# RSA® NETWITNESS®
# Logs
# Implementation Guide

## PAS Global, LLC ICS 5.5

Daniel R. Pintal, RSA Partner Engineering
Last Modified: October 30, 2017

RSA READY

## Solution Summary

Through the integration of PAS Global ICS and RSA NetWitness, our partnership provides our mutual customers with a deep view of events occurring within the network.

| RSA NetWitness Features | |
|---|---|
| **PAS Global ICS 5.5** | |
| **Integration package name** | pasics.envision |
| **Device display name within RSA NetWitness** | pasics |
| **Event source class** | ics |
| **Collection method** | File Collection |

# RSA NetWitness Community

The RSA NetWitness Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the NetWitness Integration Package for this guide. All NetWitness customers and partners are invited to register and participate in the **RSA NetWitness Community**.

Once you have downloaded the NetWitness Integration Package, the next steps are to deploy this on all log decoders. For steps to disable or remove the NetWitness Integration Package, please refer to the **Appendix** of this Guide.

The RSA NetWitness package consists of the following files:

| Filename | File Function |
|---|---|
| **pasics.envision** | NetWitness package deployed to parse events from devices. |
| **v20_pasicsmsg.xml** | The device xml contained within the NetWitness pasics.envision package. |
| **typespec_v3.zip** | The NetWitness typespec file. |
| **pasics.xml** | The typespec pasics.xml file contained within typespec_v3.zip. |
| | |

# Release Notes

| Release Date | What's New In This Release |
|---|---|
| October 30, 2017 | Initial support for PAS Global, ICS. |
| | |

# Partner Product Configuration

## *Before You Begin*

This section provides instructions for integrating PAS Global ICS 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 PAS Global ICS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

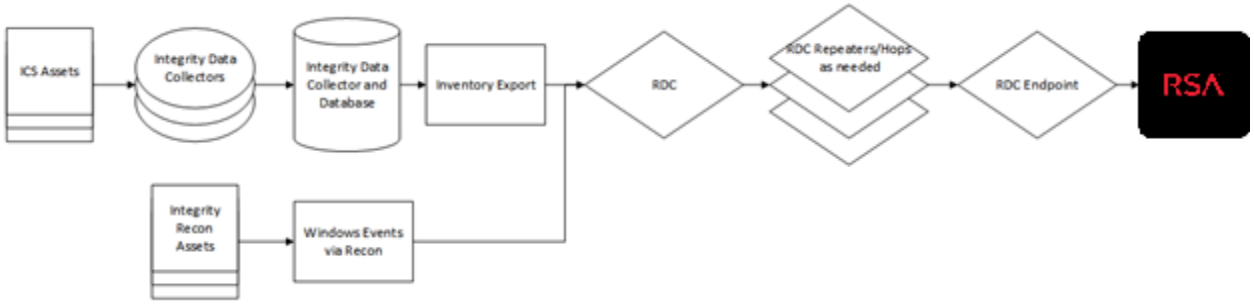
**Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure PAS Global ICS is properly configured and secured before deploying to a production environment.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

## *PAS Global ICS Configuration*

This implementation guide assumes that the PAS Cyber Integrity product with Integrity Recon is already deployed and functional at site. The focus of this guide is to detail the steps to integrate an existing Cyber Integrity deployment with RSA NetWitness.

### Overview of data collection process

Existing Integrity Data Collectors and Asset Models collect information periodically from the Industrial Control System (ICS) Assets. This information is consolidated within the Integrity Database. The [PAS Integration] Asset Model is then scheduled to generate CSV files containing the Integrity Inventory information. Windows Events are collected via the Integrity Recon Asset Model. Both the inventory CSV and the Windows Event Data files are placed into the appropriate location to be consumed by RSA NetWitness or to be transferred via the Remote Data Collector (RDC) component to the location where the RSA NetWitness application will then consume the data.

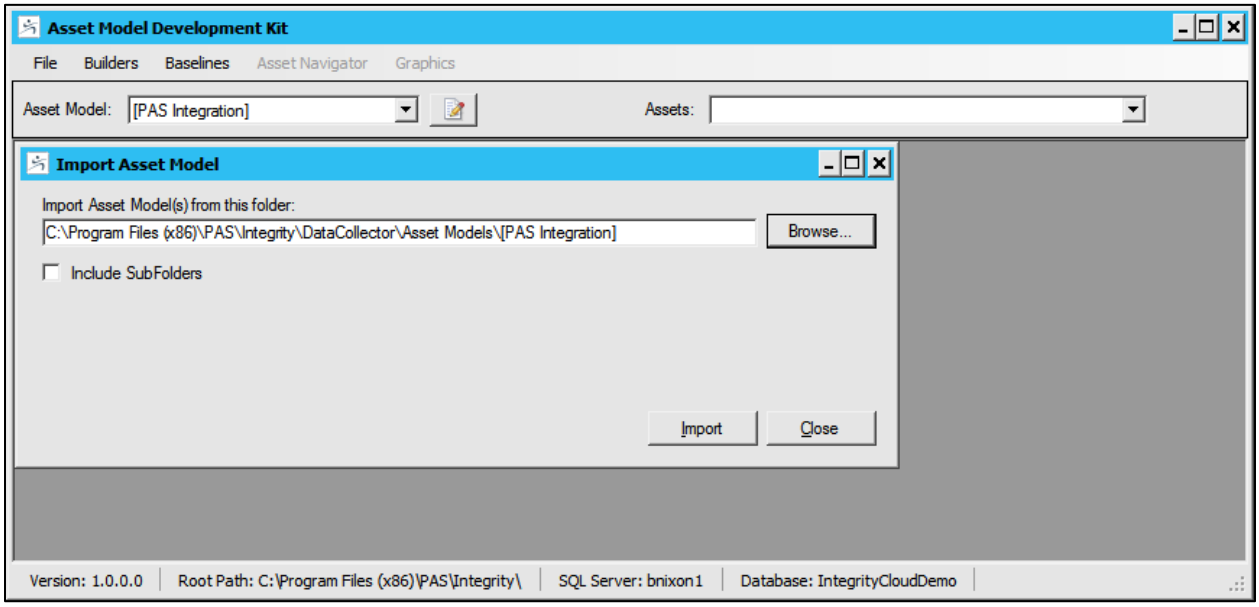


## Contacting PAS

PAS can be reached by telephone at +1 281 268 6565, or via email at **rapidsupport@pas.com**. For email requests, please allow up to 24 hours for a response.

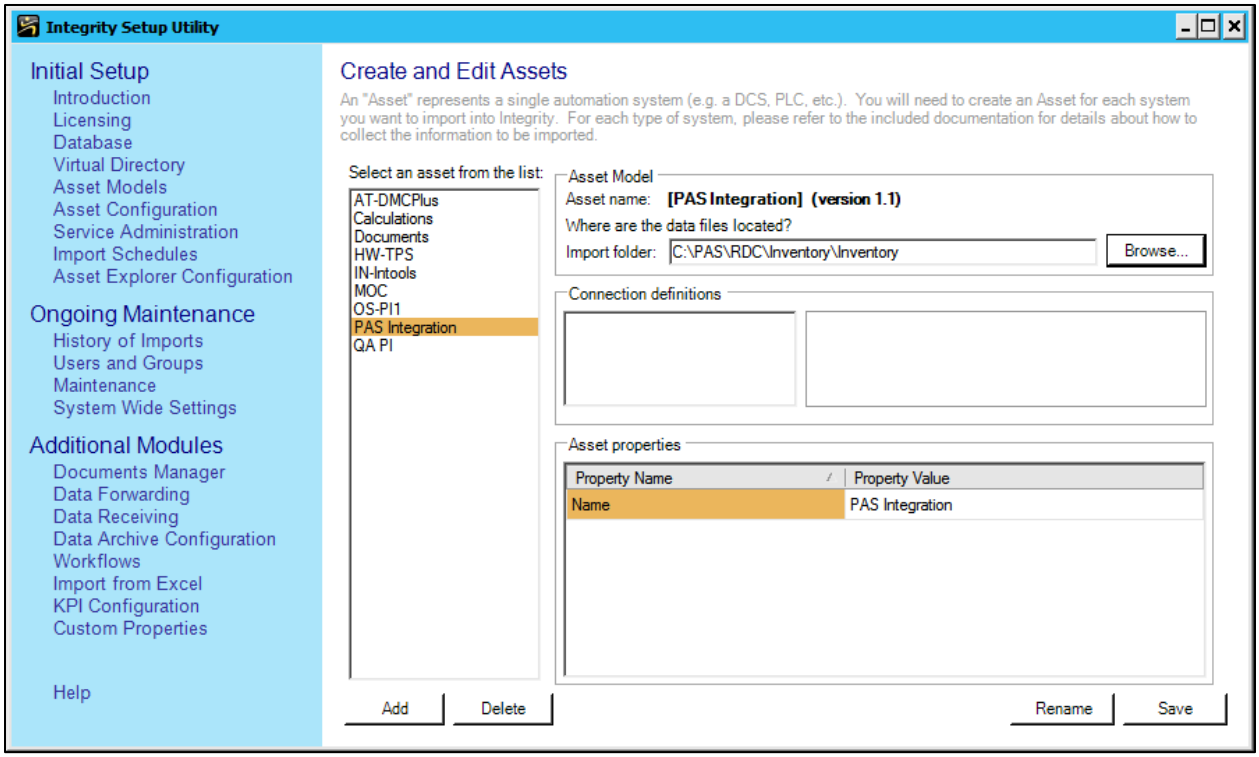
## Obtaining Cyber Integrity Normalized Inventory Exports

1. Contact PAS for the latest [PAS Integration] Asset Model.
2. Import the [PAS Integration] Asset Model using the Asset Model Development Kit (AMDK).
    a. Launch the AMDK from the **AMDK.exe** executable located in the "DataCollector" folder under the primary Integrity installation directory.
    b. Select **File** > **Import Asset Models** from the menu options.
    c. Click the **Browse** button to browse to the location of the [PAS Integration] asset model.
    d. Click the **Import** button to import the asset model.



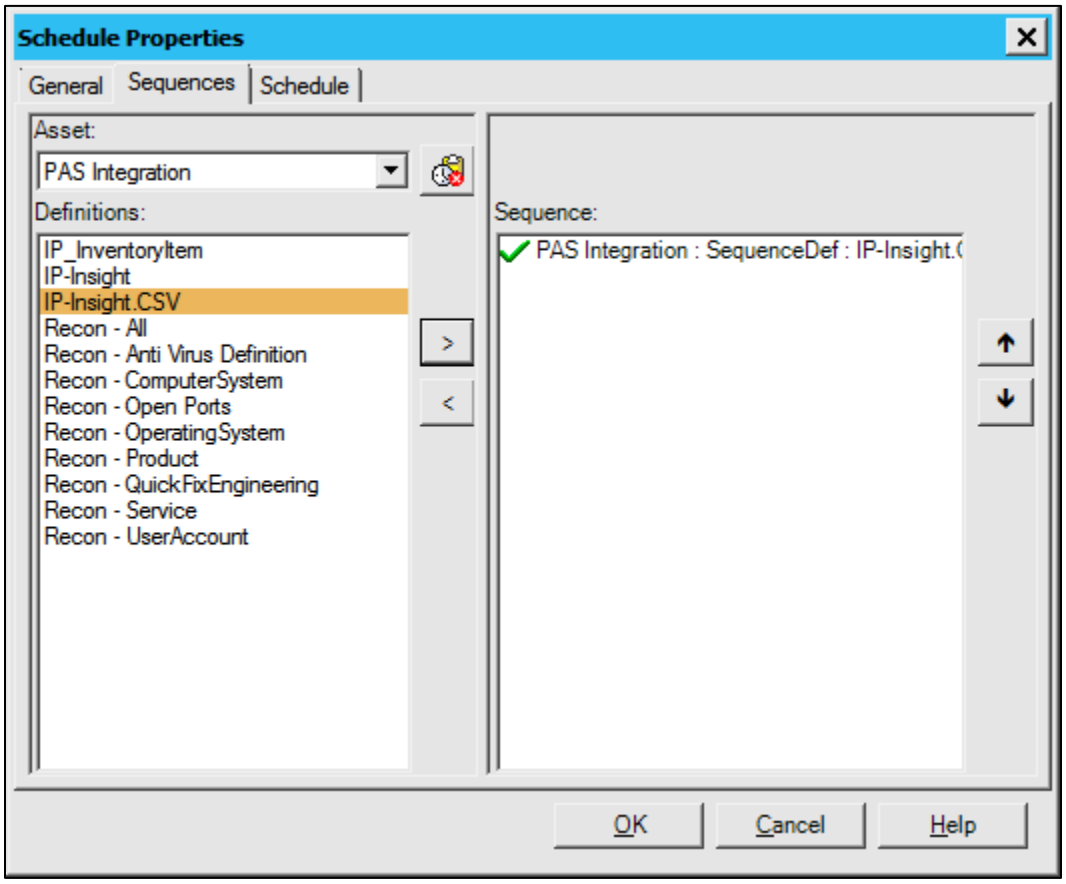
3. Create and Configure an asset that uses the [PAS Integration] Asset Model.

    a) Launch the Integrity Admin Utility from the **AdminUtility.exe** executable located in the "DataCollector" folder under the primary Integrity Installation directory.
    b) In the Integrity Admin Utility, select **Asset Configuration** from the available options on the left side of the UI.
    c) Click the **Add** button to add an asset.
    d) Give the asset a meaningful name and select **PAS Integration** as the asset model.
    e) Click the **Browse** button to select a directory where the inventory CSV file will be generated.



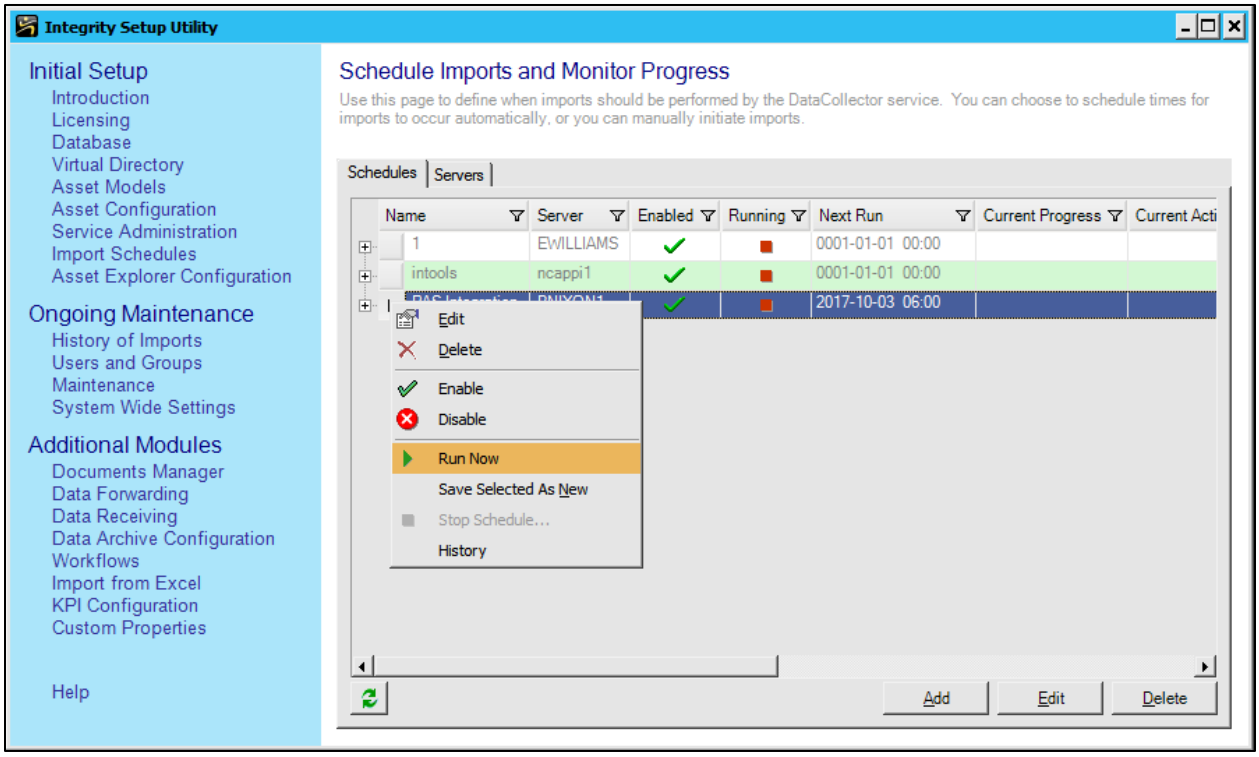
4. Schedule the asset to export the inventory CSV file at the desired frequency.

    a) Select the **Import Schedules** option on the left side of the UI.
    b) Click the **Add** button to add a scheduled task.
    c) Give the schedule a meaningful name and specify the Server to run the task on.
    d) This will typically be the Integrity Data Collector installed where the Integrity database is installed, but can be any Integrity data collector.
    e) On the Sequences tab, select the **PAS integration** asset from the drop down list.
    f) In the Definitions area, select the **IP-Insight.CSV** definition and use the **right point arrow** to add the definition to the schedule sequence.
    g) Click the **clipboard/clock** icon to specify the schedule for the export task.




    h) Click **OK** when finished.

i) Test the export sequence by right-clicking on the **schedule** and selecting **Run Now**.

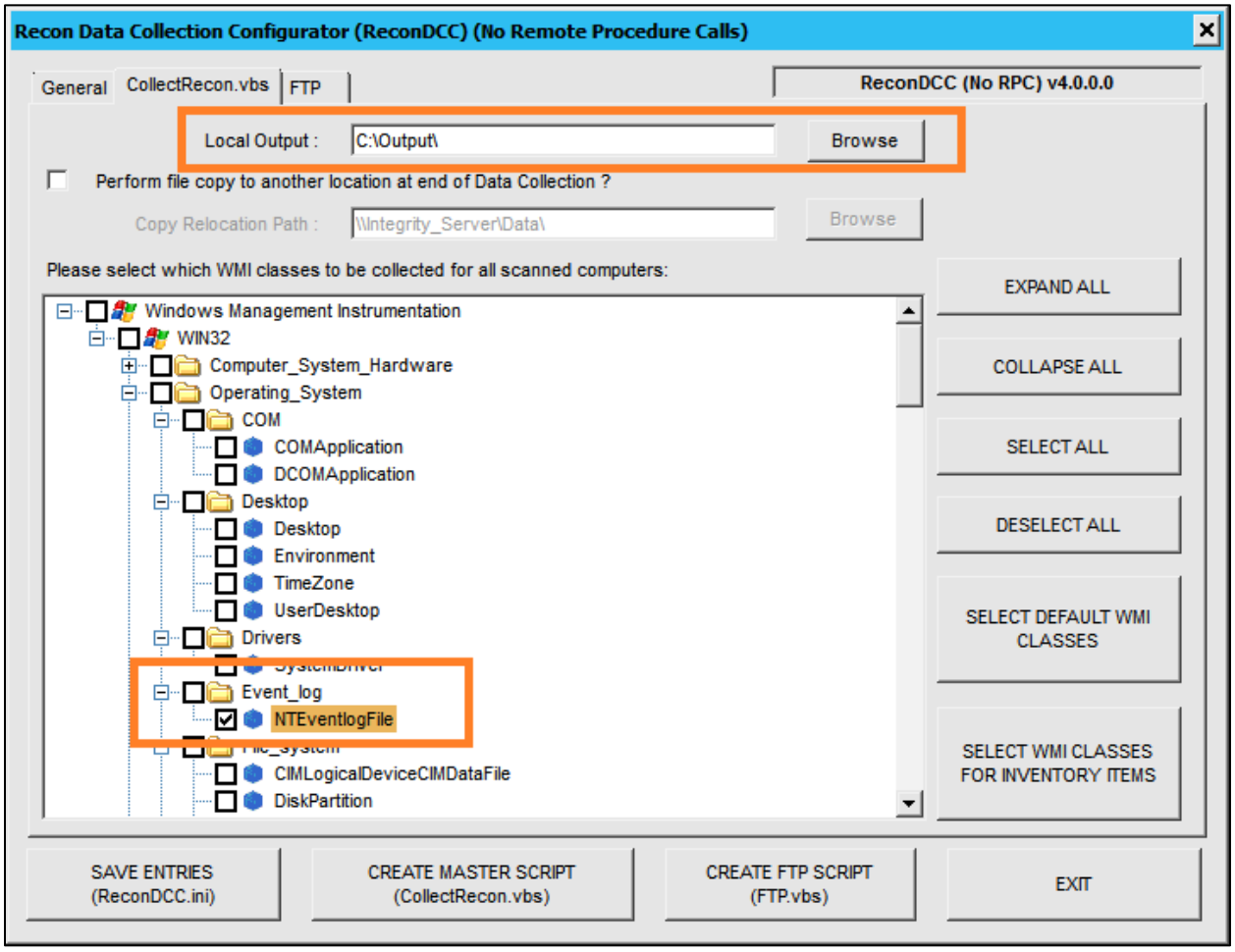



j) Verify that the inventory csv file was generated in the output directory.

## Collecting Windows Event Data via Integrity Recon

1. Contact PAS for the latest Integrity Recon Asset Model and Recon Data Collection Configurator (ReconDCC with or without RPC depending on the implementation at site).
2. Run the data collection utility and update the data collection to ensure that windows events are being collected and output to an appropriate directory.

    a) Ensure the **NTEventlogFile** box is checked and specify the **Local Output** parameter.



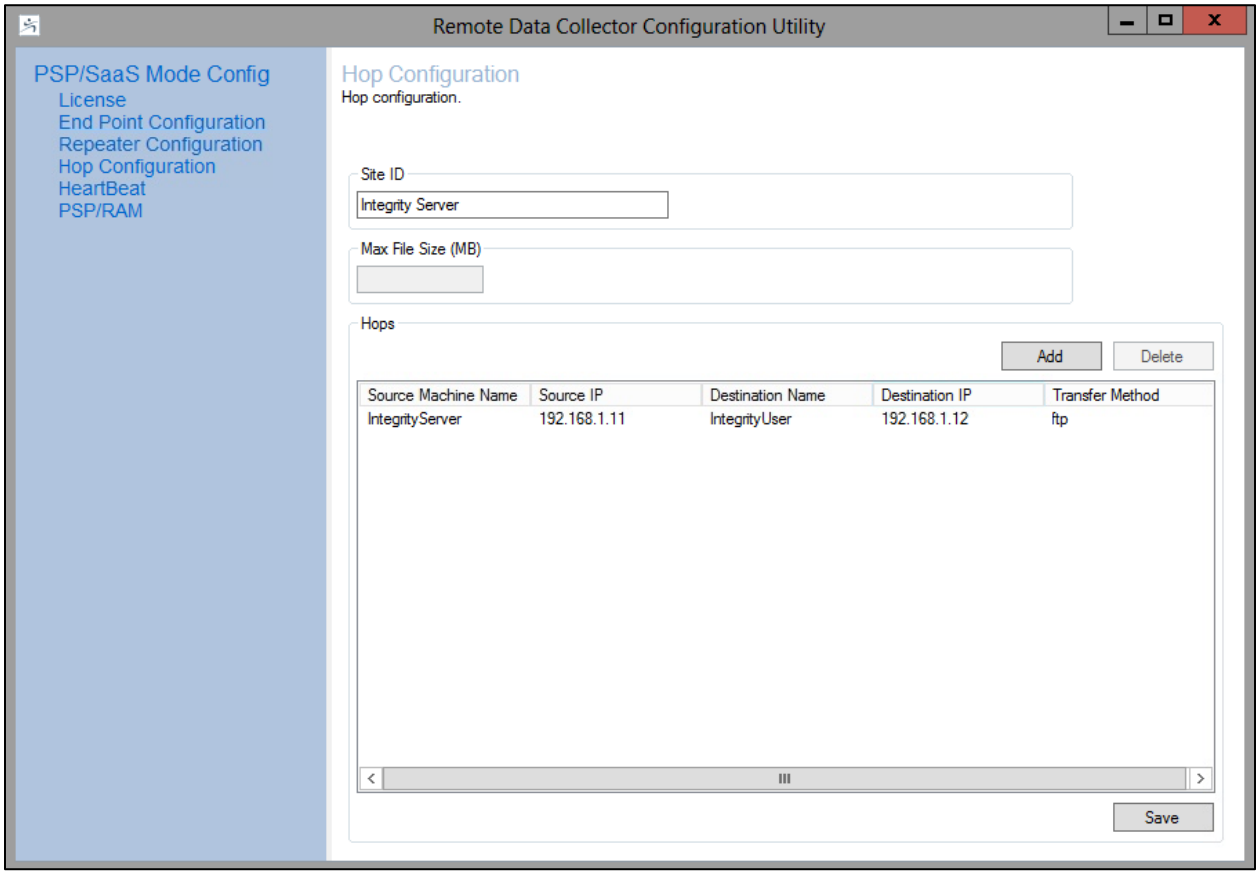

3. Click the **Create Master Script** button to generate the data collection vbscript.
4. Use Windows Scheduled tasks to execute the Recon data collection for Windows Events at the desired frequency.

> **! Important: Refer to the Integrity Recon Implementation Guide as needed for additional details.**

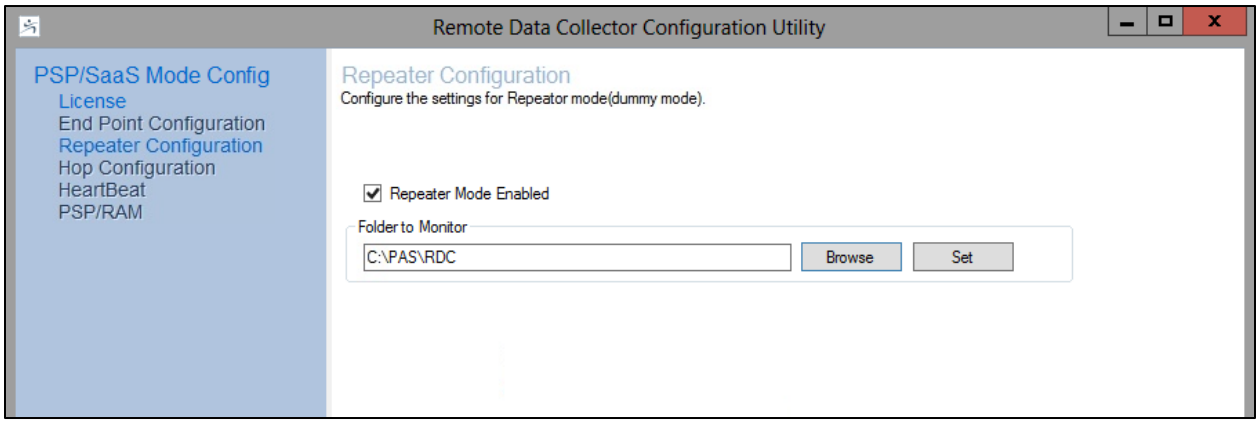
## Transferring Files via the PAS RDC Utility

1. Contact PAS for the latest PAS Remote Data Collection (RDC) Utility.
2. Install and license the PAS Remote Data Collector utility (RDC).
3. Open the RDC Configuration Utility.
4. If the machine is an origination point of data:

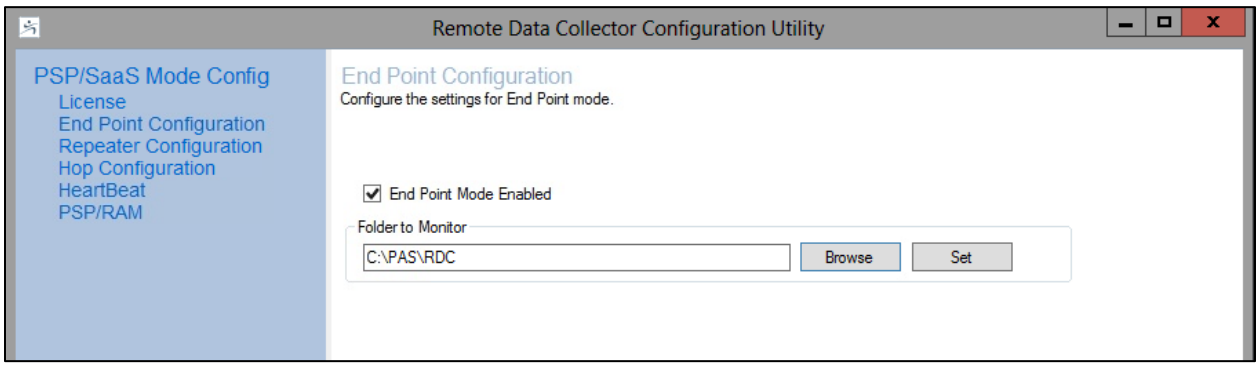
    a) Proceed to the "Hop Configuration" screen in the RDC Configuration Utility.
    b) Click on the **Add** button to add a hop to the RDC.
    c) Specify the **source name** and **IP address.**
    d) Specify the Transfer method (FTP or SFTP).
    e) Specify the details of the destination machine.



5. If the machine is a repeater of data:
    a) Proceed to the "Repeater Configuration" screen in the RDC Configuration Utility.
    b) Click on the **Repeater Mode Enabled** checkbox and specify the directory to monitor for new files.
    c) The specified directory will be the "root" directory of the RDC application, where the newfiles.txt file is located.




6. If the machine is an endpoint of data:
    a) Proceed to the "End Point Configuration" screen in the RDC Configuration Utility.
    b) Specify the location where the files transferred to the Endpoint will be stored.



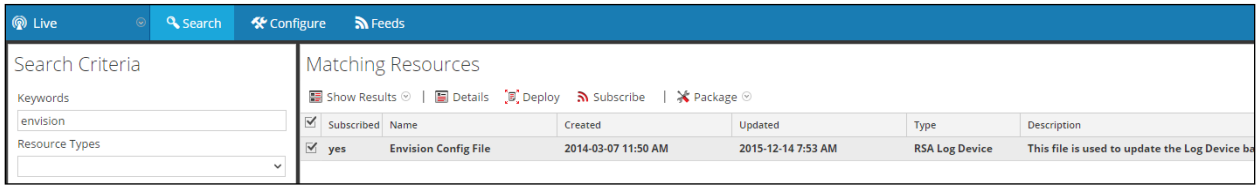
# RSA NetWitness Configuration

## *Deploy the enVision Config File*

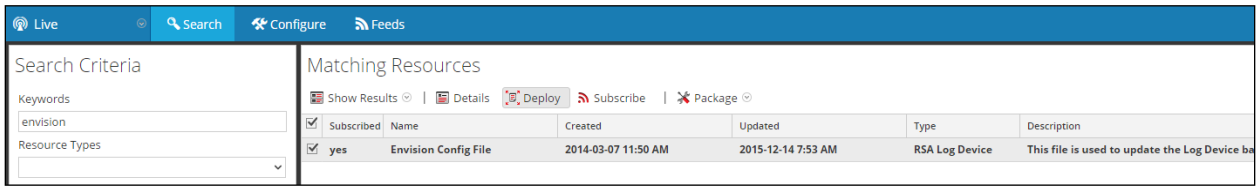
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **NetWitness Live** module. Log into RSA NetWitness and perform the following actions:

> **Important: Using this procedure will overwrite the existing table_map.xml.**

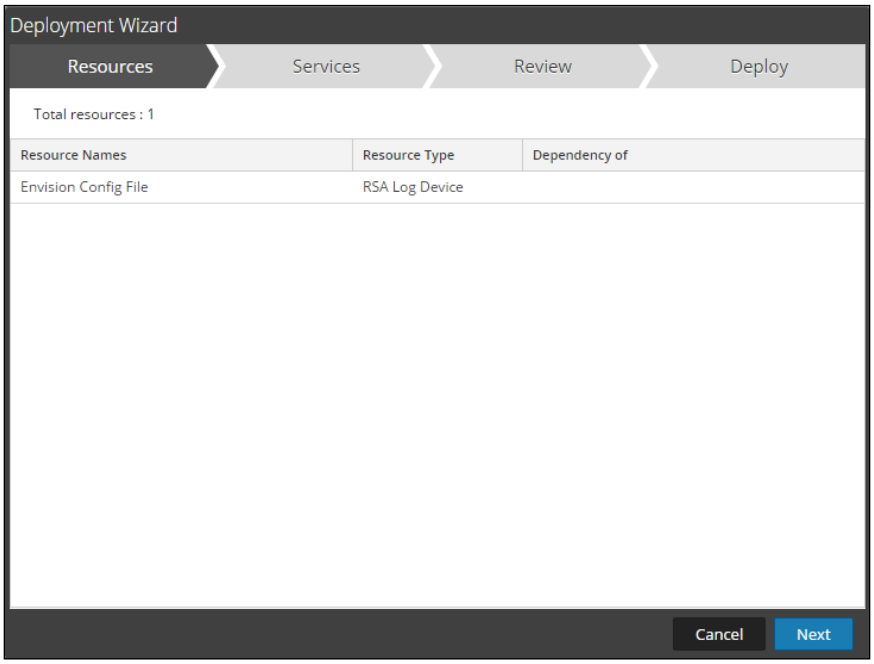
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



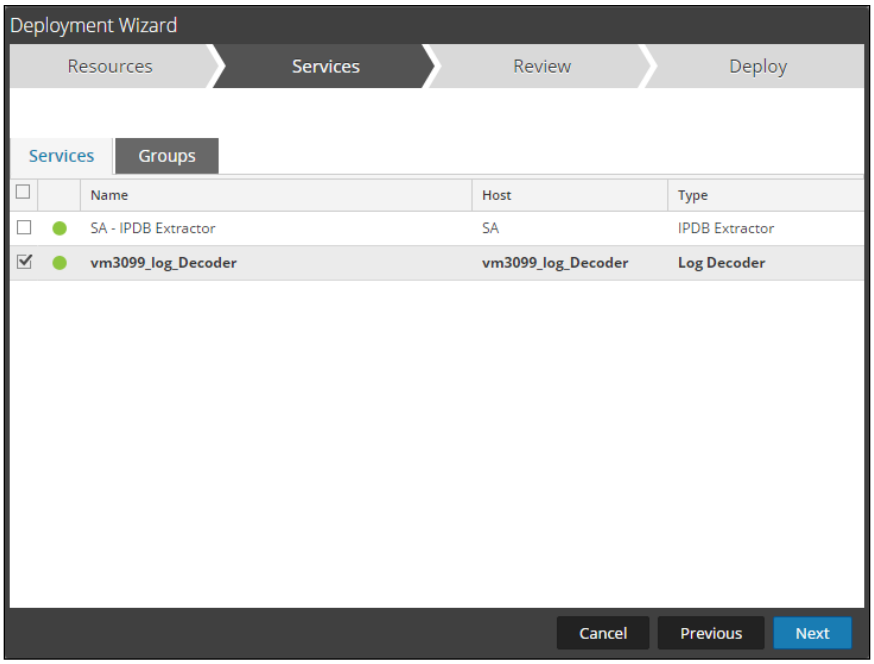

5. Click **Deploy** in the menu bar.



6. Select **Next**.

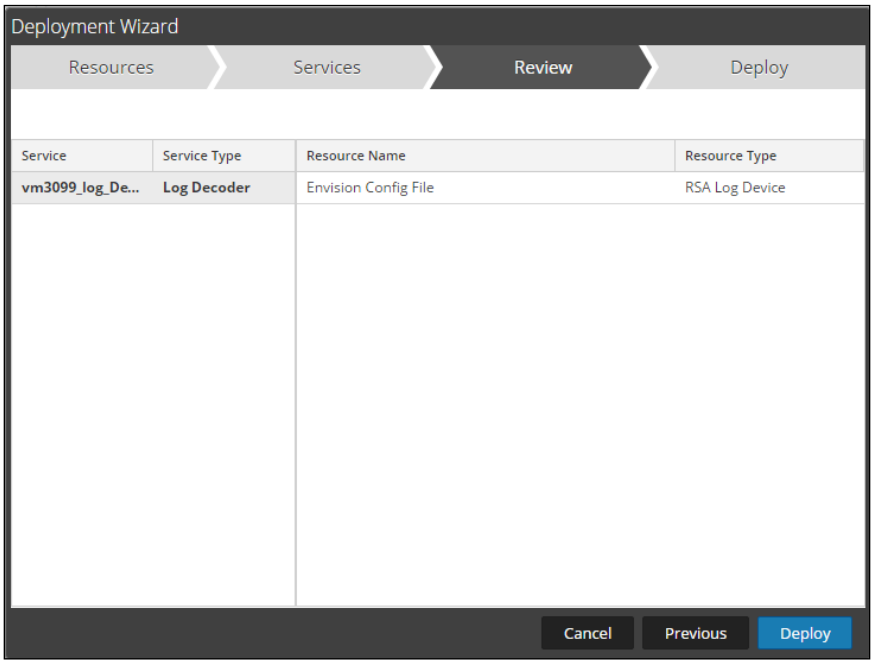



7. Select the **Log Decoder** and select **Next**.

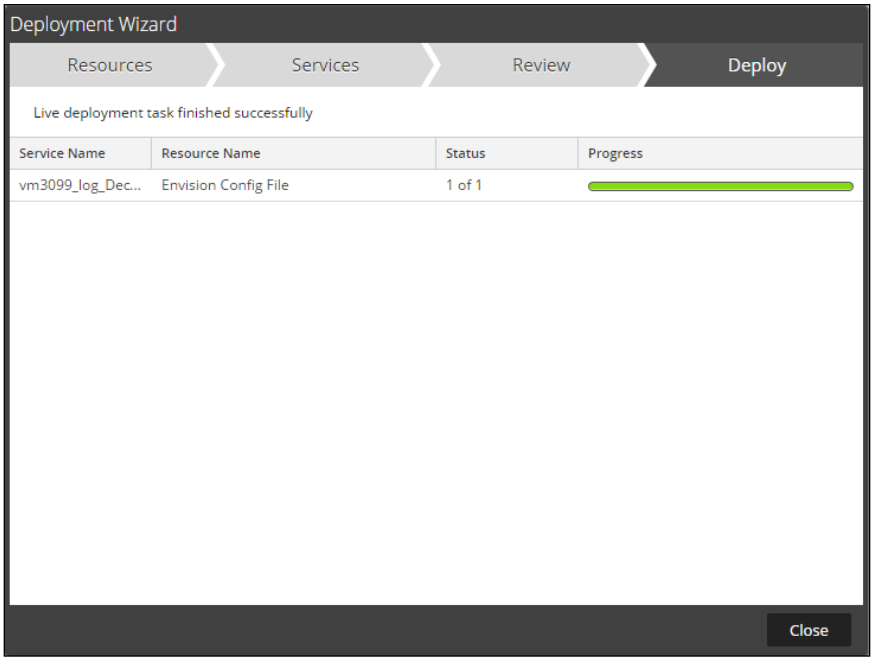



**! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.**

8. Select **Deploy**.



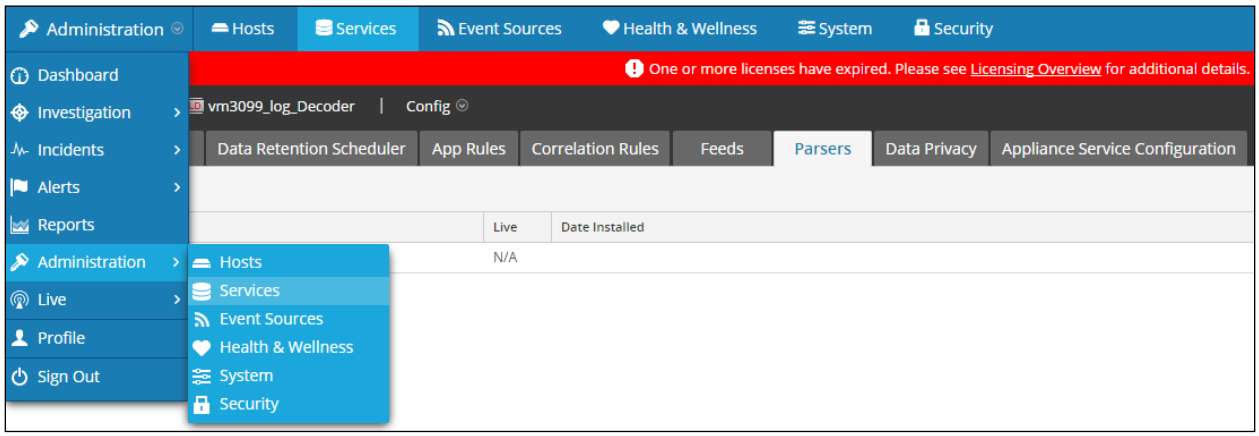

9. Select **Close**, to complete the deployment of the Envision Config file.



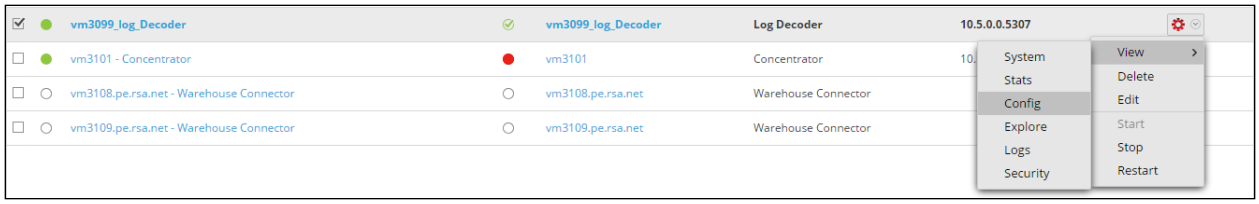
## *Deploy the RSA NetWitness Integration Package*

After completing the previous section, ***Deploy the enVision Config File***, you can now deploy the NetWitness Integration Package. Download the appropriate RSA Partner Integration Package, then log into RSA NetWitness to perform the following actions:

1. From the NetWitness menu, select **Administration > Services.**

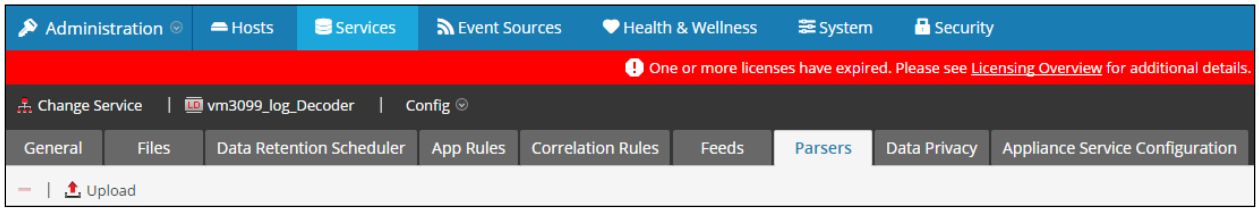



2. Select your Log Decoder from the list, select **View > Config**.



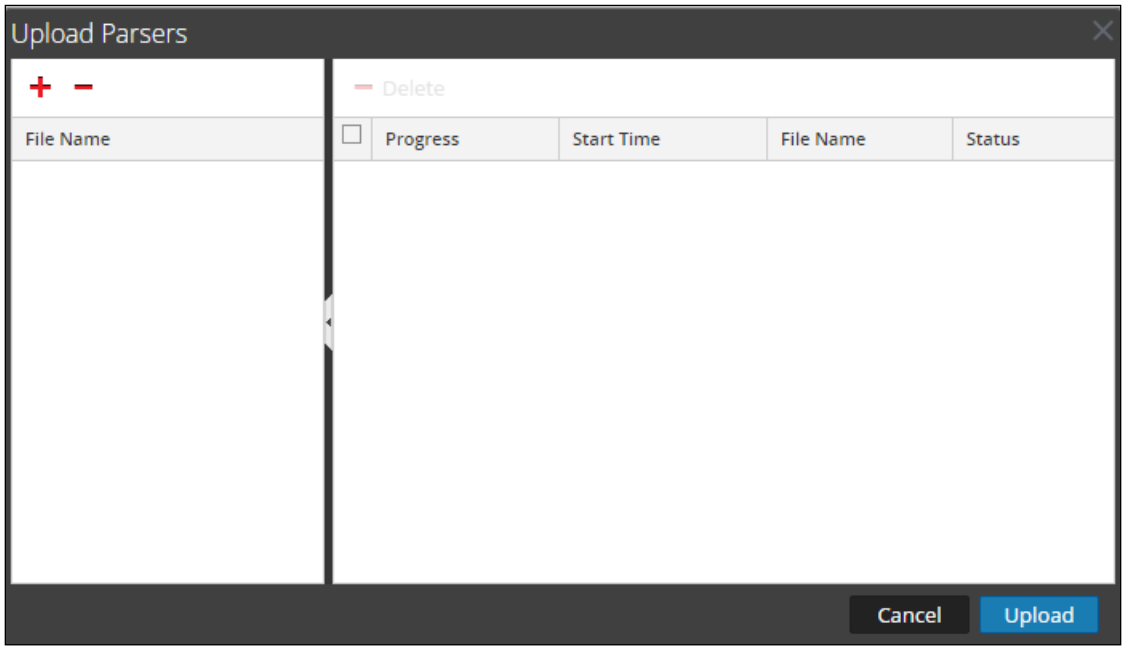

> **! Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.**

3. Next, select the **Parsers** tab and click the **Upload** button.

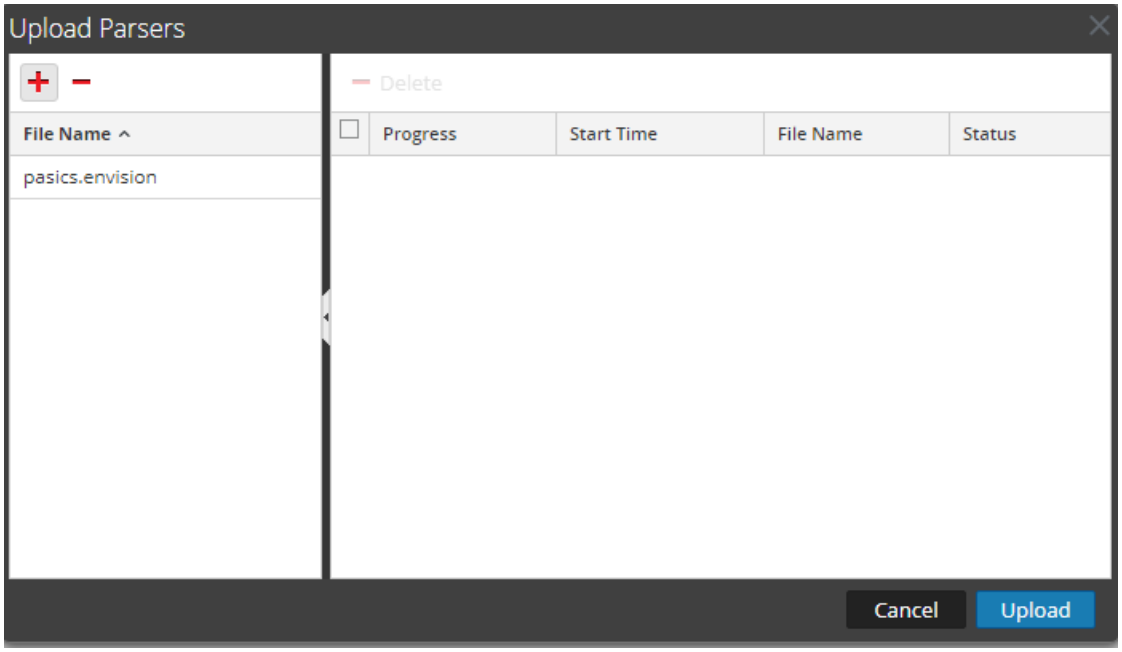


4. From the *Upload Parsers* window, click the + **Add** button and select the *.envision* file.

> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**

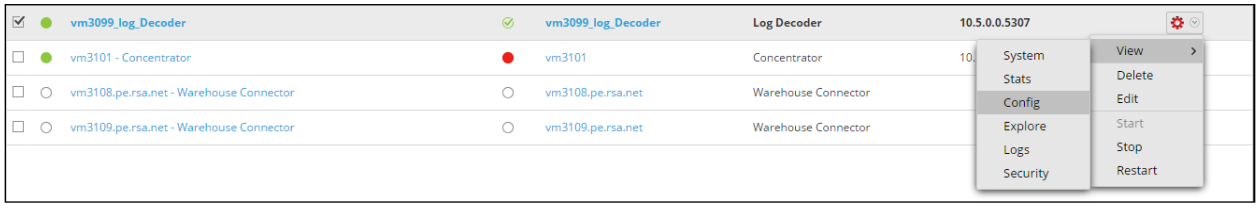



5. Under the file name column, select the integration package name and click **Upload**.



6. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**


7. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View> Config.**




8. The new device is listed under the Log Decoder(s) General Tab within the Service Parsers Configuration.

## *Edit the NetWtness Table-Map-Custom.xml file*

**! Important: The Table-Map-Custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.**

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/** folder.
2. If one exists, backup the **table-map-custom.xml** and then edit the existing table-map-custom.xml file.
3. Copy and paste the entire section below into a new file or only the lines between the **<mappings>…</mappings>** if the **table-map-custom.xml** file exists;

```
Example.
	<?xml version="1.0" encoding="utf-8"?>
	<!--
	# attributes:
	#	envisionName: The name of the column in the universal table
	#	nwName:			The name of the NetWitness meta field
	#	format:			Optional. The language key data type. See
	LanguageManager. Defaults to "Text".
	#	flags:		Optional. One of None|File|Duration|Transient.
	Defaults to "None".
	#	failureKey:	Optional. The name of the NW key to write data if
	conversion fails. Defaults to system generated "parse.error" meta.
	#	nullTokens:	Optional. The list of "null" tokens. Pipe separated.
	Default is no null tokens.
	-->
	<mappings>

		<mapping envisionName="starttime" nwName="start" flags="None"
	format="TimeT" envisionDisplayName="StartTime"/>
		<mapping envisionName="endtime" nwName="endtime" flags="None"
	format="TimeT" envisionDisplayName="EndTime,rt,end"/>
		<mapping envisionName="version" nwName="version" flags="None"/>
		<mapping envisionName="severity" nwName="severity" flags="None"
	envisionDisplayName="Severity|SeverityLevel"/>
		<mapping envisionName="node" nwName="node" flags="None"
	envisionDisplayName="NodeName"/>
		<mapping envisionName="event_cat" nwName="event.cat" flags="None"
	envisionDisplayName="EventCategory" format="UInt32"/>
		<mapping envisionName="event_log" nwName="event.log" flags="None"/>
		<mapping envisionName="doc_number" nwName="doc.number" flags="None"
	format="Int32"/>

	</mappings>
```

## *Deploy the RSA NetWitness Log Collector Event Source*

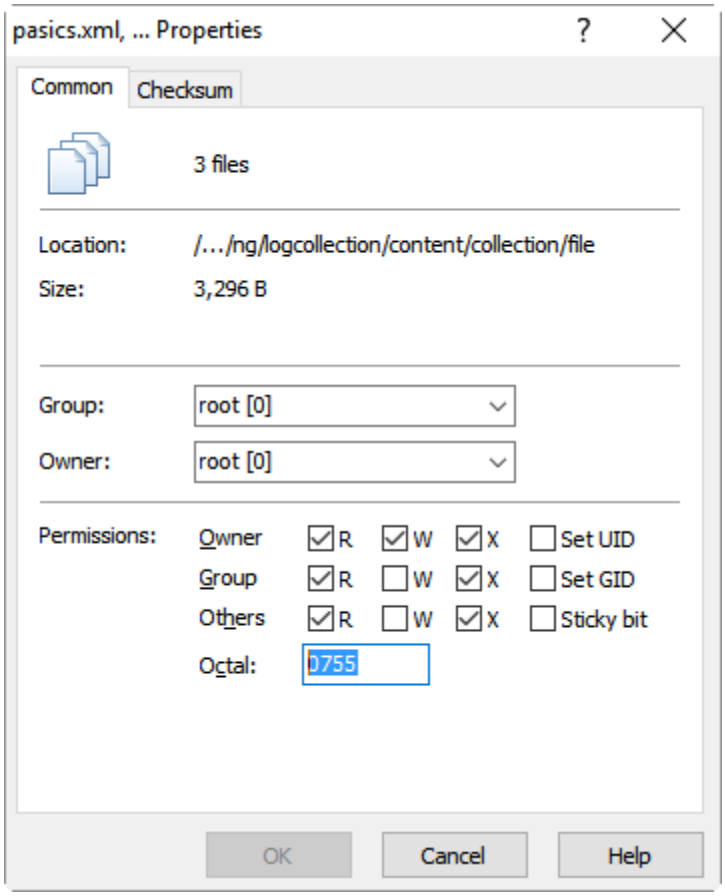
1. Unzip the file **typespec_v3.zip** and using an SCP utility (ie. WinSCP, Filezilla) copy the *.xml file onto log collector to the following location;

   `/etc/netwitness/ng/logcollection/content/collection/file/`

2. Modify xml file permissions for the pasics.xml file by executing the following command;

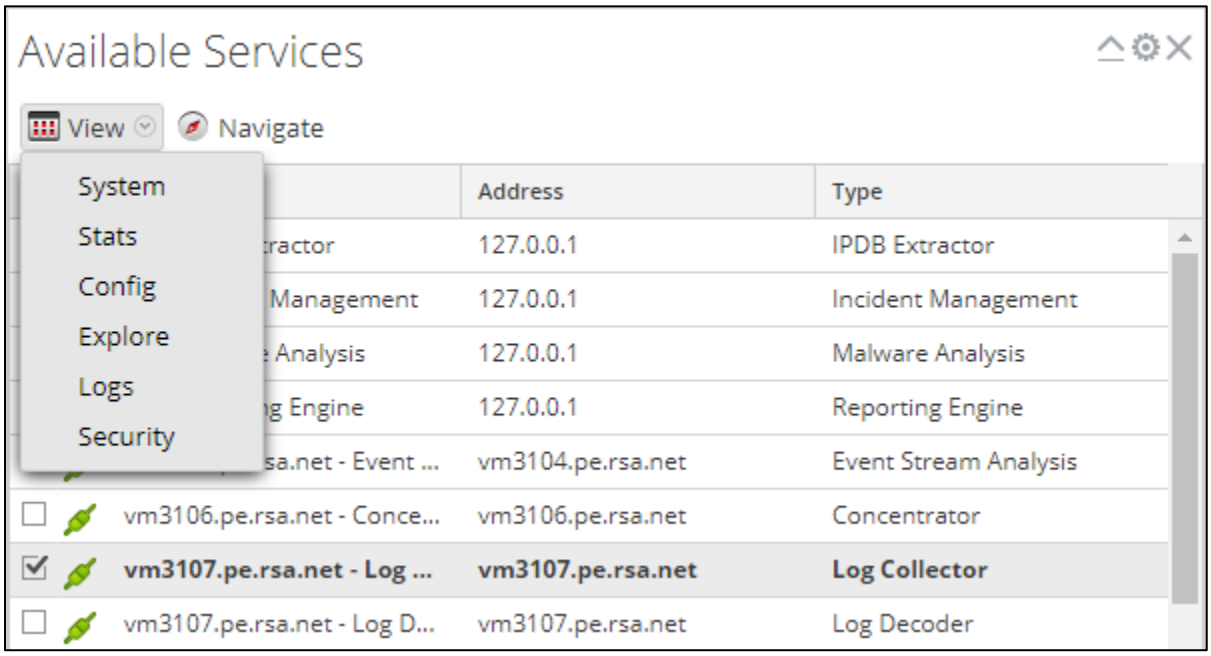
   `chmod +x pasics.xml`

   If using WinSCP of Filezilla select the pasics.xml file and set the permission to Octal: 0755.

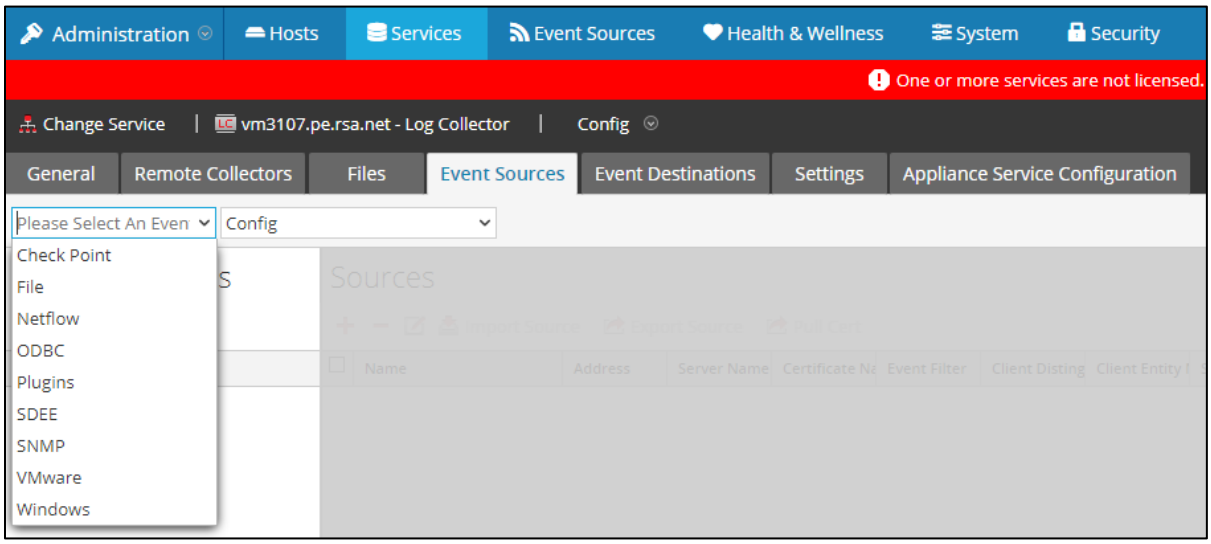



3. Restart the log decoder and log collector services.

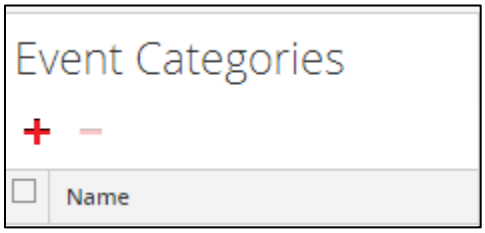
4. Create the File Reader event source from the NetWitness Dashboard within the Available Services window, check **Log Collector**, then select **View** > **Config**.



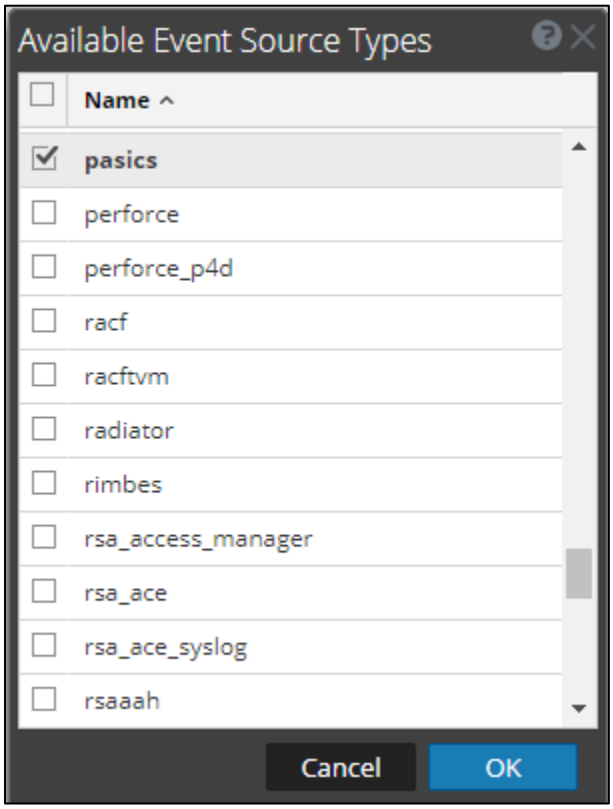

5. Select the **Event Sources** tab and from the drop down box select **File**.



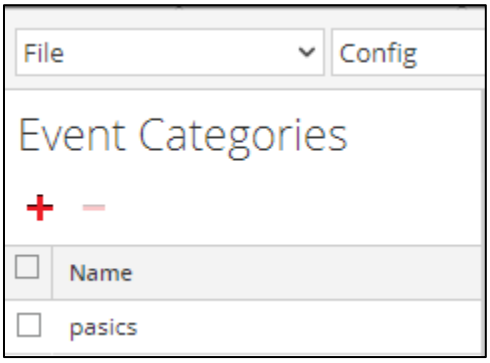
6. Click the + within the Event Categories browser frame.



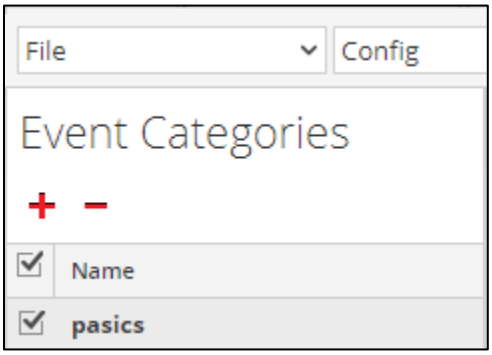

7. Select the **pasics** Event Source Type, Select **OK**.



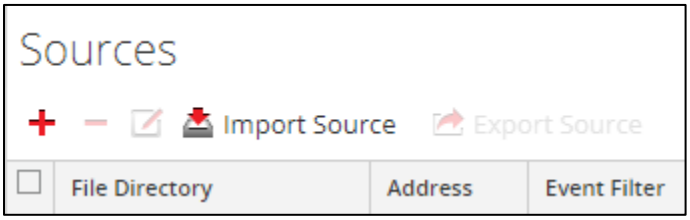
8. The **pasics** event category is now displayed and available as an event source.




9. To configure the Log Collector to read logs from a location on the log decoder/collector check the box next to the pasics Event Category.

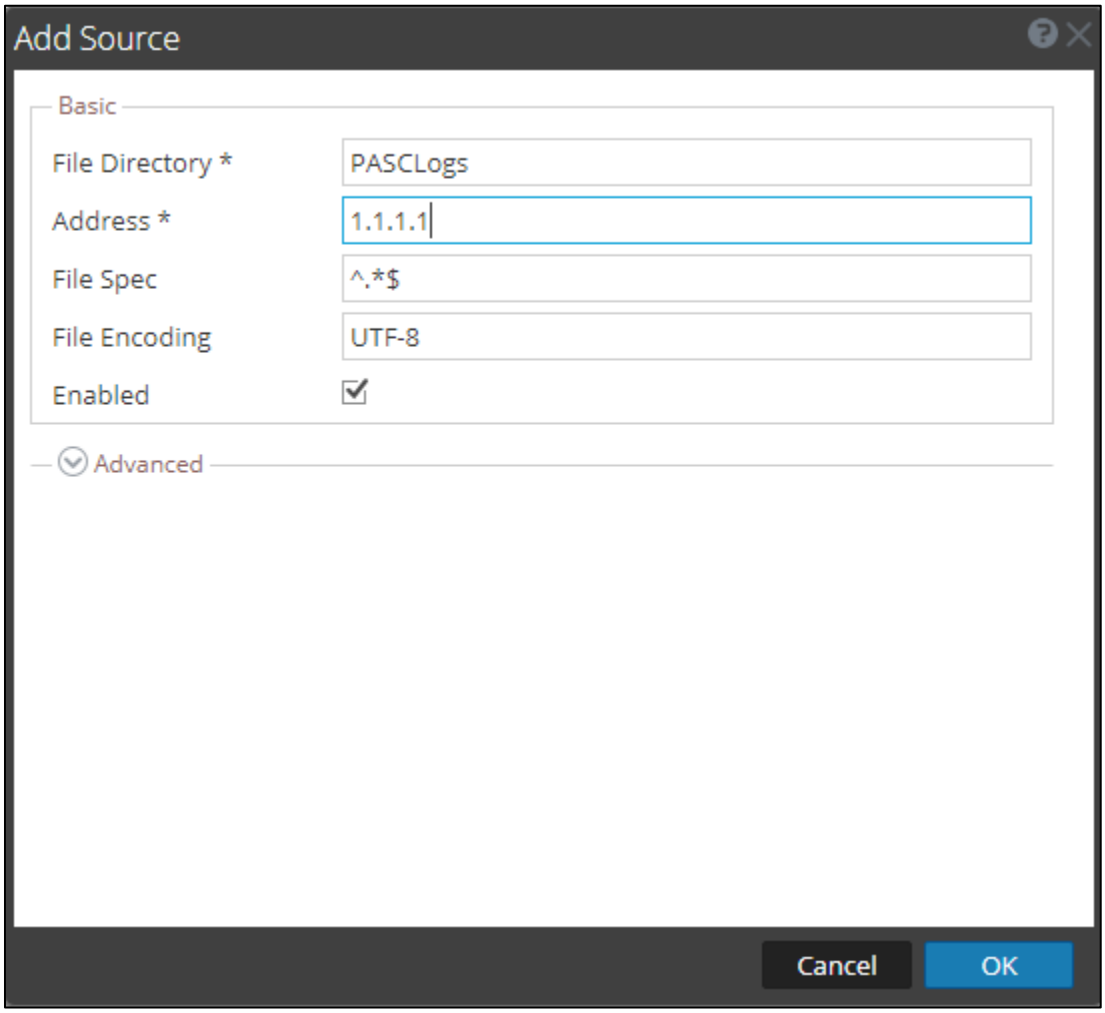



10. In the right Sources frame click the + .



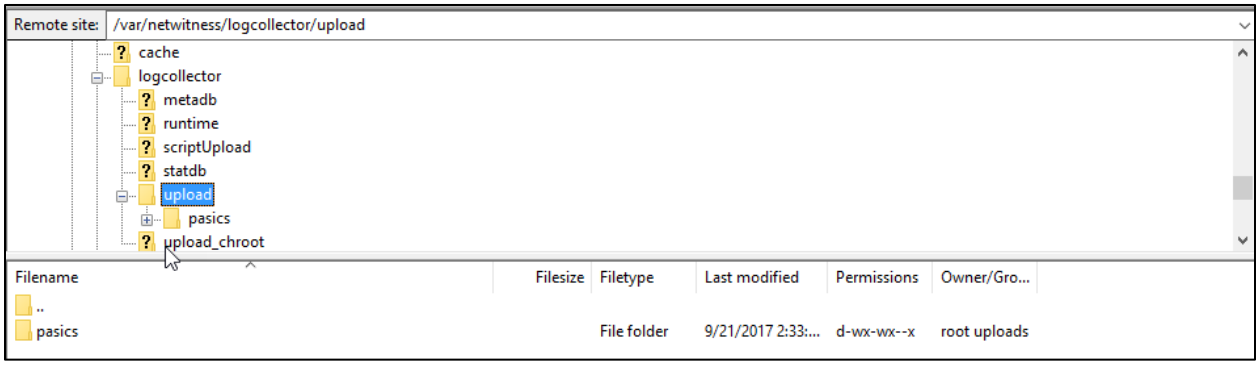
11. Enter a File Directory (PASCLogs) and an IP Address (1.1.1.1).

> **Important: The File Directory is a location within the NetWitness Log Collector/Decoder file system and the IP address will be visible as a reference through NetWitness Investigator in a later step.**



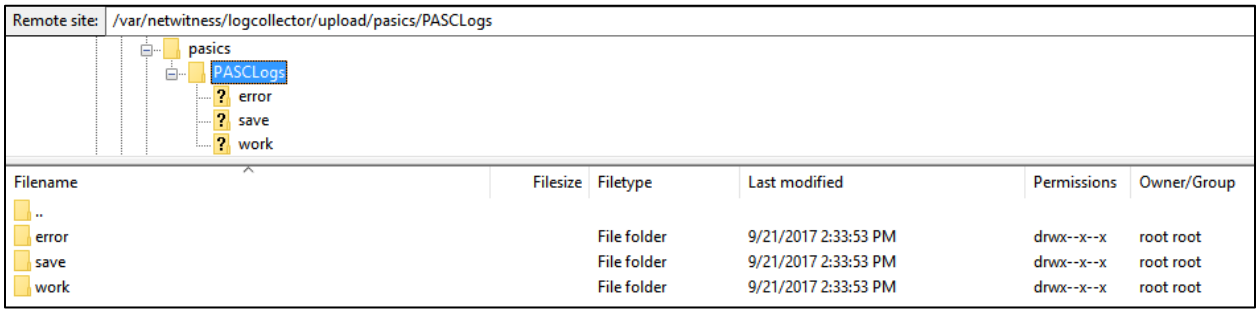
12. Once configured, a new folder structure on the Log Collector/Decoder will be created within the /var/netwitness/logcollector/upload/ folder.

**! Important: A third party tool was used to provide a visual representation of the folder created in this step and is depicted below.**

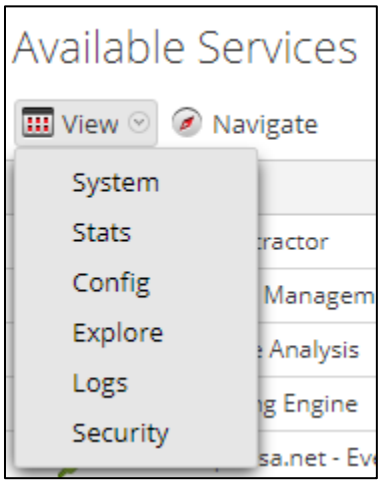



13. Within the pascis folder a new folder structure is created.

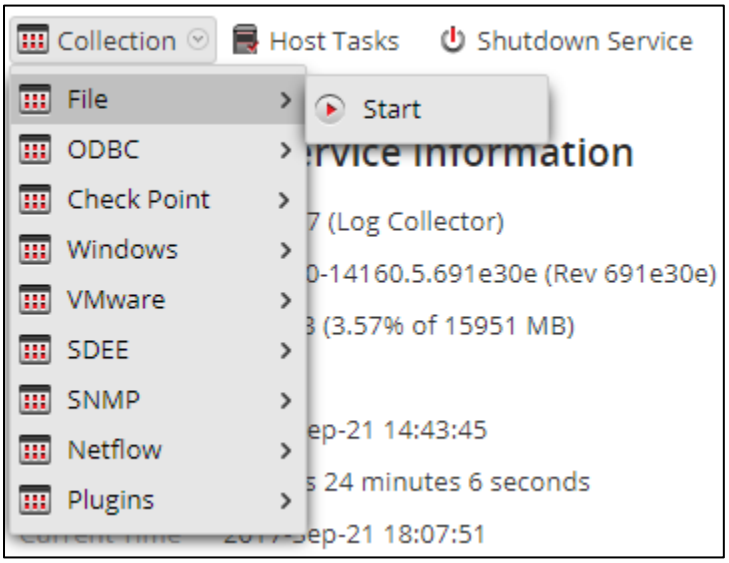
**! Important: A third party tool was used to provide a visual representation of the folders created in this step and is depicted below.**



14. Restart the Log Collector Service, open the NetWitness Administrator console and from within Avaiable Services, select **View> System**.




15. Click Collection and select **File> Start** from the drop down list.

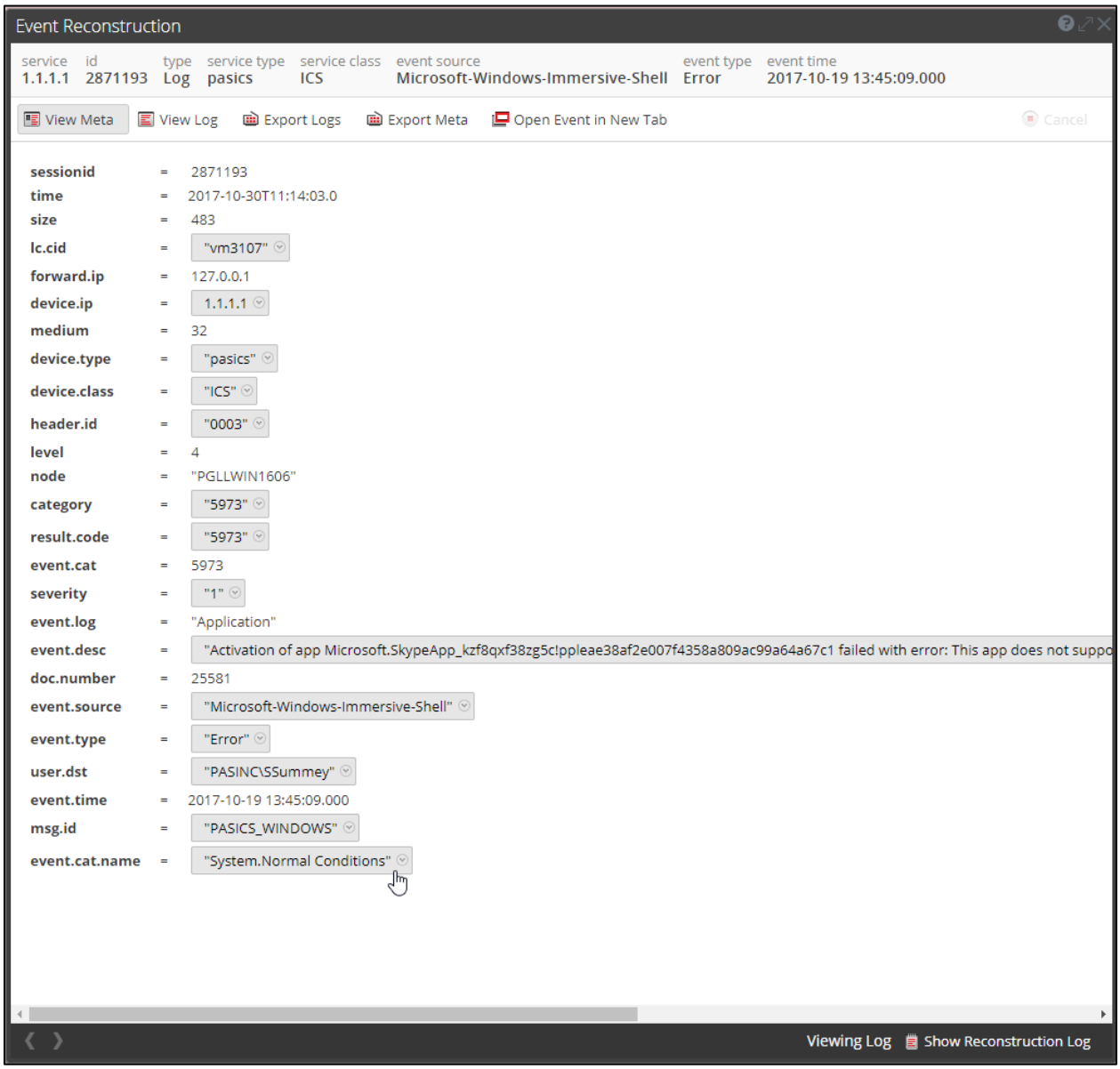



16. To process a PAS Comma Delimited log, copy the PAS Comma delimited file into the /var/NetWitness/logcollector/upload/pasics/PASCLogs folder. NetWitness will immediately ingest the event logs and remove the file. Once the file no longer appears, this indicates that the file was ingested by RSA NetWitness.

| Filename | Filesize | Filetype | Last modified | Permissions | Owner/Gro... |
|---|---|---|---|---|---|
| .. | | | | | |
| error | | File folder | 9/21/2017 2:33:... | drwx--x--x | root root |
| save | | File folder | 9/21/2017 2:33:... | drwx--x--x | root root |
| work | | File folder | 10/27/2017 3:1... | drwx--x--x | root root |
| PGLLWIN1606_NTLogEvent_Final.csv | 2,140,743 | Microsoft ... | | | |

17. Open NetWitness Investigator to display the logs from this source. The logs will appear within RSA NetWitness Investigator and can be referenced by either Device IP 1.1.1.1 or Device.Type pasics.


18. Below is an example of the RSA NetWitness metadata collected from the PAS ICS log.



# Certification Checklist for RSA NetWitness

Date Tested: October 30, 2017

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA NetWitness | 10.6.4 | Hardware or Virtual Appliance |
| PAS Global, ICS | 5.5 | Windows 2008 R2 and newer |
| | | |

| Security Analytics Test Case | Result |
|---|---|
| **Device Administration** | |
| Partner's device name appears in Device Parsers Configuration | ✓ |
| Device can be enabled from Device Parsers Configuration | ✓ |
| Device can be disabled from Device Parsers Configuration | ✓ |
| Device can be removed from Device Parsers Configuration | ✓ |
| | |
| **Investigation** | |
| Device name displays properly from Device Type | ✓ |
| Displays Meta Data properly within Investigator | ✓ |

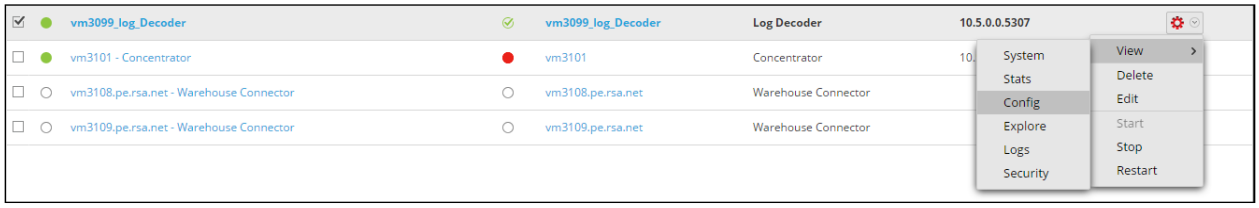
✓ = Pass ✗ = Fail N/A = Non-Available Function

# Appendix

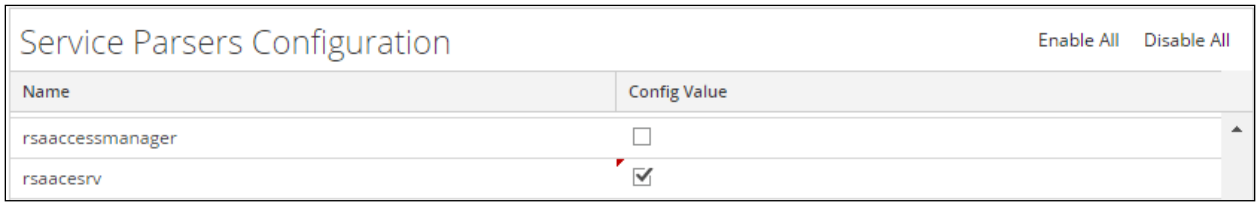
## Security Analytics Disable Device Parser

To disable the NetWitness Integration Package but not delete the XML from the system, perform the following:

1. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View> Config.**




2. From the **Service Parses Configuration** window, scroll down to the device you wish to disable and uncheck the Config Value checkbox.




3. Click **Apply** to save settings.

## NetWitness Remove Device Parser

To remove the NetWitness Integration Package files from the environment, perform the following:

1. Connect to the NetWitness Log Decoder/Collector Server using SSH and open the **/etc/netwitness/ng/envision/etc/devices** folder.
2. Search for the device you are targeting for removal and delete the folder containing the device xml.
3. Returning the system to its original state will require either modifying or removing the **table-map-custom.xml** based on your systems configuration. The table-map-custom.xml file is located in the **/etc/netwitness/ng/envision/etc** folder of the NetWitness Log Decoder(s).