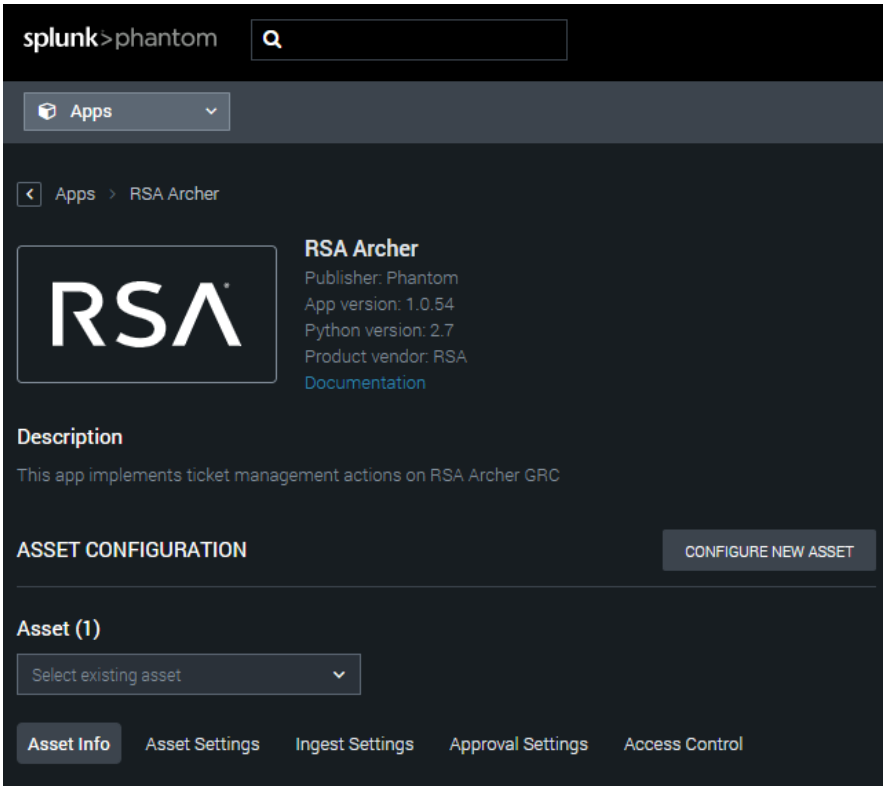
Locating the RSA Archer Application

1. After Signing into the Splunk> Phantom Platform, select **Apps** on the main navigation menu.



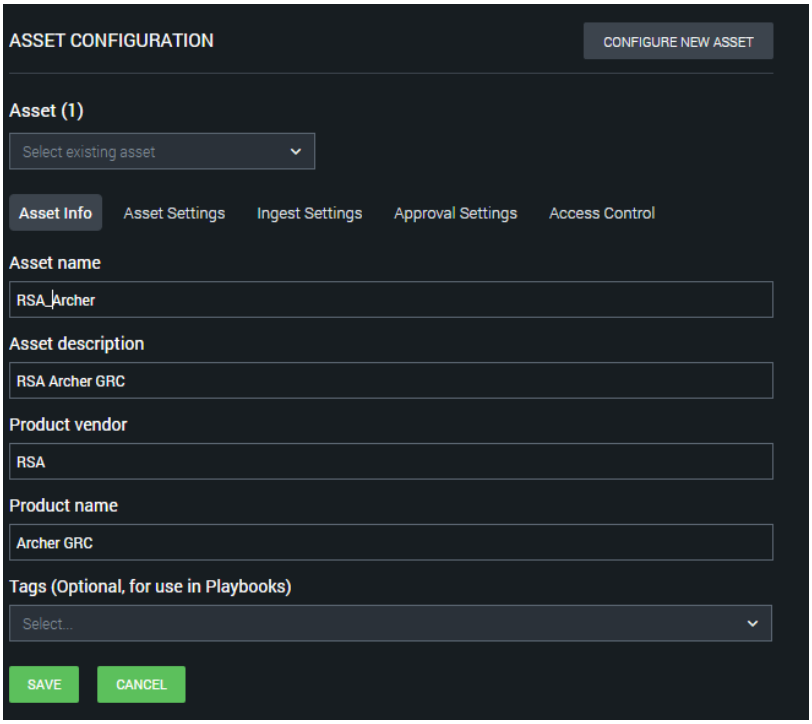
2. Enter “Archer” in the search field to locate the RSA Archer App. Select **Configure New Asset** to access the **Asset Configuration** settings.





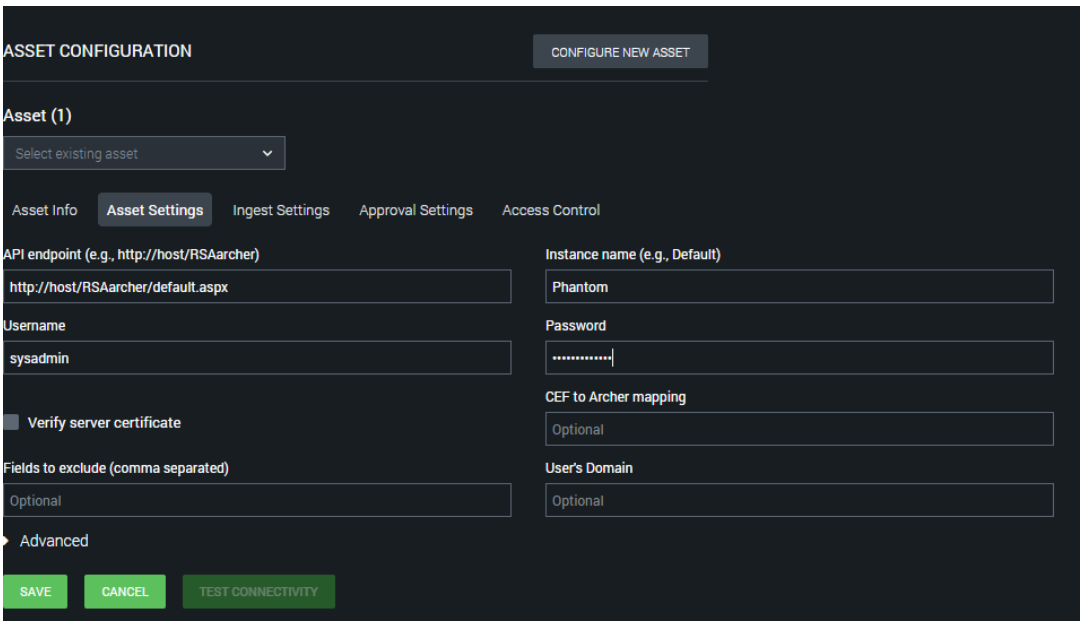
RSA Archer Asset-Configuration

1. On the **Asset Configuration** page, select the **Asset Info** tab then enter an **Asset Name** and **Asset Description** for RSA Archer.



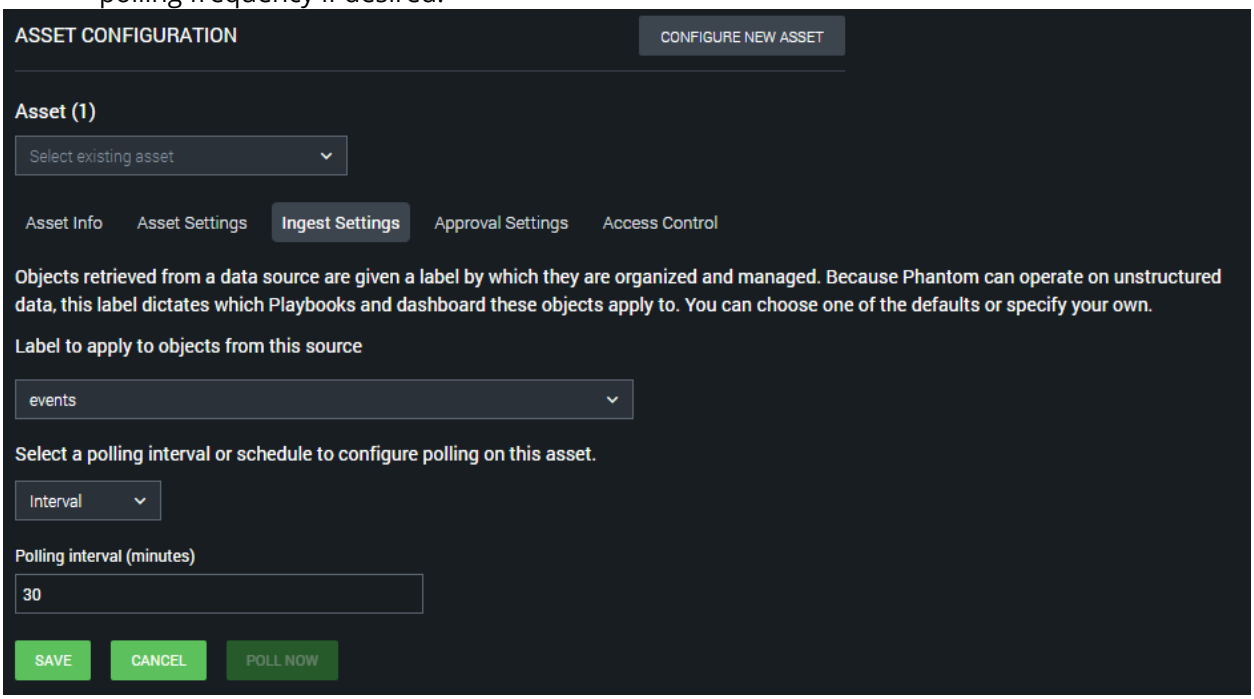
2. Select the **Asset Settings** tab and enter the RSA Archer connection information: **API Endpoint, Instance name, Username,** and **Password**.

Important: The Instance name must match the RSA Archer Instance name configured by the RSA Archer administrator.

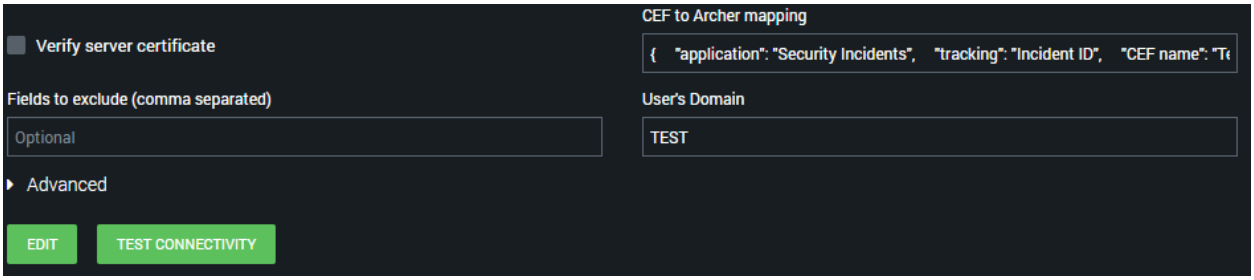


3. When setting up a connection for **Domain Users**, the **User's Domain** field is mandatory in the **Asset Settings** tab, and the **Username** field must be that of a **Domain User.**

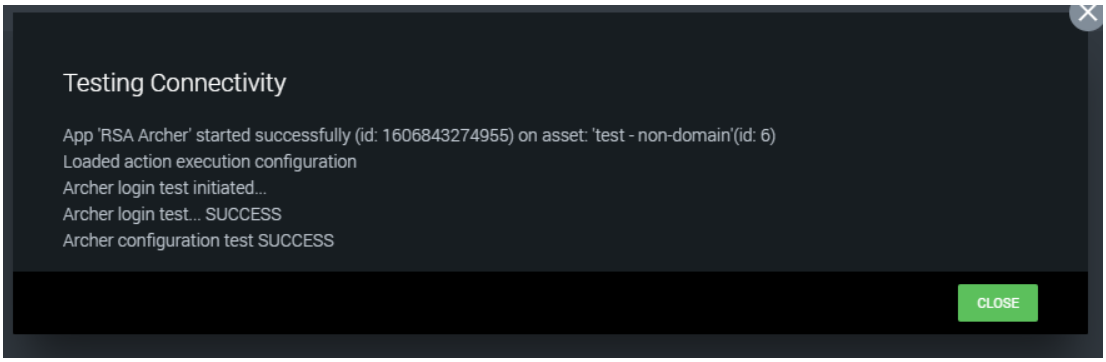
4. Select the **Ingest Settings** tab and choose a label for data ingested from RSA Archer or select **NEW ENTRY** in the dropdown list to create a new label. By default, ingest from RSA Archer is triggered through manual polling by a Splunk> Phantom user. Select **Enable Polling** to configure Splunk> Phantom to poll RSA Archer automatically, then change the polling frequency if desired.



5. Select **SAVE** to save the asset configuration. Switch back to the **Asset Settings** tab, then select **Test Connectivity** to verify the asset settings.



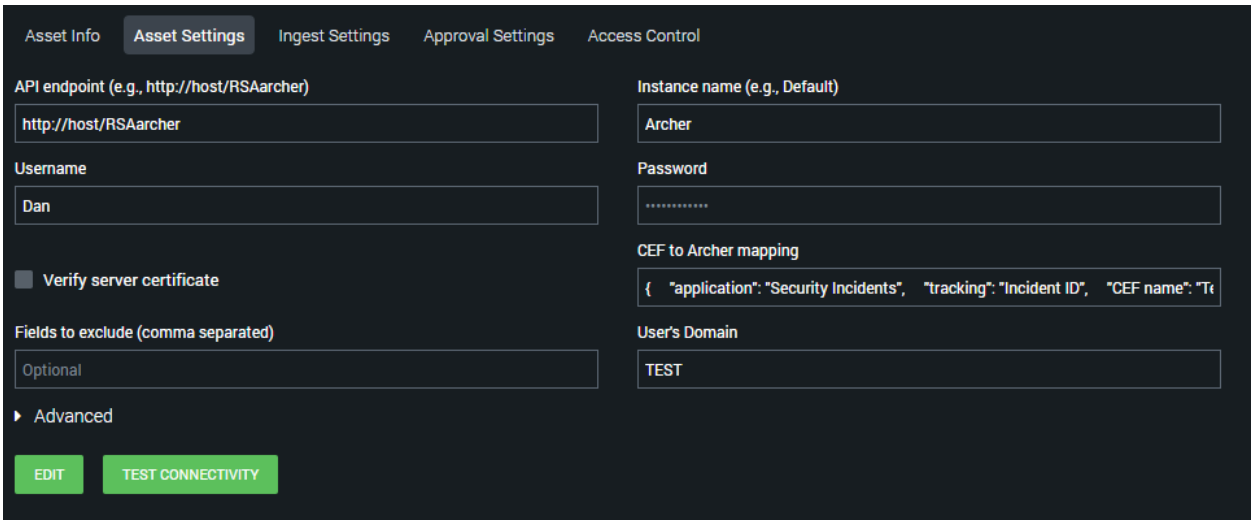
6. The message **RSA Archer configuration test SUCCESS** indicates that the asset has been correctly configured. Select **Close** to finish asset-configuration. The Splunk> Phantom integration with RSA Archer is now correctly configured and enabled.



Advanced RSA Archer Asset Configuration

Understanding the CEF to RSA Archer Mapping

When configuring an Asset for the RSA Archer App, the **CEF to RSA Archer mapping** defines how CEF fields in Splunk> Phantom map to defined application fields in RSA Archer. This mapping is used when ingesting data into Splunk> Phantom from RSA Archer, and when sending updated data to RSA Archer.



Syntax of a CEF to Archer Mapping

A CEF to RSA Archer mapping can be created in any text editor, then pasted into the mapping field on the Asset Configuration screen. The following mapping example shows the basic syntax needed to create any mapping.

(This example is fully functional and can be copied into the CEF to RSA Archer mapping field on the Asset Configuration / Asset Settings screen.)

Note: If an action contains any user details for the assignment, then please make sure the user adds the RSA Archer Username in the JSON rather than the first/last name.

```
{
    "application": "Incidents",
    "tracking": "Incident ID",
    "Status": "status",
    "Category": "category",
    "Details": "details",
    "CEF name": "Archer field name"
}
```

Required Fields in a CEF to RSA Archer Mapping

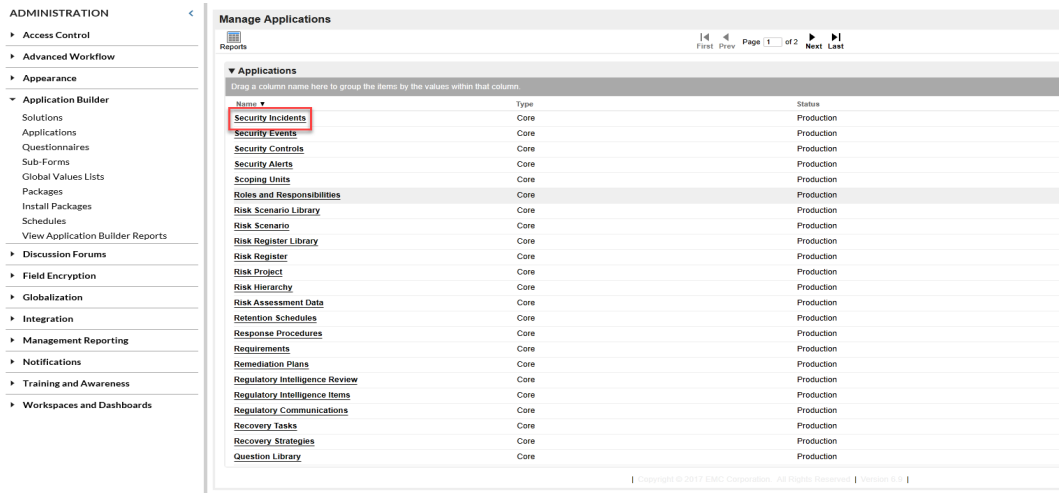
A CEF to RSA Archer mapping must include at least these two fields:

CEF field name	RSA Archer field name (examples)	Notes on RSA Archer field name
RSA Archer application	Security Incidents	The name of the application being used within RSA Archer
tracking	Incident ID	The name of the tracking ID field as defined within RSA Archer

Locating RSA Archer Applications and Field Names

The steps below cover how to locate the RSA Archer field-names that map to CEF application and CEF tracking fields, for use in a CEF to RSA Archer mapping

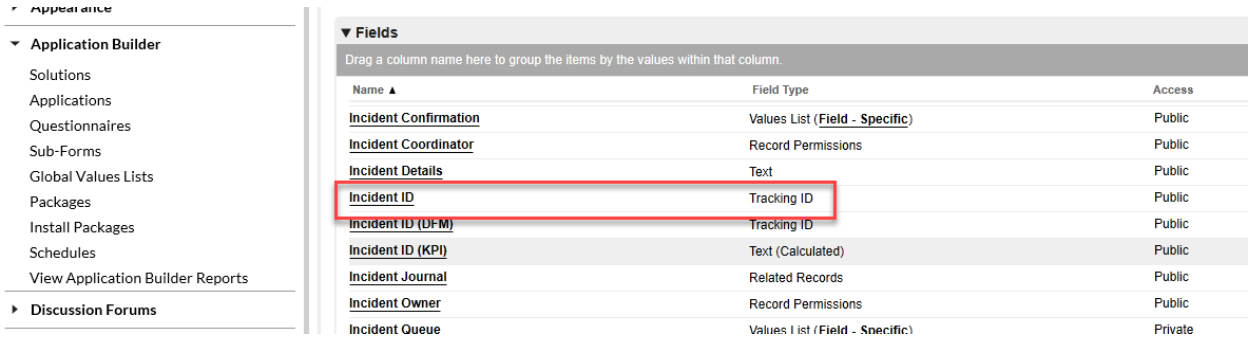
The specific RSA Archer application name that maps to a CEF **application** can be found in RSA Archer by navigating to **Administration > Application Builder > Manage Applications,** then scrolling through the **Applications** list until the specific application is found. The **Security Incidents** application used in the mapping example above is shown here, listed in RSA Archer:



Each application within RSA Archer must have one tracking field defined, as this field contains the unique ID for each data record stored in the application.

When creating a Splunk> Phantom **CEF to RSA Archer mapping**, this RSA Archer tracking field must be mapped to the CEF **tracking** field. In each RSA Archer application, the tracking field is marked with the field-type **Tracking ID**.

To locate the name of the tracking field in RSA Archer, select the application name in the **Applications** list shown above (e.g. Incidents). Next, select the **Fields** tab, then scroll through the listed fields to locate the one defined as field type **Tracking ID**. In the RSA Archer instance shown here, the Incidents application uses the field **Incident ID** as the tracking field.



In summary, the following two mappings show actual RSA Archer field names (on the right) mapped to CEF field names (on the left).

```
{
    "application": "Incidents",
    "tracking": "Incident ID"
}
```

Excluding RSA Archer Fields

Certain field types and attachments from RSA Archer are not currently supported. If they result in errors during ingestion, these field names can be added to the **Fields to exclude** list on Splunk> Phantom's Asset Configuration screen. Multiple field names are comma-separated. The previous step in this section describes how to find the specific RSA Archer field names.

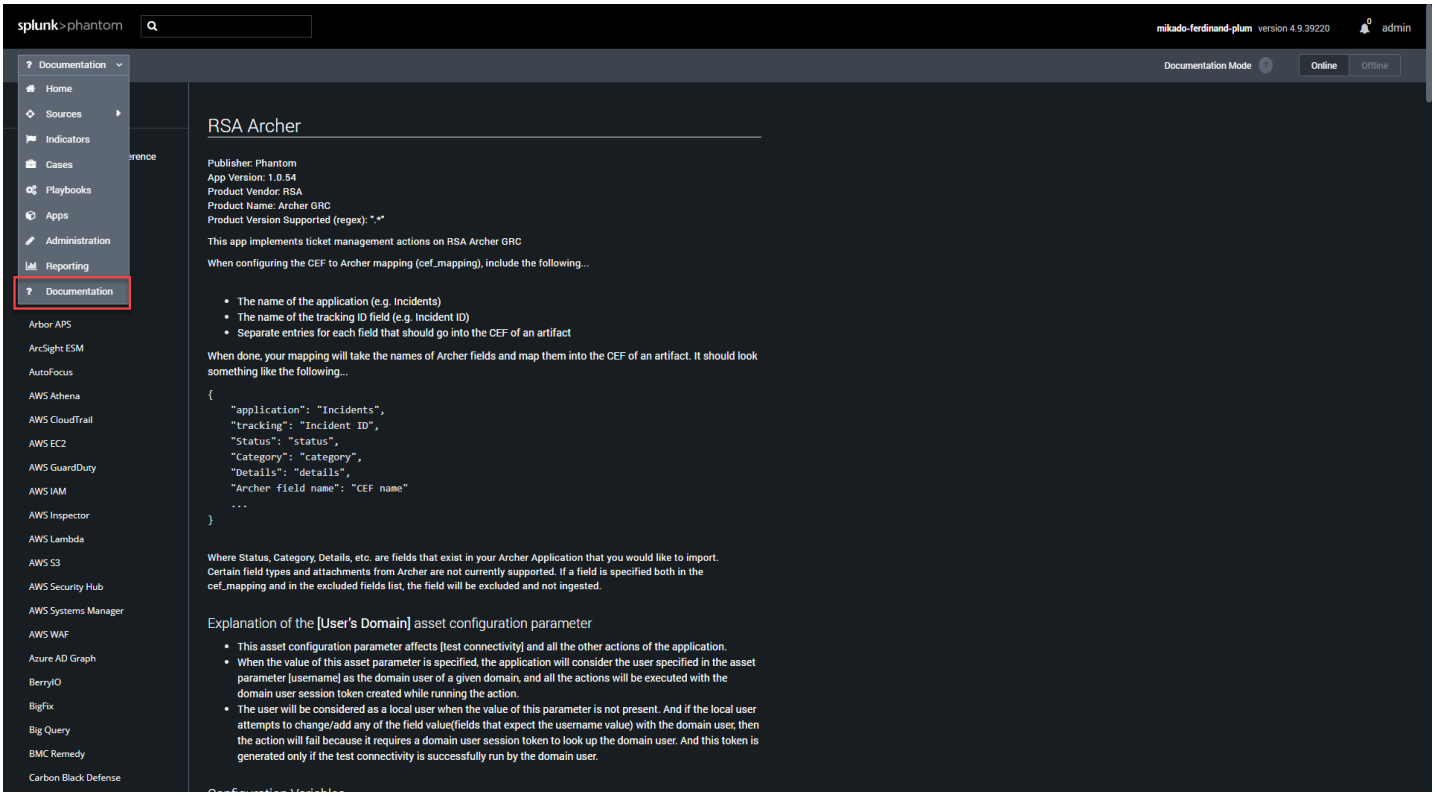
Chapter 5: Using The integration

Incidents reported in the Splunk> Phantom platform can now be accessed in the RSA Archer Security Incidents application for analysis and vice versa. In the Security Incidents application, organizations can do the following:

- Assign L1 incident handlers to review and assess the incident
- Escalate an incident to an L2 incident handler for further investigation and analysis
- Capture the timeline of the incident
- Resolve the incident and track root cause analysis and security control efficacy

Splunk> Phantom Application Features & Documentation

Comprehensive documentation for the RSA Archer App is available within the Splunk> Phantom Platform, covering supported actions and general usage of the App. It can be accessed by selecting **Documentation** from the main Splunk> Phantom menu.



Certification Environment for RSA Archer GRC

Date Tested: December 1st, 2020

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Archer	6.9 SP1	Windows 2012
Splunk> Phantom	4.9	RSA Archer App 2.0.3