RSA® NETWITNESS®
Intel Feeds Implementation Guide

Anomali ThreatStream

Jeffrey Carlson, RSA Partner Engineering
Last Modified: 06/27/2017

RSA READY

Solution Summary

Anomali ThreatStream combines threat data from feeds and other sources with data from inside the network to surface relevant threats to an organization. By mapping Indicators of Compromise (IOCs) with a strategic threat model, analysts using the ThreatStream platform are able to quickly identify, investigate and react to security threats. Anomali ThreatStream enables customers to combine intelligence information from the service with their own data within RSA NetWitness Suite, enabling them to apply current, relevant threat intelligence to their environment.

RSA NetWitness Features	
Anomali ThreatStream	
Feed format	csv
Collection method	http
Feed Collection Frequency	Hourly

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Anomali ThreatStream 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 ThreatStream 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 Anomali ThreatStream is properly configured and secured before deploying to a production environment. For more information, please refer to the Anomali ThreatStream documentation or website.**

Anomali ThreatStream Configuration

After you complete the ThreatStream Link setup, ThreatStream Link will download threat intelligence from the ThreatStream platform, which it stores locally until the RSA NetWitness platform is ready to obtain this information from it. To ensure completeness of threat intelligence information, Anomali recommends allowing ThreatStream Link to run for about 24 hours before enabling the NetWitness platform to receive threat intelligence from ThreatStream Link the first time.

To enable your RSA NetWitness platform to start receiving threat intelligence feeds from ThreatStream Link, you must do the following:

1. Download the Anomali content pack from the Downloads page of the ThreatStream platform. Unzip the package to access these files:

   RSA_TS_Plugin.txt

   ThreatStreamRules.zip

   ThreatStreamReports.zip

   tsdomain.xml

   tshash.xml

   tsurl.xml

   tsip.xml

   tsemail.xml

2. Create ThreatStream feeds for all five Indicator of compromise (IOC) types on the RSA NetWitness platform. See the **RSA NetWitness Analytics Feed Configuration** section of this document.

3. Install the Anomali plug-in for RSA for context menu actions. See **Installing the Anomali ThreatStream Context Menu Action** below.

4. **Install the Anomali ThreatStream Rules and Reports** as described below.

RSA NetWitness Configuration

RSA NetWitness Custom Feed Configuration

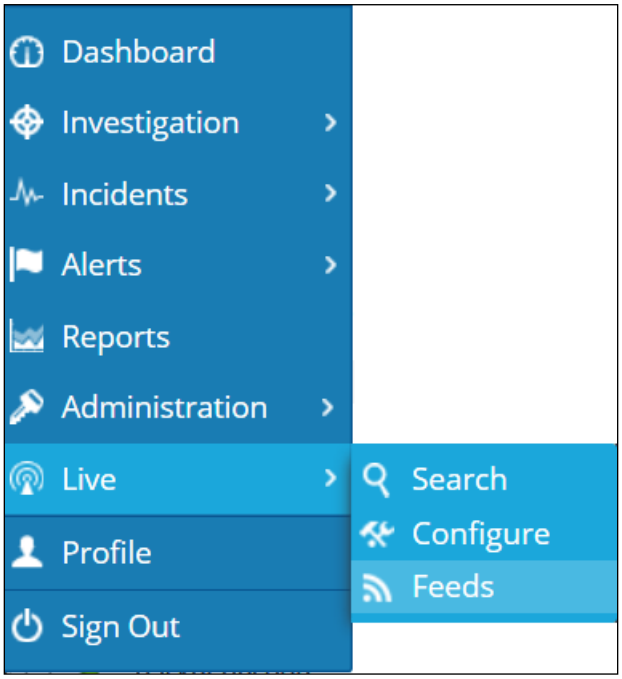
Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder follow the steps below for your integration.

To extend the functionality of RSA NetWitness Feeds for use with NetWitness rules and notifications please refer to **http://sadocs.emc.com/**.

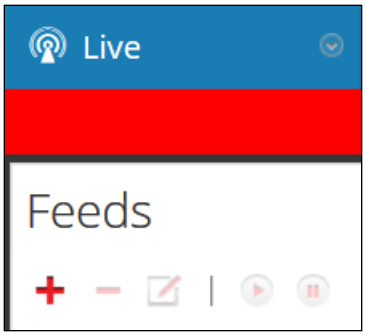
Packet Decoder Configuration

RSA NetWitness Analytics Feed Configuration

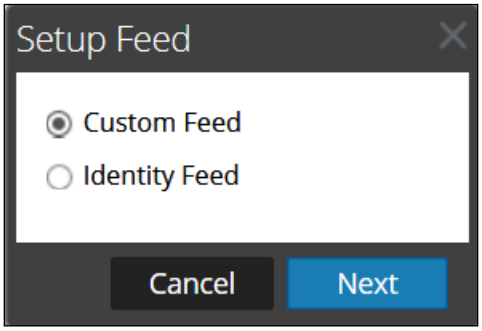
1. From the RSA NetWitness Dashboard Select **Live**, **Feeds**.



2. Select the + in the Live Feeds Window to setup the feed.



3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.

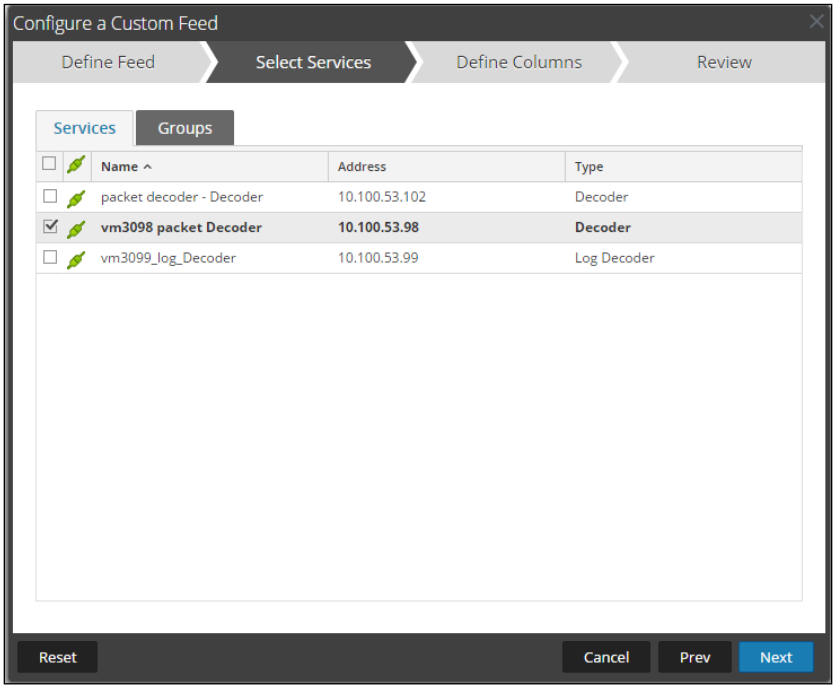


4. Enter the following parameters:

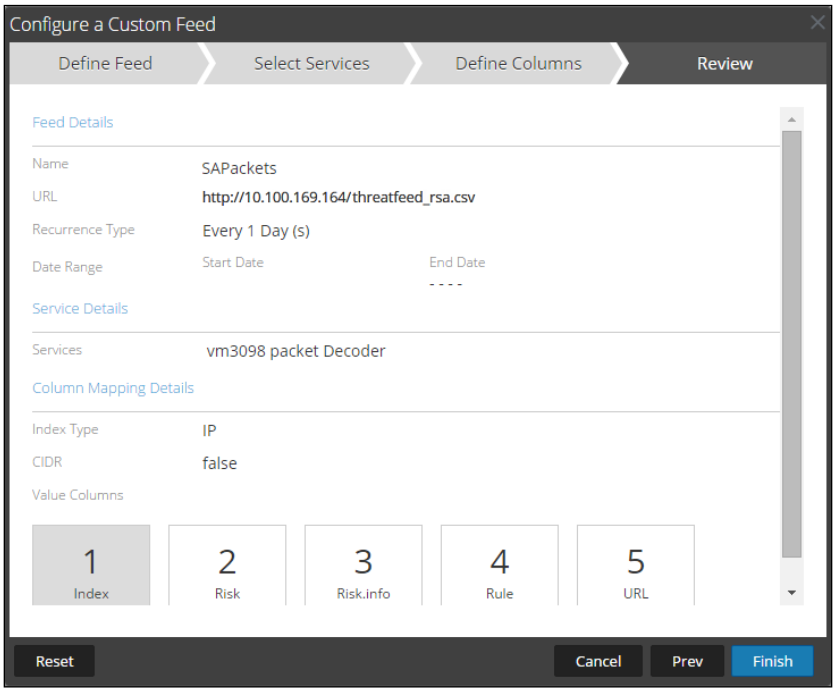
Feed Task Type	Whether the feed will be refreshed on demand or on a recurring basis. Select **Recurring**
Name	A meaningful name for the feed. Enter the following: **tsdomain**—for the domain IOC feed **tshash**—for the hash IOC feed **tsurl**—for the URL IOC feed **tsip**—for the IP IOC feed **tsemail**—for the email IOC feed
URL	URL to which RSA NetWitness will make an HTTP connection to ThreatStream Link. Use this format: **http://<your_ ThreatStream _link_host>:8789/<CSV_file_ name>** where CSV_file_name is: **threatstream_rsa_domain.csv** **threatstream_rsa_hash.csv** **threatstream_rsa_url.csv** **threatstream_rsa_ip.csv**

	threatstream_rsa_email.csv **NOTE:** Click **Verify** to ensure RSA NetWitness can access the URL.
Recur Every	How frequently RSA NetWitness will poll ThreatStream Link for updates. Enter 1 hour
Advanced Options	Browse to access the .xml files that were included in the content pack that you downloaded earlier. Depending on the feed you are configuring, select one of the following: **tsdomain.xml** **tshash.xml** **tsurl.xml** **tsip.xml** **tsemail.xml**

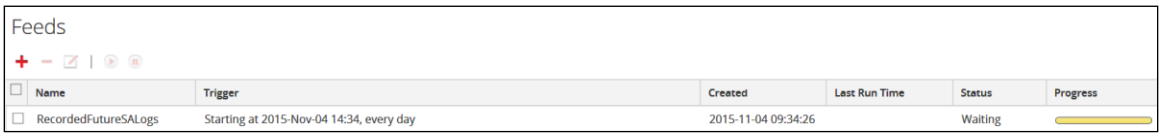
5. Select the RSA NetWitness Packet Decoder Service checkbox and select **Next**.



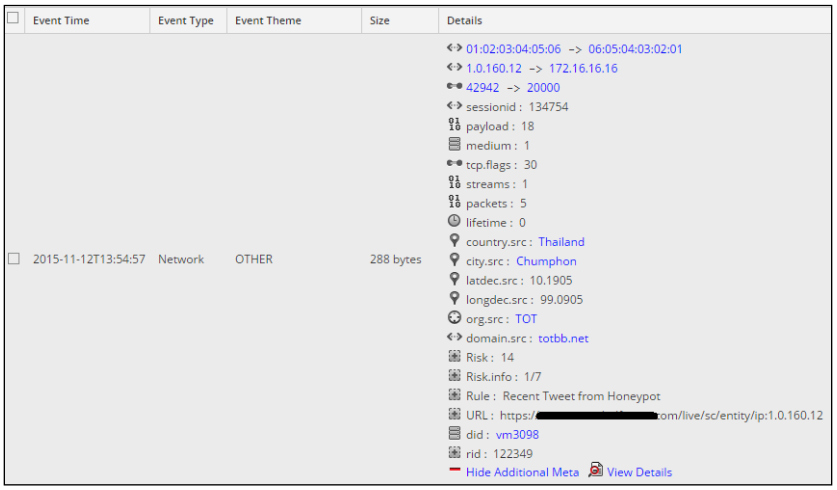
6. Select **Finish**, to complete the setup of the Feed Integration.



7. Initially the status will appear as **Waiting** and the Progress will be **yellow** until RSA NetWitness completes the transfer of the Feed. Once completed the Status will display **Completed** and the Progress will be **green**. Depending on the size of the feed it may take a while for RSA NetWitness to download all Threat Intel from your provider.



8. Once completed and if you have any threat events, the meta will appear as normal text.



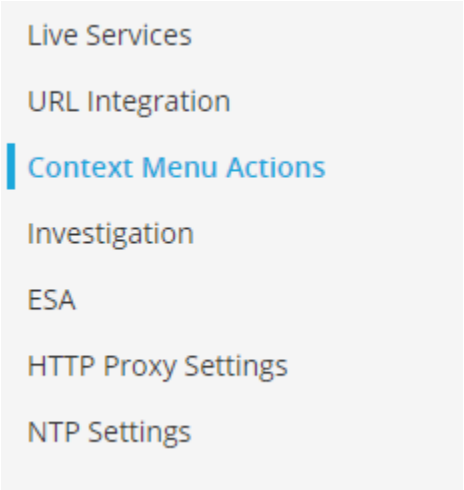
Installing the Anomali ThreatStream Context Menu Action

To install the Anomali ThreatStream plug-in that enables "right-click" functionality in NetWitness Investigator, perform the following steps:

1. Log in to the NetWitness platform as a user who has privileges to install a context menu action.

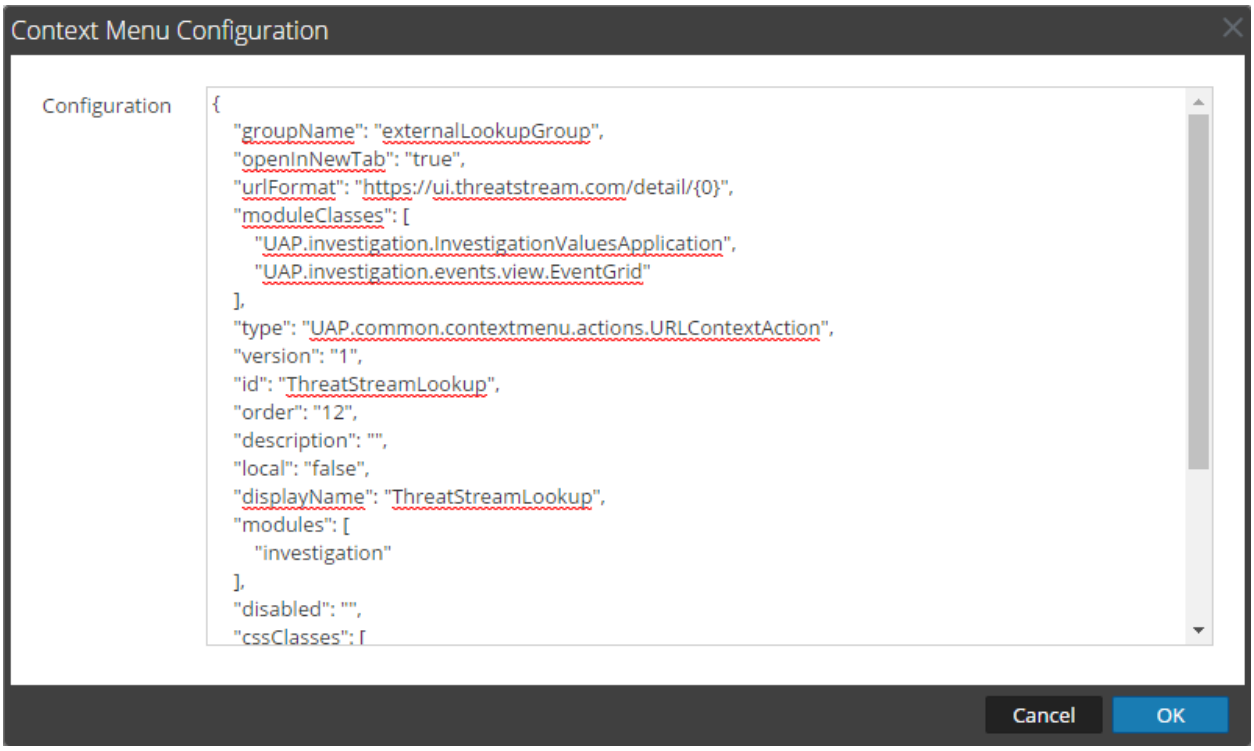
2. Open the **RSA_TS_Plugin.txt** file you downloaded earlier using a text editor such as Notepad. Copy the contents of this file.

3. Click **Dashboard > Administration > System > Context Menu Actions**.



4. Click the **+** sign to create a new Context Menu Configuration.

5. Paste the contents of the **RSA_TS_Plugin.txt** file you copied earlier.

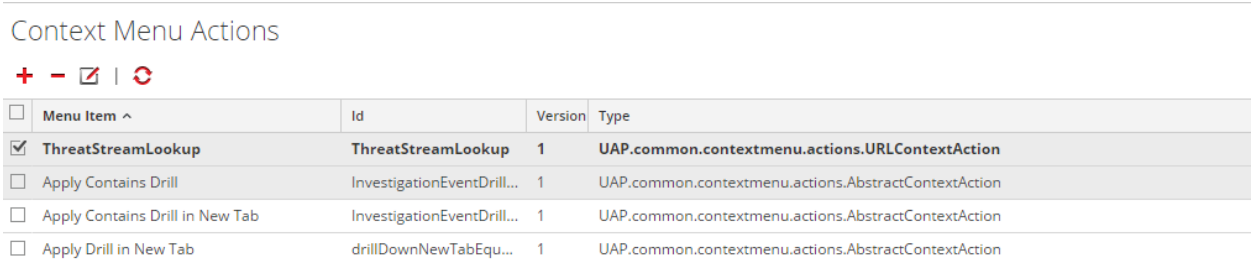


6. Change the following line:
   `UAP.investigation.InvestigationValuesApplication` to
   `UAP.investigation.navigate.view.NavigationPanel`

7. Remove the `"order": "12",` line (optional).

8. Click **OK**.

A Context Menu Action called **ThreatStreamLookup** is created, as shown in the following figure:

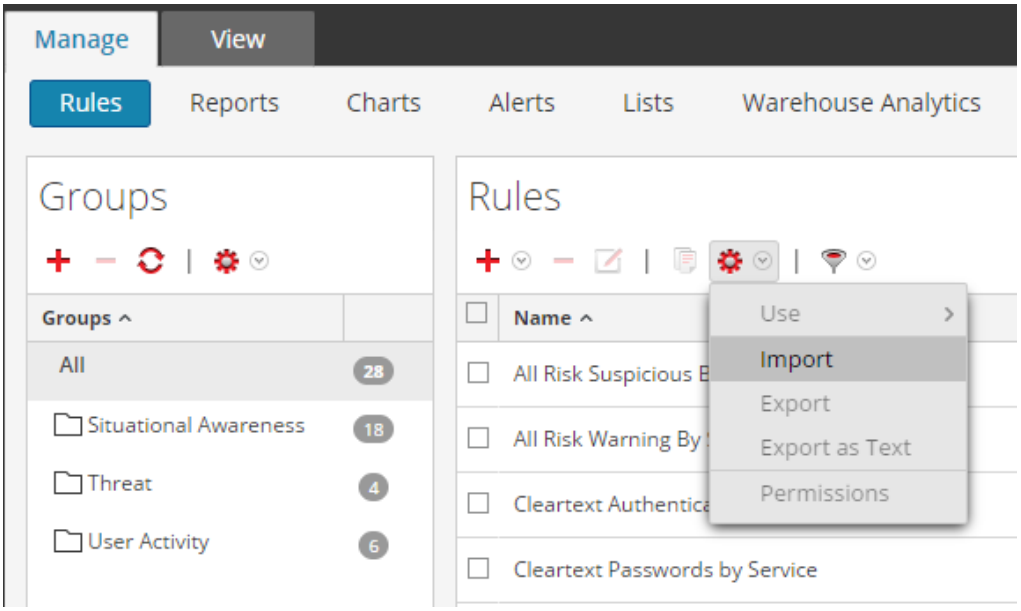


Installing the Anomali ThreatStream Rules and Reports

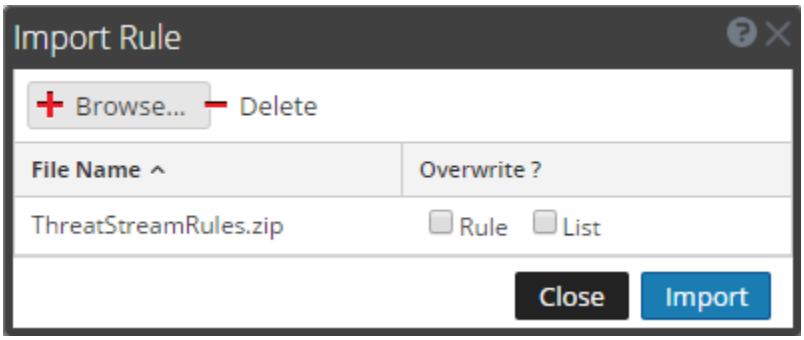
The Anomali RSA Content Pack contains two .zip files for creating rules and reports. To create the appropriate rules in RSA NetWitness, perform the following steps:

To Create Rules:

1. Log in to the NetWitness platform as a user who has privileges to create rules and reports.
2. Click **Dashboard > Reports**.
3. Click **Rules**.
4. Under Groups, click the settings icon and select **Import**.



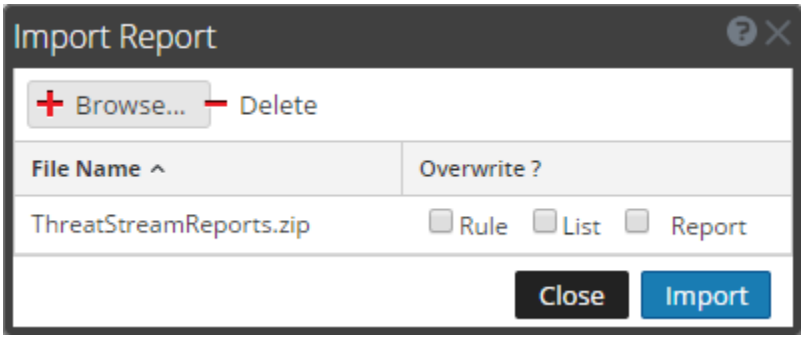
5. Click **Browse** and locate the **ThreatStreamRules.zip** file that you downloaded earlier.



6. Click **Import**.

To Create Reports:

1. Log in to the NetWitness platform as a user who has privileges to create rules and reports.
2. Click **Dashboard > Reports**.
3. Click **Reports**.
4. Under **Groups**, click the settings icon and select **Import**.
5. Click **Browse** and locate the **ThreatStreamReports.zip** file that you downloaded earlier.



6. Click **Import**.

Once the rules and reports have been imported they can be added to any custom Dashboards you wish to create. For more information on this topic, visit:

https://community.rsa.com/docs/DOC-75250

Certification Checklist for RSA NetWitness

Date Tested: June 6th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
Anomali ThreatStream	SaaS	SaaS

Security Analytics Test Case	Result
Investigation	
Threat Intelligence Feed is received through Decoder Meta	✓
Threat Intelligence Feed is received through Packet Decoder	✓

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

Known Issues

Please note that two of the feed configuration files:

tshash.xml

tsurl.xml

were not validated as of the publishing of this document. They should, however, function as designed.

Please also note that if you are intending to use the **tshash.xml** file with other products that populate the **checksum** metakey, you may wish to change the following line:

```
<MetaCallback valuetype="Text" name="ir.md5"/>
```

to:

```
<MetaCallback valuetype="Text" name="checksum"/>
```