



RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: January 14, 2016

Partner Information

Product Information	
Partner Name	Absolute
Web Site	www.absolute.com
Product Name	Absolute Data and Device Security (DDS)
Version & Platform	Absolute DDS Customer Center 5.26+, SIEM Connector 1.1
Product Description	Absolute provides persistent endpoint security and data risk management solutions for computers, tablets, and smartphones. Our customers depend on us to provide them with a unique and trusted layer of security so they can manage mobility while remaining firmly in control. By providing them with a reliable two-way connection with all of their devices, our customers can secure endpoints, assess risk, and respond appropriately to security incidents.



Solution Summary

What We Do

Absolute provides persistent endpoint security and data risk management solutions for computers, tablets, and smartphones. Our customers depend on us to provide them with a unique and trusted layer of security so they can manage mobility while remaining firmly in control. By providing them with a reliable two-way connection with all of their devices, our customers can secure endpoints, assess risk, and respond appropriately to security incidents.

How We Do It

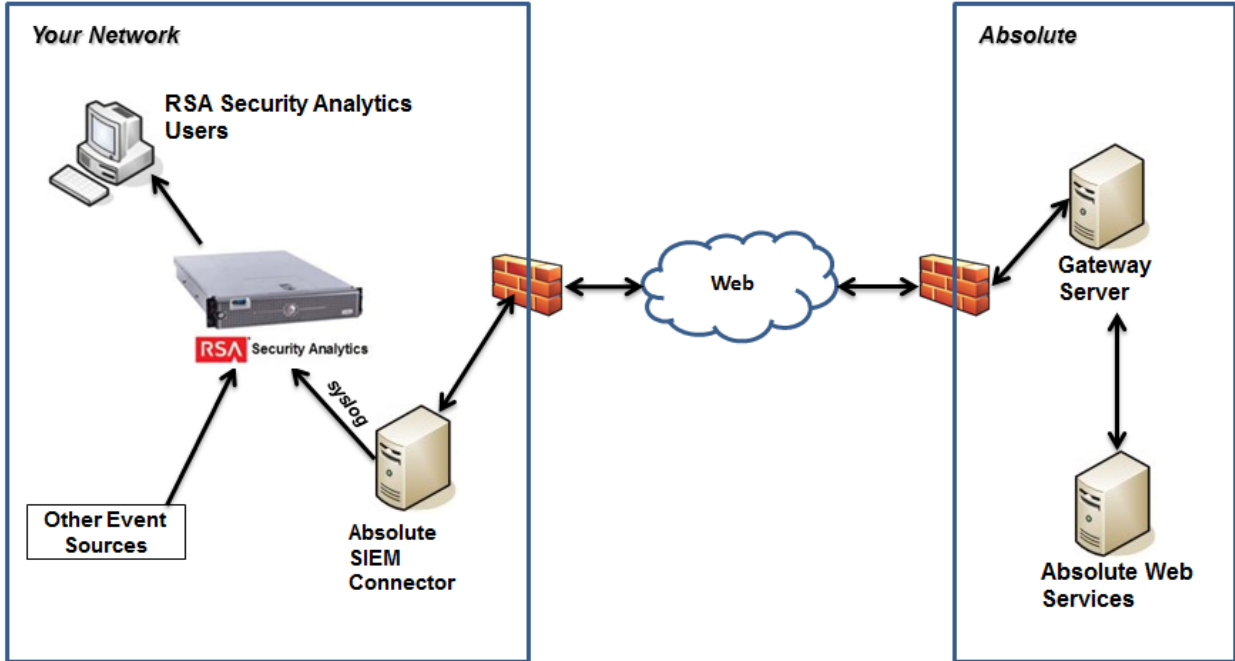
Persistence technology by Absolute provides you with visibility and control over all of your devices, regardless of user or location. If an Absolute client is removed from an endpoint, it will automatically reinstall so you can secure each device and the sensitive data it contains. No other technology can do this. With patented Persistence technology, you can consistently assess risk, secure the lifecycle of each device, and preemptively respond to security incidents.

Absolute SIEM Connector for RSA Security Analytics

Absolute also provides customers with a cloud-based service where they can access their account, monitor the state of each device, and invoke security commands if a device is in trouble. They can also define conditions that they want to flag and receive alerts if they occur. It's like a sticky advance notification system.

The Absolute SIEM Connector for RSA Security Analytics allows customers to ensure that security alerts generated by Absolute DDS are made available in RSA Security Analytics so that customers can identify security incidents quickly and correlated with other security events received by Security Analytics , to derive additional value from their investments in RSA Security Analytics and Absolute DDS.

RSA Security Analytics Features	
Absolute DDS Customer Center 5.26+, SIEM Connector 1.1	
Integration package name	absolutesiemconnector.envision
Device display name within Security Analytics	absolutesiemconnectorpe
Event source class	Analysis
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 package from the Security Analytics Community, the next steps are to deploy this on all log decoders. Follow the rest of this Implementation Guide to proceed.

 **Note:** For steps to disable or remove the Security Analytics Integration Package, please refer to the Appendix of this Guide.

An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
absolutesiemconnector.envision	This file is deployed during the Deploy Security Analytics Integration Package section in this guide.

Release Notes

Release Date	What's New In This Release
1/14/2016	Integration between RSA Security Analytics and Absolute Data & Device Security.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Absolute DDS 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 Absolute DDS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Absolute Data & Device Security Configuration

To integrating Absolute DDS with RSA Security Analytics, you need to install Absolute SIEM Connector in your network. The following steps describe how to download and install Absolute SIEM Connector.

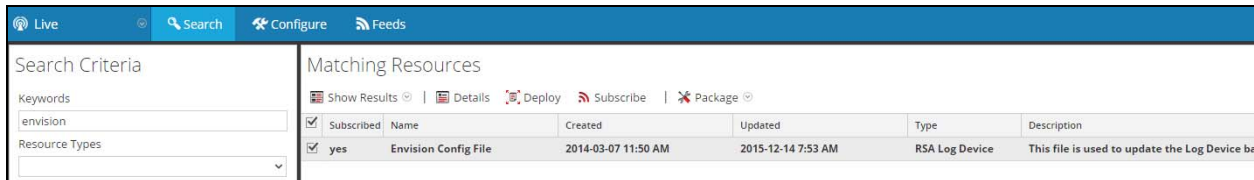
1. Go to the **Download Packages** page in the **Absolute Customer Center** web site and download the Absolute SIEM Connector 1.1.
2. Go to **Documentation** page in the **Absolute Customer Center** web site and click **Absolute SIEM Connector Install Guide**.
3. Follow the install guide to install the Absolute SIEM Connector in your network.

Deploy 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:

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

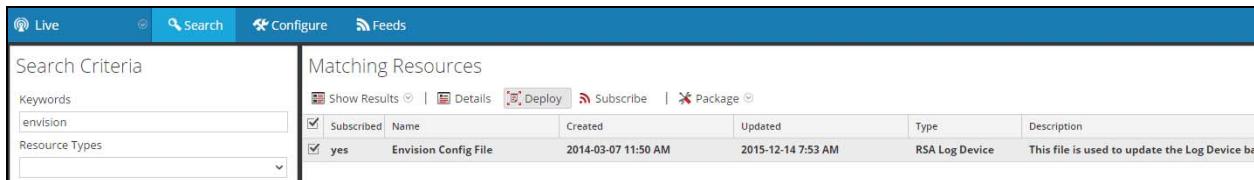
4. From the Security Analytics menu, select **Live > Search**.
5. In the keywords field, enter: **Envision**.
6. Security Analytics will display the **Envision Config File** in Matching Resources.
7. Select the checkbox next to **Envision Config File**.



The screenshot shows the 'Live' module interface. On the left, the 'Search Criteria' section has 'Envision' entered in the 'Keywords' field. On the right, the 'Matching Resources' section displays a table with one entry: 'Envision Config File'. The 'Deploy' button is highlighted in the menu bar above the table.

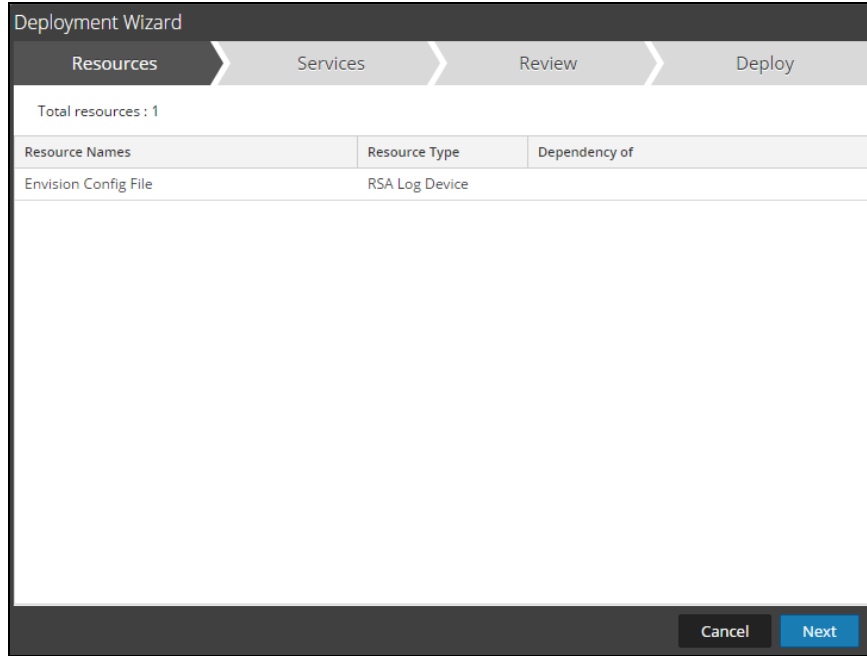
Subscribed	Name	Created	Updated	Type	Description
<input checked="" type="checkbox"/>	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

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

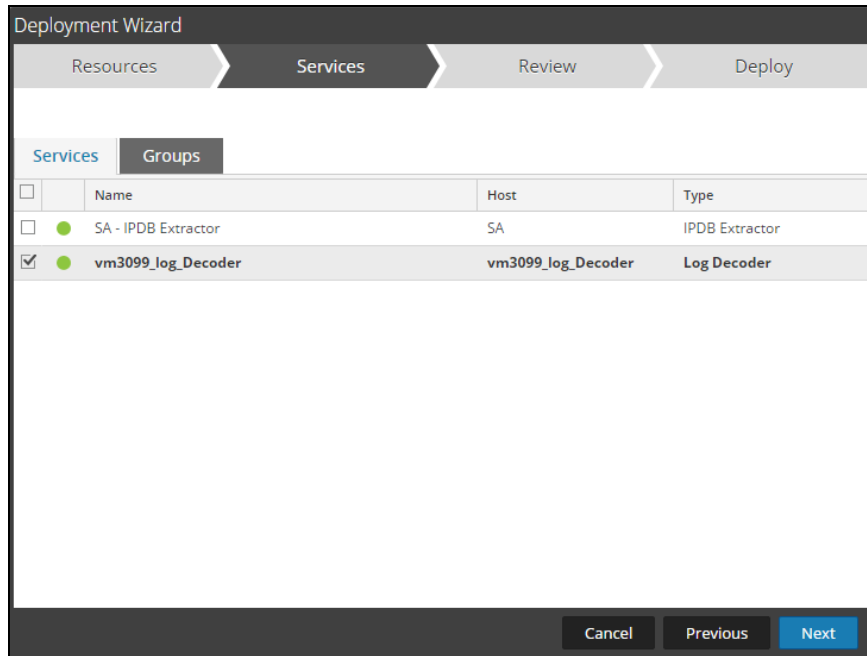


This screenshot is identical to the previous one, but the 'Deploy' button in the 'Matching Resources' menu bar is now highlighted in red, indicating it has been selected.

9. Select **Next**.

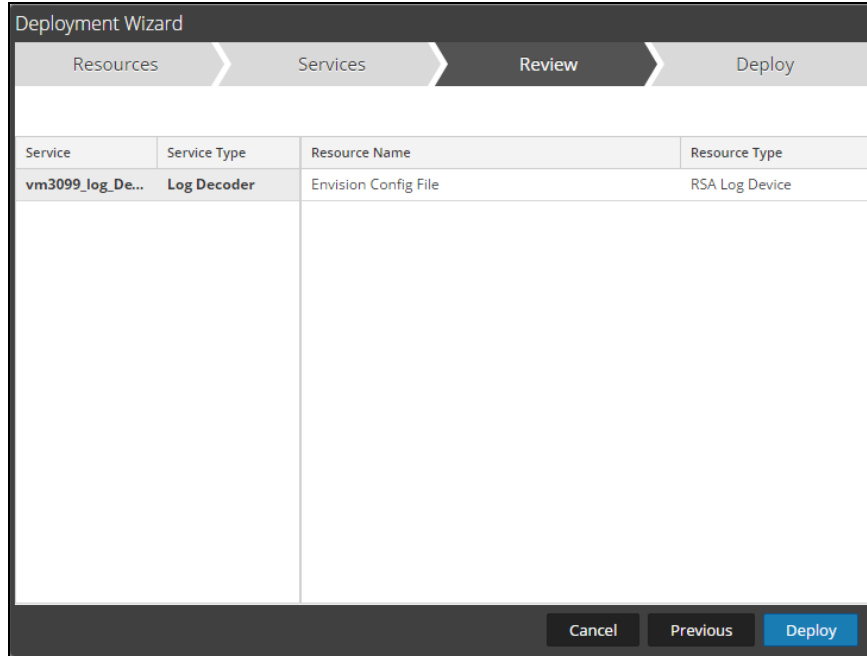


10. Select the **Log Decoder** and select **Next**.

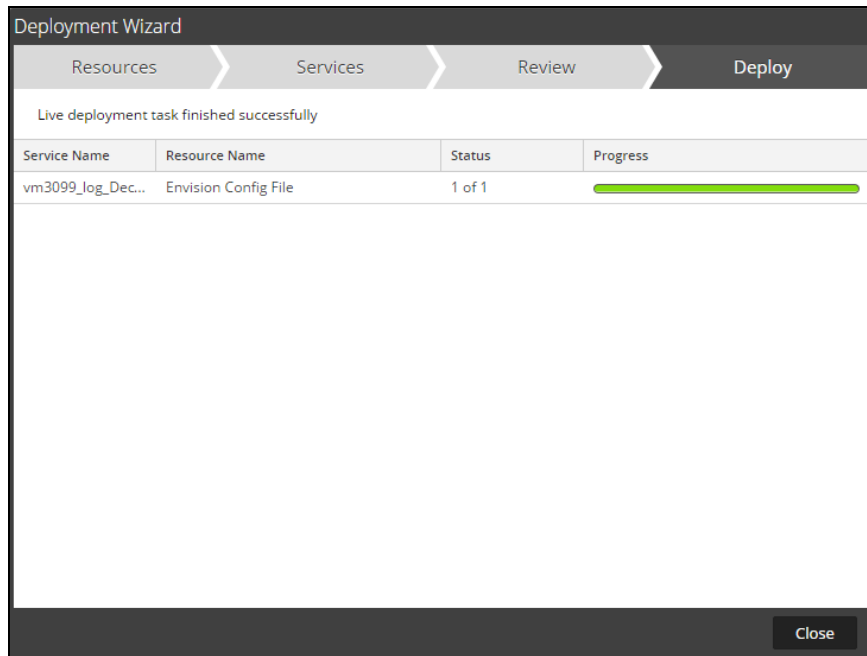


 **Note:** In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

11. Select **Deploy**.



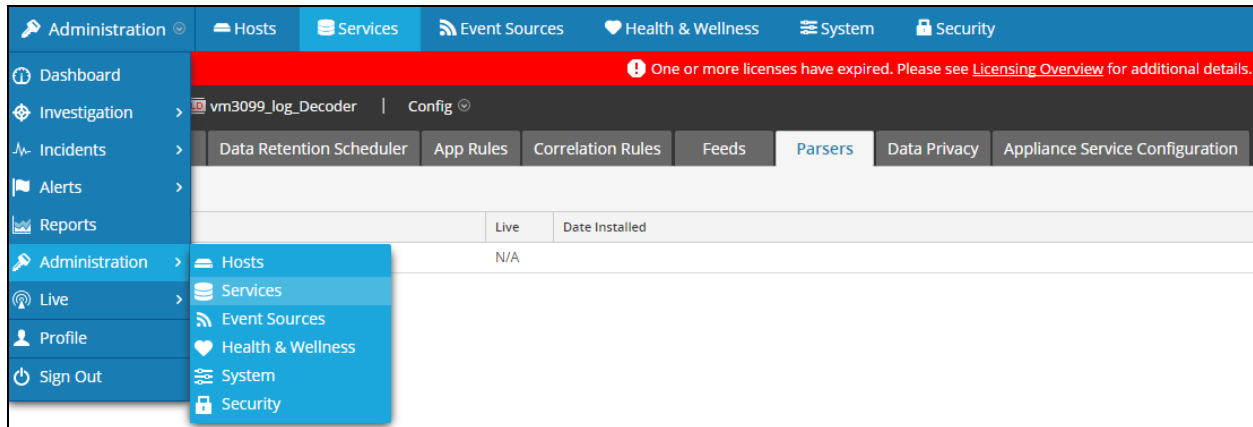
12. Select **Close**, to complete the deployment of the Envision Config file.



Deploy Security Analytics Integration Package

After completing the previous section, *Deploy 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**.

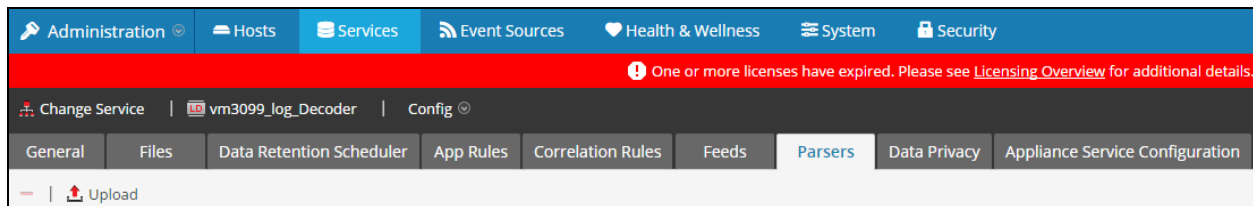


2. Select your Log Decoder from the list, select **View > Config**.



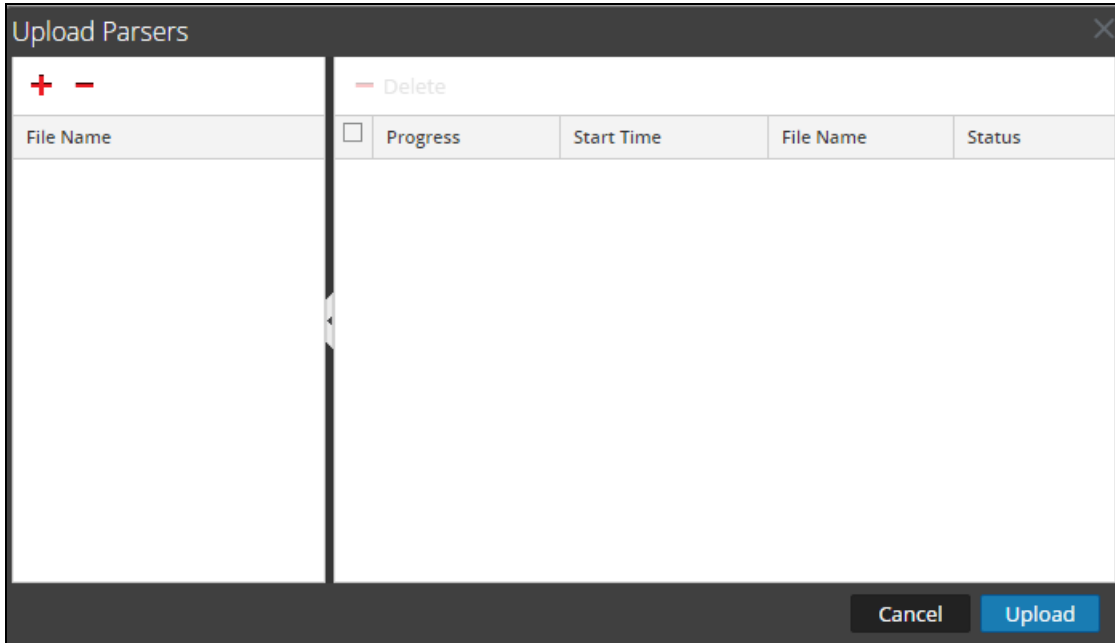
 **Note:** In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.

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

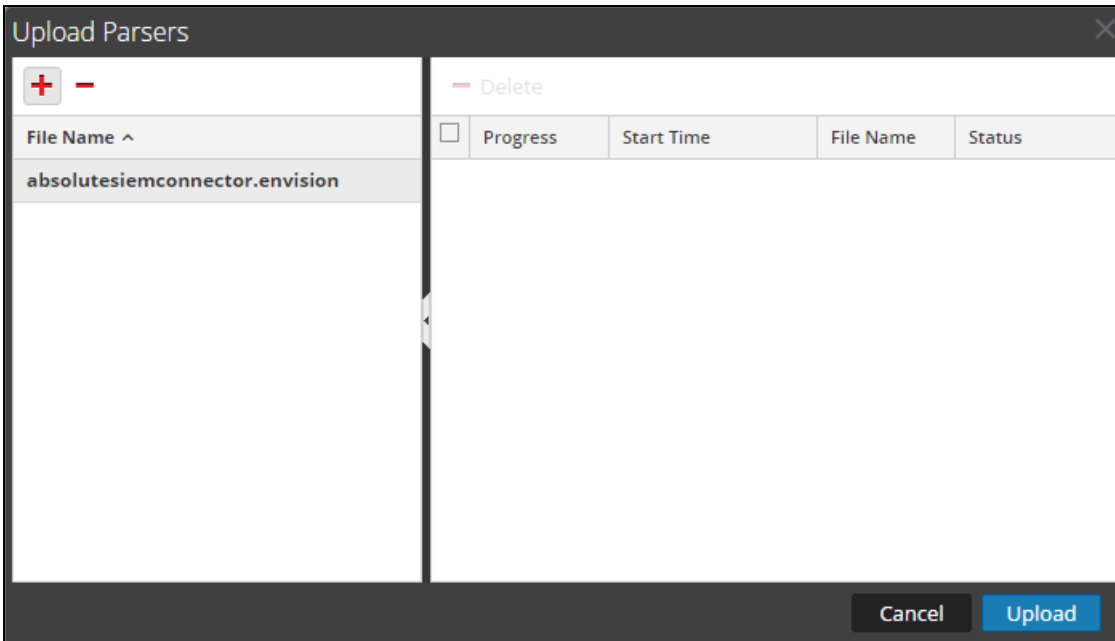


4. From the *Upload Parsers* window, click the **+** **Add** button and select the *.envision* file.

 **Note: 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**.



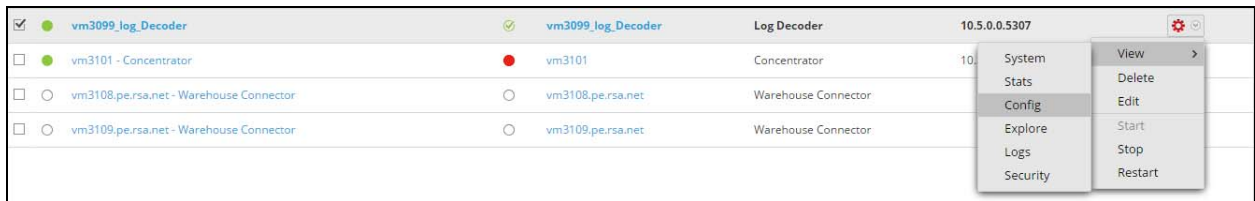
1. Enter the text below into notepad and save the file as table-map-custom.xml.

```
< mappings >
  < mapping envisionName="info" nwName="index" flags="None" />
  < mapping envisionName="operation_id" nwName="operation.id" flags="None" />
  < mapping envisionName="event_time_string" nwName="event.time.str" flags="None" envisionDisplayName="EventTimeString" />
< / mappings >
```

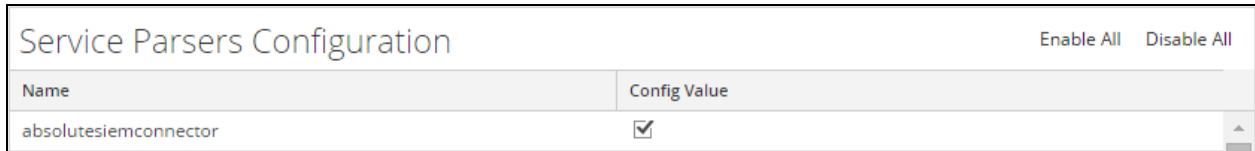
2. Connect to the Security Analytics Log Decoder Server using WinSCP. Upload the newly created table-map-custom.xml file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the log decoder(s), enter only the contents between the < mappings >...< / mappings >.
3. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart**.



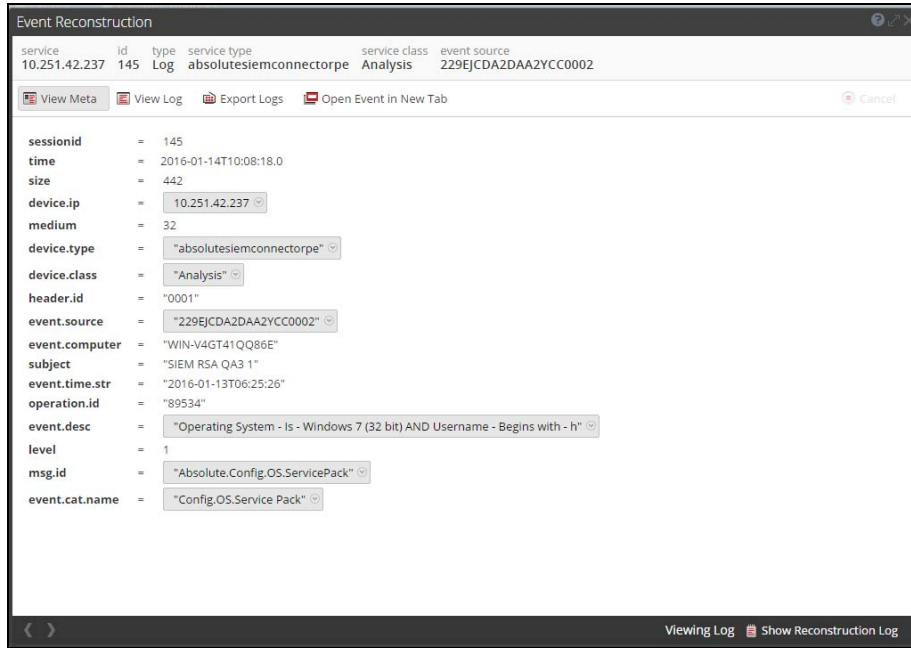
4. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View > Config**.



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



- 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.



Certification Checklist for RSA Security Analytics

Date Tested: January 14, 2016

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.5	Virtual Appliance
Absolute Data & Device Security	CC 5.26+, Absolute SIEM Connector 1.1	Windows

Security Analytics Test Case	Result
Device Administration	
Partners 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	✓

DRP / PAR

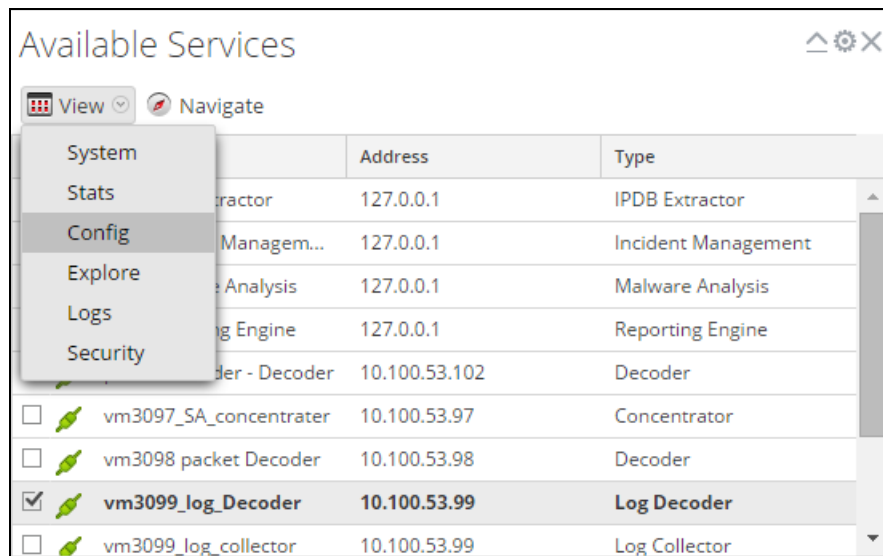
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

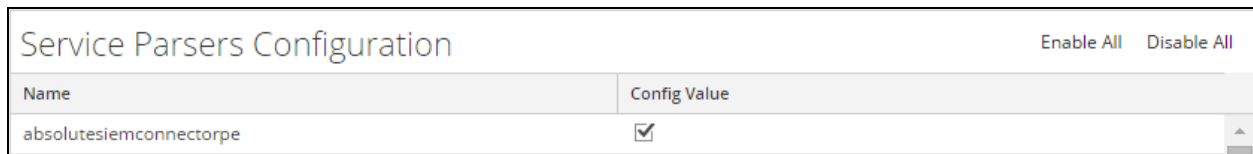
Security Analytics Disable Device Parser

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

1. From the Security Analytics Available Services menu, select the Log Decoder.
2. Then select **View > Config**.



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



4. Click **Apply** to save settings.

Security Analytics Remove Device Parser

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

5. Connect to the Security Analytics Log Decoder/Collector Server using SSH and open the **/etc/netwitness/ng/envision/etc/devices** folder.
6. Search for the device you are targeting for removal and delete the folder containing the device xml.
7. Returning the system to its original state may require additional changes to the **table-map-custom.xml**