RSA Ready Implementation Guide for RSA Security Analytics

AirTight Networks SpectraGuard Enterprise (SGE) 6.7

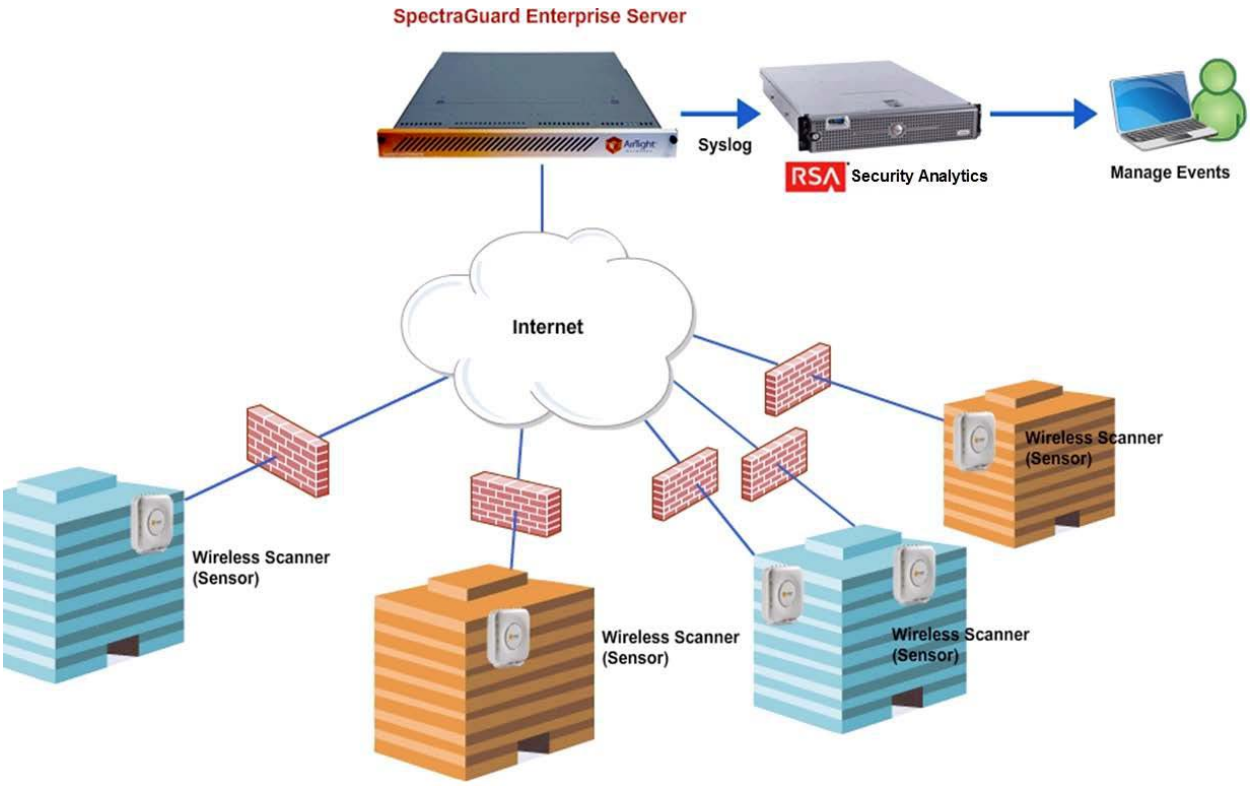
Daniel R. Pintal, RSA Partner Engineering
Last Modified: February 12, 2016

RSA READY

Solution Summary

AirTight Networks SpectraGuard Enterprise (SGE) enables enterprises to protect both wired and wireless networks and mobile client security from wireless vulnerabilities. AirTight delivers threat monitoring and automatic intrusion prevention and manages wireless network performance for maximum capacity and uptime. SpectraGuard Enterprise protects organizations from emerging threats including comprehensive 802.11n rogue APs, Multi-Pot threats, Denial of Service, and WEP cracking attacks. By integrating with RSA Security Analytics, SGE log activity can be used in an effective security log management solution for real-time alerting, correlated rules and events, and scheduled reporting.

RSA Security Analytics Features	
SpectraGuard Enterprise 6.7	
Integration package name	atnspectraguardpe.envision
Device display name within Security Analytics	atnspectraguardpe
Event source class	IPS
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
atnspectraguardpe.envision	SA package deployed to parse events from device integrations.
atnspectraguardpe.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 AirTight Networks SpectraGuard Enterprise (SGE) 6.7
2/12/2016	SA 10.5 support

RSA Security Analytics Configuration

Before You Begin

This section provides instructions for configuring the AirTight Networks SpectraGuard Enterprise (SGE) 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 AirTight Networks SpectraGuard Enterprise (SGE) components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

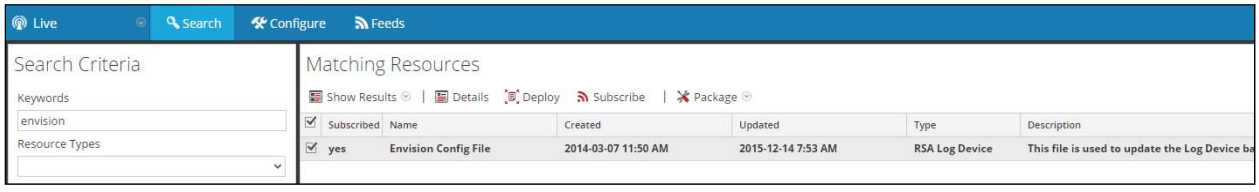
> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure AirTight Networks SpectraGuard Enterprise (SGE) is properly configured and secured before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

Deploy the enVision Config File

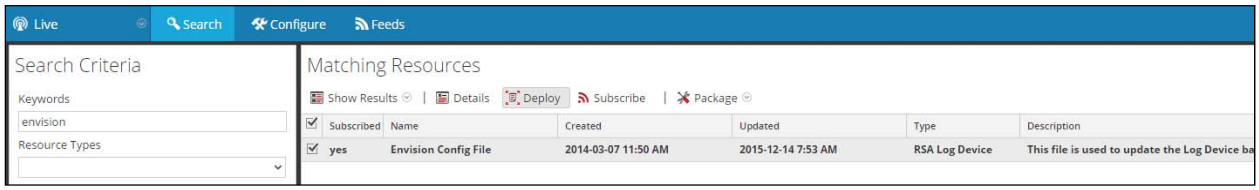
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

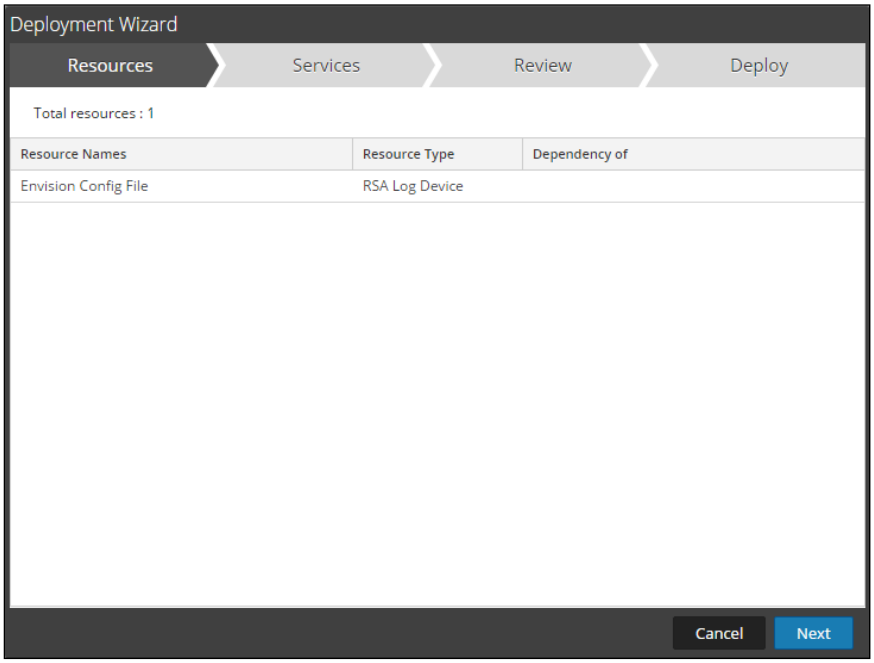
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



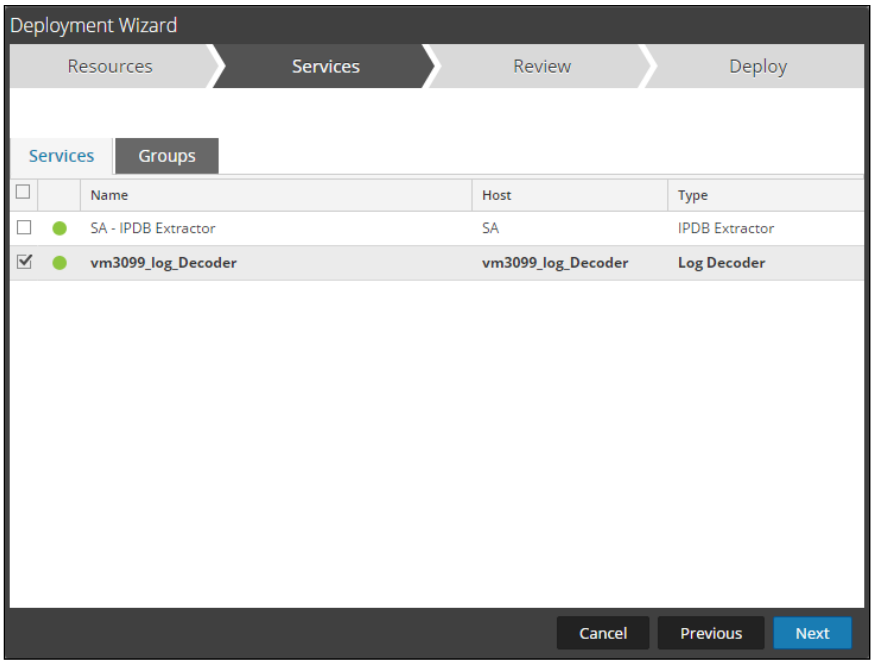
5. Click **Deploy** in the menu bar.



6. Select **Next**.

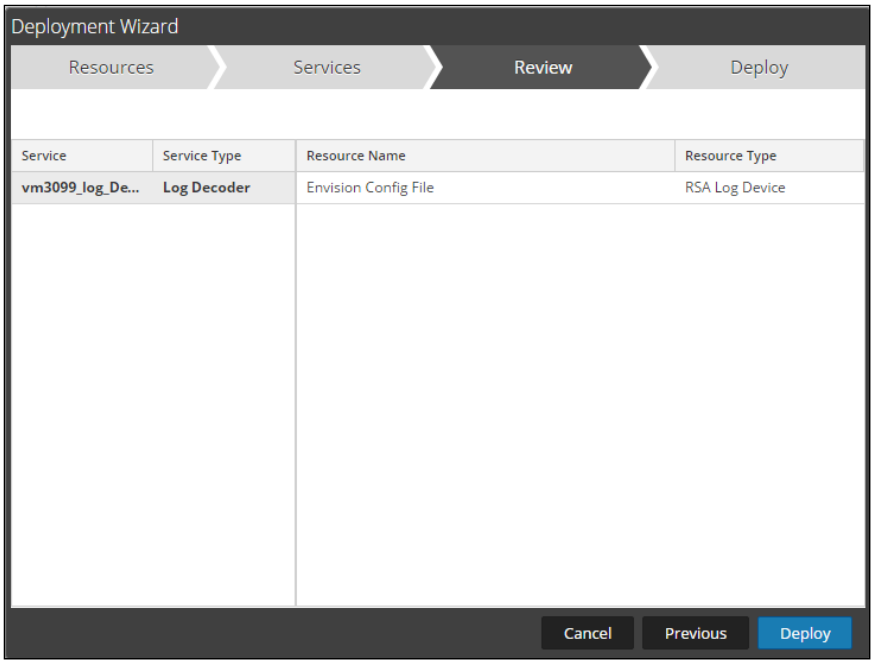


7. Select the **Log Decoder** and select **Next**.

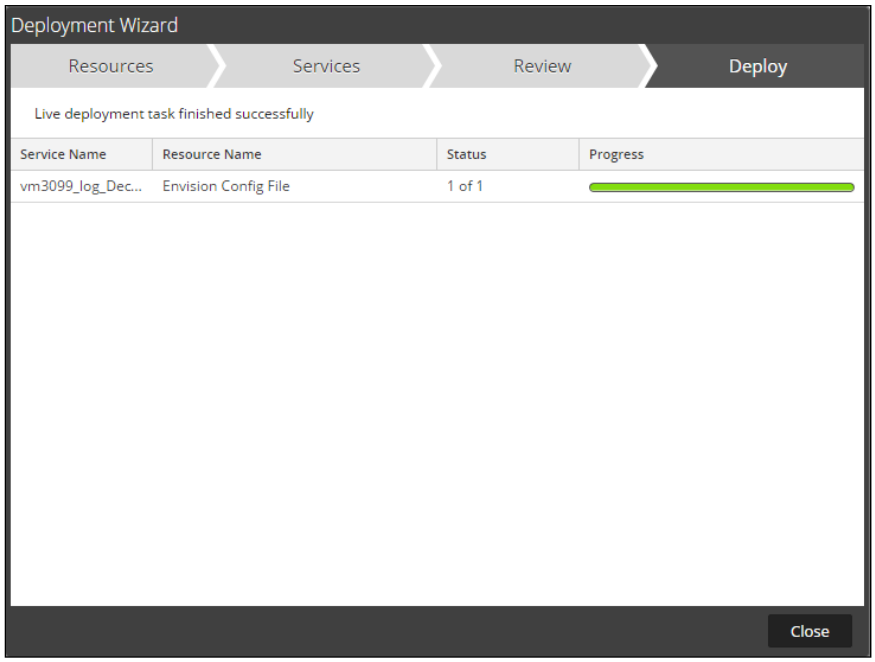


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



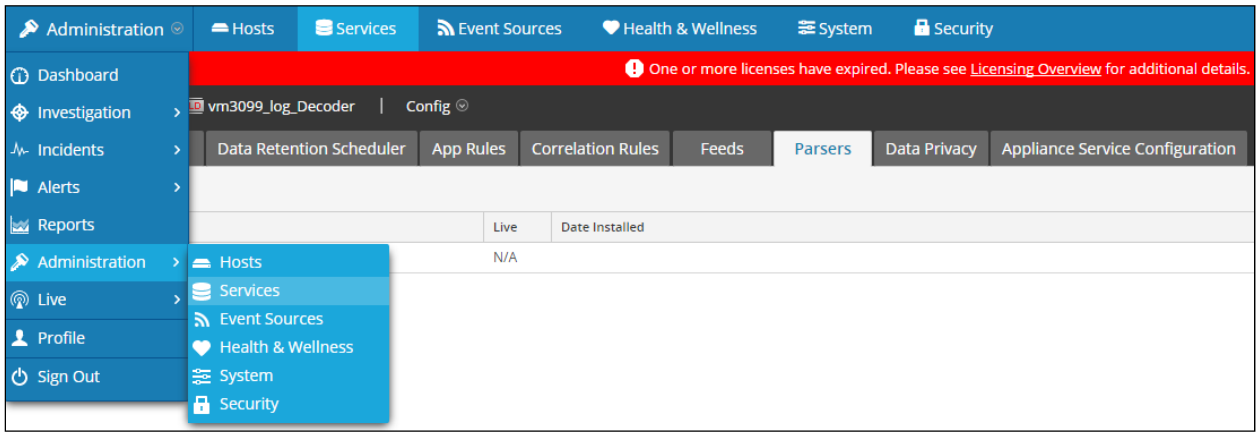
9. Select **Close**, to complete the deployment of the Envision Config file.



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.**



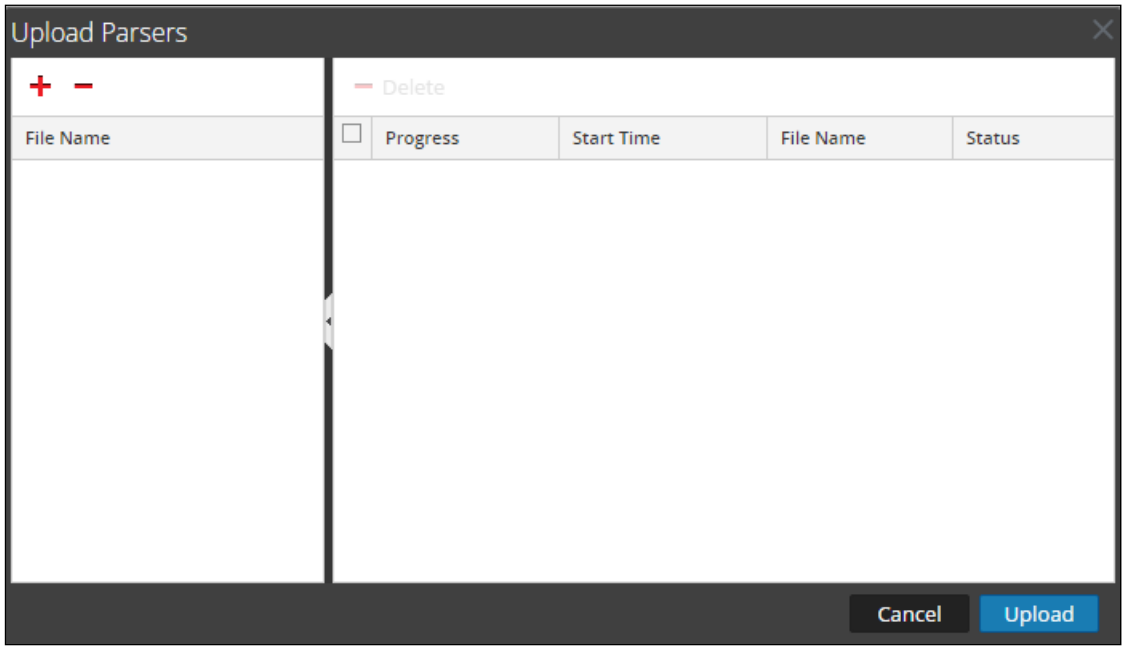
2. Select your Log Decoder from the list, select **View > Config**.

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

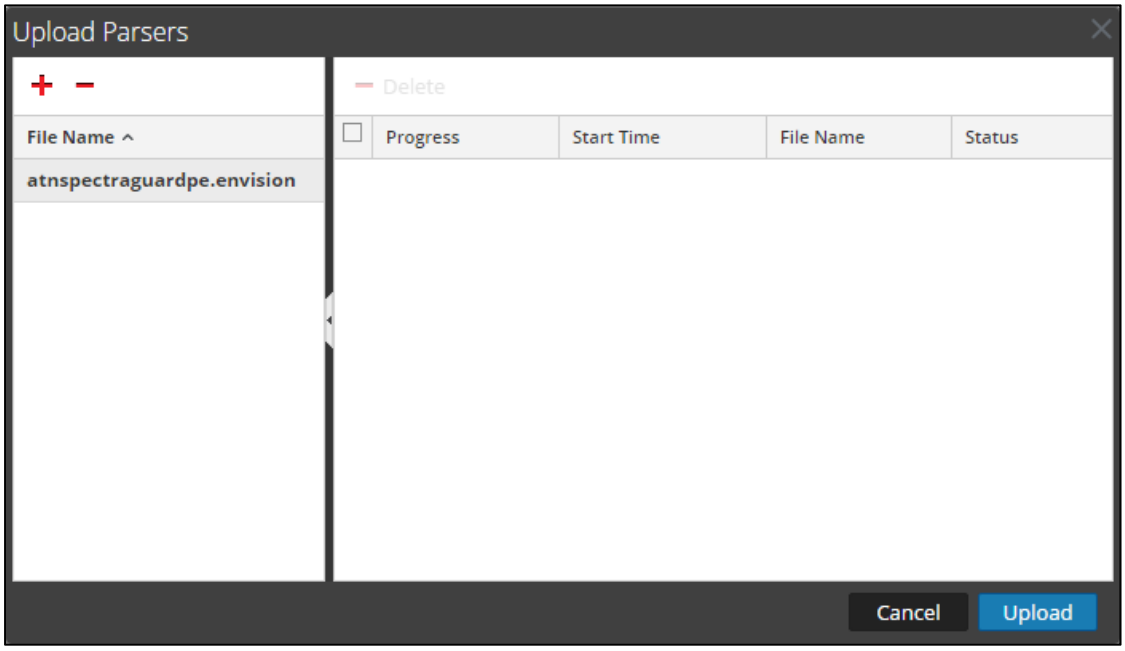
3. Next, select the **Parsers** tab and click the **Upload** button.

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

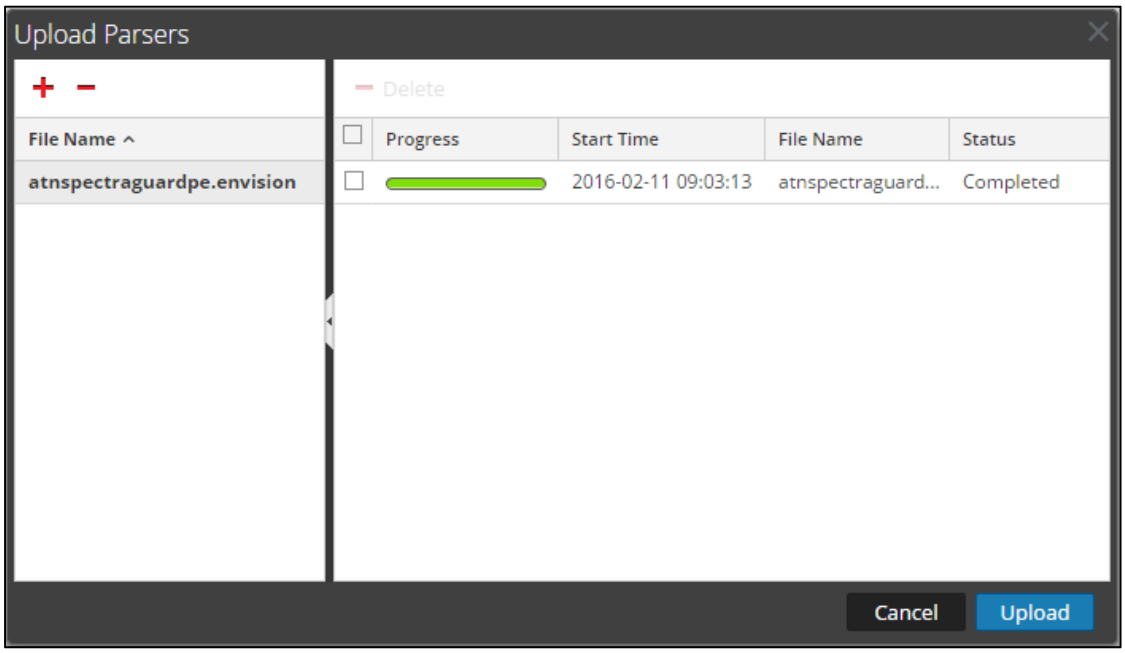
Important: The .envision file is contained within the .zip file downloaded from the RSA Community.



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



6. 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>.

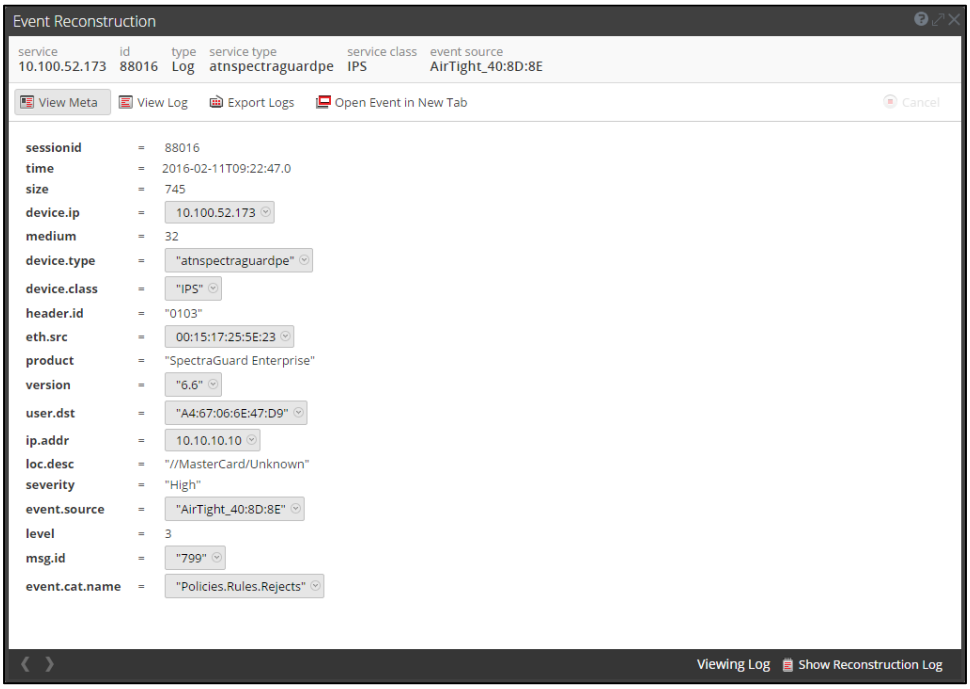
```
<mappings>
        <mapping envisionName="wifi_channel" nwName="wlan.channel" flags="None" format="UInt16"/>
        <mapping envisionName="mask" nwName="mask" flags="None" envisionDisplayName="IPMask"/>
        <mapping envisionName="location_desc" nwName="loc.desc" flags="None"/>
        <mapping envisionName="version" nwName="version" flags="None"/>
        <mapping envisionName="macaddr" nwName="eth.host" flags="None" format="MAC" envisionDisplayName="DeviceMacAddress"/>
        <mapping envisionName="ssid" nwName="wlan.ssid" flags="None" envisionDisplayName="SSID"/>
        <mapping envisionName="change_old" nwName="change.old" flags="None" envisionDisplayName="ChangeOldValue"/>
        <mapping envisionName="severity" nwName="severity" flags="None" envisionDisplayName="Severity|SeverityLevel"/>
        <mapping envisionName="change_new" nwName="change.new" flags="None" envisionDisplayName="ChangeNewValue"/>
        <mapping envisionName="product" nwName="product" flags="None"/>
        <mapping envisionName="bssid" nwName="wlan.ssid" flags="None" envisionDisplayName="BSSID"/>
        <mapping envisionName="smacaddr" nwName="eth.src" flags="None" format="MAC" envisionDisplayName="SourceMacAddress" nullTokens="Unknown"/>
        <mapping envisionName="context" nwName="context" flags="None"/>
        <mapping envisionName="encryption_type" nwName="crypto" 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.



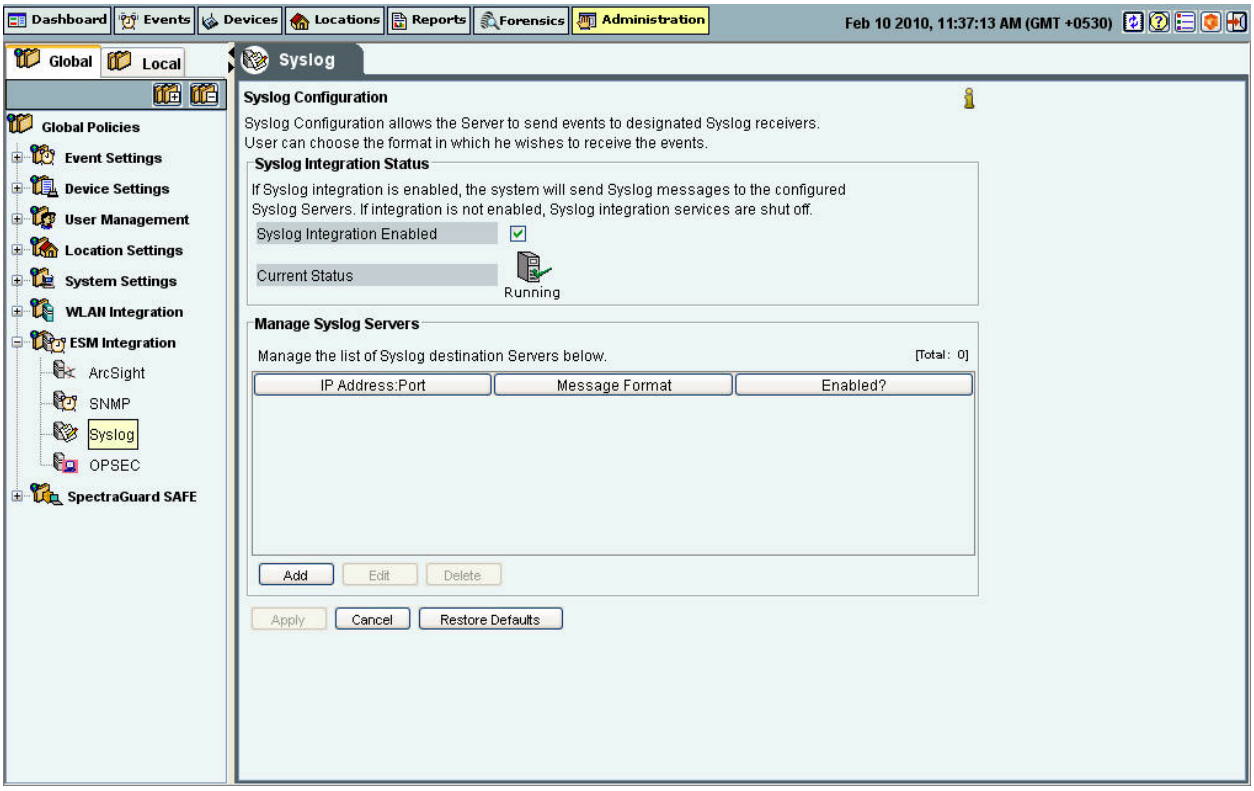
AirTight Networks SpectraGuard Enterprise Configuration

The SpectraGuard Enterprise server should be configured to send syslog events to the RSA Security Analytics appliance. The following steps give a brief overview to configure RSA Security Analytics as a syslog event receiver. For detailed description of the SpectraGuard Enterprise user interface, please refer to SpectraGuard Enterprise User Guide document.

1. Login to SpectraGuard Enterprise UI as a user with administrator privileges.
2. Select the Administration tab and then the Global Policies view.
3. Select ESM Integration, then Syslog. The Syslog Configuration screen will now open.

Syslog Configuration

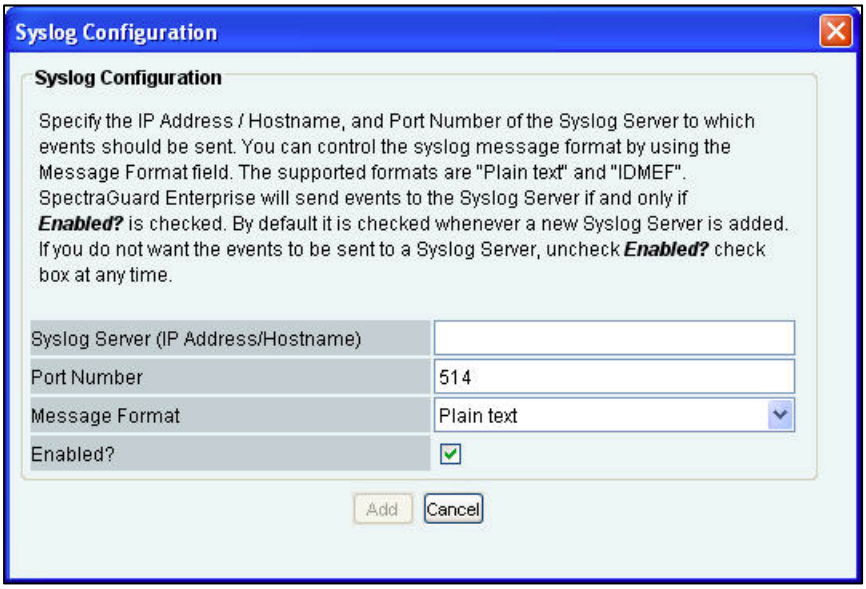
The Syslog Configuration screen allows the SpectraGuard Enterprise to send events to designated Syslog receivers.



- **Syslog Integration Status:** If **Syslog Integration Enabled** is checked, the system sends messages to the configured Syslog Servers. Otherwise, Syslog integration services are shut-off and you cannot manage the Syslog Servers.
- **Current Status**: Displays the Current Status of the Syslog Server: ***Running*** or ***Stopped***. An ***Error*** status is shown in one of the following cases:
    - One of the configured and enabled Syslog Servers has a hostname, which cannot be resolved
    - System Server is stopped
    - Internal error, in which case you need to contact AirTight Networks Technical Support

Adding RSA Security Analytics Server as Syslog receiver

1. Under **Manage Syslog Severs**, click **Add** to open the **Syslog Configuration** screen.



2. Enter the **Syslog Server (IP Address or Hostname)** of the RSA Security Analytics server.
3. Enter the **Port Number** of the Security Analytics syslog port (Default: 514).
4. From the **Message Format pull-down menu,** select **Plain text**. This specifics the format in-which events are sent to Security Analytics.
5. Next, check the **Enabled** checkbox. This enables events to be sent to this Syslog receiver.
6. Finish by clicking the **Add** button.

Certification Checklist for RSA Security Analytics

Date Tested: 2/12/2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
AirTight SpectraGuard (SGE)	6.7	Linux/Centos

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

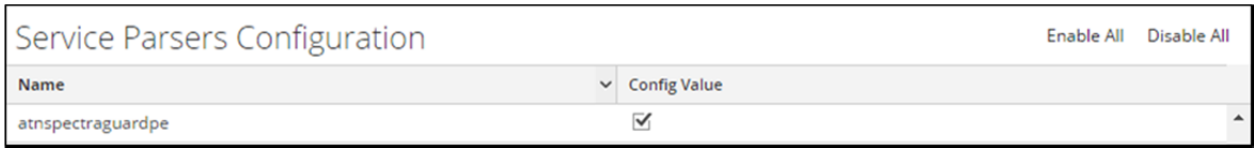
Appendix

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).