RSA® NETWITNESS®
Security Operations Implementation Guide

Phantom RSA Security Analytics App

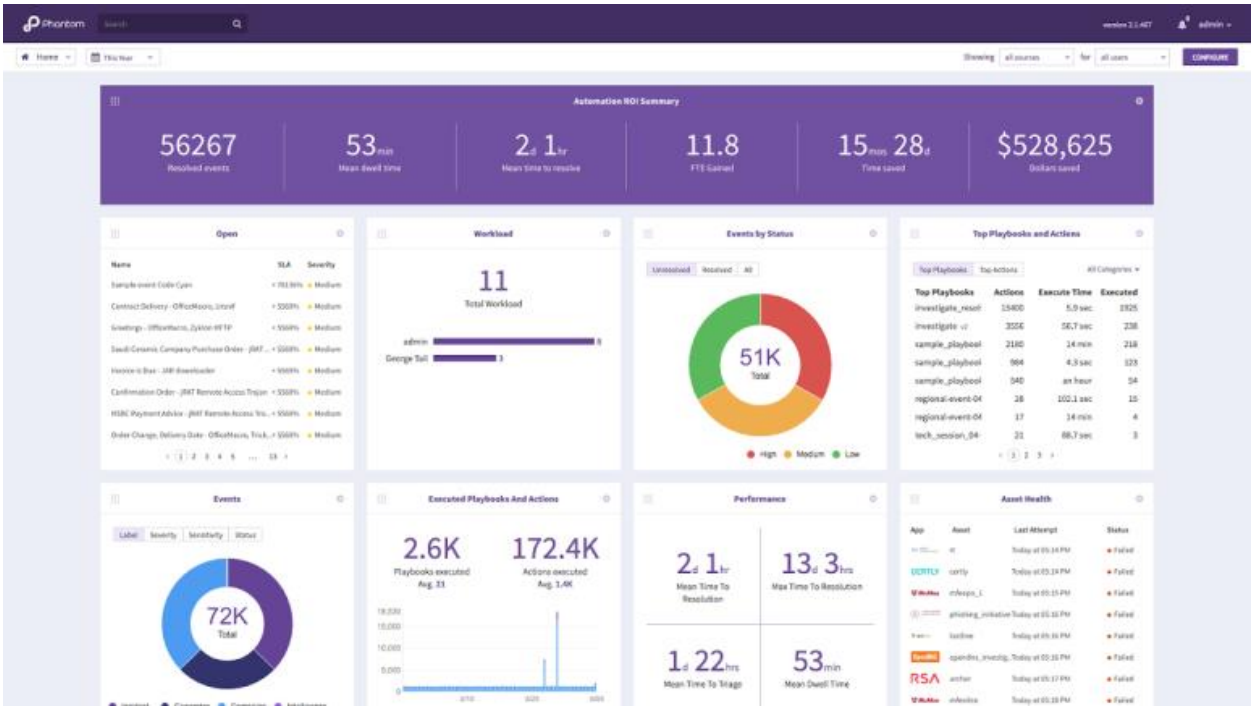
Jeffrey Carlson, RSA Partner Engineering
Last Modified: July 19th, 2017

RSA READY

Solution Summary

Phantom is a community-powered security automation and orchestration solution. The Phantom Platform integrates with existing security technologies, such as RSA Security Analytics, forming a layer of connective tissue among individual security products.

The RSA Security Analytics integration allows Phantom to work with Security Analytics Incident Management to ingest incidents, as well as perform investigative actions, by retrieving lists of incidents, alerts, events, and devices from RSA Security Analytics. These incidents and artifacts can be leveraged in Phantom automation playbooks and used in orchestration use-cases.



The RSA Security Analytics App is available within the Phantom Platform, and supports the following actions on Security Analytics:

on poll - Ingest incidents from RSA Security Analytics

list incidents - List incidents within a time frame

list alerts - List alerts for an incident

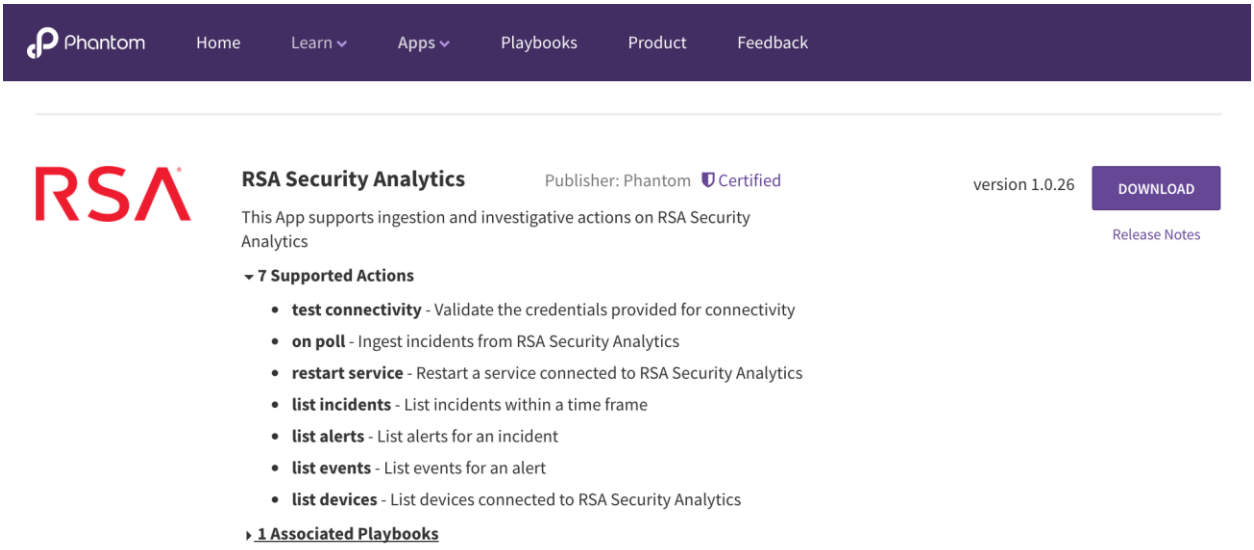
list events - List events for an alert

list devices - List devices connected to RSA Security Analytics

restart service - Restart a service connected to RSA Security Analytics

test connectivity - Validate credentials and connection configuration of an asset

The instructions in this document explain how to configure the RSA Security Analytics App on the Phantom Platform to enable this integration. Once configured, all actions supported by this App will be available within Phantom.



RSA NetWitness Product Configuration

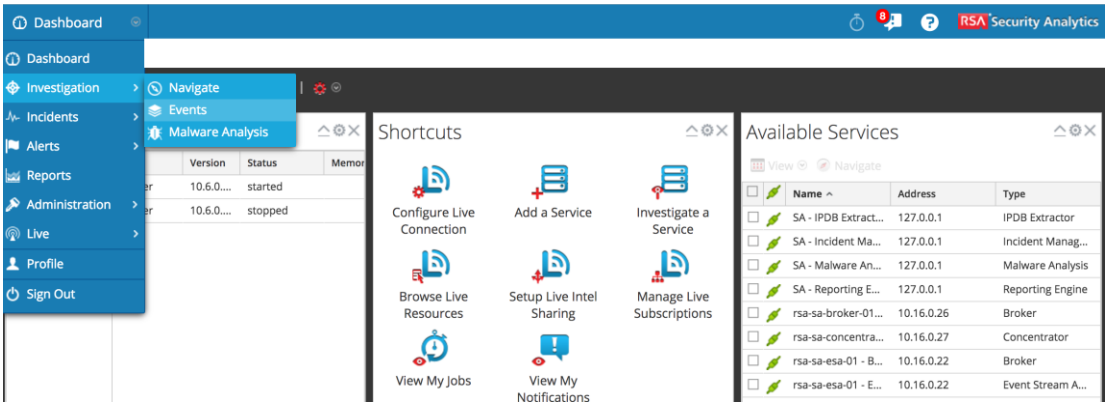
Creating Incidents

This section reviews how incidents are created within RSA Security Analytics. A later section of this document shows the incident within Phantom after ingestion.

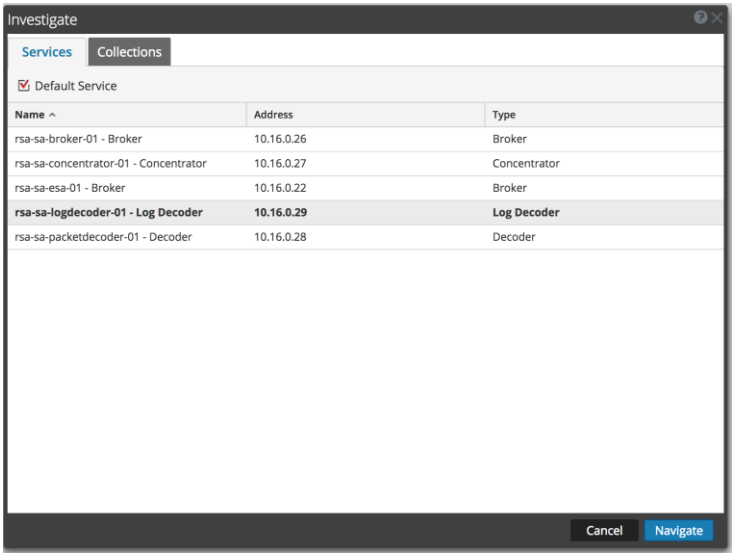
> **Note: The instructions below are provided as an example of how to create an incident in NetWitness. There are other ways that incidents are created in NetWitness, such as aggregation rules, that can be leveraged as part of this integration. For more information on this topic, please visit** https://community.rsa.com/docs/DOC-74477**.**

Once the RSA Security Analytics App is configured on Phantom, these incidents can be ingested into Phantom.

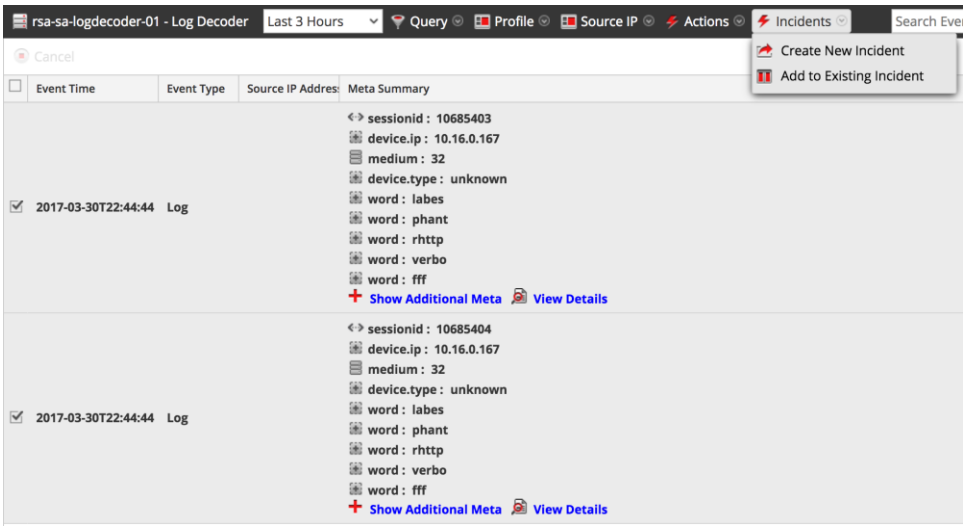
1. In Security Analytics, select **Investigation > Events**.



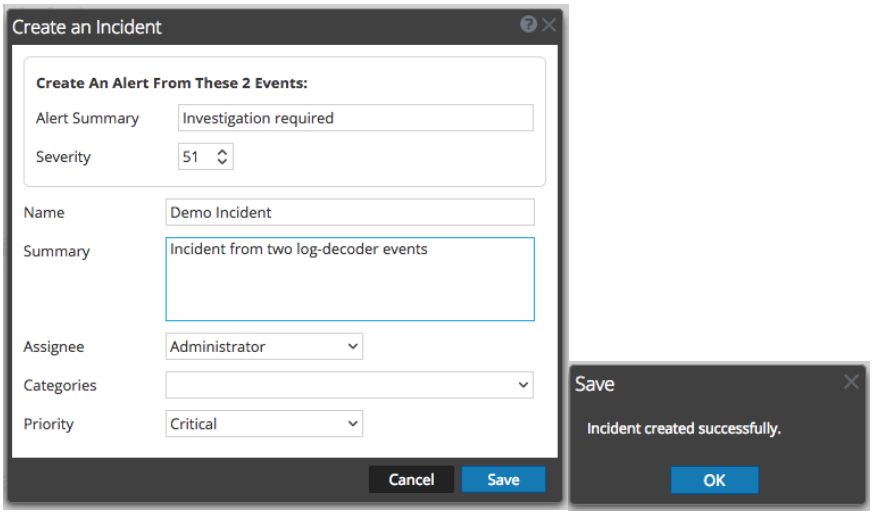
2. On the Investigate dialog, select an RSA service from which to view events (such as the Log Decoder service), then select **Navigate**.



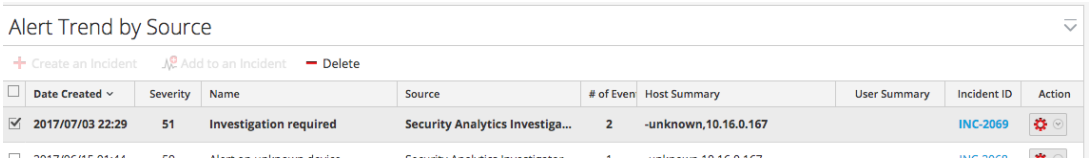
3. Within the listing of events, select one or more events to be included in a new incident. Next, select **Incident > Create New Incident**.



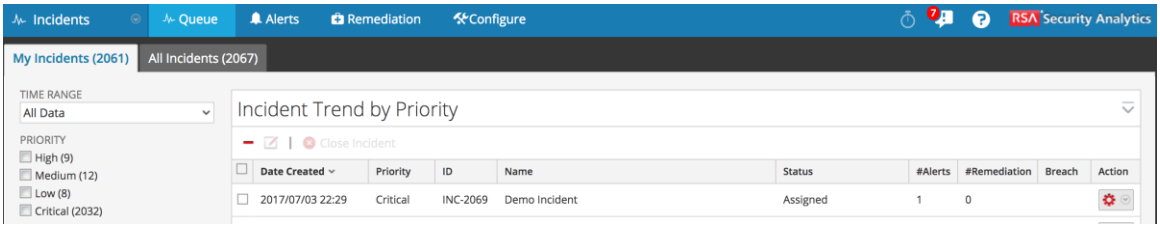
4. Fill in the Create an Incident dialog, select **Save**, then select **OK**.



5. The *Alert Trend by Source* view appears, listing the alert associated with the new incident, along with the Incident ID (INC-2069 in this example).



6. The **Incident Trend by Priority** view (**Incidents > Queue**) lists the incident that was created. Such incidents can be ingested by Phantom once the RSA Security Analytics App has been configured.



Partner Product Configuration

Before you Begin

This section provides instructions for configuring the Phantom Platform with RSA Security Analytics. 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.

All Phantom Platform components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Phantom is properly configured and secured before deploying to a production environment. For more information, please refer to the Phantom documentation or website.

Phantom Apps & Integration – Key Concepts

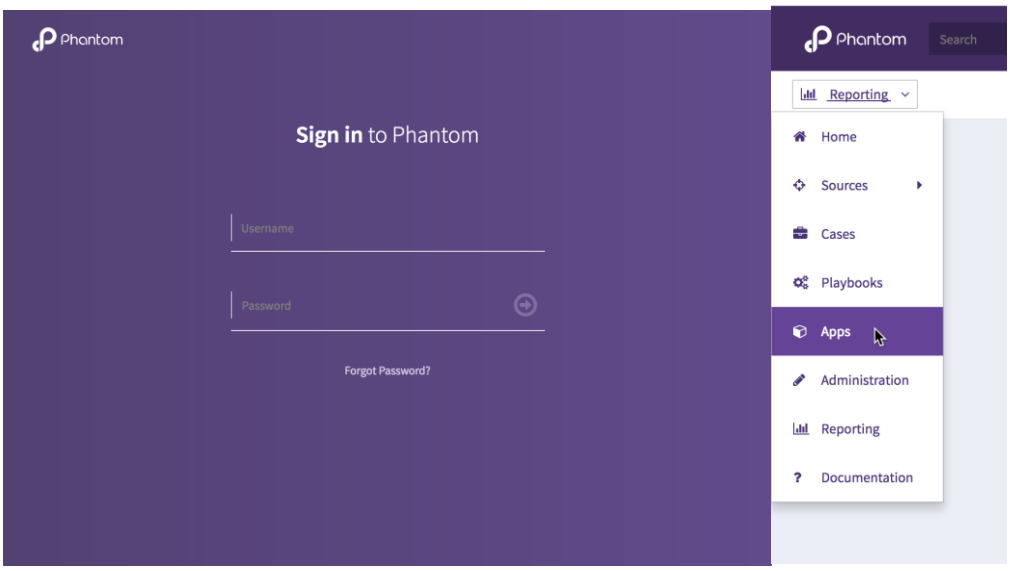
A Phantom App is designed to connect with a matching point product. An Asset is a specific connection-configuration. By default, configuring an App on Phantom involves configuring an Asset of that App. Complex deployments, such as multiple instances of a point product, may involve configuring multiple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

Phantom App	A module designed to communicate with a point product. Examples: • RSA Security Analytics App • RSA Archer App • RSA NetWitness Logs & Packets App
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.

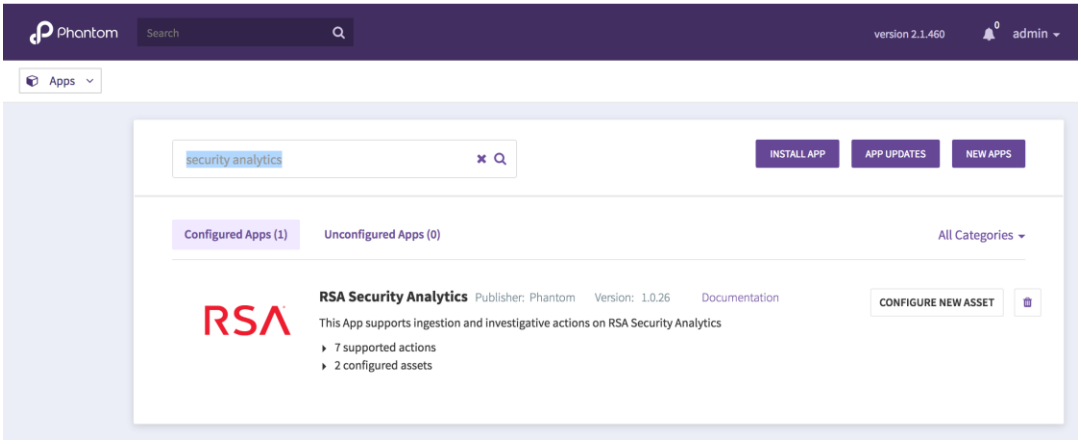
In summary, an Asset is a unique-connection-configuration of an App. In some circumstances, you may choose to configure *multiple* Assets for an App.

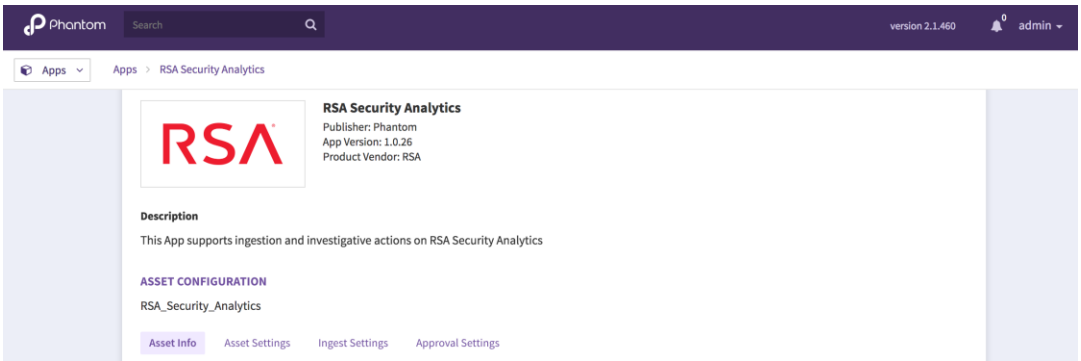
Phantom Configuration – Locating the RSA Security Analytics App

1. After signing in to the Phantom Platform, select **Apps** on the main navigation menu.



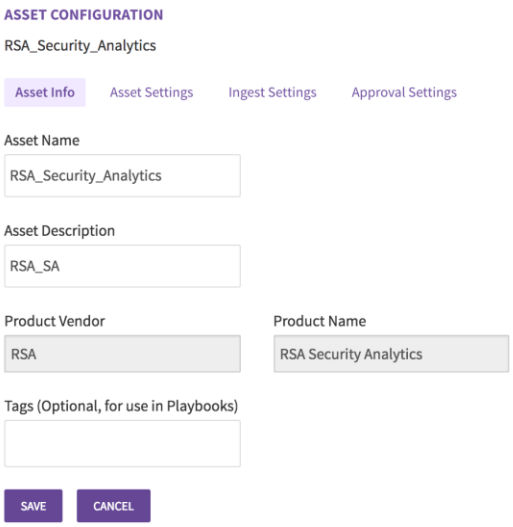
2. Enter "security analytics" in the search field to locate the RSA Security Analytics App. Select **Configure New Asset** to access the **Asset Configuration** settings.



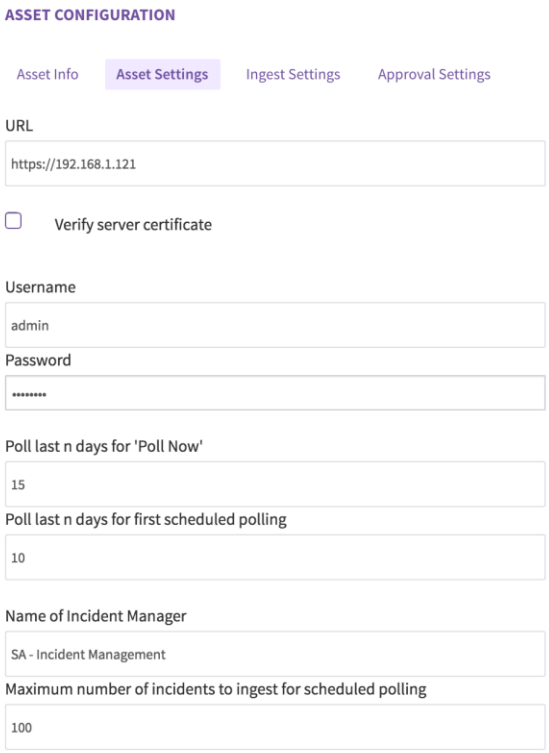


Phantom Configuration – RSA Security Analytics Asset Configuration

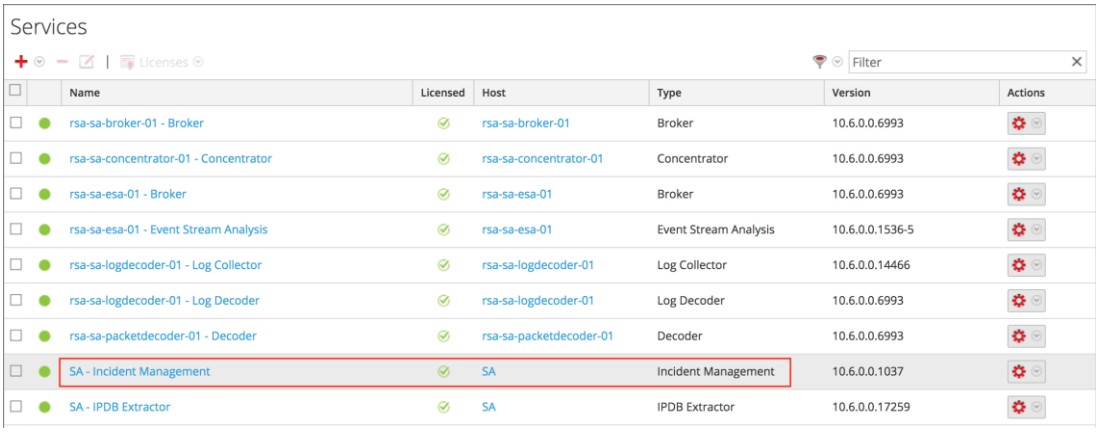
1. On the **Asset Configuration** page, select the **Asset Info** tab then enter an **Asset Name** and **Asset Description**.



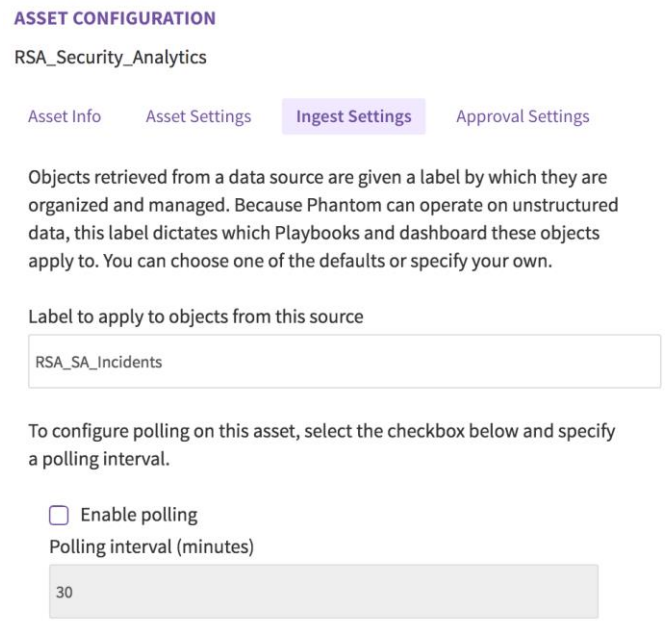
2. Select the **Asset Settings** tab, and enter the connection information for your instance of RSA Security Analytics: **URL, Username, Password,** and **Name of Incident Manager** (see below).



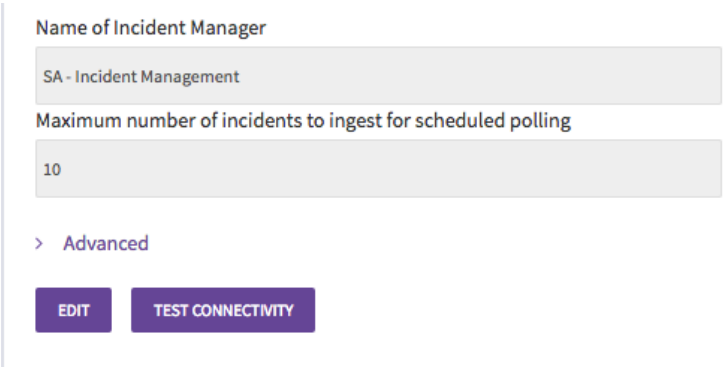
3. Note that the value for the **Name of Incident Manager** field in the Asset must exactly match the **Name** configured in RSA Security Analytics for the service type **Incident Management**, which can be viewed in the Security Analytics **Services** list.



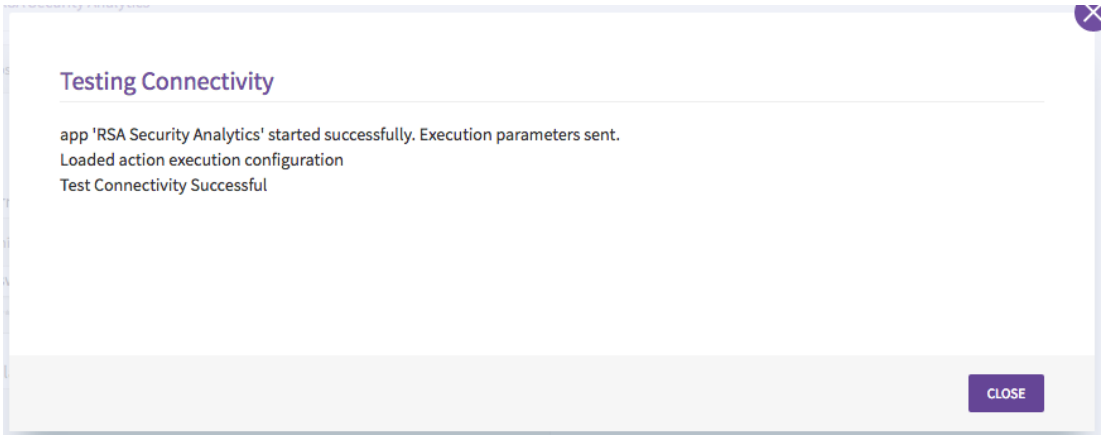
4. Select the **Ingest Settings** tab, and choose a label for data ingested from Security Analytics, or select **NEW ENTRY** in the dropdown list to create a new label. By default, ingest from Security Analytics is triggered through manual polling by a Phantom user. To configure Phantom to poll RSA Security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

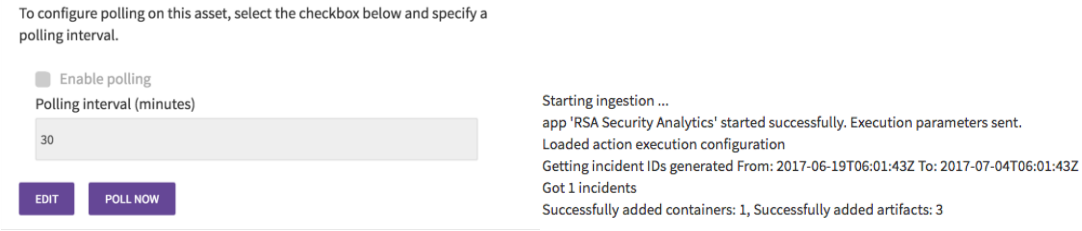


6. The message **Test Connectivity Successful** indicates that the asset has been correctly configured. Select **Close** to finish asset-configuration. The Phantom integration with RSA Security Analytics is now correctly configured and enabled.



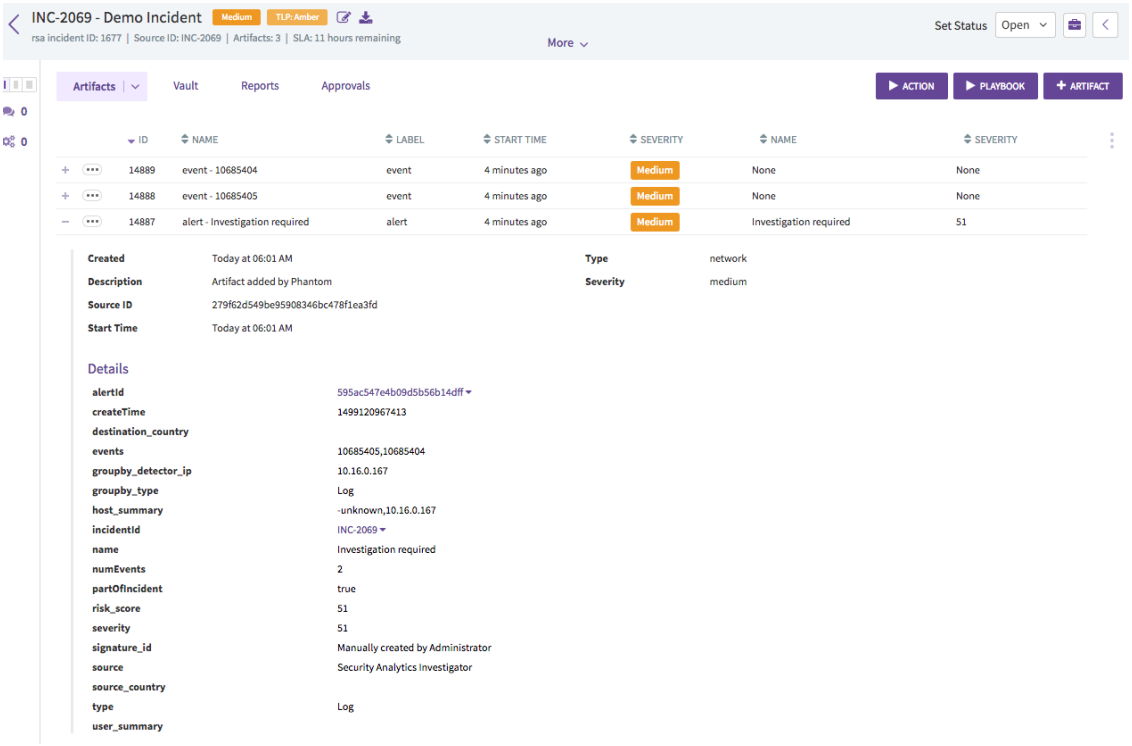
Phantom Configuration – Usage & Documentation

1. Phantom's **Poll Now** feature can be used to ingest incidents on-demand from RSA Security Analytics (SA). It can be found on the **Asset Configuration** screen, under the **Ingest Settings** tab.



2. An earlier section in this guide explained how to create a Security Analytics incident within RSA Security Analytics. Phantom ingested that incident during a polling operation, and that example incident appears in Phantom as shown below.

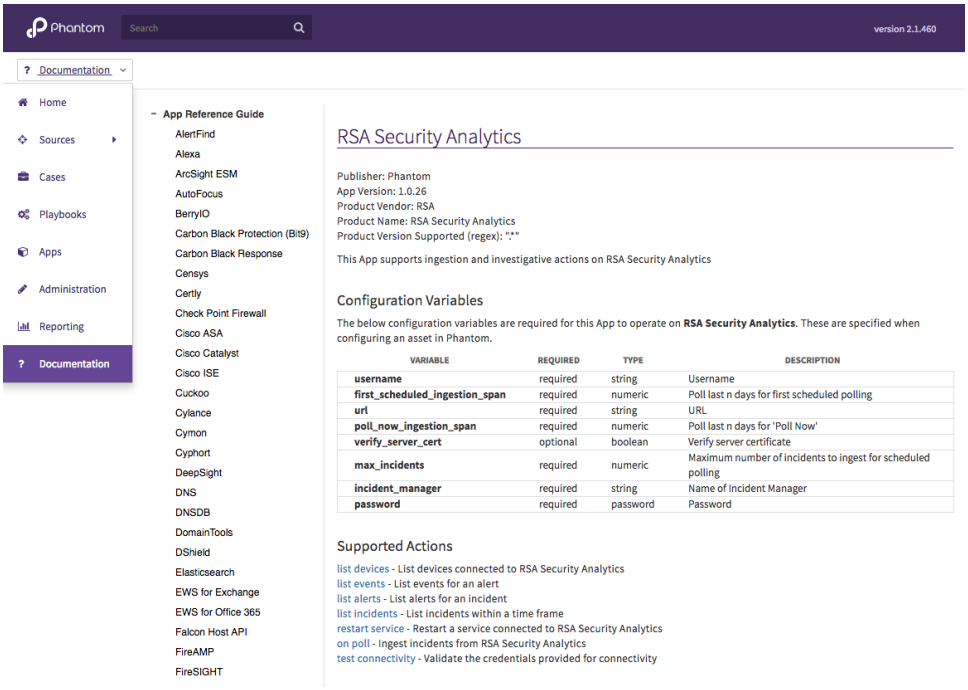
During ingestion, Phantom creates one container per incident. As seen below, the container name includes the SA Incident ID and Incident Name. The container contains one artifact for the alert, and one artifact for each event included in the incident.



3. Several additional actions are supported by the RSA Security Analytics App, along with incident ingestion.

on poll	Ingest incidents from RSA Security Analytics
list incidents	List incidents within a time frame
list alerts	List alerts for an incident
list events	List events for an alert
list devices	List devices connected to RSA Security Analytics
restart service	Restart a service connected to RSA Security Analytics
test connectivity	Validate credentials and connection configuration of an asset

4. Comprehensive documentation of supported actions and general usage of the RSA Security Analytics App is available within the Phantom Platform. The documentation can be accessed by selecting **Documentation** from the main Phantom menu.



Certification Checklist for RSA NetWitness

Date Tested: July 7h, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
Phantom Platform	2.x	RSA Security Analytics App

RSA NetWitness Test Case	Result
RSA NetWitness Incident Management	
Retrieve NetWitness Incidents	✓
Retrieve NetWitness Alerts	✓
Retrieve NetWitness Events	✓
Retrieve NetWitness Device Info	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function