RSA® NETWITNESS®
Security Operations Implementation Guide

Swimlane 2.x

Jeffrey Carlson, RSA Partner Engineering
Last Modified: 05/01/2017

RSA READY

Solution Summary

The RSA NetWitness integration allows Swimlane to search within NetWitness for any traffic relating to an IP address within a specific time frame and attach the relevant PCAP to a record. The following steps will allow a Swimlane user to import the official RSA NetWitness Swimlane bundle and use its functionality within their specific workflow or playbook.

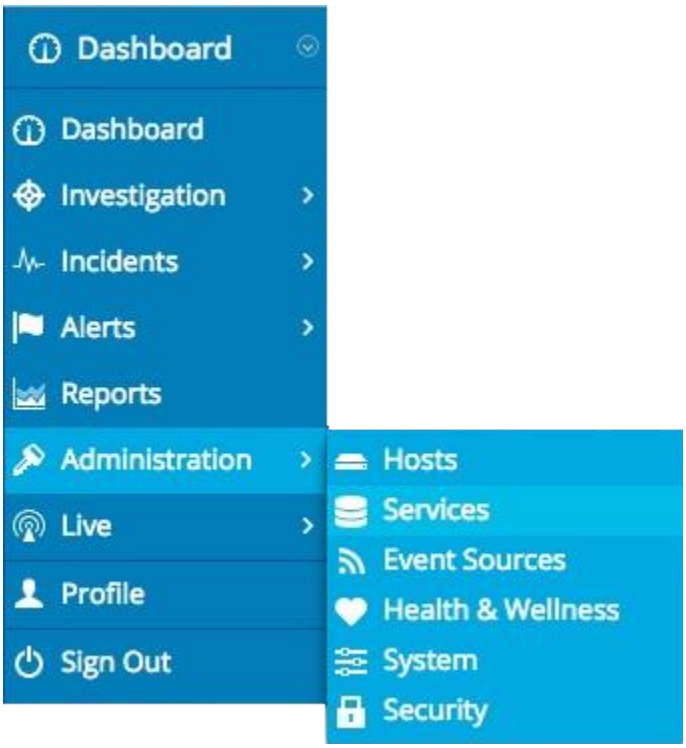
RSA NetWitness Configuration

RSA NetWitness API Broker Account Creation

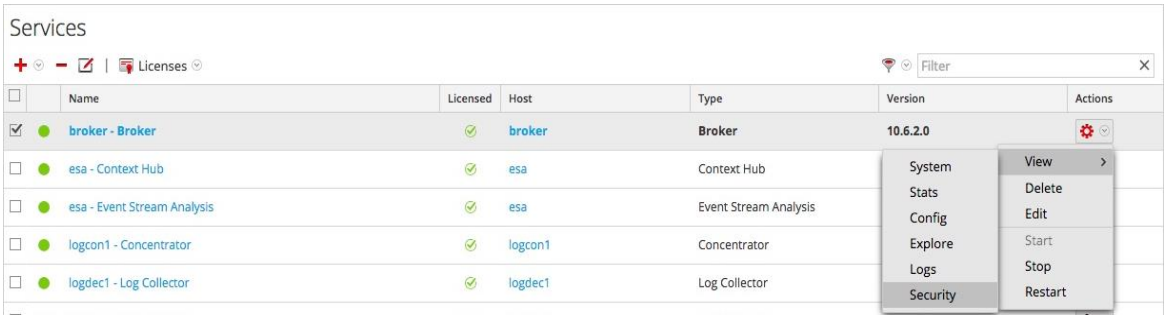
In order for the Swimlane integration to successfully connect to the RSA NetWitness Broker service, an API account needs to be created. The following steps show how to create the API service account used for Swimlane.

RSA NetWitness Broker Configuration

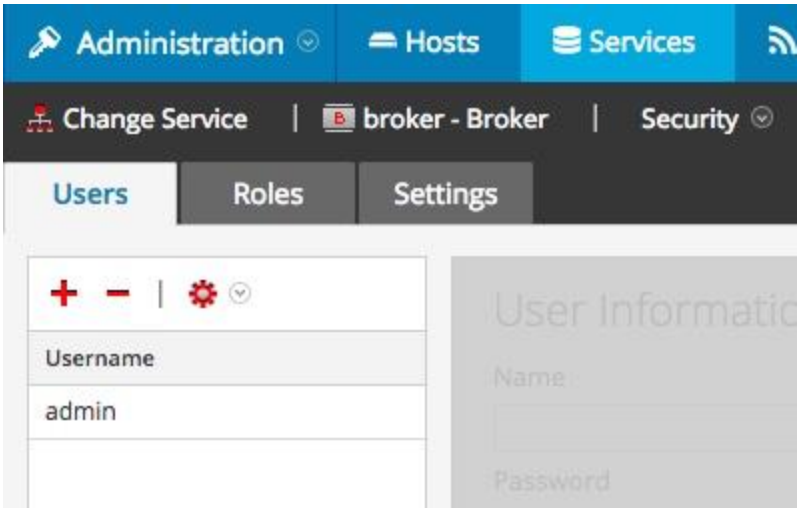
1. From the NetWitness Dashboard, Select **Administration > Services**.



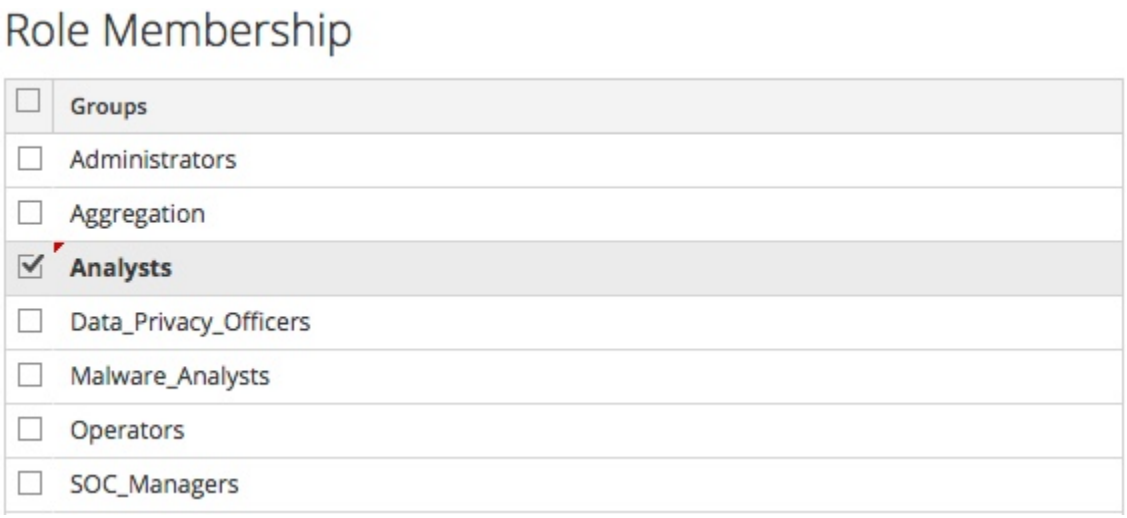
2. In **Services**, Select the **Broker**. Under **Actions**, click **View** and **Security**



3. Within the Security settings of the Broker, Select the + button to add the new API user.



4. Fill out the **User Information** and select the **Analyst** Role Membership and click **Apply**.



5. The API service account is now created. Swimlane will use this account to authenticate to the NetWitness Broker service in order to successfully launch the PCAP retrieval integration.

RSA NetWitness ESA Syslog Alert Configuration

In order to use RSA NetWitness Event Stream Analysis (ESA) as an ingestion source for Swimlane, ESA alerting must be configured to send syslog alerts to the Swimlane server. The RSA NetWitness documentation on how to setup the alerting the configuration for ESA can be found here:

https://community.rsa.com/docs/DOC-74872

To configure ESA to send events and consolidate logs in syslog format to a syslog server, consult the RSA NetWitness **System Configuration Guide** found here:

https://community.rsa.com/docs/DOC-74398

Swimlane can leverage your existing syslog architecture in order to receive syslog messages from ESA. If there is no existing architecture in place, Swimlane can act as a syslog receiver. Follow the steps in the **Swimlane Configuration – RSA NetWitness ESA Syslog Ingestion** section of this document in order to configure Swimlane to accept logs from ESA.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Swimlane with RSA NetWitness. 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.

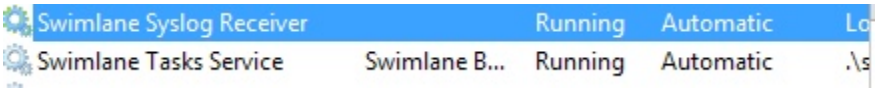
All Swimlane components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

> **! 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 Swimlane is properly configured and secured before deploying to a production environment. For more information, please refer to the Swimlane 2.x documentation or website.**

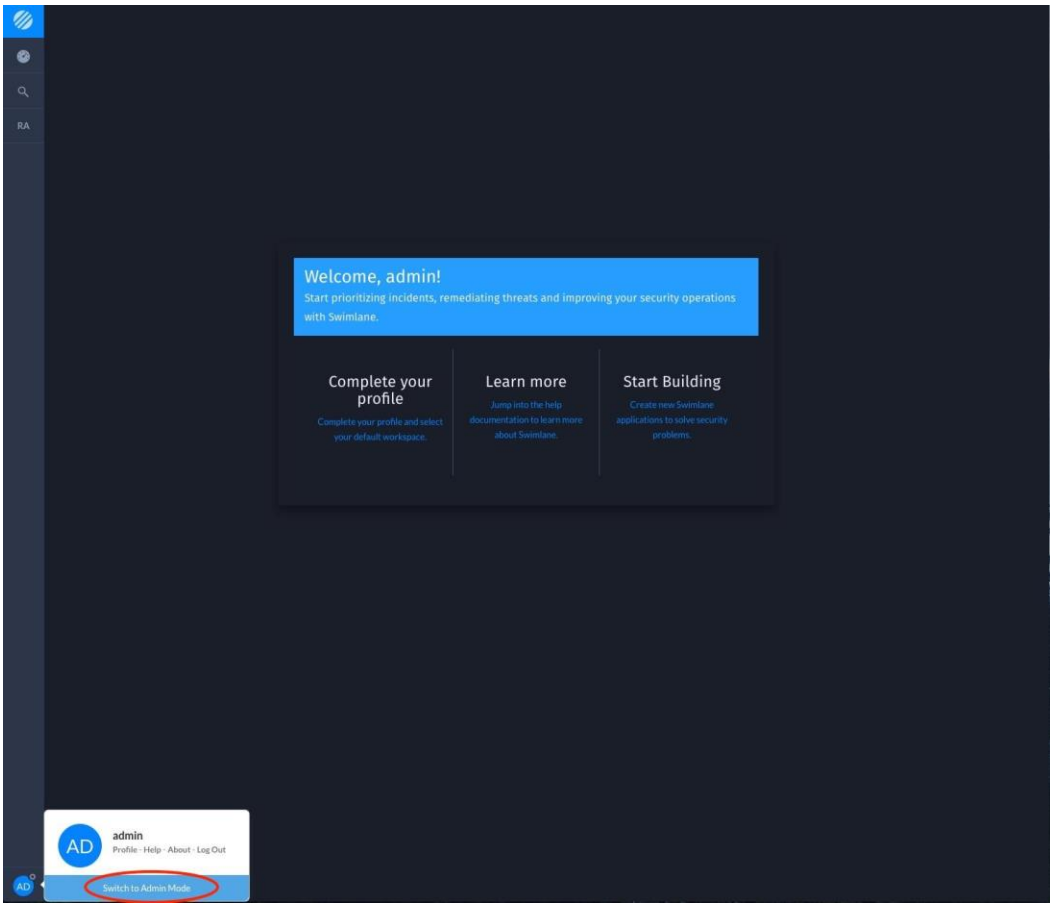
Swimlane Configuration – RSA NetWitness ESA Syslog Ingestion

The following steps will provide instructions on how to install, configure, and deploy the Swimlane RSA NetWitness ESA syslog ingestion.

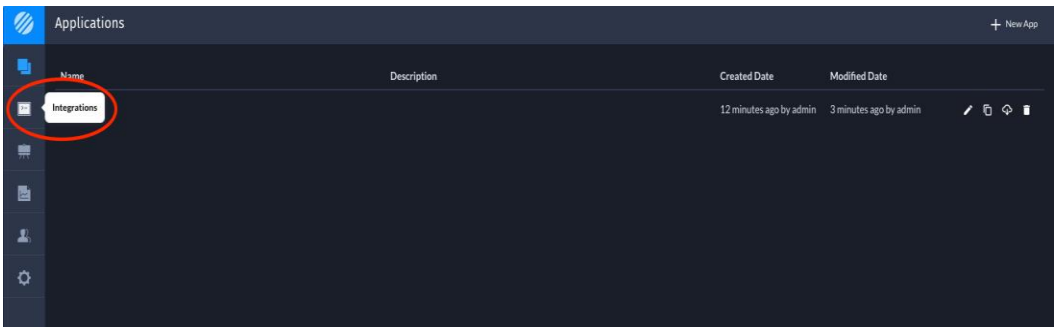
1. In order for Swimlane to receive the ESA alerts, the syslog service needs to be started on the Swimlane server. Change the **Server IP** and **Server Port** within ESA to match the Swimlane IP and port of the syslog receiver.



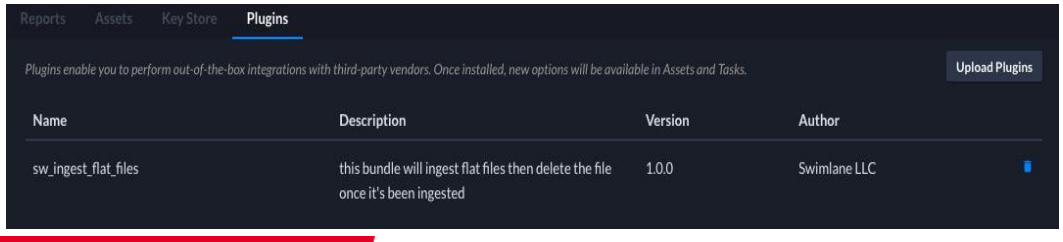
2. Login in to Swimlane and go to **Admin Mode:**



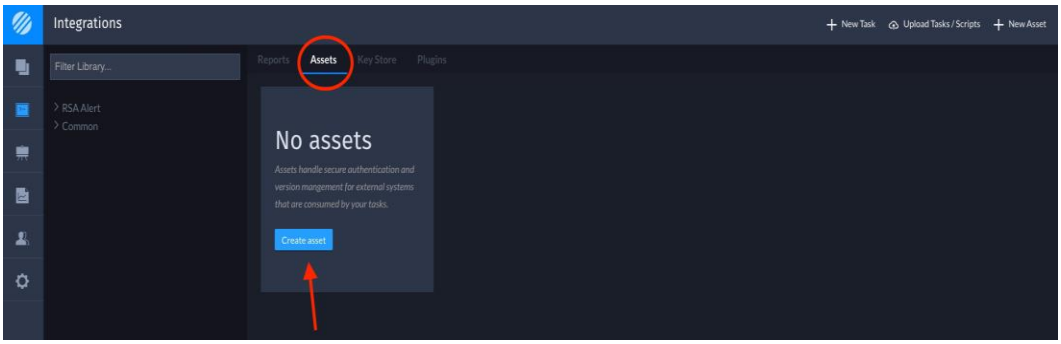
3. Once in Admin mode, click on the **Integrations** button on the left toolbar:



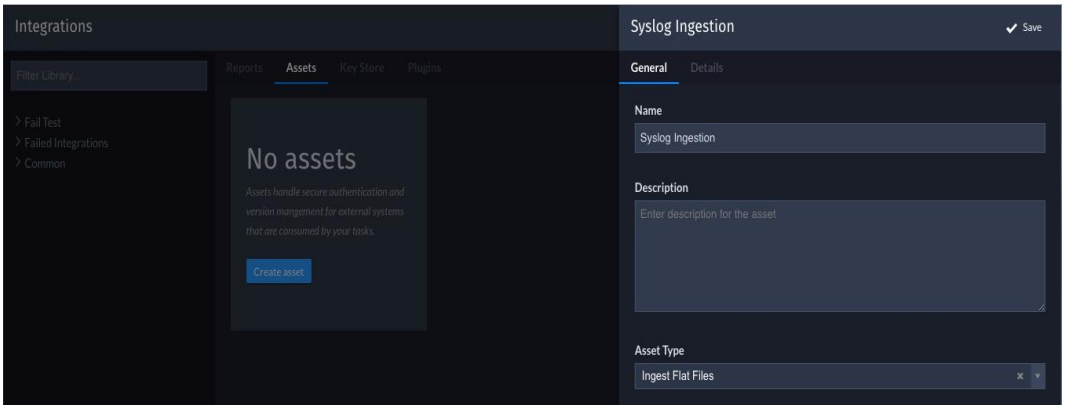
4. Within **Integrations**, click on **Upload Plugins** and choose the official **Flat File Ingest** bundle. You should see the plugin show up once it is installed.



5. Now that the plugin has been installed, we can create an **Asset**. The Asset for the **Flat File Ingestion** designates which folder and log files will be ingested into Swimlane.



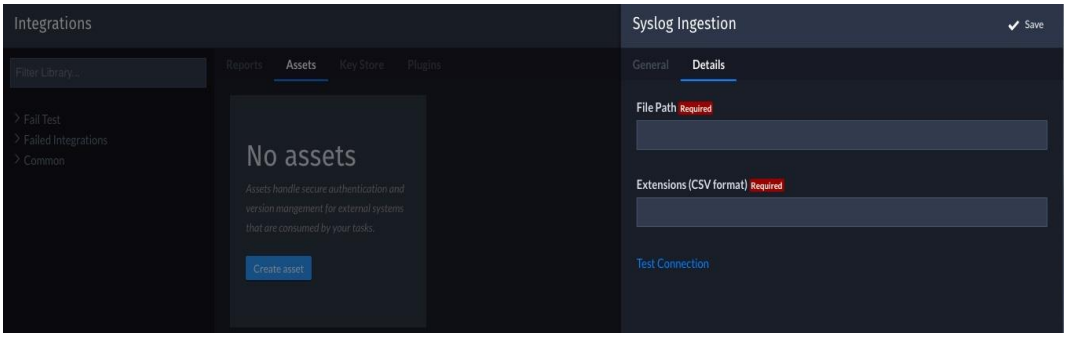
6. Set the asset name and select the asset type, as shown below.



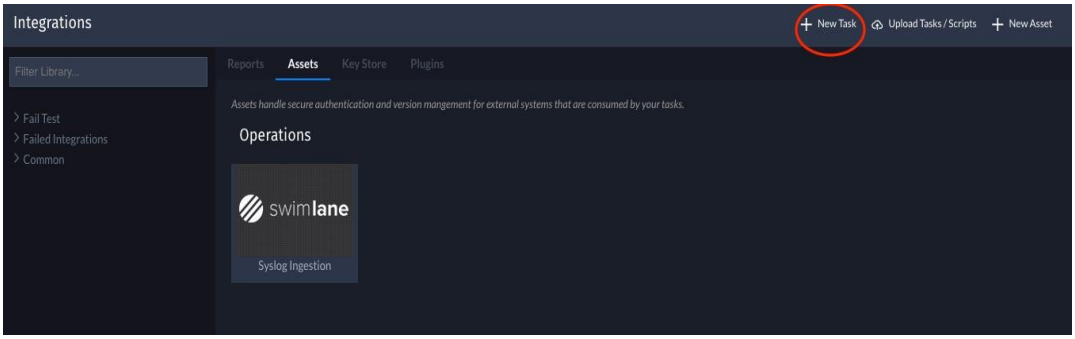
7. Click the **Details** tab and fill in **File Path** and the **Extension fields**. Set the **File Path** to the directory where the syslog files are written to. The **Extension** field is a comma separated list of the extension of the syslog file. For example:

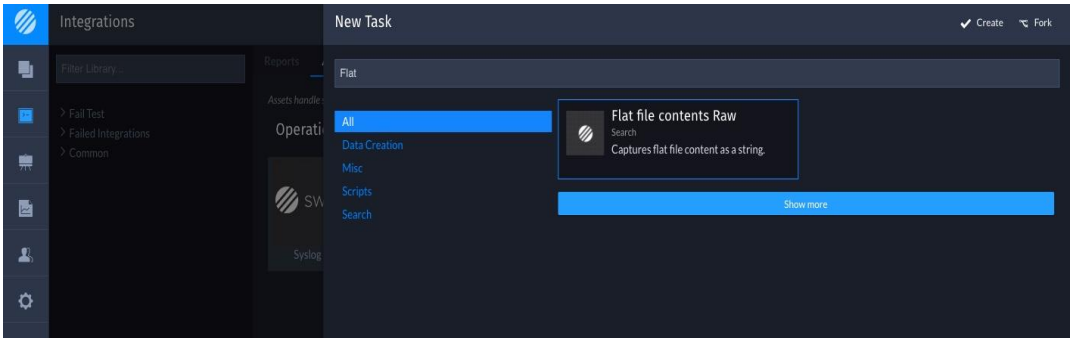
   File Path: c:\syslog

   Extension: .log

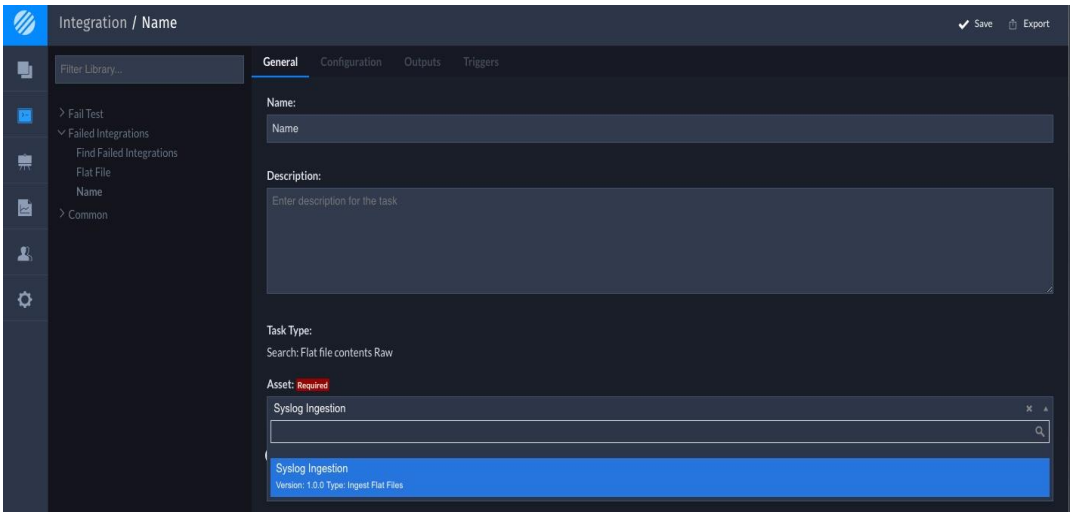


8. Once the Asset is saved, you can now create a task associated with the NetWitness Broker. Click on the **New Task** button, then select the **Flat Files Content Raw** task. Once selected, name the task and select the **Related Application** and click **save**.



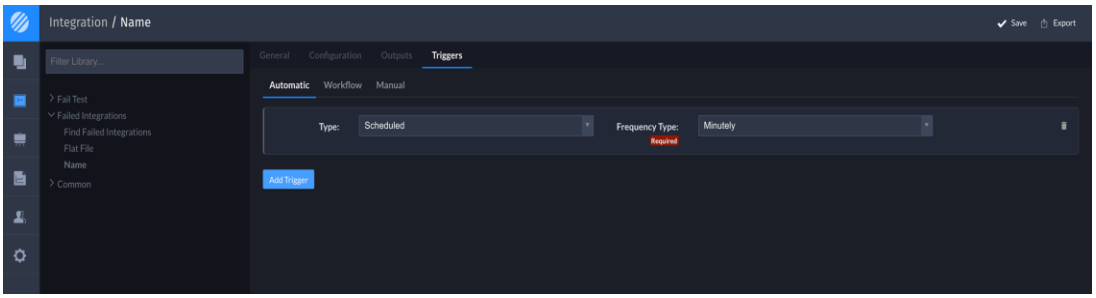


9. Next, set the **Asset** to the Flat File Asset that we created in step 7 within the **General** tab.



10. There are no **Configuration** options to set for this integration. Move on to the **Outputs** tab and map the data expected out of ESA into fields created within the subsequent Swimlane application.

11. After the **Outputs** are configured, move on to the **Triggers** tab. This task should be configured using an **Automatic** Trigger setup on **Minute** schedule.

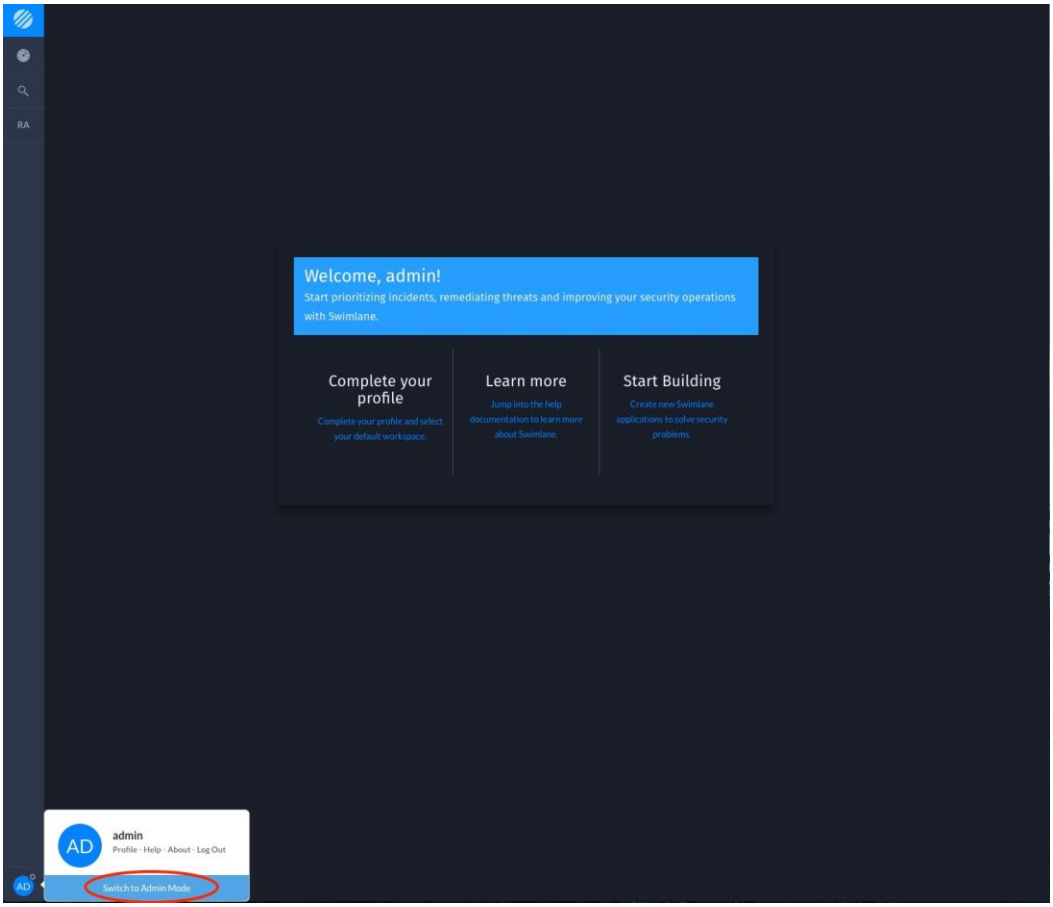


Swimlane Configuration – RSA NetWitness PCAP Retrieval

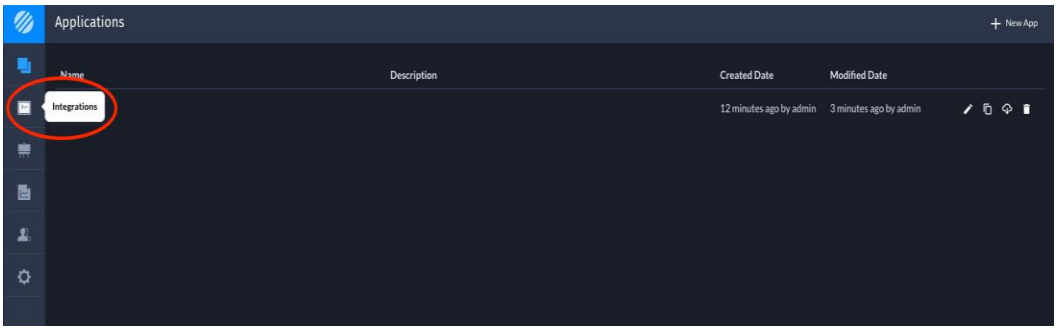
The following steps will provide instructions on how to install, configure, and deploy the Swimlane RSA NetWitness PCAP retrieval integration.

RSA NetWitness PCAP retrieval integration.

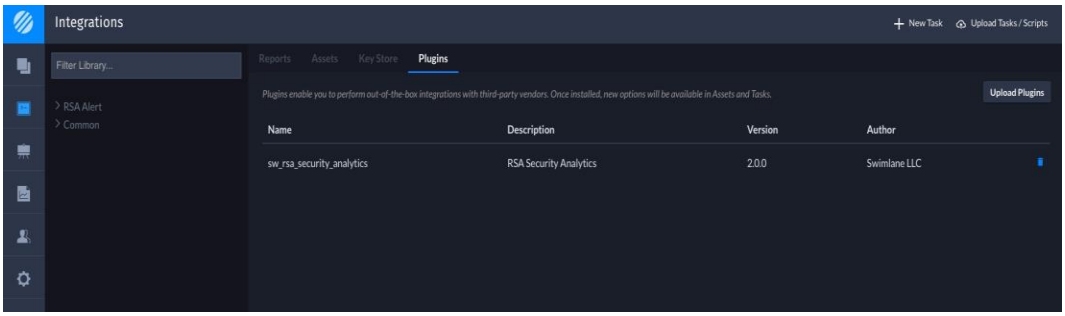
1. Login in to Swimlane and go to **Admin Mode:**



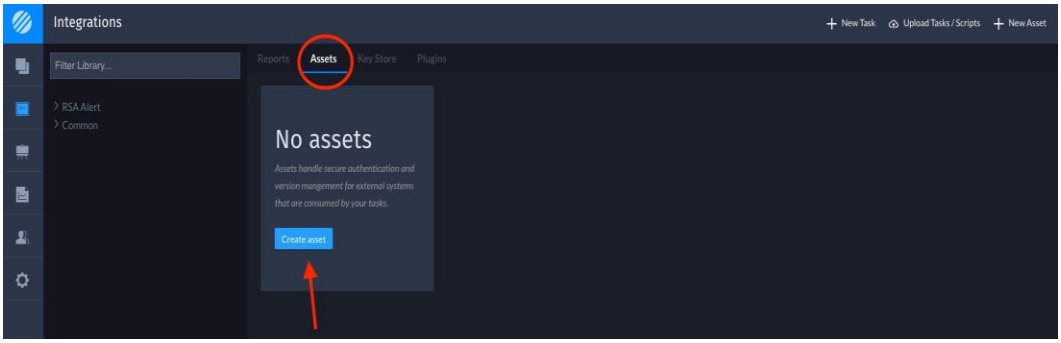
2. Once in Admin mode, click on the **Integrations** button on the left toolbar.



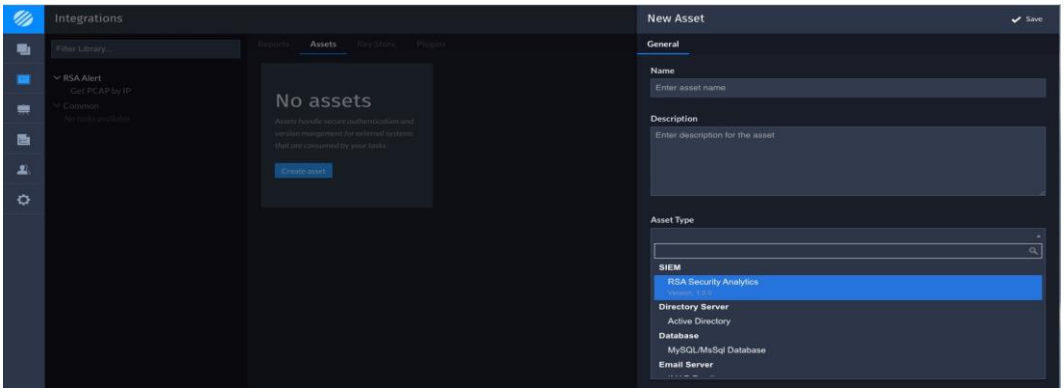
3. Within **Integrations**, click on **Upload Plugins** and choose the official **Swimlane RSA NetWitness** bundle. You should see the plugin show up once it is installed.



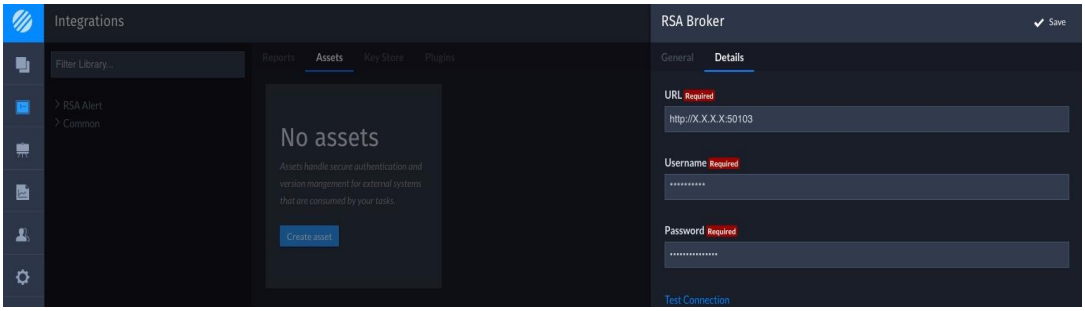
4. Now that the plugin has been installed, we can create an **Asset**. The **Asset** designates which NetWitness service Swimlane talks to. This specific task needs to be able to communicate with the NetWitness Broker.



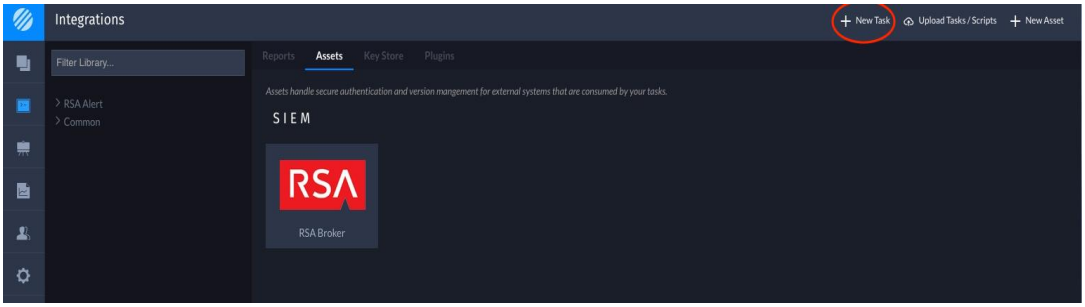
5. Set the asset name and select the asset type, as shown below.

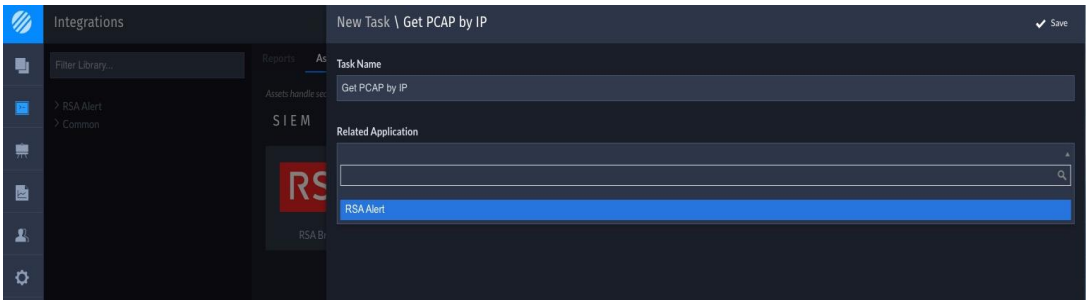


6. Click the **Details** tab and fill in the information for URL, Username, and Password. Use the correct scheme to connect to the NetWitness Broker on either **http** or **https**. The standard default port for the Broker is 50103. Use the Username and Password of the API service account created in the **RSA NetWitness API Broker Account Creation** section of this document.

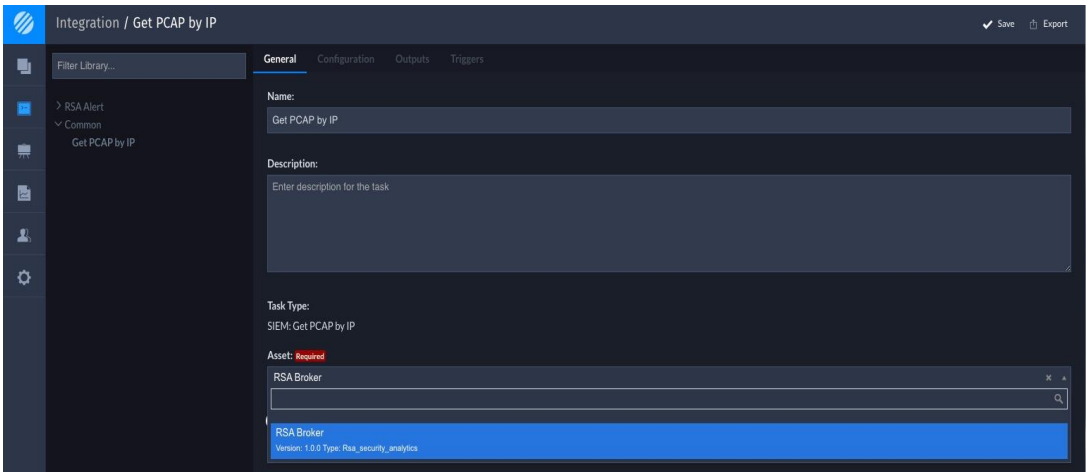


7. Once the Asset is saved, you can now create a task associated with the NetWitness Broker. Click on the **New Task** button, then select the **Get PCAP by IP** task. Once selected, name the task and select the **Related Application** and click **save**.

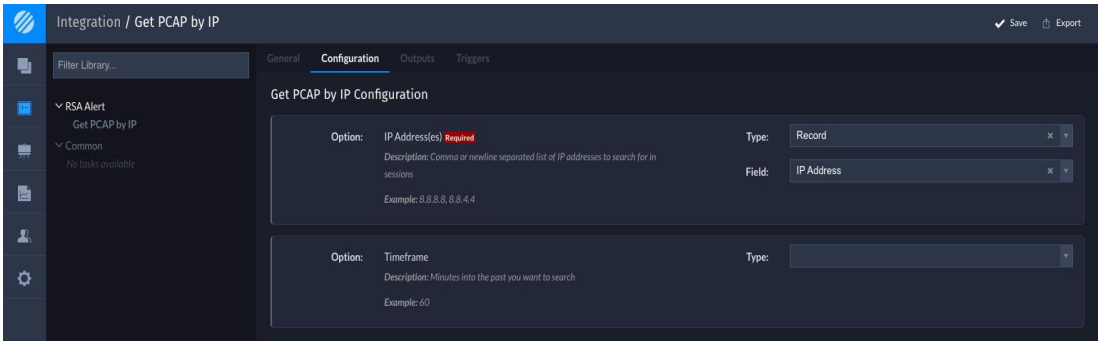




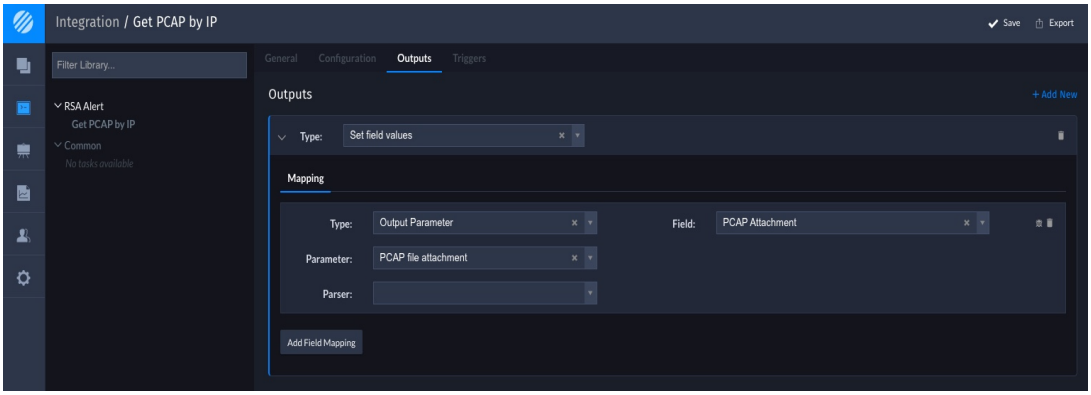
8. Next, set the Asset to the NetWitness Broker that we created in step 4 within the **General** tab.



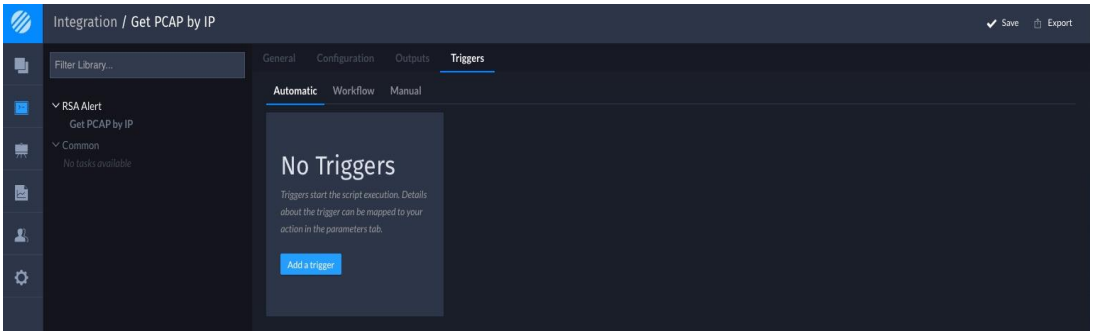
9. Now, move to the **Configuration** tab. Set the IP address or addresses to search for within NetWitness. For most deployments, the **Type** would be set as **Record**, and the **Field** would be set to a field within the record that is populated with one or more IP addresses. An example is the **Source or Destination IP** from an alert. The **Timeframe** field is optional. The default setting is 60 minutes. The **Type** can be set to **Static** and the **Field** value can be set to any number of minutes in the past the user wants to search.



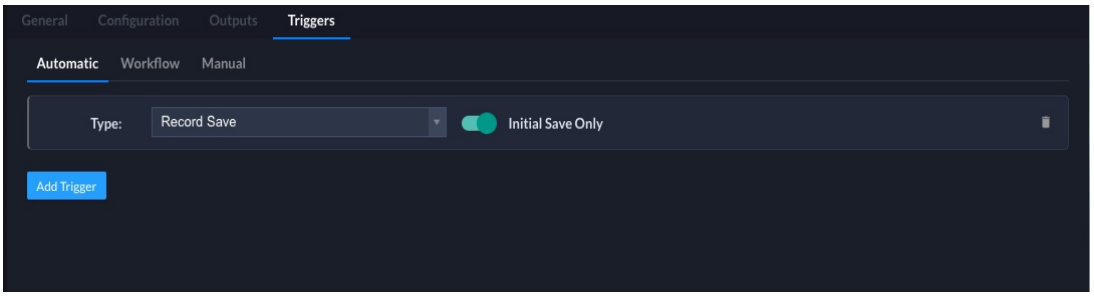
10. Once the **Configuration** tab is complete, click on the **Outputs** tab. Follow the example to set the **Output Parameter** to the **PCAP file attachment**. Set the output field to be an attachment field within the associated application. In this example the attachment field is called **PCAP Attachment**.



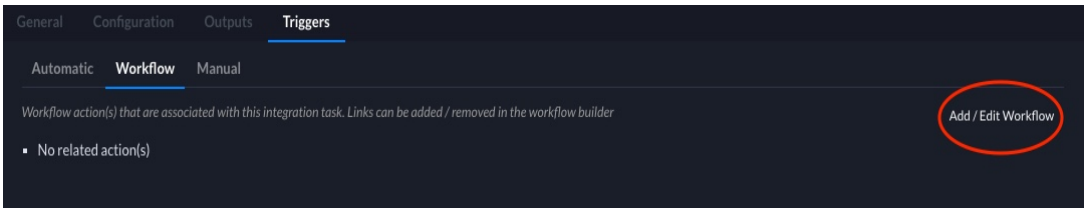
11. Click on the last tab **Triggers**. This task can either be run automatically based on some workflow criteria, or as a manual button configured in the associated application.



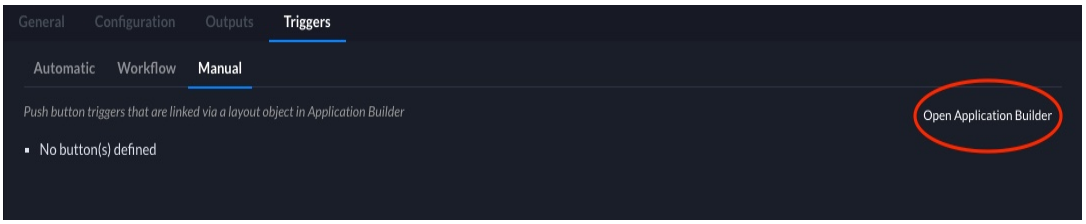
12. If using an **Automatic** trigger, configure the trigger to run on **Record Save** and set the toggle for **Initial Save Only**.



13. If using a **Workflow** trigger, configure the workflow in the workflow editor.



14. If using a **Manual** trigger, configure a manual integration within the Application editor.



Certification Checklist for RSA NetWitness

Date Tested: April 14th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6	Virtual Appliance
Swimlane	2.x	Virtual Appliance

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	✓
Query NetWitness for User Info (usernames, user behavior)	N/A
Query NetWitness for Specific Meta (Other)	N/A
Retrieve NetWitness Log/Packet Data	N/A
Retrieve NetWitness PCAP files	✓
Alerting / Incident Creation	
NetWitness alert via syslog	✓
NetWitness alert via email	N/A
NetWitness alert via ESA/scripting	N/A
Send alert to NetWitness (Syslog, CEF, or custom parser)	N/A
RSA NetWitness Intel Feeds	
Update NetWitness Intel Feed (CSV, STIX)	N/A

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