RSA Ready Implementation Guide for RSA Security Analytics

Nominum Vantio 5.2

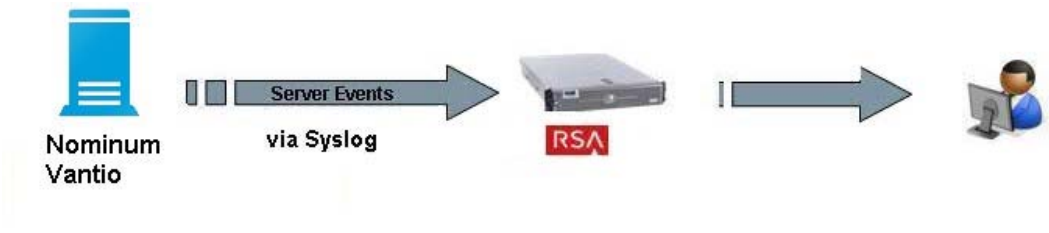
Daniel R. Pintal, RSA Partner Engineering
Last Modified: 3/1/2016

RSA READY

Solution Summary

Nominum's Vantio caching name server outputs events that are easily consumed by RSA Security Analytics for the purpose of monitoring and alerting on network activity. In doing so, security threats directed at an organization or directed at specific clients can be exposed prior to an actual security event. For example, Vantio can send an alert to Security Analytics when query loads increase beyond normal levels, indicating a potential denial of service attack. Using this same output and reporting structure, another example of the power of this combined offering is how Vantio and Security Analytics provide visibility into resource utilization. When utilization reaches abnormal levels due to non-responding name servers, an alert is generated to show the potential of a misconfigured "popular" zone. To make use of this combined solution, Vantio simply needs to be configured to send syslog messages to RSA Security Analytics. Vantio has a number of options that can be set to best match the organization's requirements on security or operations monitoring, making the overall solution both flexible and powerful.

RSA Security Analytics Features	
Vantio 5.2	
Integration package name	nominumvantiope.envision
Device display name within Security Analytics	nominumvantiope
Event source class	Application Server
Collection method	Syslog



RSA Security Analytics (SA) Community

The RSA Security Analytics (SA) 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 SA Integration Package for this guide. All Security Analytics customers and partners are invited to register and participate in the **RSA Security Analytics Community**.

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

The RSA Security Analytics package consists of the following files:

Filename	File Function
nominumvantiope.envision	SA package deployed to parse events from device integrations.
nominumvantiopemsg.xml	A copy of the device xml contained within the SA package.
table-map-custom.xml	Enables Security Analytics variables disabled by default.

Release Notes

Release Date	What's New In This Release
12/02/2013	Initial support for Nominum Vantio.
3/1/2016	RSA Security Analytics 10.5 support.

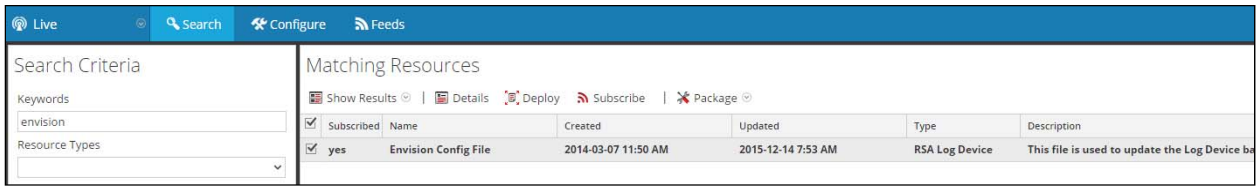
RSA Security Analytics Configuration

Deploy the enVision Config File

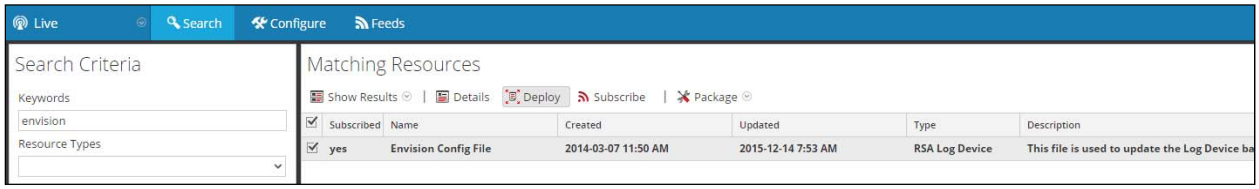
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

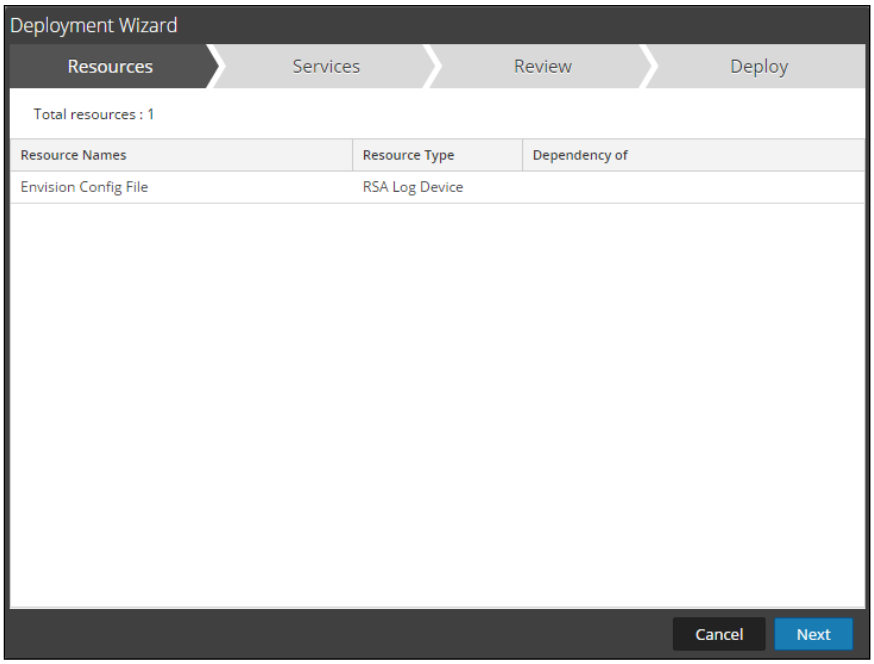
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in *Matching Resources*.
4. Select the checkbox next to **Envision Config File**.



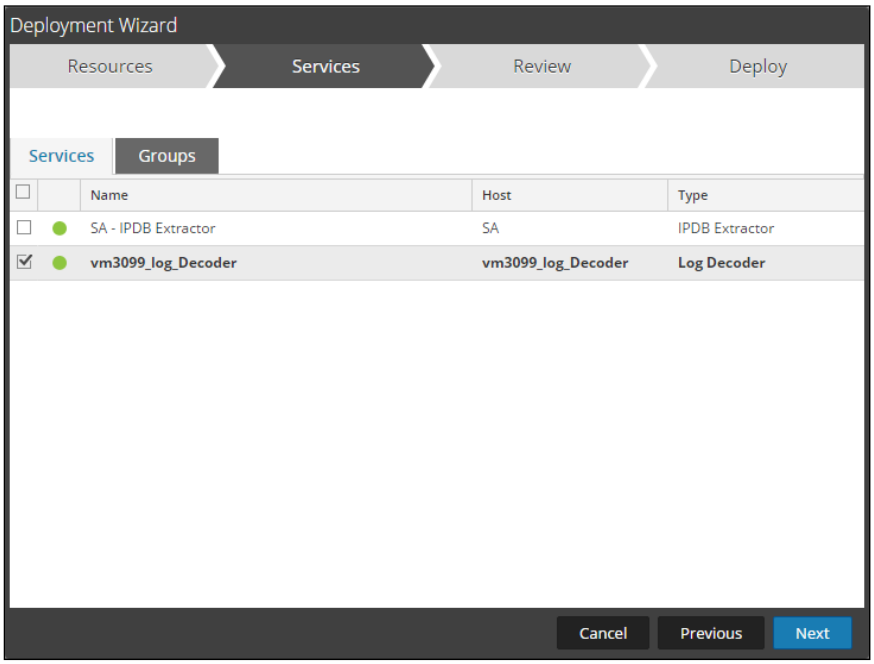
5. Click **Deploy** in the menu bar.



6. Select **Next**.

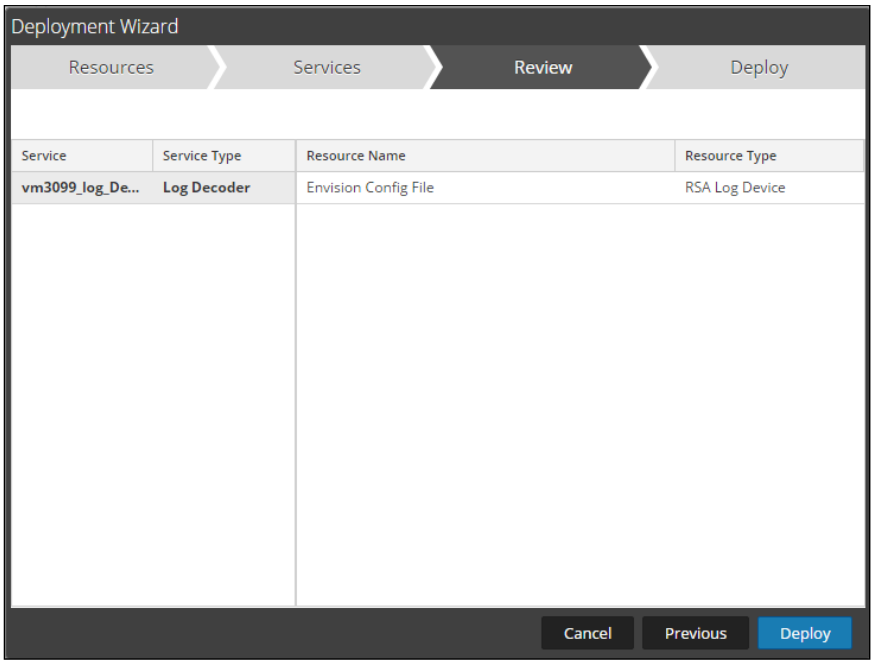


7. Select the **Log Decoder** and select **Next**.

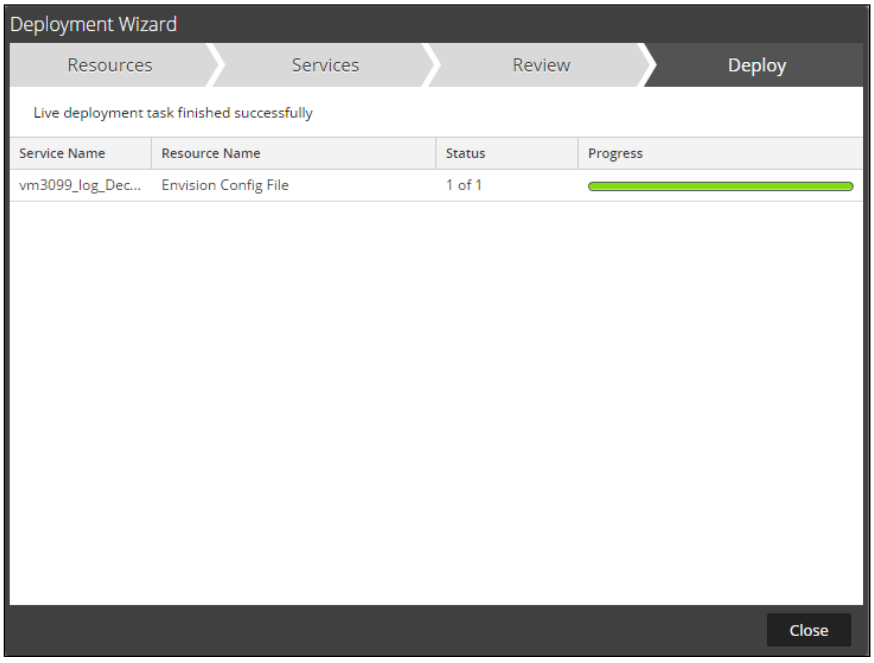


! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



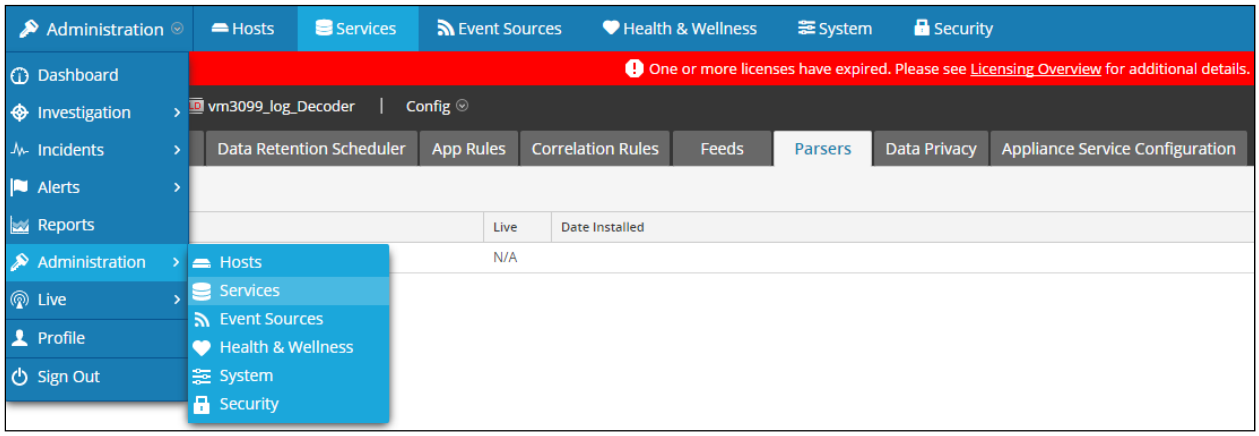
9. Select **Close**, to complete the deployment of the Envision Config file.



Deploy the Security Analytics Integration Package

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

1. From the Security Analytics menu, select **Administration > Services.**



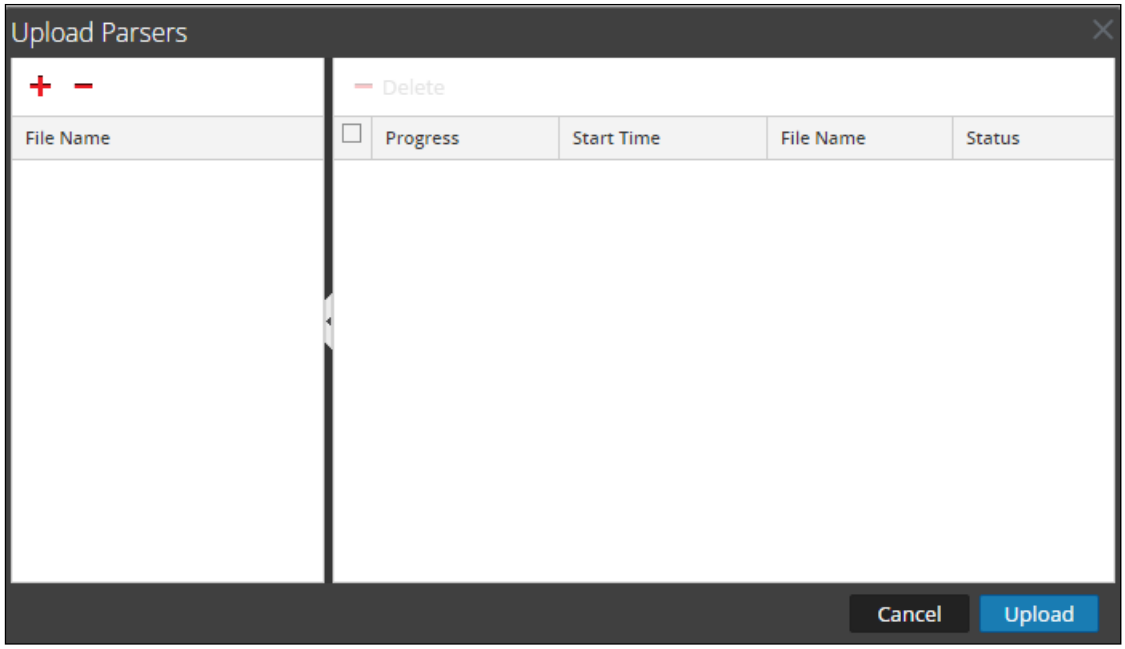
2. Select your Log Decoder from the list, select **View > Config**.

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

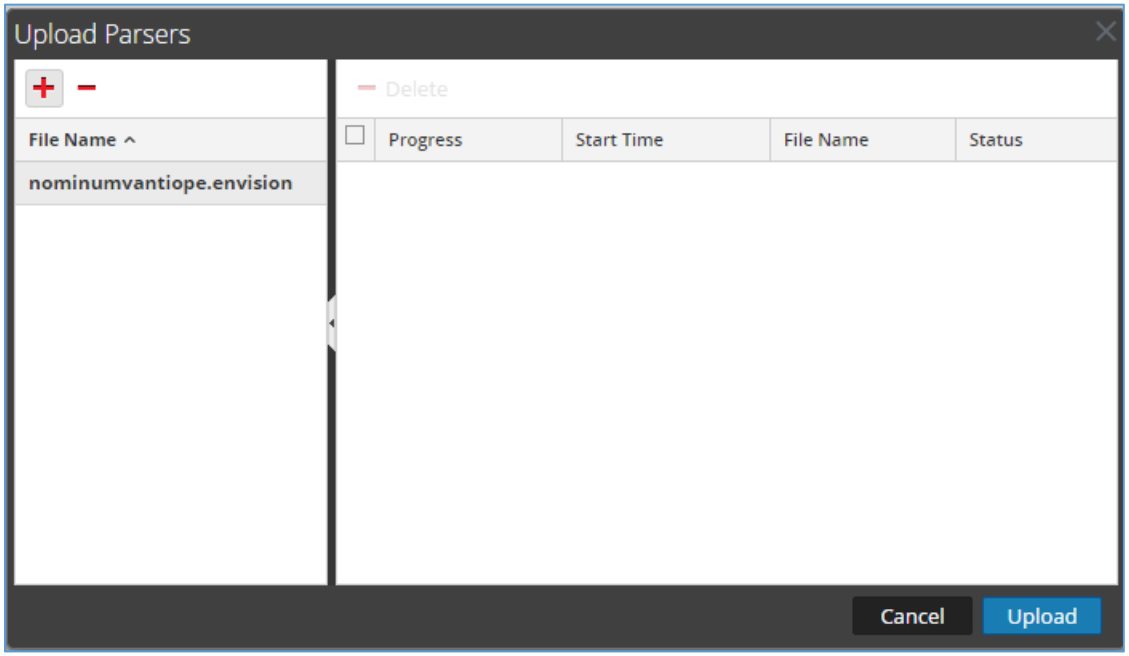
3. Next, select the **Parsers** tab and click the **Upload** button.

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

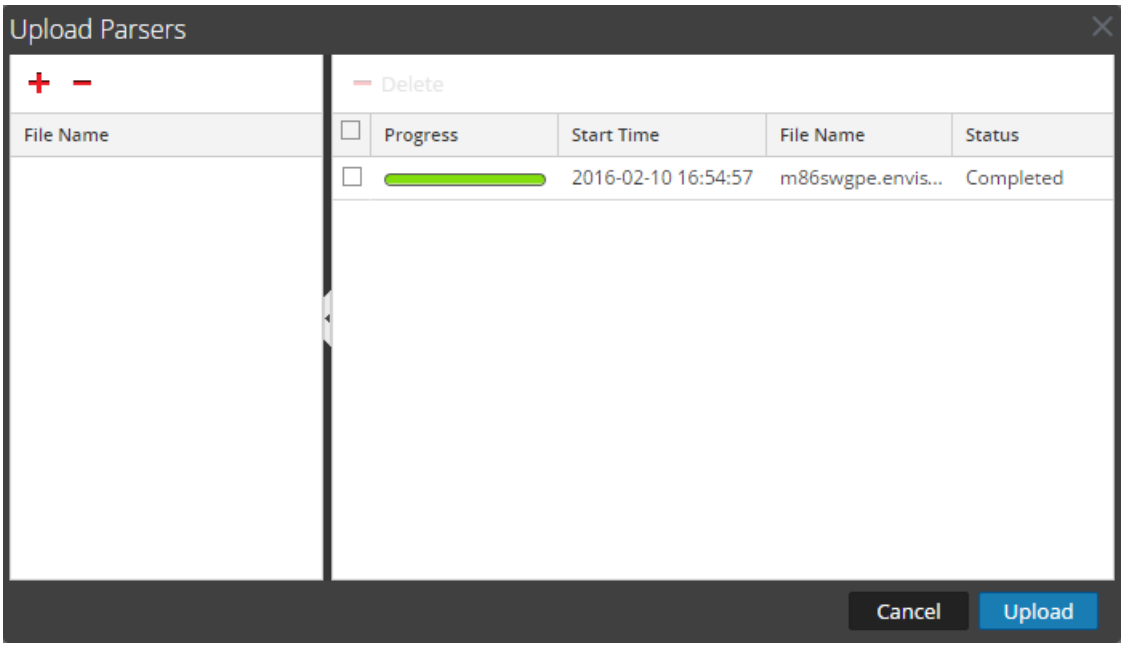
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**



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



6. Upon completion of the upload click **Cancel**.



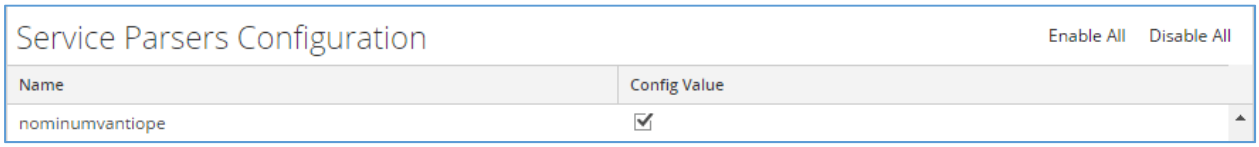
7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the *table-map-custom.xml* file from the contents of the .zip file to the */etc/netwitness/ng/envision/etc* folder. If the *table-map-custom.xml* file already exists on the log decoder(s), enter only the contents between the *<mappings>…</mappings>*.

```
<mappings>

        <mapping envisionName="result" nwName="result" flags="None" envisionDisplayName="Result|Volume|Information|Reason|Succeed/Failed"/>
        <mapping envisionName="event_state" nwName="event.state" flags="None"/>
        <mapping envisionName="domain" nwName="domain" flags="None" envisionDisplayName="DomainName"/>
        <mapping envisionName="info" nwName="index" flags="None"/>

</mappings>
```

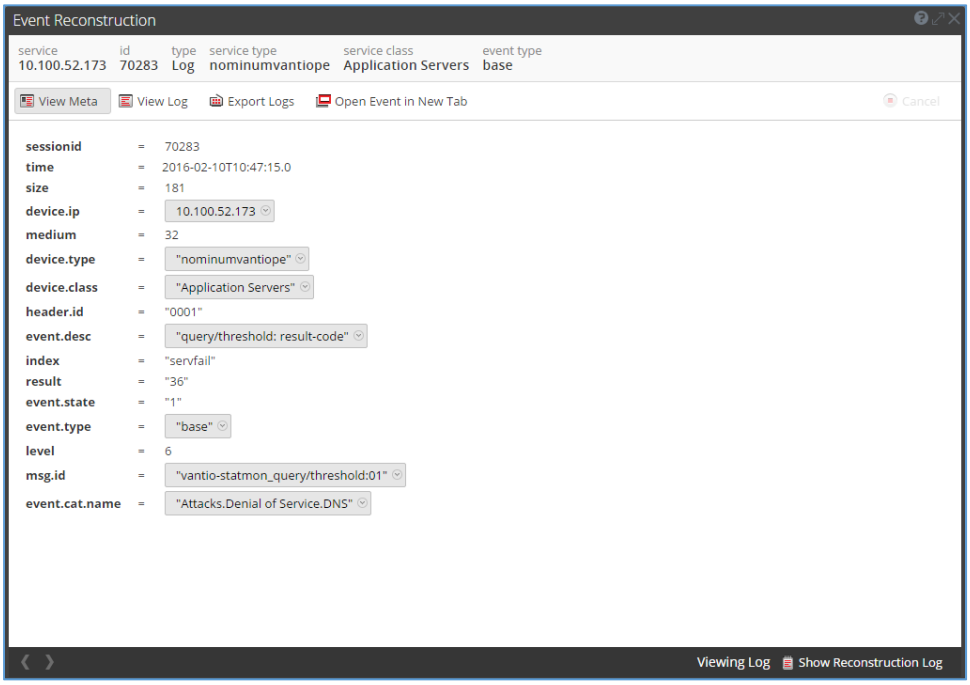
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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

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



11. The Log Decoder is now ready to parse events for this device. Below is an example of the RSA SA metadata collected from an Absolute DDS logfile.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Nominum Vantio with RSA Security Analytics. 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 Nominum Vantio 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 Nominum Vantio is properly configured and secured before deploying to a production environment. For more information, please refer to the Nominum Vantio documentation or website.**

Vantio Configuration

The first step is to configure Vantio to send all log messages to RSA Security Analytics.

1. Edit **/etc/syslog.conf** to include the following lines
   # Log Nominum remotely to RSA Security Analytics
   local1.* @<*IP address of Security Analytics*>
2. Restart the syslogd daemon:
   > **kill -HUP `cat /var/run/syslogd.pid`**
3. Edit the file **/usr/local/nom/etc/sysconfig/vantio** and add the following line:
   VANTIO_SYSLOG_FACILITY=local1
4. Restart Vantio:
   >/etc/init.d/vantio restart

As the next step you want to consider the security releated events of interest and configure Vantio to emit log messages accordingly. Please refer to the Vantio user guide for more details.

Certification Checklist for RSA Security Analytics

Date Tested: March 9, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
Nominum Vantio	5.2	5.2, Redhat Enterprise Linux 5/6

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

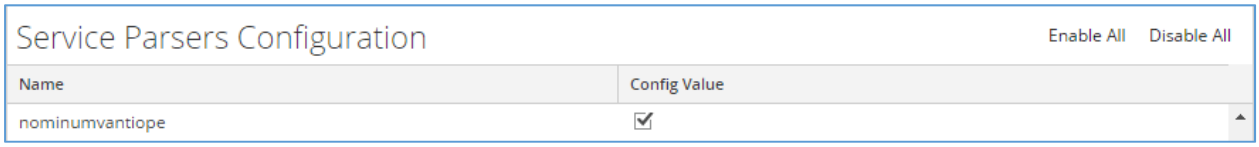
Appendix

Security Analytics Disable Device Parser

To disable the Security Analytics 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.

Security Analytics Remove Device Parser

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

1. Connect to the Security Analytics 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 SA Log Decoder(s).