RSA Ready Implementation Guide for RSA Security Analytics

Altor Security Suite 4.0

Daniel Pintal, RSA Partner Engineering
Last Modified: February 4, 2016

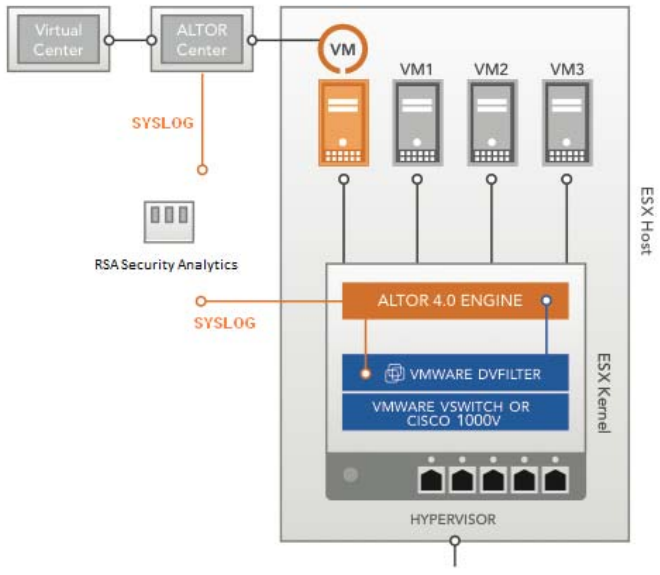
RSA READY

Solution Summary

Altor's Security Suite is fully integrated into the virtual environment. The product uses a number of interfaces to monitor the VMware environment and proactively protect the virtual machines. The firewall engine, IDS engine and other advanced Altor security components will generate logs based on the settings the security administrator selects. Instead of just writing these various logs and events to the Altor management center, an administrator can choose to have them written into RSA Security Analytics. This allows advanced storage and correlation of all the virtual security events alongside the physical security events so customers can see the full picture of security across their environment.

Altor can send syslog from either the Altor Center or the individual Security Virtual Machines located on each physical ESX/ESXi Host in the environment. See below architecture diagram.

RSA Security Analytics Features	
Security Suite 4.0	
Integration package name	altorpe.envision
Device display name within Security Analytics	altorpe
Event source class	Firewall
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
altorpe.envision	SA package deployed to parse events from device integrations.
altorpemsg.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
12/9/2013	Initial support for Altor Networks.
2/4/2016	SA 10.5 support

RSA Security Analytics Configuration

Before You Begin

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

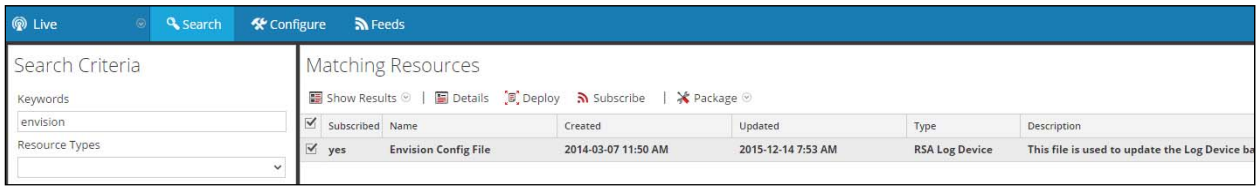
> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Altor Security Suite is properly configured and secured before deploying to a production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

Deploy the enVision Config File

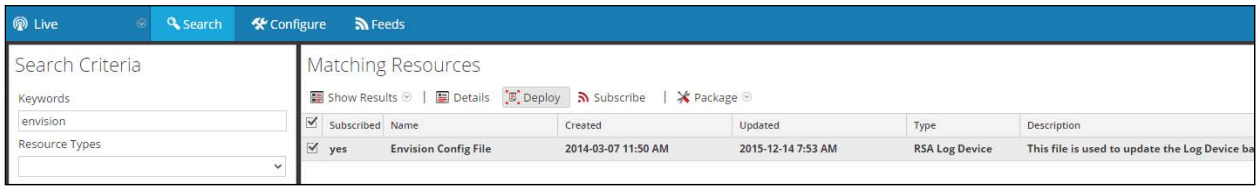
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

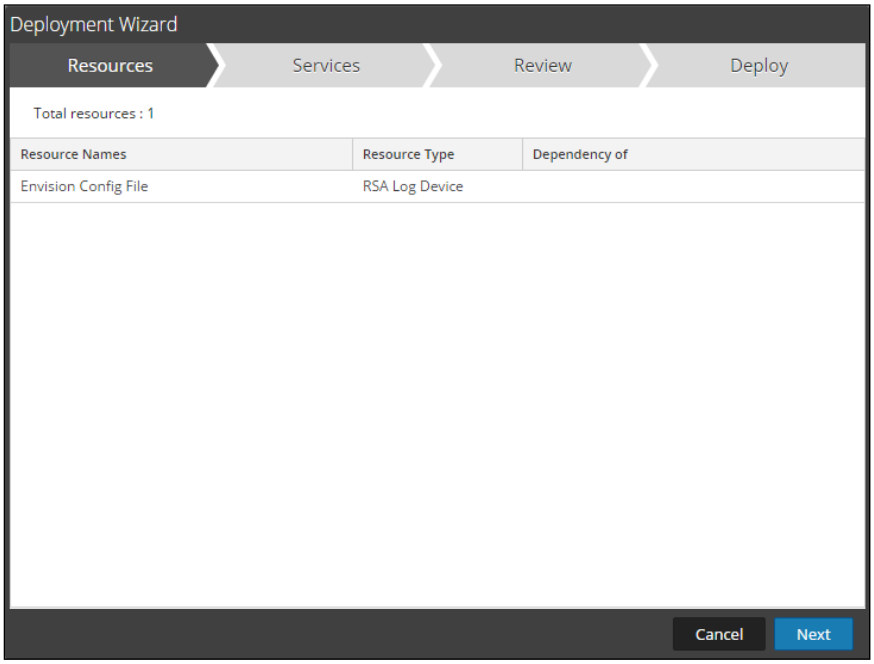
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



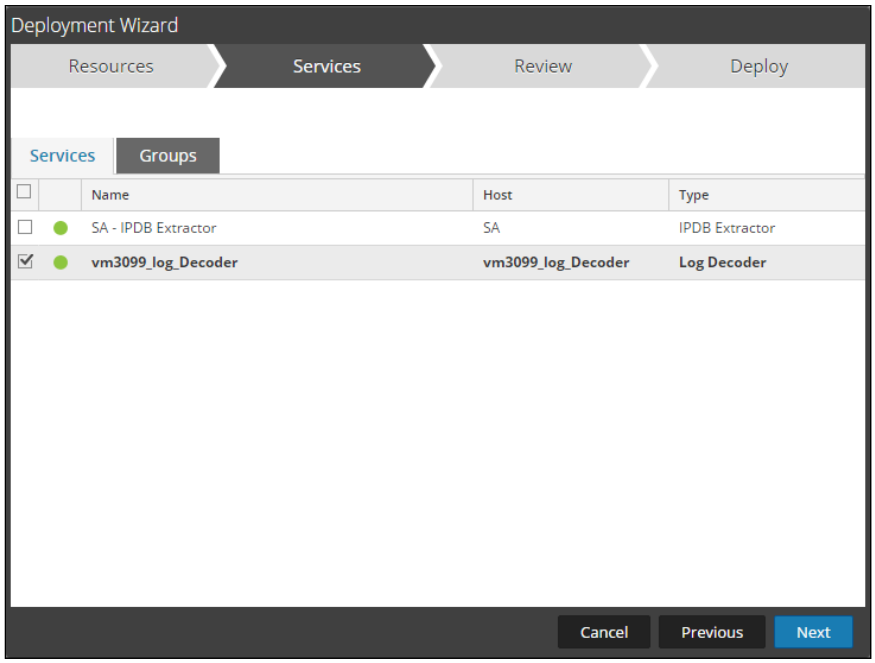
5. Click **Deploy** in the menu bar.



6. Select **Next**.

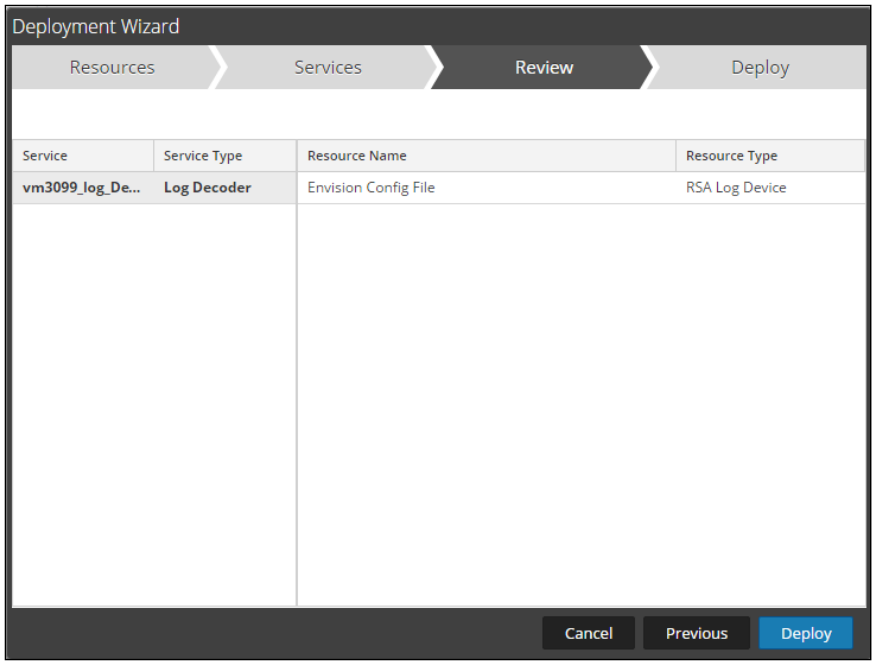


7. Select the **Log Decoder** and select **Next**.

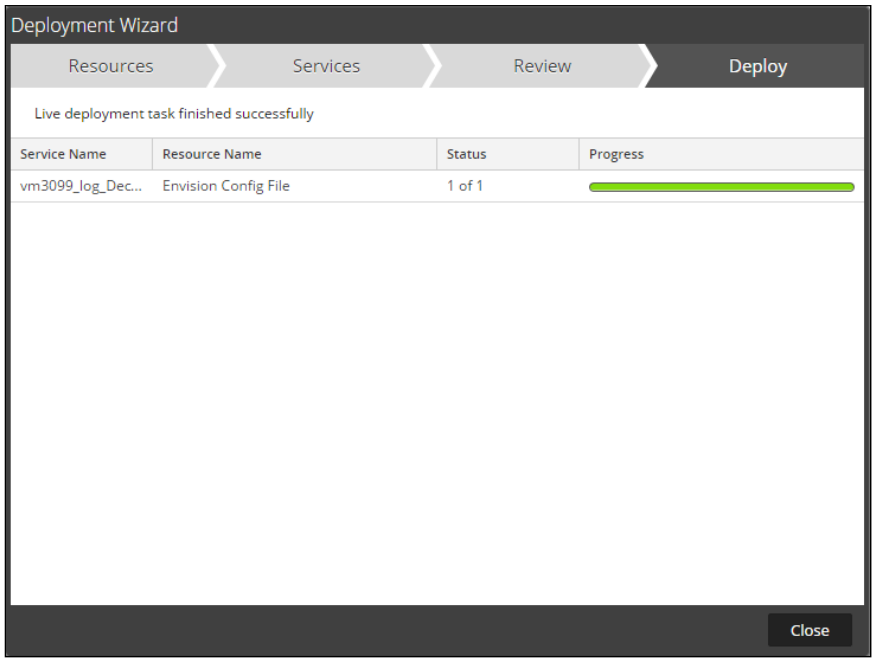


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



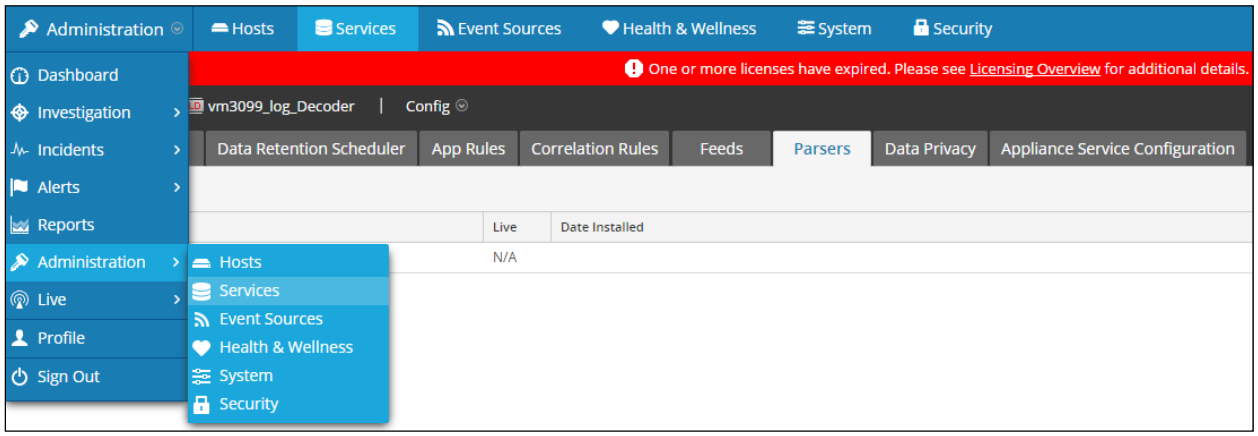
9. Select **Close**, to complete the deployment of the Envision Config file.



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:

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



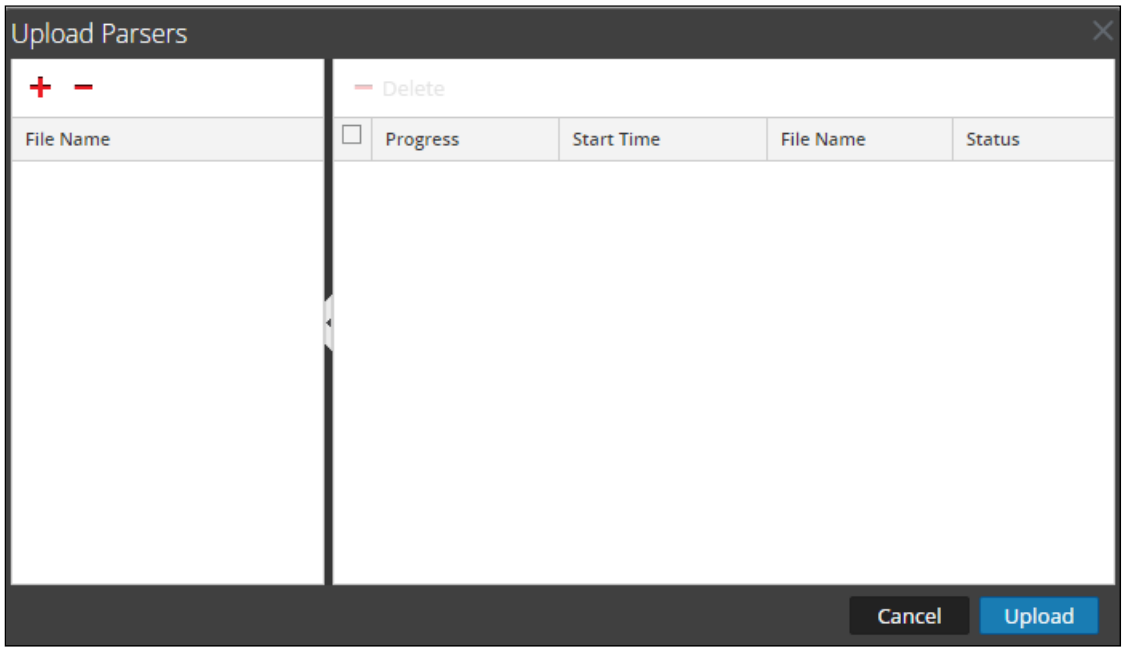
11. Select your Log Decoder from the list, select **View > Config**.

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

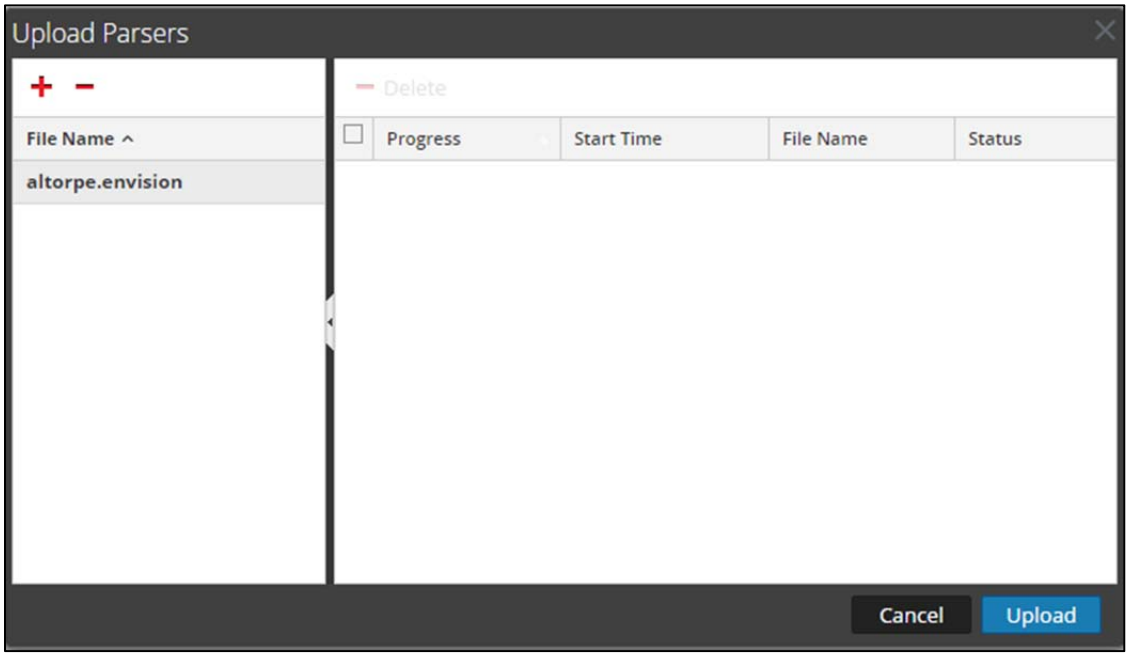
12. Next, select the **Parsers** tab and click the **Upload** button.

13. 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.**



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



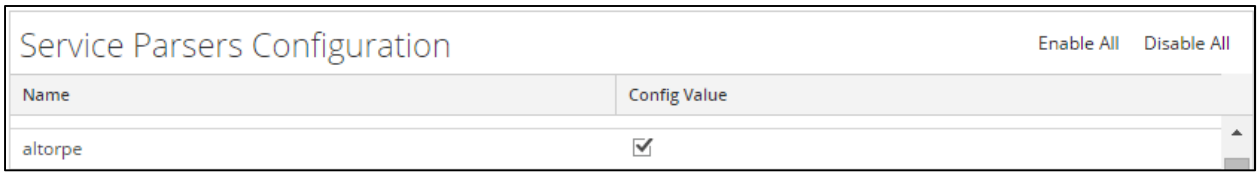
15. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the table-map-custom.xml file from the contents of the .zip file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the log decoder(s), enter only the contents between the <mappings>…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

```
<mappings>
        <mapping envisionName="protocol" nwName="protocol" flags="None" envisionDisplayName="Protocol"/>
        <mapping envisionName="sport" nwName="ip.srcport" flags="None" format="UInt16" envisionDisplayName="SourcePort|LocalPort|ServerPort|src_ip|saddr|src_port" nullTokens="-|(null)"/>
        <mapping envisionName="rule" nwName="rule" flags="None" envisionDisplayName="Rule"/>
        <mapping envisionName="msg" nwName="msg" flags="None" format="Text" envisionDisplayName="Message"/>
        <mapping envisionName="info" nwName="index" flags="None"/>
        <mapping envisionName="logon_id" nwName="username" flags="None" envisionDisplayName="LogonID|usr|username" nullTokens="none|-"/>
        <mapping envisionName="event_computer" nwName="alias.host" flags="None"/>
</mappings>
```

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

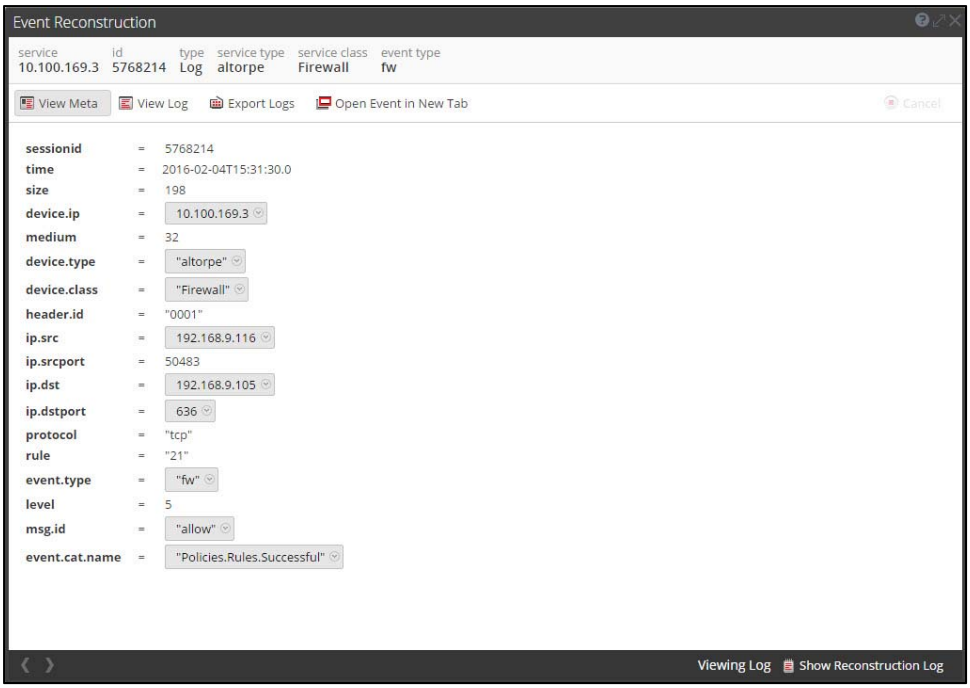
17. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View> Config.**

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



Important: The device parser above is an example and not the actual parser for this integration.

19. 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.



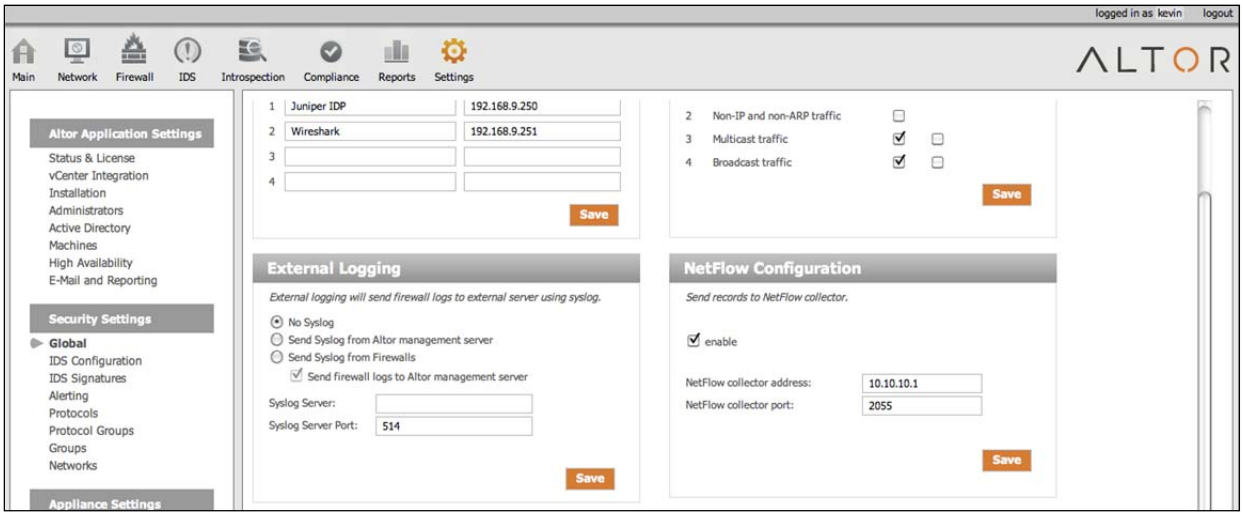
Altor Security Suite Configuration

Altor stores log records for rules in the security policy and IDS events, in an internal database. However, it's also possible to automatically write these logs to RSA Security Analytics via syslog.

Logs can be sent directly from the Altor Center management system or from the Altor Security VMs.

To configure the Altor Security Suite;

1. Select **Settings** and then select **Global** from the Security Settings list on the left side of the management console window.
2. On the right hand side of the management console window locate the External Logging item.
3. Select **Send Syslog from Firewalls**.
4. Enter the **Syslog Server IP Address** the **Syslog Server Port and** select **Save** to complete the configuration.



If you don't want the logs to all be sent from the Security VMs, then to the Altor Center, then to RSA Security Analytics you can optionally decide to send the logs straight from the Security VMs by selecting 'Send Syslog from Firewalls'. This configuration is suggested when the components are geographically separated and or when performance is a concern. In either case you will need to enter the IP address and default port number the RSA Security Analytics system and click save.

Once this configuration is set, Altor will begin sending IDS, Firewall and configuration change logs to RSA Security Analytics.

Certification Checklist for RSA Security Analytics

Date Tested: February 4, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
Altor Security Suite	4.0	ESX/ESXi 3.5 and later

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

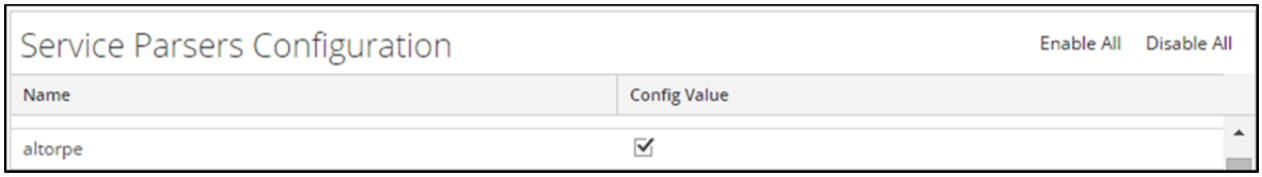
Appendix

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).