RSA® NETWITNESS®
Intel Feeds
Implementation Guide

Recorded Future Cyber Threat Intelligence

Daniel R. Pintal, RSA Partner Engineering
Last Modified: October 2, 2017

RSA READY

Solution Summary

Recorded Future arms you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, Recorded Future's patented Web Intelligence Engine continuously analyzes the entire web to give you unmatched insight into emerging threats.

Security Analytics imports the intelligence from Recorded Future and enhances the events collected from third party sources by appending threat intelligence to metadata when and where needed.

By using SA Event Stream Analysis (ESA) for notification the events and the combined threat intelligence can be used to create alerts to advise security staff of potential malicious activity.

RSA NetWitness Features	
Recorded Future Cyber Threat Intelligence	
Feed format	xml, csv
Collection method	http, local file
Feed Collection Frequency	Hourly, Daily, Weekly

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Recorded Future integrations 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 Recorded Future 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 the Recorded Future content is properly configured. For more information, please email support@recordedfuture.com **or visit or visit the** Recorded Future support site.

Intelligence Feed	File Function
Feed Contents	IP address or Domain Name, Threat Feed Provider, Risk, Risk Score, Threat type and Evidence Details (URL).

RSA NetWitness Configuration

RSA NetWitness Custom Feed Configuration

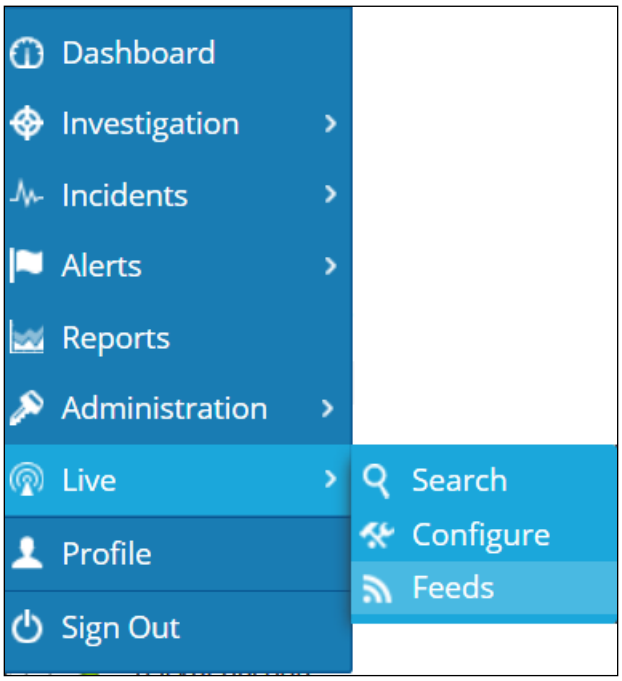
Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder, follow the steps below for your integration.

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

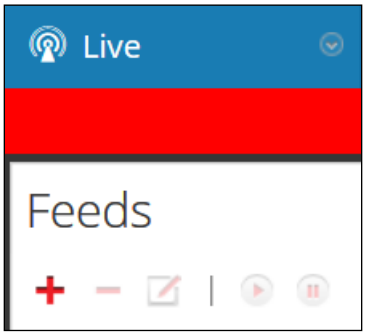
Lorg and Packet Decoder Configuration

RSA NetWitness Feed Configuration

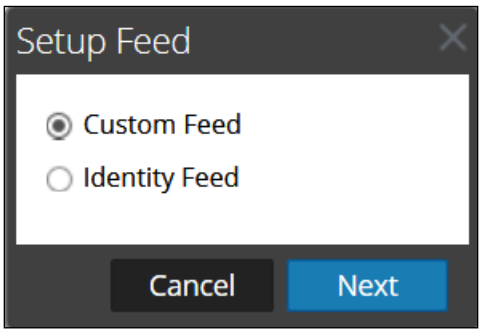
1. From the RSA NetWitness Dashboard Select **Live**, **Feeds**.



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

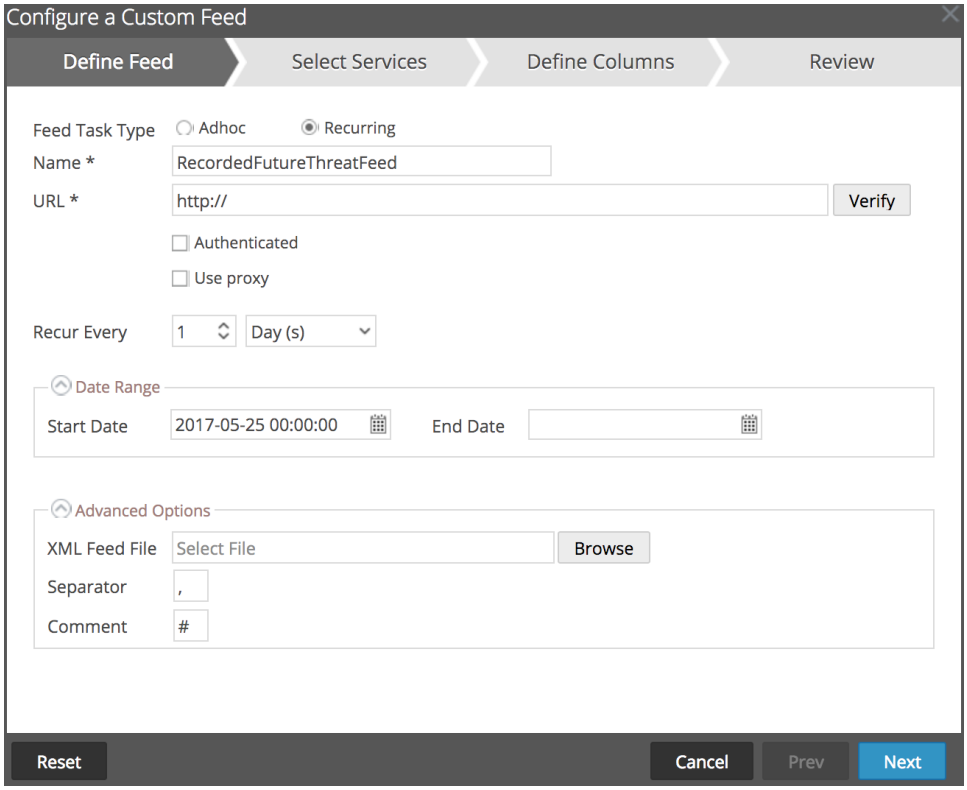


3. Select the **Custom Feed** radio button within the Setup Feed pop-up window and select **Next**.



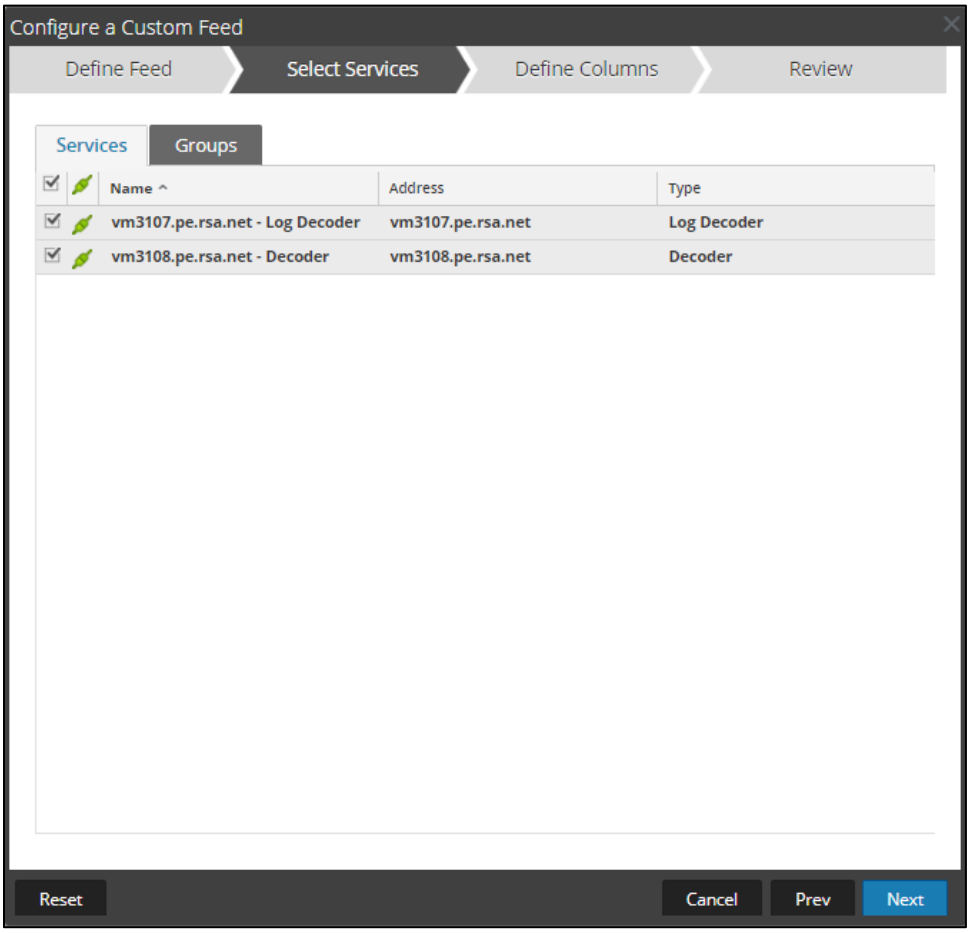
4. Select **Adhoc** if you are uploading the file once or select the **Recurring** radio button if you plan to automate the feed. Enter the **URL** of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**. Note: please contact your Recorded Future Account Manager for the correct URL to use as a custom feed.

Important: Please contact your Recorded Future Account Manager or support@recordedfuture.com for the correct URL to use as a custom feed.



Important: If using an XML feed you must configure the RSA NetWitness Advanced Options and use an XML Feed File.

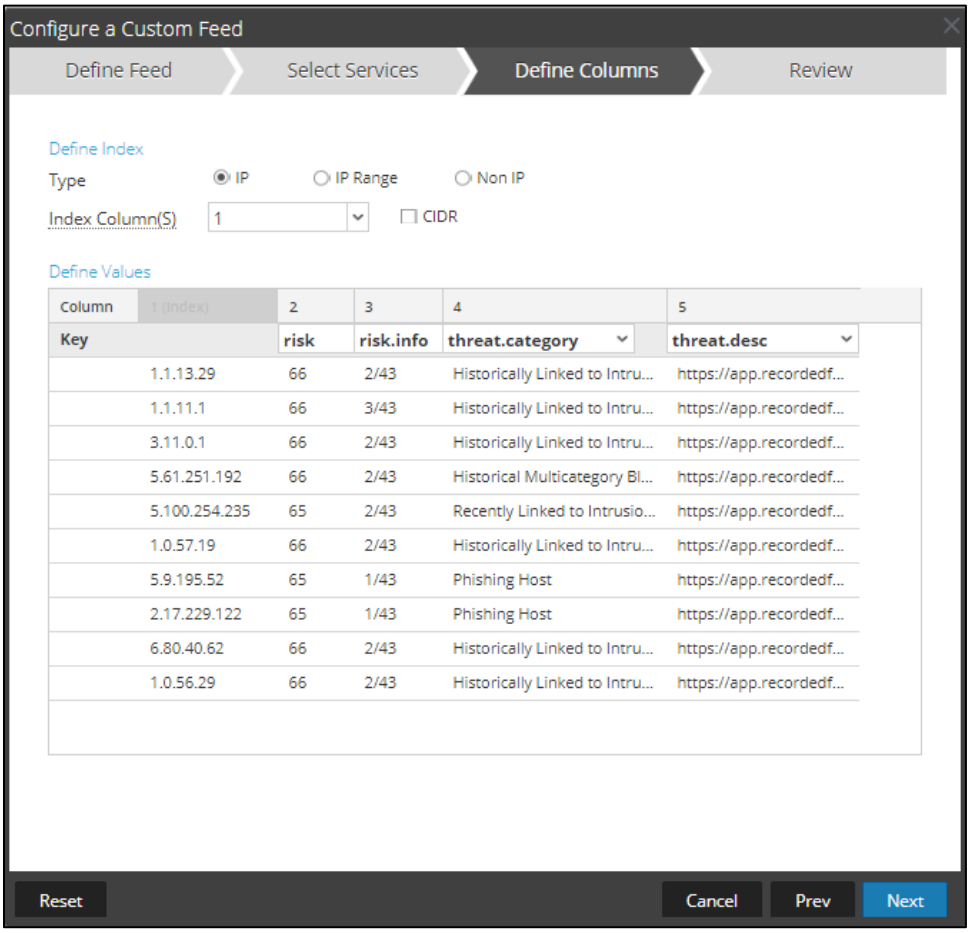
5. Select the **RSA NetWitness Log Decoder Service checkbox** and/or the **RSA NetWitness (Packet) Decoder Service checkbox** select **Next**.



Important: NetWitness installations having only a Log Decoder or a Packet Decoder will display one or the other, not both.

Deploying the Feed to both Log and Packet Decoders enable matching of IP event sources such as ip.dst, ip-src, ipv6-src, ipv6-dst.

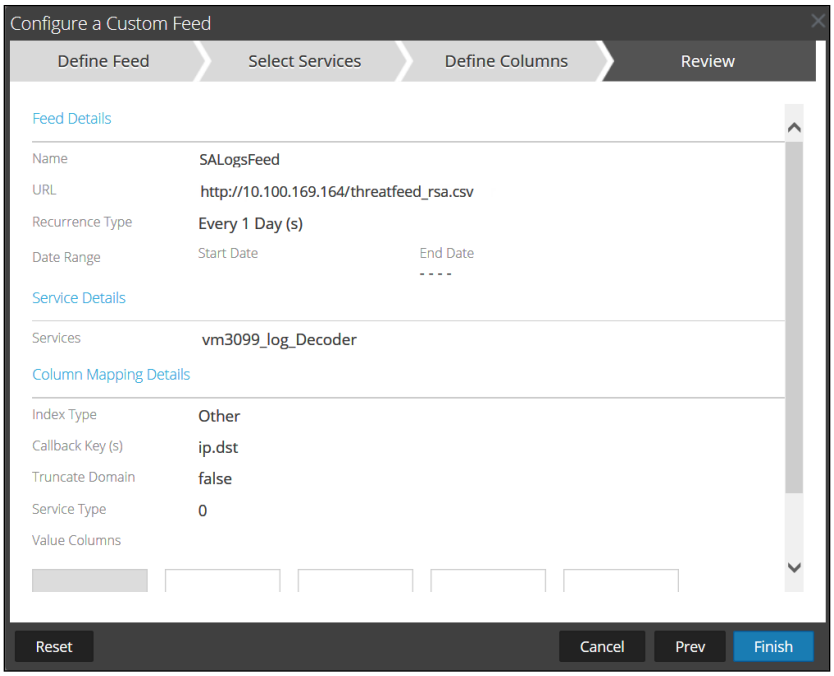
6. Define the **Type** as **IP** and **Index Column 1** (IP Address Field). Set the header of each column as needed and select **Next**.



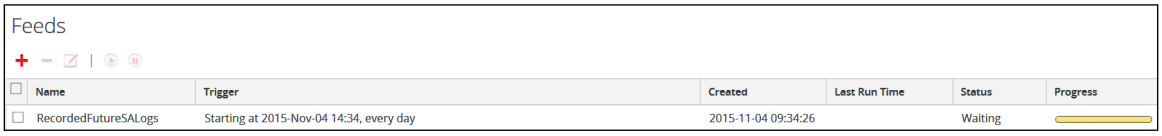
Important: The example used in this document is IP based.

Use Type Non IP for DNS threat intelligence, Callback Key(s) for alias-host or domain.dst keys.

7. Select **Finish** to complete the setup of the Feed Integration.



8. 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 some time for RSA NetWitness to download all Threat Intelligence from your provider.

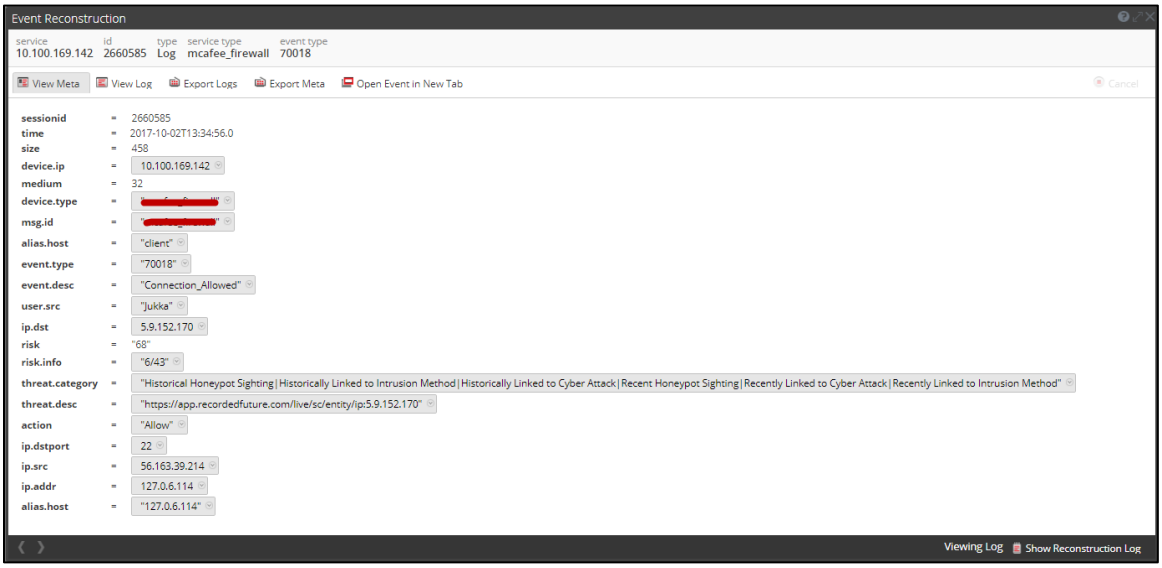


9. Modification of the table-map-custom.xml file located in the Log Decoders /etc/netwitness/ng/envision/etc folder may be required if using transient keys.

```
<?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>

<!-- Recorded Future Threat Intel Meta Keys-->

       <mapping envisionName="risk" nwName="risk" flags="None"
envisionDisplayName="Risk"/>
       <mapping envisionName="threat_name" nwName="threat.category"
       flags="None"/>
       <mapping envisionName="risk_info" nwName="risk.info" flags="None"/>
       <mapping envisionName="threat_val" nwName="threat.desc" flags="None"/>

</mappings>
```

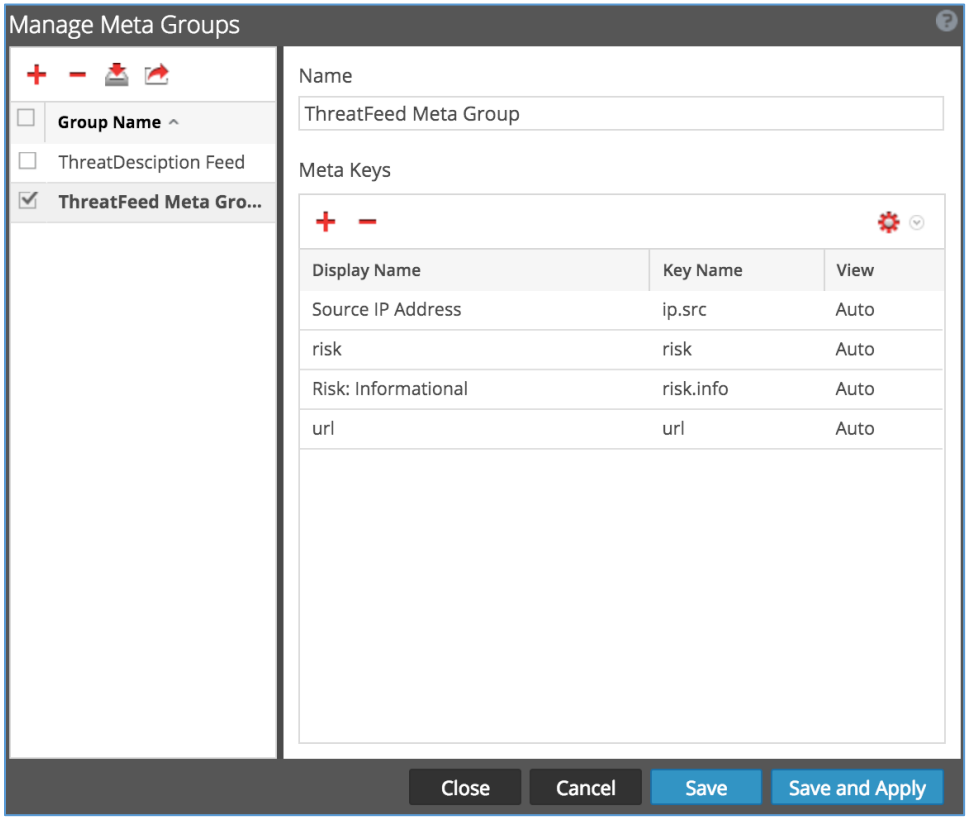
10. Once completed, restart the (Log and/or Packet) Decoder if you have any threat events, the meta will within the meta keys defined for the Recorded Future Threat feed in steps 6.

Log Example



Optional

1. Set up the **Meta Group** by going to **Investigation** and then **Navigate**. Select **Meta** and then **Manage Meta Groups**. Create a new Meta Group by clicking on the '+' icon and then set up the four key names as follows:



Certification Checklist for RSA NetWitness

Date Tested: October 2, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
Recorded Future Cyber Threat Intel.	N/A	N/A

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