RSA® NETWITNESS®
Security Operations Implementation Guide

Phantom RSA NetWitness Logs & Packets App

Jeffrey Carlson, RSA Partner Engineering

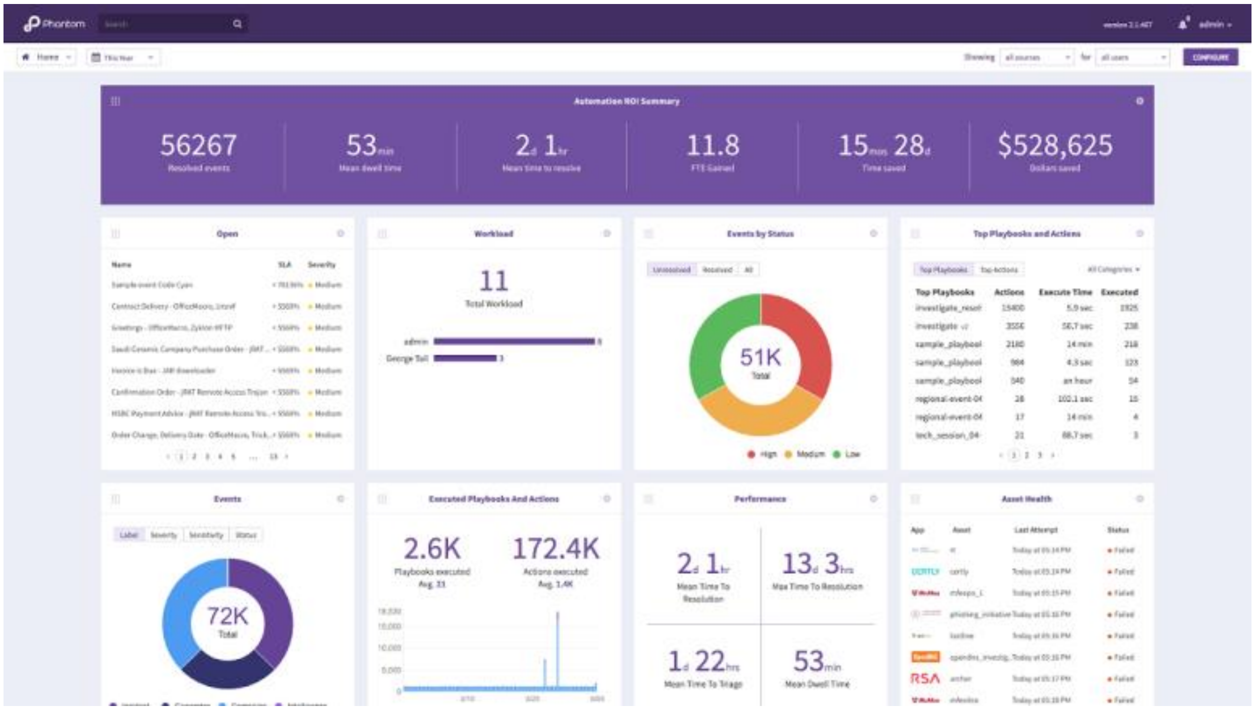
Last Modified: July 19th, 2017

RSA READY

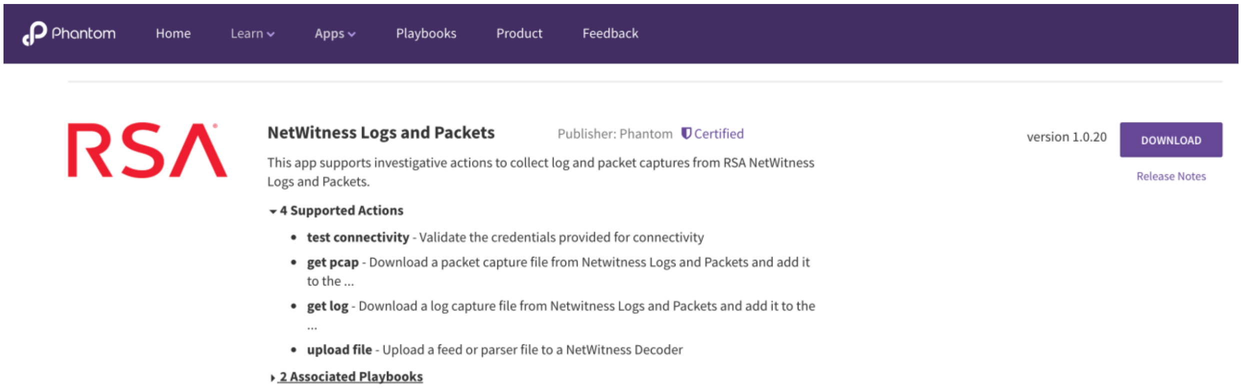
Solution Summary

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

The RSA NetWitness Logs & Packets integration allows Phantom to retrieve log and packet captures from NetWitness. These log and packet captures can be leveraged in Phantom automation playbooks and used in orchestration use-cases. Phantom can also update NetWitness Decoder configurations by uploading new feed or parser files to the log-decoder or packet-decoder.



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



NetWitness Logs and Packets Publisher: Phantom Certified

This app supports investigative actions to collect log and packet captures from RSA NetWitness Logs and Packets.

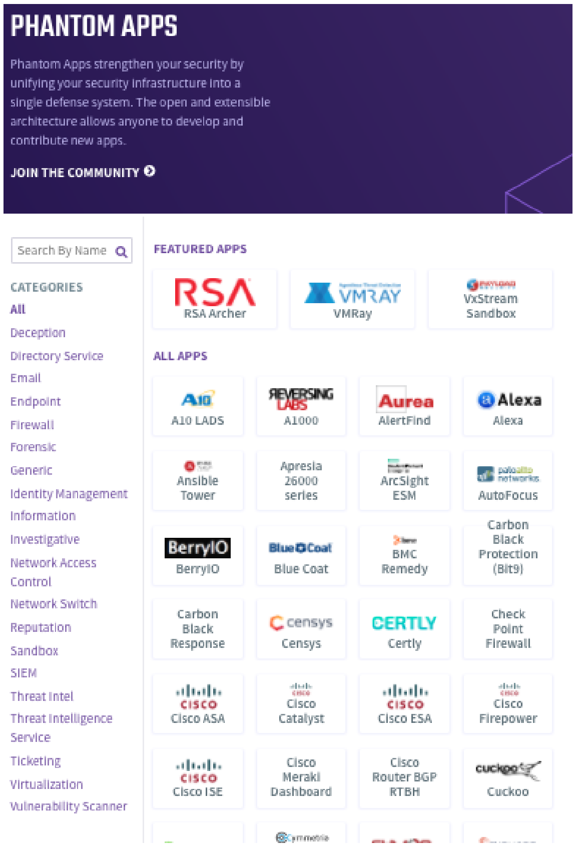
4 Supported Actions

- **test connectivity** - Validate the credentials provided for connectivity
- **get pcap** - Download a packet capture file from Netwitness Logs and Packets and add it to the ...
- **get log** - Download a log capture file from Netwitness Logs and Packets and add it to the ...
- **upload file** - Upload a feed or parser file to a NetWitness Decoder

2 Associated Playbooks

The RSA NetWitness Logs & Packets App is available within the Phantom Platform and on the Phantom community portal. The App supports the following actions using NetWitness Logs & Packets:

get log	Download a log capture file from a NetWitness log-decoder, and add it to the vault on Phantom
get pcap	Download a packet capture file from a NetWitness packet-decoder, and add it to the vault on Phantom
upload file	Upload a feed or parser file to a NetWitness Decoder
test connectivity	Validate credentials and connection configuration of an asset



Phantom Apps strengthen your security by unifying your security infrastructure into a single defense system. The open and extensible architecture allows anyone to develop and contribute new apps.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Phantom Platform 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 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 & Assets – Key Concepts

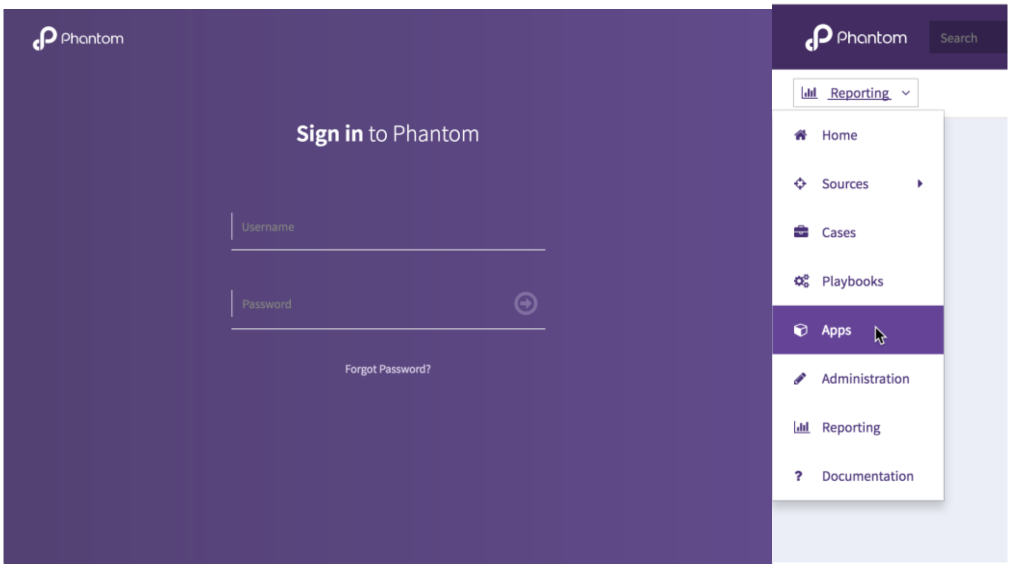
A Phantom App is designed to connect with a matching point product. An Asset is a specific connection-configuration. By default, configuring an App on Phantom involves configuring an Asset of that App. Complex deployments, such as multiple instances of a point product, may involve configuring multiple 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 NetWitness Logs & Packets App • RSA Archer App • RSA Security Analytics 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. • Connecting to different product modules, such as NetWitness Logs versus NetWitness Packets.

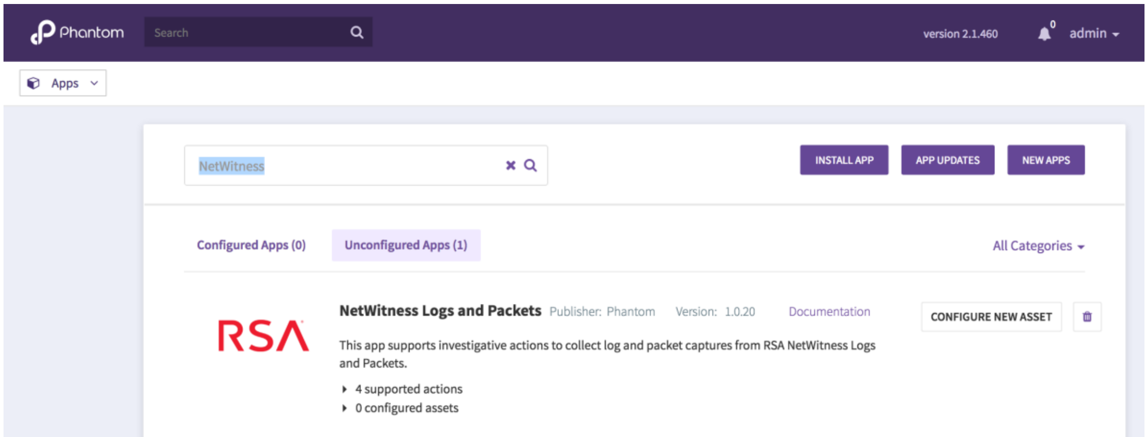
The NetWitness Logs & Packets App uses separate Assets to connect to the log-decoder versus the packet-decoder.

Phantom Configuration – Locating / Installing the RSA NetWitness Logs & Packets App

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



2. Enter **NetWitness** in the search field to locate the RSA NetWitness Logs & Packets App.

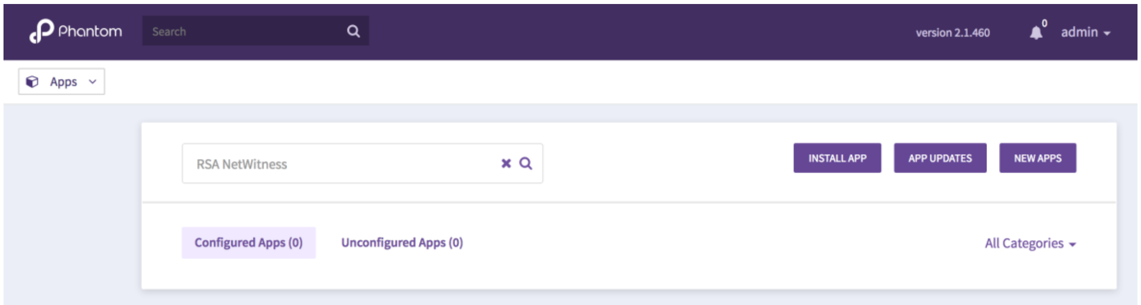


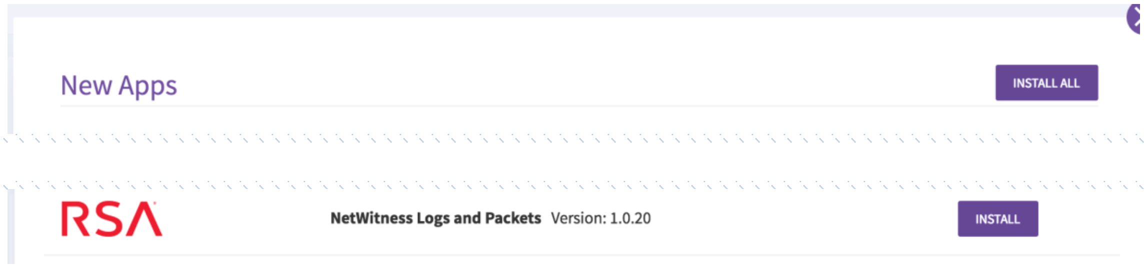
NetWitness Logs and Packets Publisher: Phantom Version: 1.0.20 Documentation

This app supports investigative actions to collect log and packet captures from RSA NetWitness Logs and Packets.

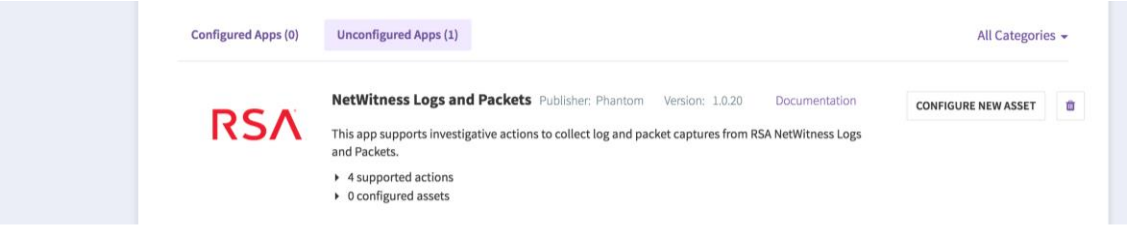
- 4 supported actions
- 0 configured assets

3. If the App does not appear under either Configured Apps or Unconfigured Apps, select **New Apps** to locate the installable App, then select **Install**.

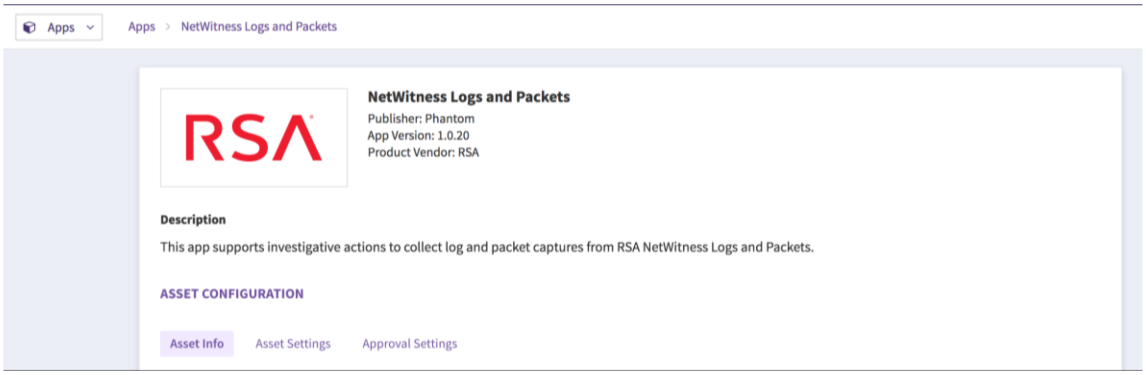




4. Select **Configure New Asset** to access the **Asset Configuration** settings.


Configured Apps (0)
Unconfigured Apps (1)
All Categories
RSA
NetWitness Logs and Packets Publisher: Phantom Version: 1.0.20 Documentation
CONFIGURE NEW ASSET

This app supports investigative actions to collect log and packet captures from RSA NetWitness Logs and Packets.



NetWitness Logs and Packets
Publisher: Phantom
App Version: 1.0.20
Product Vendor: RSA

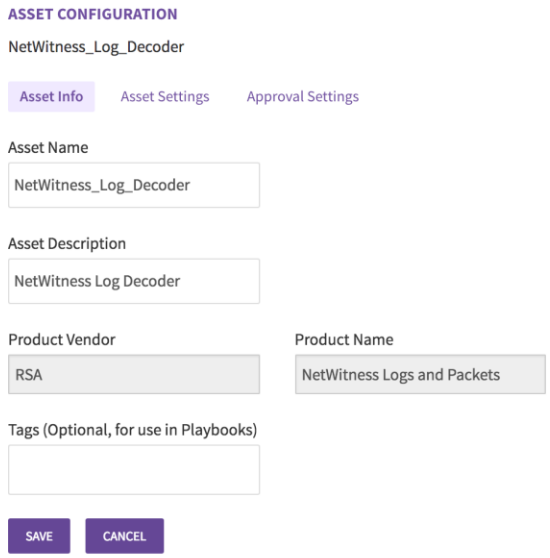
Description
This app supports investigative actions to collect log and packet captures from RSA NetWitness Logs and Packets.

Phantom Asset Configuration – RSA NetWitness Logs

The RSA NetWitness Logs & Packets App configures as two separate assets – One asset will connect to the NetWitness Log Decoder service for retrieving log-captures, and a separate asset will connect to the NetWitness Packet Decoder service for retrieving packet-captures.

This asset will be configured to retrieve log-captures.

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



ASSET CONFIGURATION

NetWitness_Log_Decoder

Asset Name: NetWitness_Log_Decoder

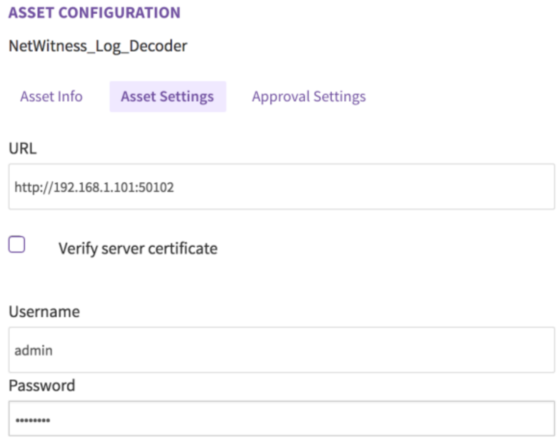
Asset Description: NetWitness Log Decoder

Product Vendor: RSA

Product Name: NetWitness Logs and Packets

Tags (Optional, for use in Playbooks):

2. Select the **Asset Settings** tab, and enter the NetWitness Log Decoder connection information: **URL, Username, and Password**. (Default log-decoder API port: 50102)



ASSET CONFIGURATION

NetWitness_Log_Decoder

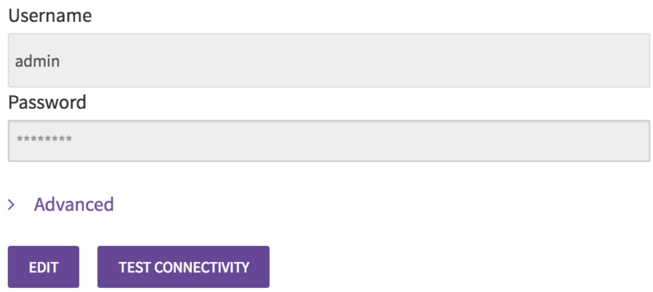
URL: http://192.168.1.101:50102

□ Verify server certificate

Username: admin

Password: ••••••••

3. Select **SAVE** to save the log-decoder asset configuration, then select **Test Connectivity** to verify the asset connection settings.



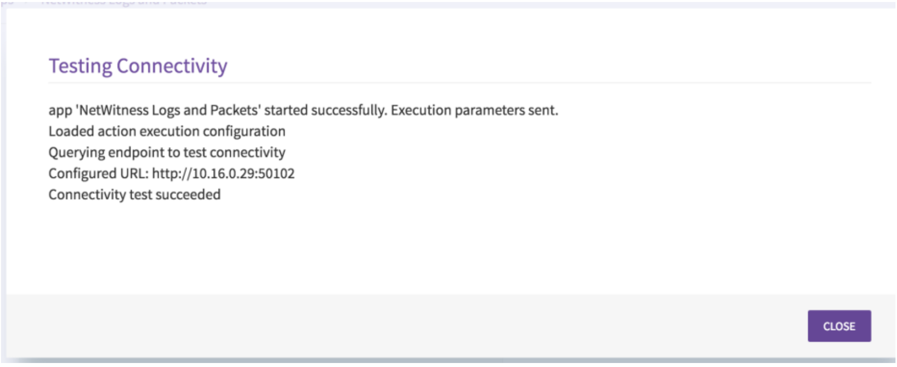
Username

admin

Password

****

4. The message **Connectivity test succeeded** indicates that the log-decoder asset has been correctly configured. Select **Close** to finish asset-configuration. The RSA NetWitness Log Decoder asset is now correctly configured and enabled.



Testing Connectivity

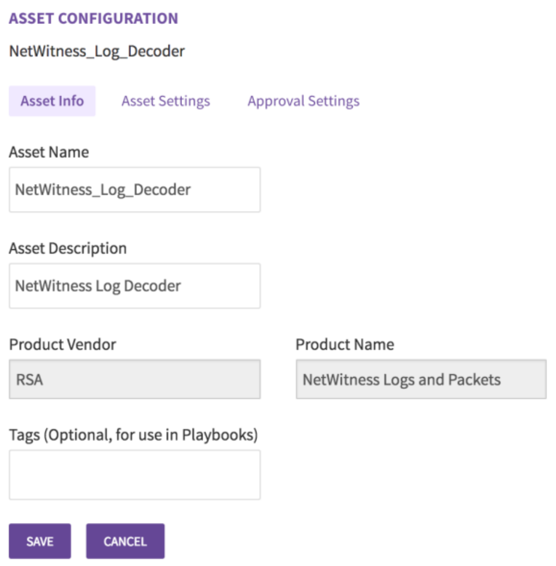
```
app 'NetWitness Logs and Packets' started successfully. Execution parameters sent.
Loaded action execution configuration
Querying endpoint to test connectivity
Configured URL: http://10.16.0.29:50102
Connectivity test succeeded
```

Phantom Asset Configuration – RSA NetWitness Packets

The RSA NetWitness Logs & Packets App configures as two separate assets – One asset will connect to the NetWitness **Log Decoder** service for retrieving log-captures, and a separate asset will connect to the NetWitness **Packet Decoder** service for retrieving packet-captures.

This asset will be configured to retrieve packet-captures.

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



NetWitness_Log_Decoder

Asset Name: NetWitness_Log_Decoder

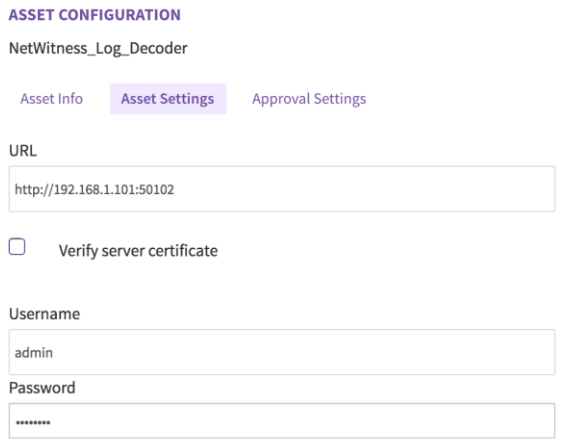
Asset Description: NetWitness Log Decoder

Product Vendor: RSA

Product Name: NetWitness Logs and Packets

Tags (Optional, for use in Playbooks):

2. Select **Asset Settings**, then enter connection information for the NetWitness Packet Decoder: **URL**, **Username**, and **Password**. (Default packet-decoder API port: 50104)



NetWitness_Log_Decoder

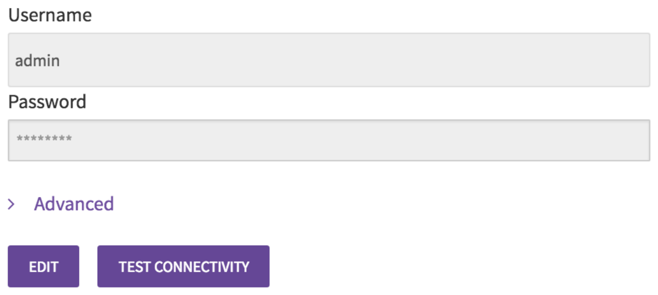
URL: http://192.168.1.101:50102

☐ Verify server certificate

Username: admin

Password: ••••••••

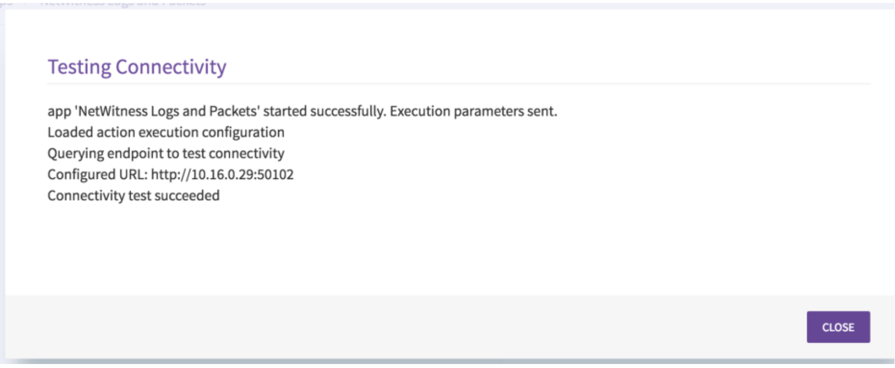
3. Select **SAVE** to save the packet-decoder asset configuration, then select **Test Connectivity** to verify the asset settings.



Username: admin

Password: ********

4. The message **Connectivity test succeeded** indicates that the packet-decoder asset has been correctly configured. Select **Close** to finish asset-configuration. The RSA NetWitness Packet Decoder asset is now correctly configured and enabled.



Testing Connectivity

```
app 'NetWitness Logs and Packets' started successfully. Execution parameters sent.
Loaded action execution configuration
Querying endpoint to test connectivity
Configured URL: http://10.16.0.29:50102
Connectivity test succeeded
```

Phantom & RSA NetWitness Logs & Packets Usage

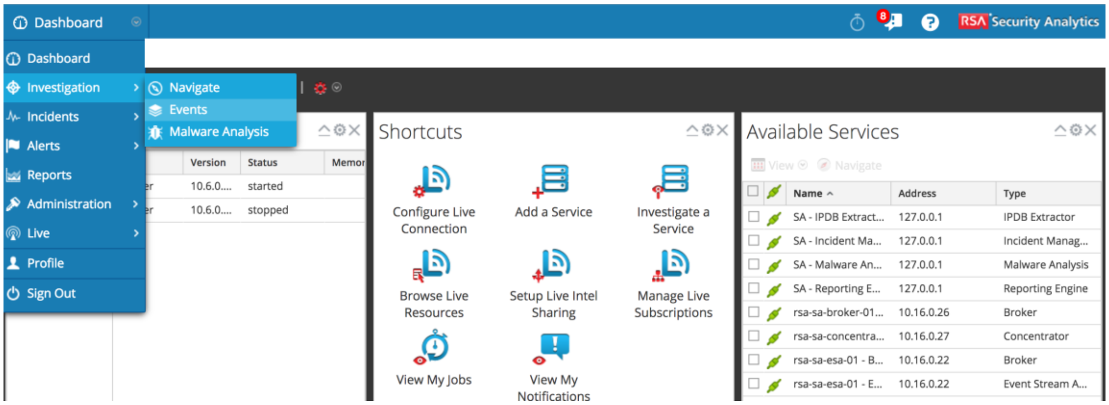
Log-Capture Retrieval

This section reviews NetWitness log-decoder events, and shows how log-decoder captures can be downloaded into Phantom. Packet-captures follow the same model.

The following steps first show how incidents are created within RSA, followed by incident-ingestion into Phantom using the RSA Security Analytics App. The log-capture for that incident is then retrieved into Phantom.

(See the *RSA Security Analytics App for Phantom Integration Guide* for more information on the Security Analytics App and Phantom configuration.)

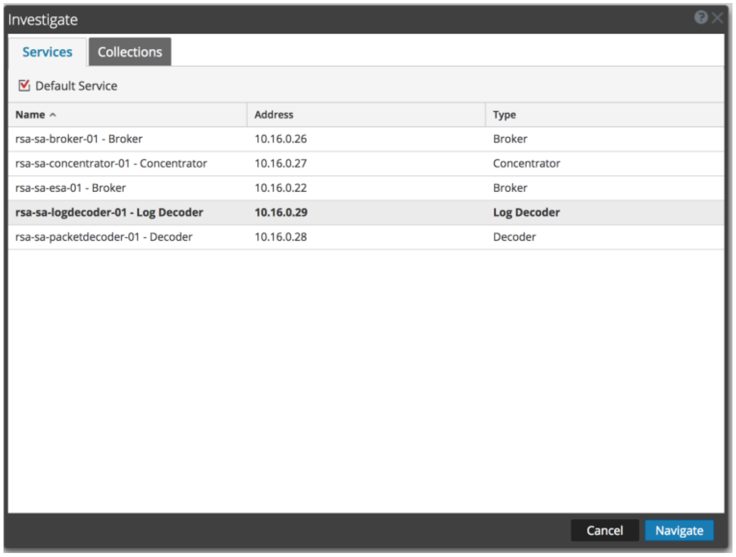
1. In RSA Security Analytics, select **Investigation > Events**.



	Version	Status	Memor
er	10.6.0....	started	
er	10.6.0....	stopped	

Name	Address	Type
SA - IPDB Extract...	127.0.0.1	IPDB Extractor
SA - Incident Ma...	127.0.0.1	Incident Manag...
SA - Malware An...	127.0.0.1	Malware Analysis
SA - Reporting E...	127.0.0.1	Reporting Engine
rsa-sa-broker-01...	10.16.0.26	Broker
rsa-sa-concentra...	10.16.0.27	Concentrator
rsa-sa-esa-01 - B...	10.16.0.22	Broker
rsa-sa-esa-01 - E...	10.16.0.22	Event Stream A...

2. On the Investigate dialog, select the log-decoder service, then select **Navigate**.

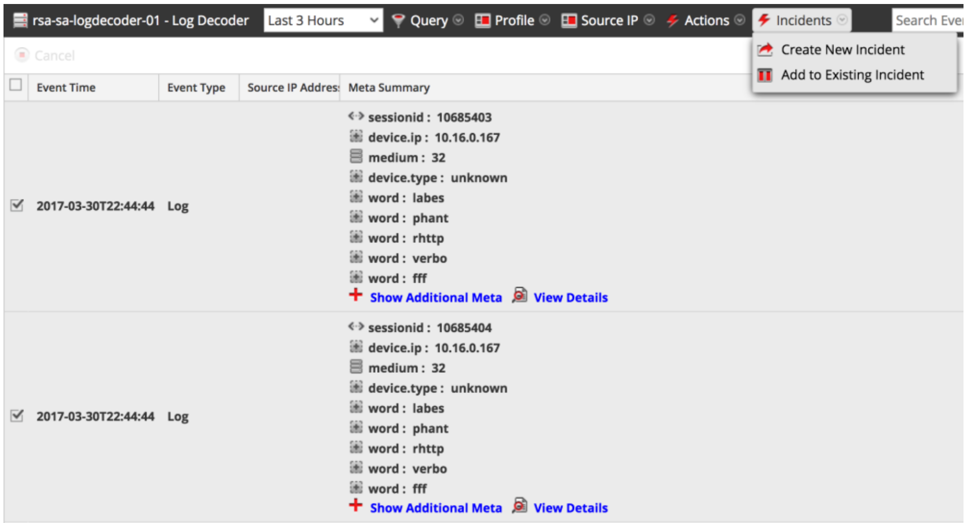


☑ Default Service

Name ^	Address	Type
rsa-sa-broker-01 - Broker	10.16.0.26	Broker
rsa-sa-concentrator-01 - Concentrator	10.16.0.27	Concentrator
rsa-sa-esa-01 - Broker	10.16.0.22	Broker
rsa-sa-logdecoder-01 - Log Decoder	**10.16.0.29**	**Log Decoder**
rsa-sa-packetdecoder-01 - Decoder	10.16.0.28	Decoder

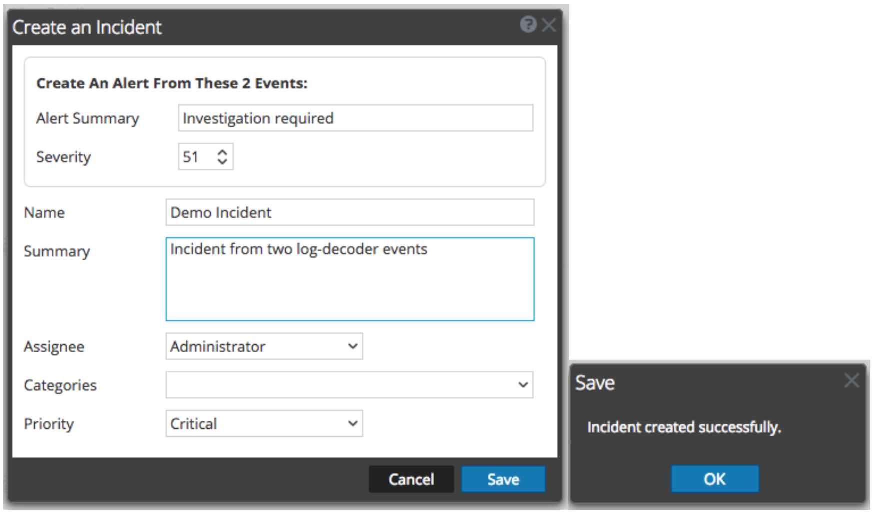
3. Within the listing of events, select one or more events to be included in a new incident. Next, select **Incident > Create New Incident**.

   (Note the sessionid of the second event in this example: 10685404)



□	Event Time	Event Type	Source IP Addres	Meta Summary
☑	2017-03-30T22:44:44	Log		sessionid : 10685403 device.ip : 10.16.0.167 medium : 32 device.type : unknown word : labes word : phant word : rhttp word : verbo word : fff
☑	2017-03-30T22:44:44	Log		sessionid : 10685404 device.ip : 10.16.0.167 medium : 32 device.type : unknown word : labes word : phant word : rhttp word : verbo word : fff

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



Create an Incident

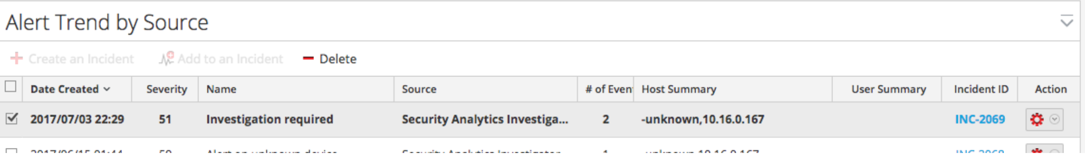
Create An Alert From These 2 Events:

Alert Summary	Investigation required
Severity	51
Name	Demo Incident
Summary	Incident from two log-decoder events
Assignee	Administrator
Categories	
Priority	Critical

Save

Incident created successfully.

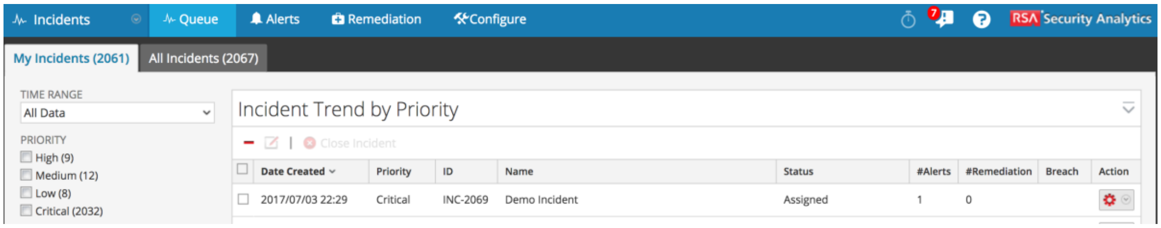
5. The *Alert Trend by Source* view appears, listing the alert associated with the new incident, along with the Incident ID (INC-2069 in this example).



Alert Trend by Source

□	Date Created	Severity	Name	Source	# of Even	Host Summary	User Summary	Incident ID	Action
☑	2017/07/03 22:29	51	Investigation required	Security Analytics Investiga...	2	-unknown,10.16.0.167		INC-2069	

6. The **Incident Trend by Priority** view (**Incidents > Queue**) lists the incident that was created. Phantom will ingest the incident by polling RSA Security Analytics App.



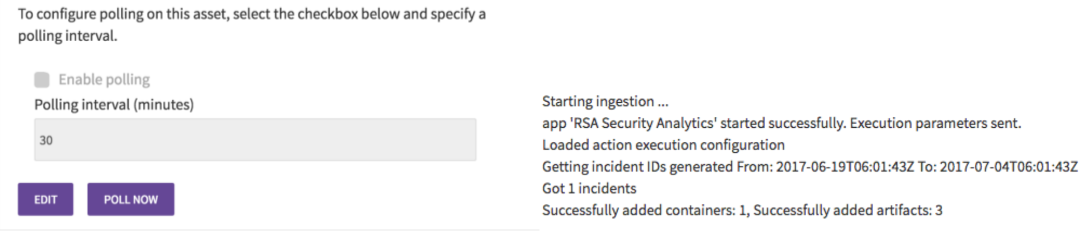
TIME RANGE: All Data

PRIORITY
- □ High (9)
- □ Medium (12)
- □ Low (8)
- □ Critical (2032)

Incident Trend by Priority

□	Date Created	Priority	ID	Name	Status	#Alerts	#Remediation	Breach	Action
□	2017/07/03 22:29	Critical	INC-2069	Demo Incident	Assigned	1	0		

7. Phantom can be configured to poll RSA Security Analytics (SA)on a defined schedule, or Phantom's **Poll Now** feature can be used to ingest incidents on-demand. **Poll Now** is located on the **Asset Configuration** screen, under the **Ingest Settings** tab.



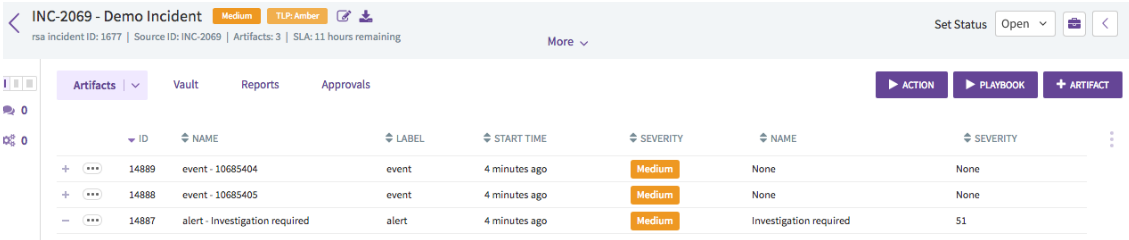
To configure polling on this asset, select the checkbox below and specify a polling interval.

□ Enable polling

Polling interval (minutes): 30

```
Starting ingestion ...
app 'RSA Security Analytics' started successfully. Execution parameters sent.
Loaded action execution configuration
Getting incident IDs generated From: 2017-06-19T06:01:43Z To: 2017-07-04T06:01:43Z
Got 1 incidents
Successfully added containers: 1, Successfully added artifacts: 3
```

8. Once Phantom ingests the incident, it can be viewed within Phantom as seen below.



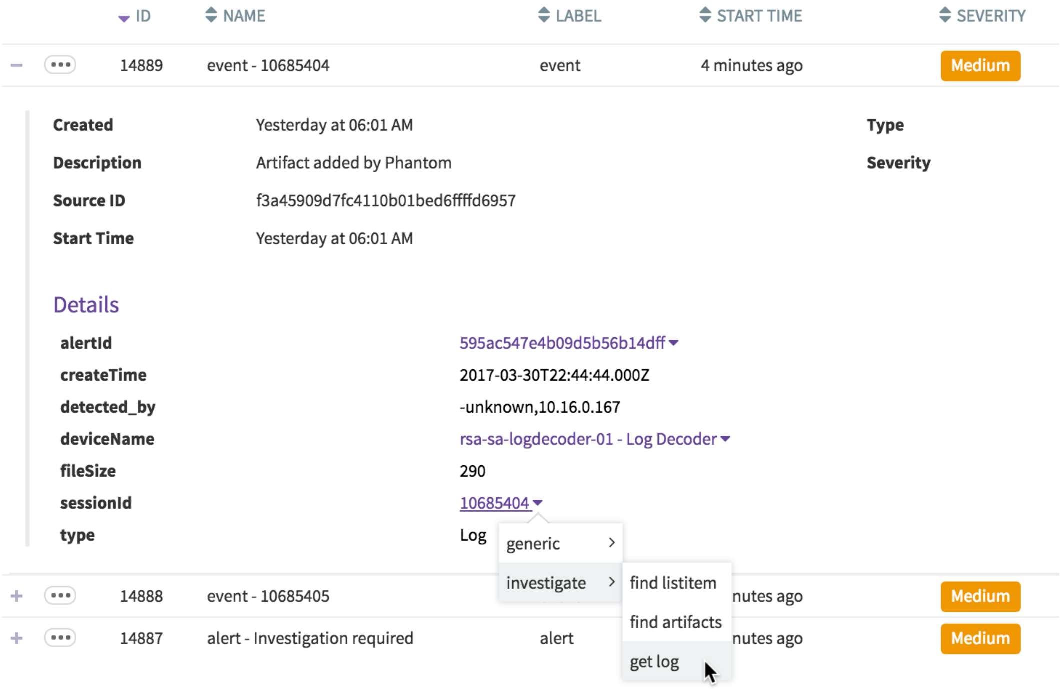
INC-2069 - Demo Incident — Medium — TLP: Amber

rsa incident ID: 1677 | Source ID: INC-2069 | Artifacts: 3 | SLA: 11 hours remaining

Set Status: Open

	ID	NAME	LABEL	START TIME	SEVERITY	NAME	SEVERITY
+	14889	event - 10685404	event	4 minutes ago	Medium	None	None
+	14888	event - 10685405	event	4 minutes ago	Medium	None	None
−	14887	alert - Investigation required	alert	4 minutes ago	Medium	Investigation required	51

9. Phantom allows the log-capture to be retrieved directly from this incident view. Select the plus icon to expand the event and display event details, including sessionid. Retrieve the log-capture by right-clicking the sessionid, then select **investigate > get log**.



	ID	NAME	LABEL	START TIME	SEVERITY
−	14889	event - 10685404	event	4 minutes ago	Medium

Created: Yesterday at 06:01 AM

Description: Artifact added by Phantom

Source ID: f3a45909d7fc4110b01bed6ffffd6957

Start Time: Yesterday at 06:01 AM

Type

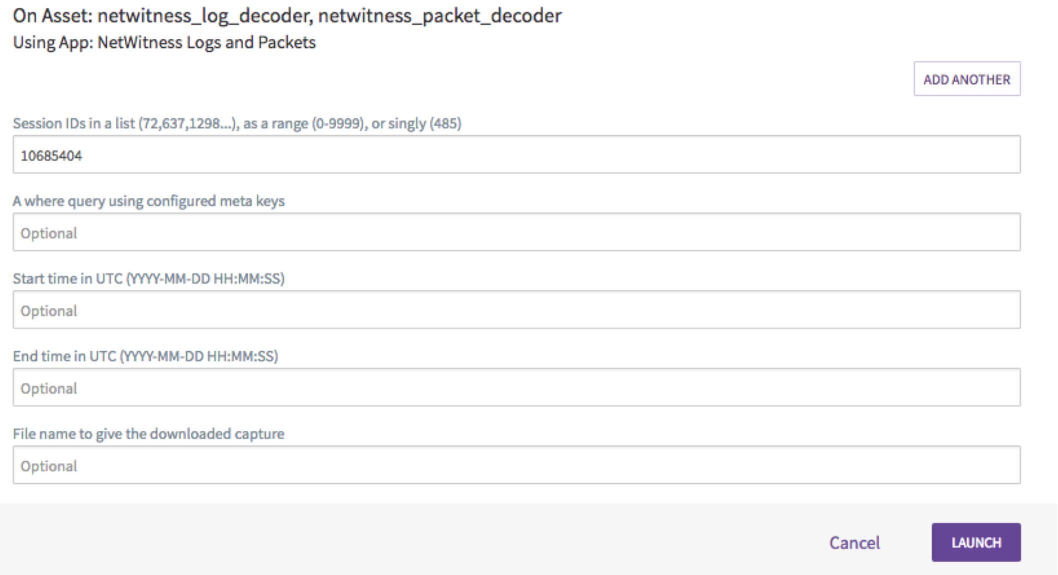
Severity

Details

alertId	595ac547e4b09d5b56b14dff
createTime	2017-03-30T22:44:44.000Z
detected_by	-unknown,10.16.0.167
deviceName	rsa-sa-logdecoder-01 - Log Decoder
fileSize	290
sessionId	10685404
type	Log

	ID	NAME	LABEL	START TIME	SEVERITY
+	14888	event - 10685405		nutes ago	Medium
+	14887	alert - Investigation required	alert	nutes ago	Medium

10. The Launch Action dialog appears, and the sessionid is pre-filled for the query and retrieval. Other supported Phantom query fields for this App can be seen below. Retrieve the log-capture by selecting **Launch**.



On Asset: netwitness_log_decoder, netwitness_packet_decoder
Using App: NetWitness Logs and Packets

Session IDs in a list (72,637,1298...), as a range (0-9999), or singly (485): 10685404

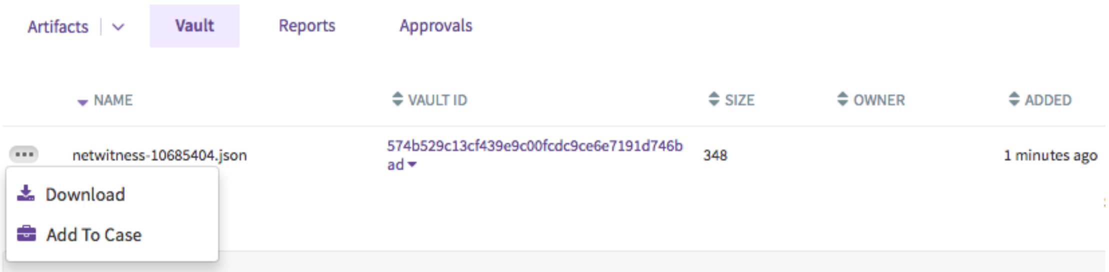
A where query using configured meta keys: Optional

Start time in UTC (YYYY-MM-DD HH:MM:SS): Optional

End time in UTC (YYYY-MM-DD HH:MM:SS): Optional

File name to give the downloaded capture: Optional

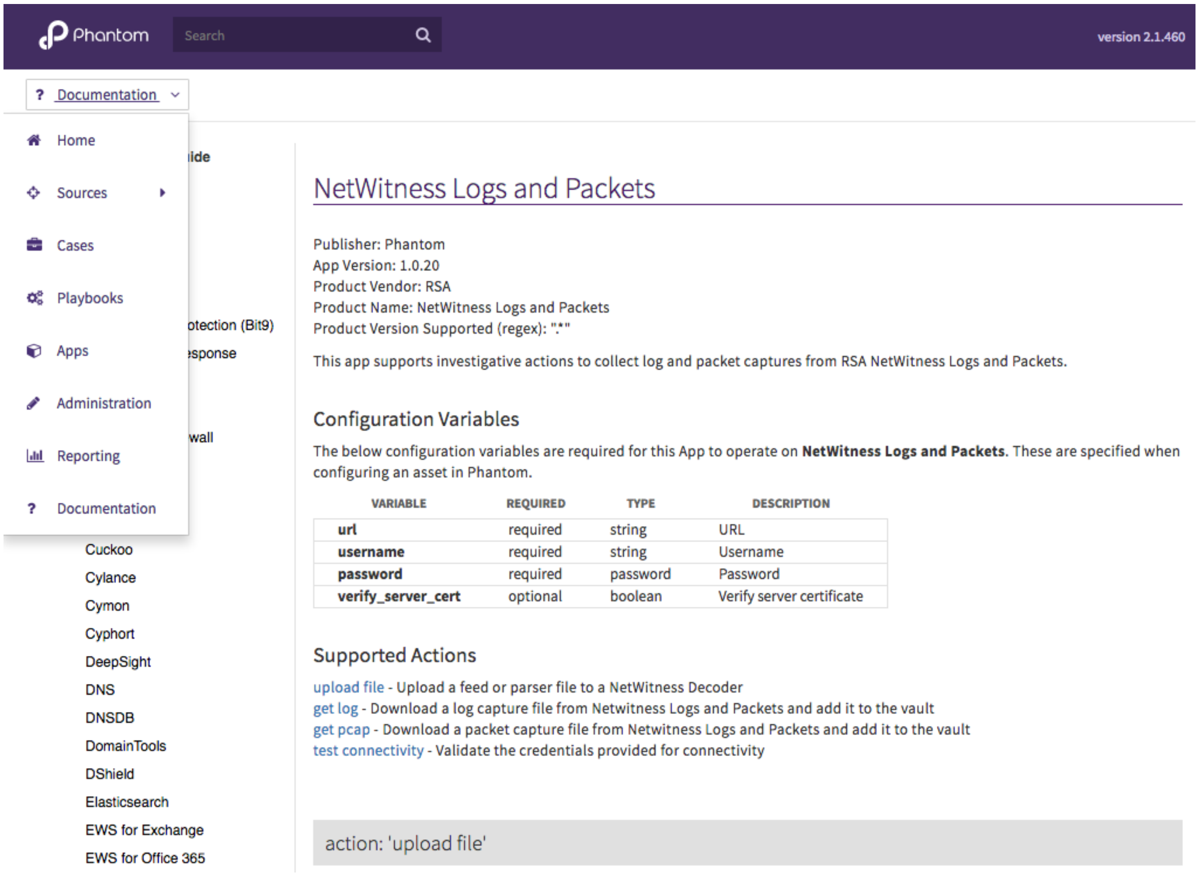
11. Once retrieved, the log-capture is stored in the Phantom vault. The log-capture can be directly downloaded for immediate review. It can also be attached to a case to be handled in Phantom's Case Management workflow.



NAME	VAULT ID	SIZE	OWNER	ADDED
netwitness-10685404.json	574b529c13cf439e9c00fcdc9ce6e7191d746bad	348		1 minutes ago

App Features & Documentation

Comprehensive documentation for the RSA NetWitness Logs & Packets App is available within the Phantom Platform, covering supported actions and general usage of the App. Documentation can be accessed by selecting **Documentation** from the main Phantom menu.



NetWitness Logs and Packets

Publisher: Phantom
App Version: 1.0.20
Product Vendor: RSA
Product Name: NetWitness Logs and Packets
Product Version Supported (regex): ".*"

This app supports investigative actions to collect log and packet captures from RSA NetWitness Logs and Packets.

Configuration Variables

The below configuration variables are required for this App to operate on **NetWitness Logs and Packets**. These are specified when configuring an asset in Phantom.

VARIABLE	REQUIRED	TYPE	DESCRIPTION
url	required	string	URL
username	required	string	Username
password	required	password	Password
verify_server_cert	optional	boolean	Verify server certificate

Supported Actions

upload file - Upload a feed or parser file to a NetWitness Decoder
get log - Download a log capture file from Netwitness Logs and Packets and add it to the vault
get pcap - Download a packet capture file from Netwitness Logs and Packets and add it to the vault
test connectivity - Validate the credentials provided for connectivity

action: 'upload file'

Certification Checklist for RSA NetWitness

Date Tested: July 7th, 2017

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

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	N/A
Query NetWitness for User Info (usernames, user behavior)	N/A
Query NetWitness for Specific Meta (Other)	N/A
Retrieve NetWitness Log/Packet Data	✓
Retrieve NetWitness PCAP files	✓
Alerting / Incident Creation	
NetWitness alert via syslog	N/A
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)	✓

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