RSA Ready Implementation Guide for RSA Security Analytics

ESET
Remote Administrator v5

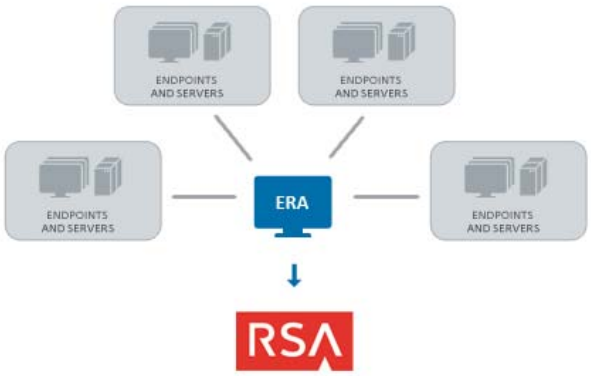
Daniel Pintal, RSA Partner Engineering
Last Modified: 2/23/2016

RSA READY

Solution Summary

All events from ESET Smart Security, ESET NOD32 Antivirus and ESET server security solutions installed across the network are collected by ESET Remote Administrator, where events are summarized and forwarded to RSA Security Analytics. All information about malware detections, blocked communication, update problems or any other events reported by ESET products are immediately available directly in RSA Security Analytics.

RSA Security Analytics Features	
ESET Remote Administrator v5	
Integration package name	eseterape.envision
Device display name within Security Analytics	eseterape
Event source class	Anti Virus
Collection method	ODBC



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
eseterape.envision	SA package deployed to parse events from device integrations.
xeseterapemsg.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
12/05/2013	Initial support for ESET Remote Administrator.
2/23/2016	SA 10.5 Support

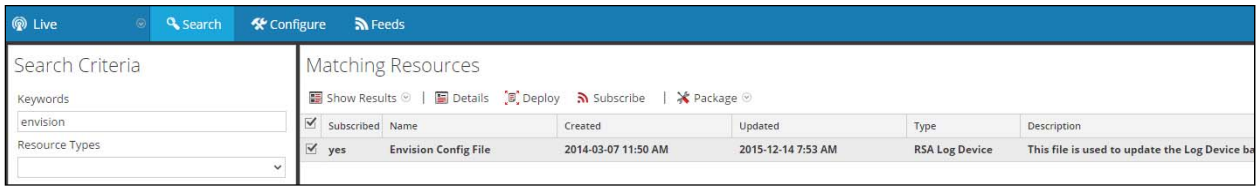
RSA Security Analytics Configuration

Deploy the enVision Config File

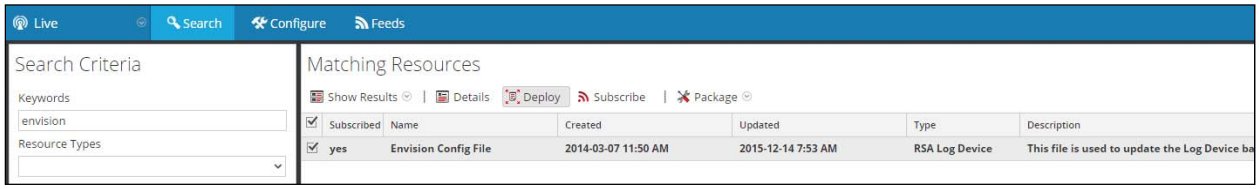
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

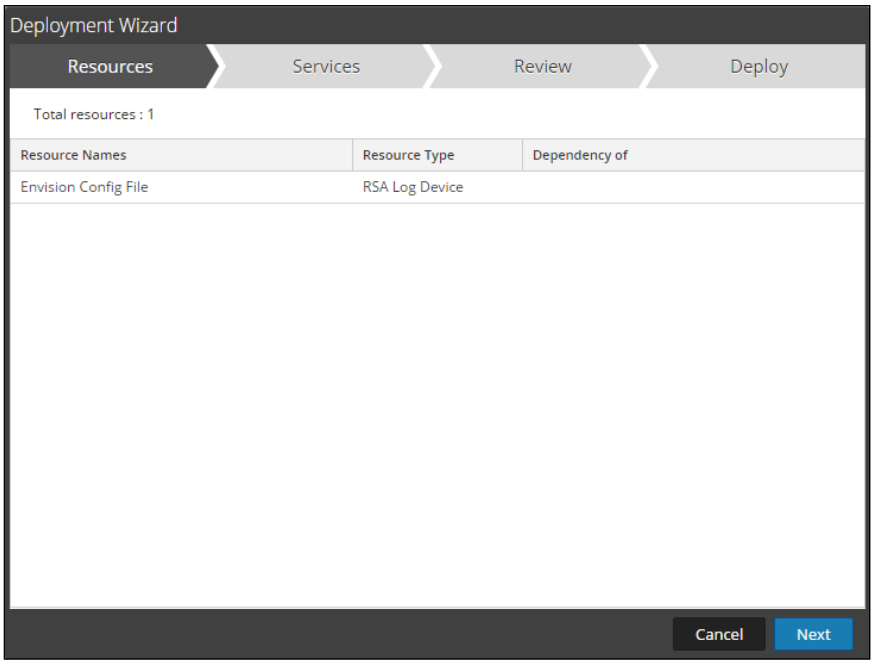
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



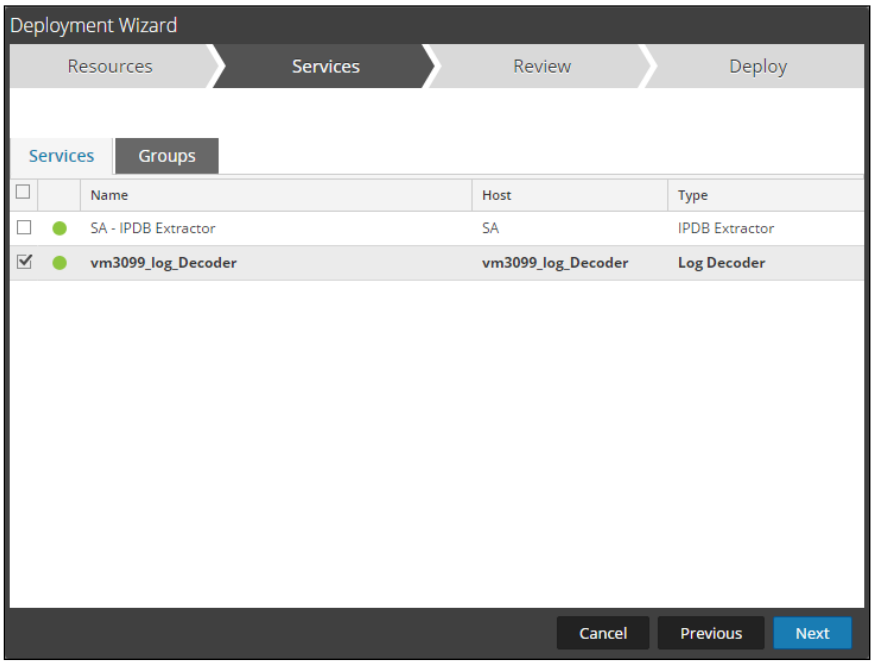
5. Click **Deploy** in the menu bar.



6. Select **Next**.

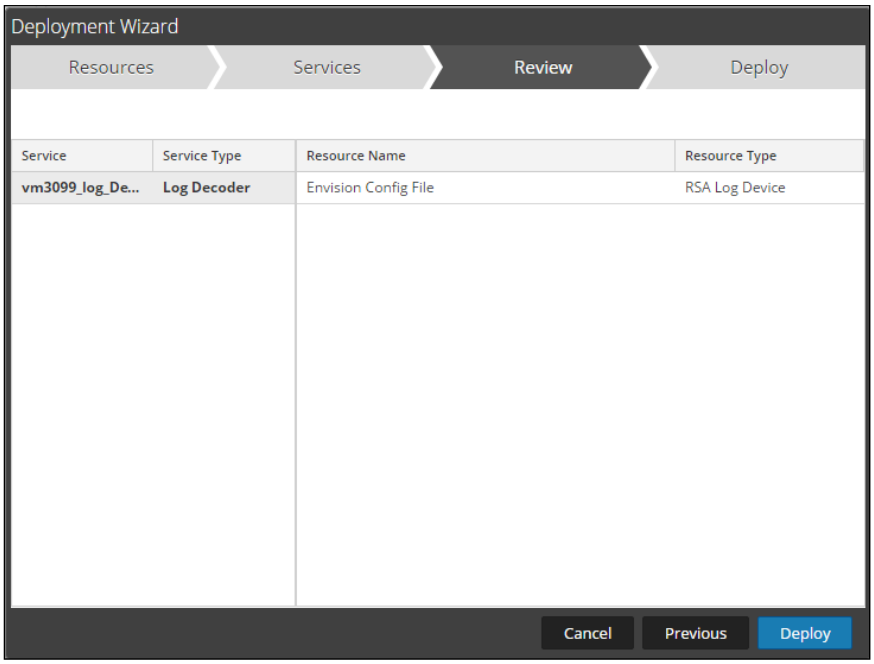


7. Select the **Log Decoder** and select **Next**.

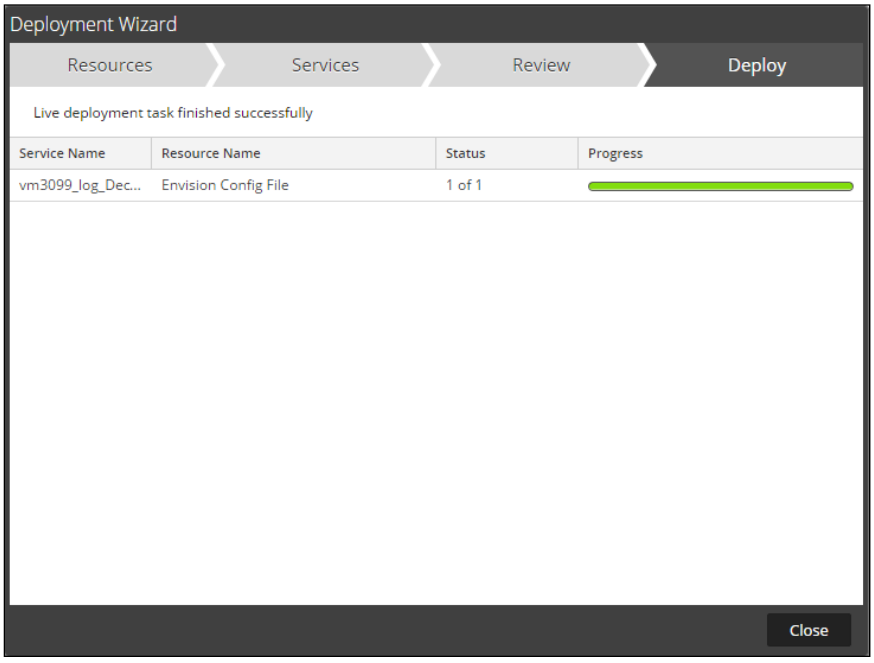


! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



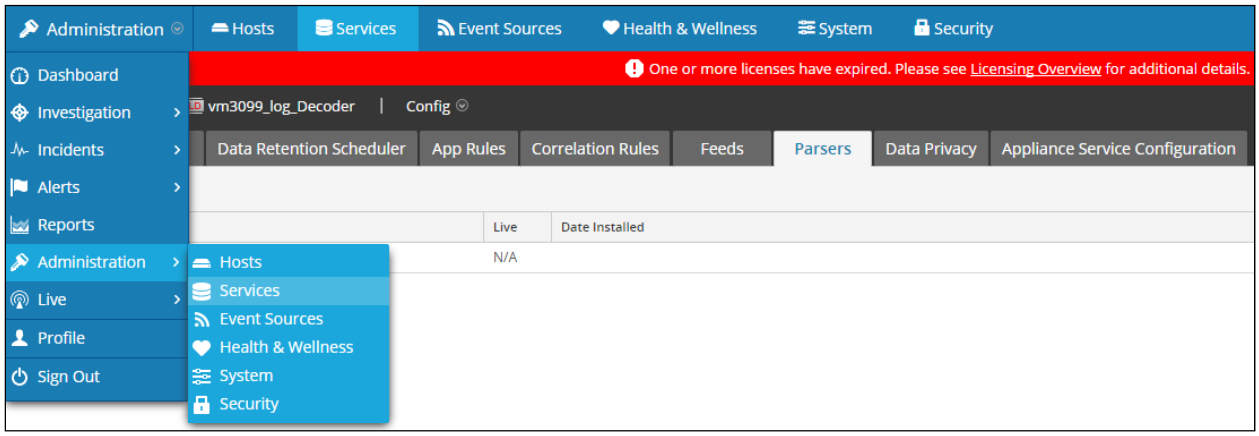
9. Select **Close**, to complete the deployment of the Envision Config file.



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.**



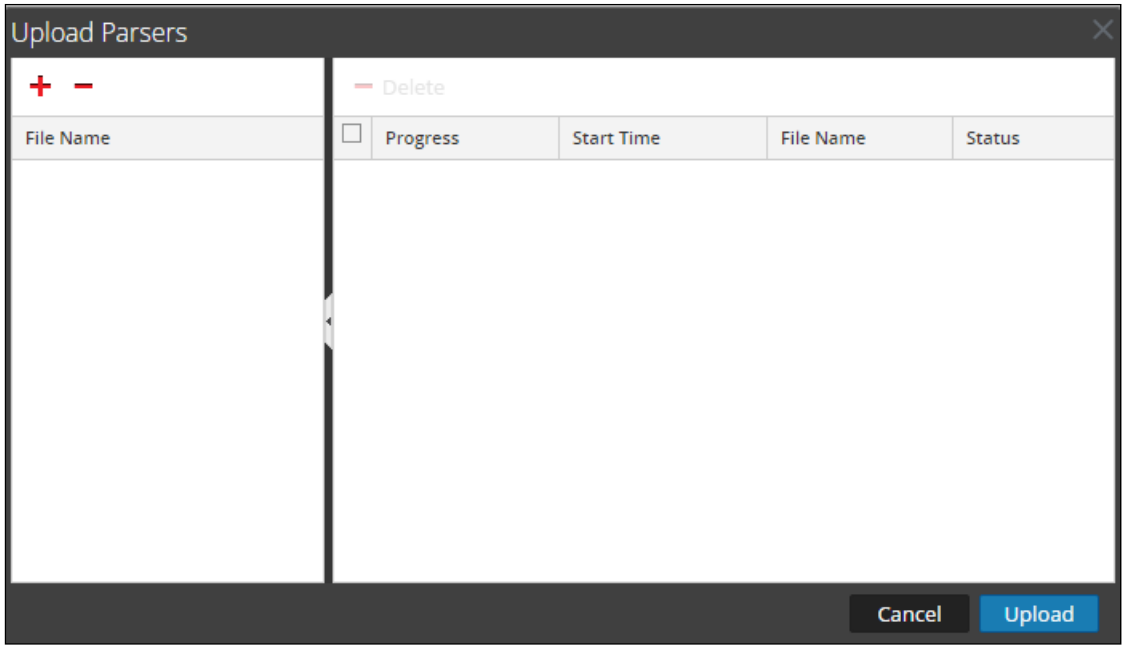
2. Select your Log Decoder from the list, select **View > Config**.

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

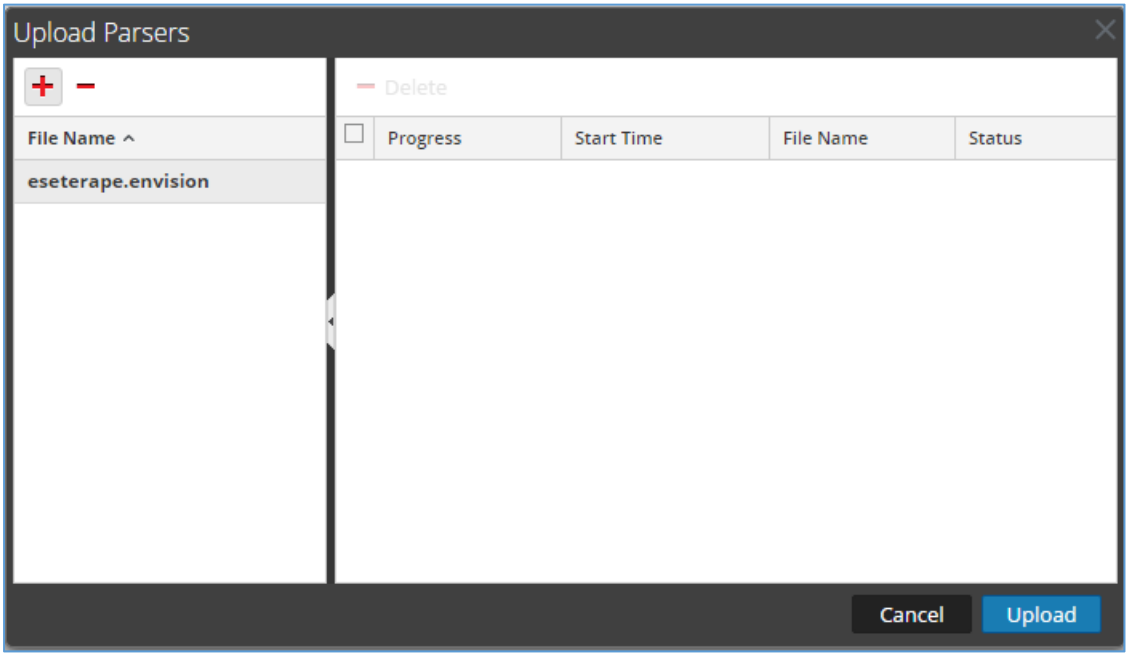
3. Next, select the **Parsers** tab and click the **Upload** button.

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

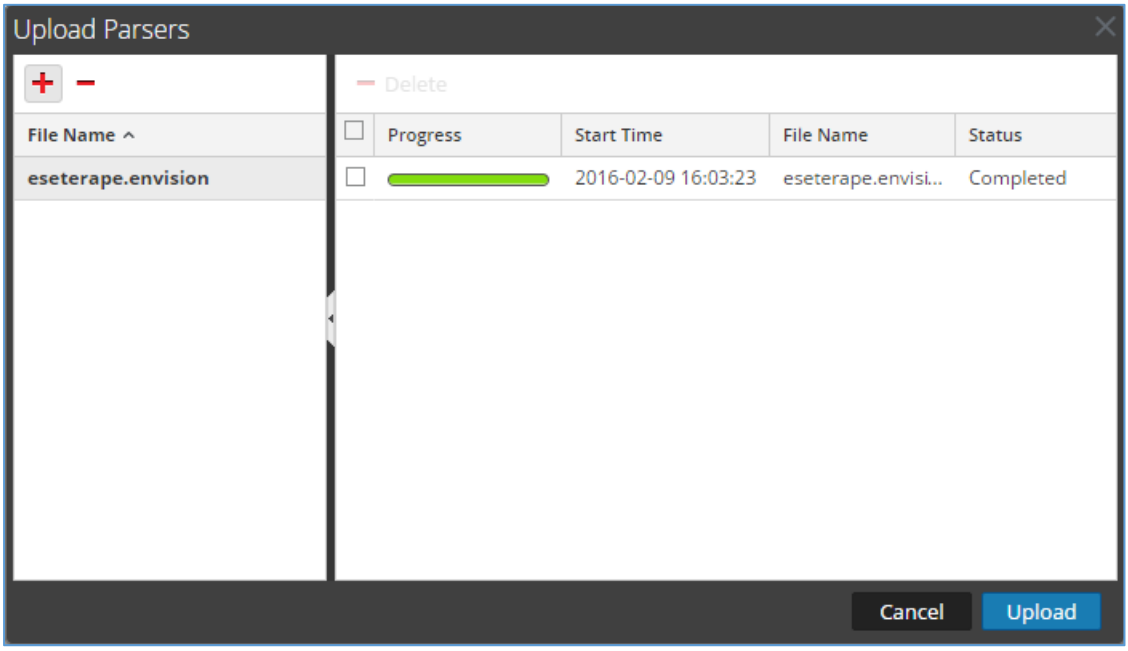
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**



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>.

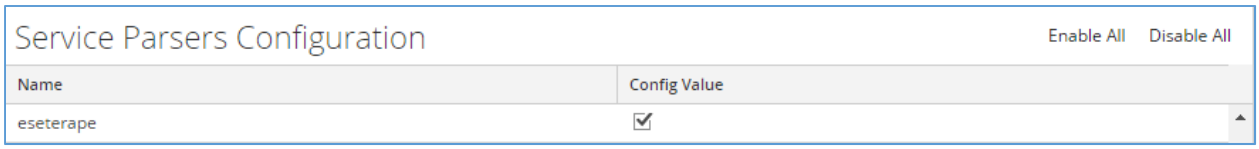
```
<mappings>
        <mapping envisionName="result" nwName="result" flags="Transient" envisionDisplayName="Result|Volume|Information|Reason|Succeed/Failed"/>
        <mapping envisionName="s_context" nwName="context.subject" flags="Transient"/>
        <mapping envisionName="rulename" nwName="rule.name" flags="Transient" envisionDisplayName="Rule|RuleName"/>
        <mapping envisionName="info" nwName="index" flags="Transient"/>
        <mapping envisionName="macaddr" nwName="eth.host" flags="Transient" format="MAC" envisionDisplayName="DeviceMacAddress"/>
        <mapping envisionName="event_counter" nwName="event.counter" flags="Transient" format="Int32"/>
        <mapping envisionName="domain" nwName="domain" flags="Transient" envisionDisplayName="DomainName"/>
        <mapping envisionName="recorded_time" nwName="recorded.time" flags="Transient" format="TimeT"/>
        <mapping envisionName="protocol" nwName="protocol" flags="Transient" envisionDisplayName="Protocol"/>
        <mapping envisionName="application" nwName="server" flags="Transient"/>
        <mapping envisionName="starttime" nwName="starttime" flags="Transient" format="TimeT" envisionDisplayName="StartTime"/>
        <mapping envisionName="component_version" nwName="comp.version" flags="Transient"/>
        <mapping envisionName="sport" nwName="ip.srcport" flags="Transient" format="UInt16" envisionDisplayName="SourcePort|LocalPort|ServerPort" nullTokens="-|(null)"/>
        <mapping envisionName="saddr_v6" nwName="ipv6.src" flags="None" format="IPv6" envisionDisplayName="ServerAddressv6|SourceAddressv6" failureKey="host.src" nullTokens="(null)|-"/>
        <mapping envisionName="daddr_v6" nwName="ipv6.dst" flags="None" format="IPv6" envisionDisplayName="DestinationAddressv6|ClientAddressv6" failureKey="host.dst" nullTokens="(null)|-"/>
        <mapping envisionName="url" nwName="url" flags="Transient" envisionDisplayName="URL"/>
        <mapping envisionName="group_object" nwName="group.object" flags="Transient"/>
        <mapping envisionName="directory" nwName="directory" flags="Transient" envisionDisplayName="Directory|WorkingDirectory"/>
        <mapping envisionName="context" nwName="context" flags="Transient"/>

</mappings>
```

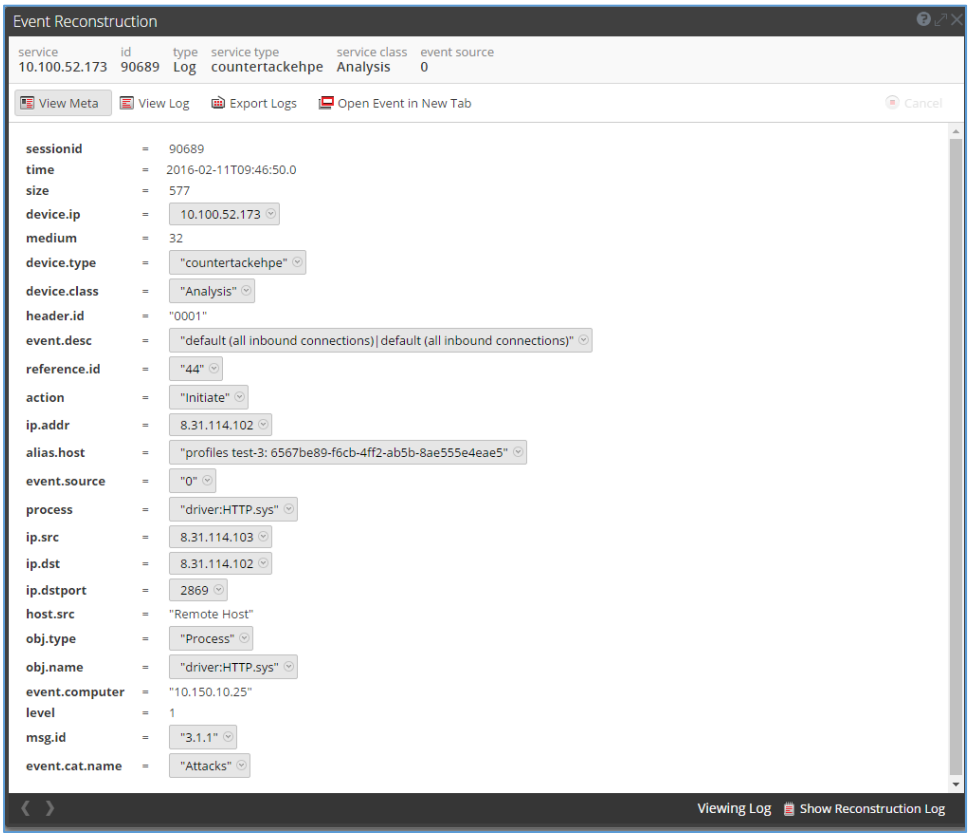
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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 ESET Remote Administrator 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 ESET 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 ESET Remote Administrator is properly configured and secured before deploying to a production environment. For more information, please refer to the ESET Remote Administrator documentation or website.**

ESET Remote Administrator Configuration

Deploy the ODBC Event Source Type XML

The ODBC Event Source Type XML, esetv5.xml, is included in the partner package downloaded from the Security Analytics Community. The first step is to deploy this file to the Security Analytics Log Collector.

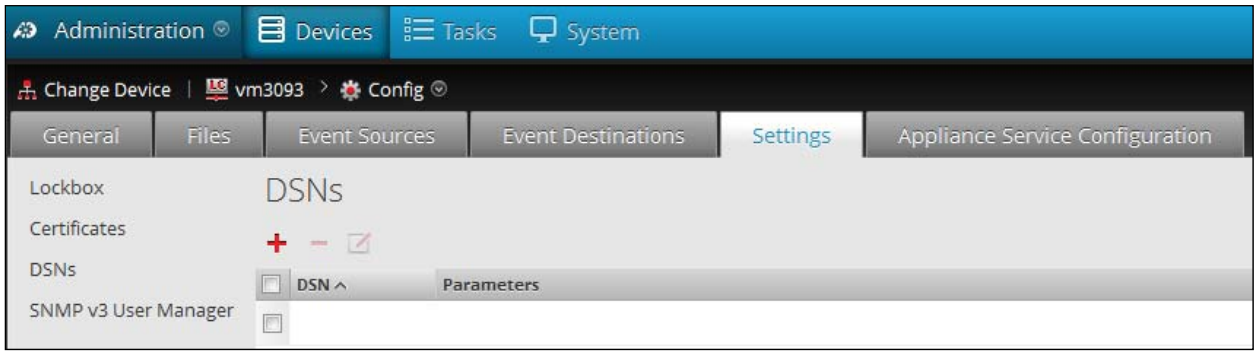
1. Log into the **Log Collector** via file transfer protocol (e.g. SFTP).
2. Transfer the XML file to the following directory: **/etc/netwitness/ng/logcollection/content/collection/odbc**.
3. Change the file permissions on the file to **755**.
4. **Restart** the Log Collector service.

Configure an ODBC Event Source

After deploying the ODBC Event Source Type XML, add the Data Source Name (DSNs) to the configuration.

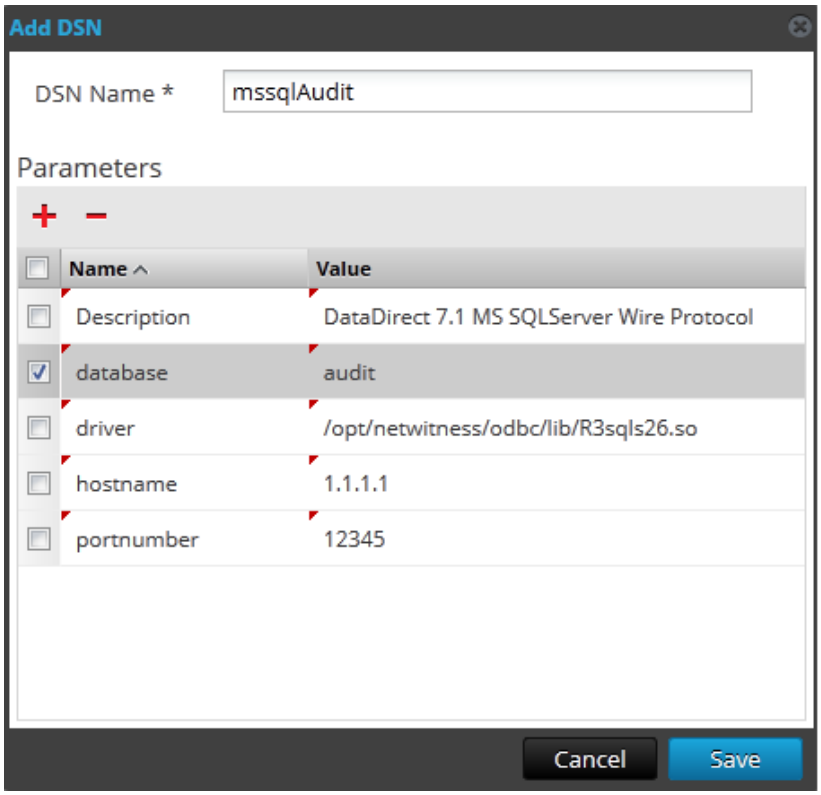
5. From the Security Analytics menu, select **Administration > Devices**.
6. In the Devices pane, select the **Log Collector** device.
7. In the toolbar, select **View > Config**.
8. Click the **Settings** tab.

9. From the left side menu, select **DSNs** and click +.



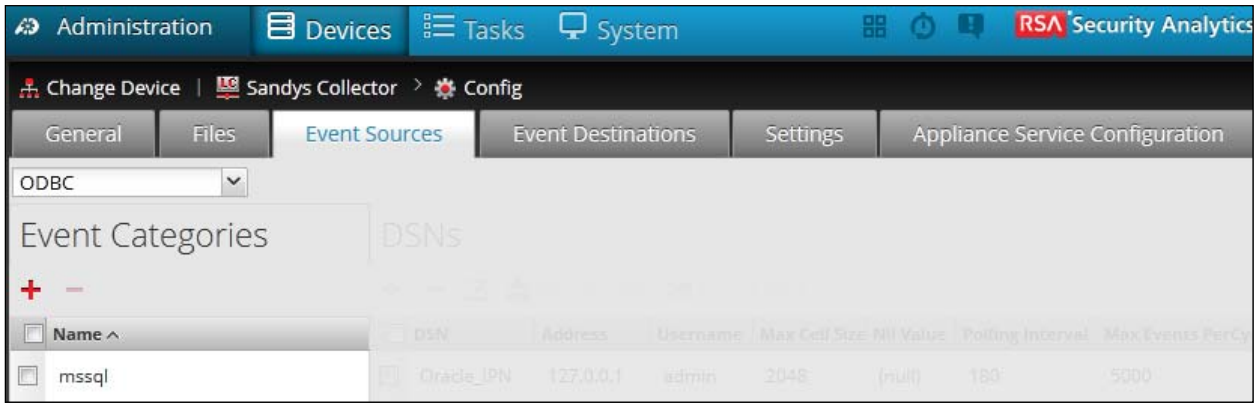
10. Enter a name in the **DSN Name** field.
11. Select the + and specify the value pairs and click **Save**.

Note: Refer to ODBC Value Pairs for a list of the value pairs for the ODBC event sources supported in this release.

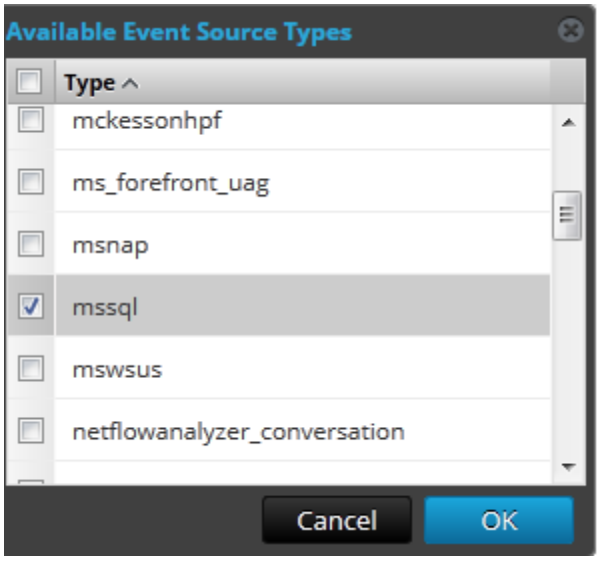


12. Select the **Event Sources** tab.

13. Select **ODBC** from the drop-down menu.

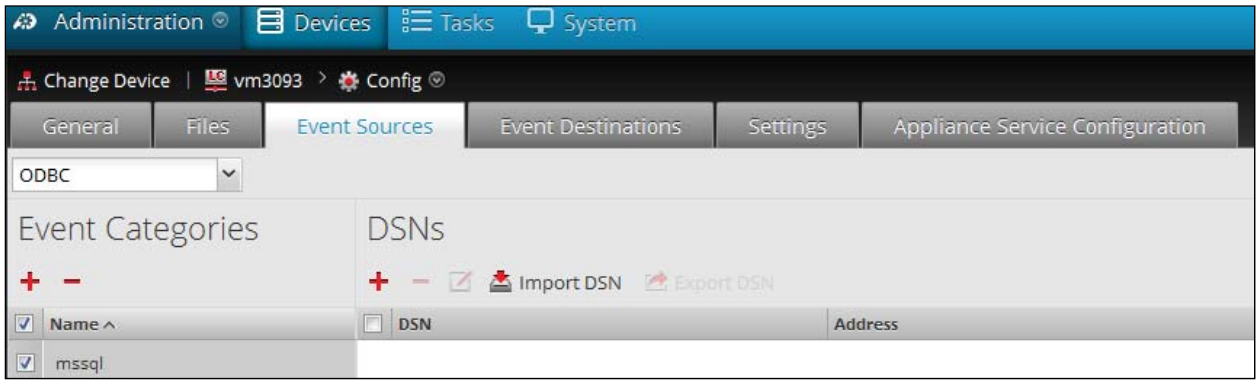


14. Click + the **Available Event Source Types** dialog is displayed.

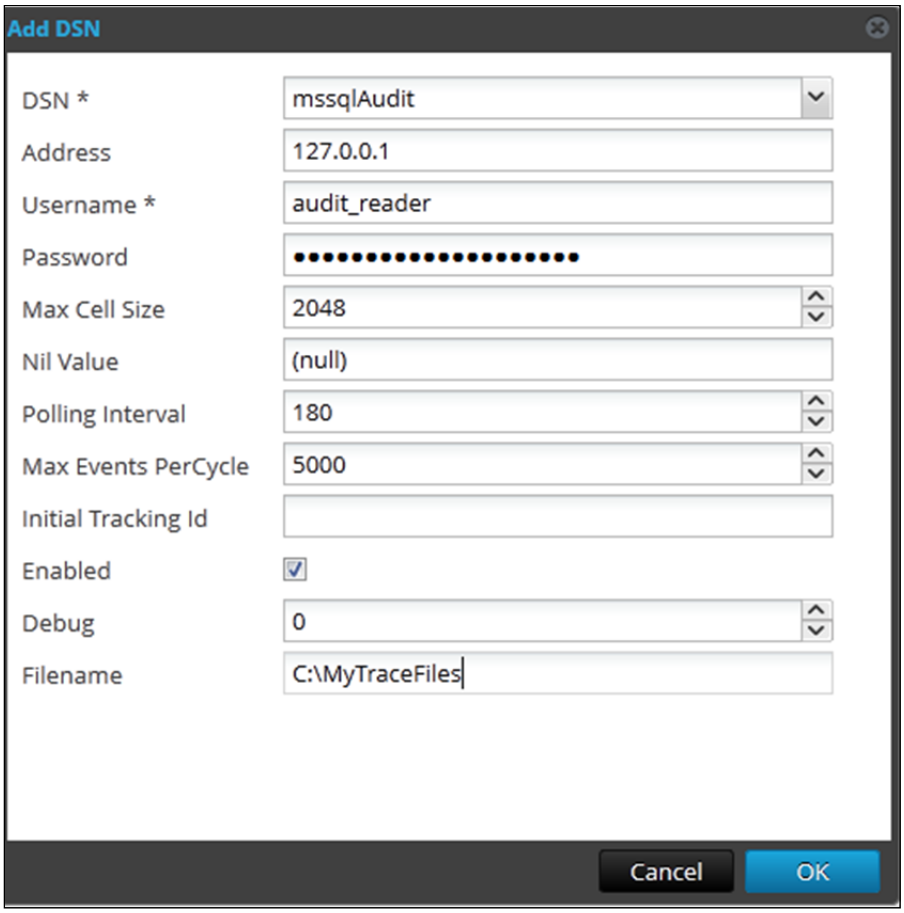


15. Select the Event Source Type which was deployed in the previous section, **Deploy the ODBC Event Source Type XML** and click **OK**. In this example we'll use a predefined event source, **mssql**.

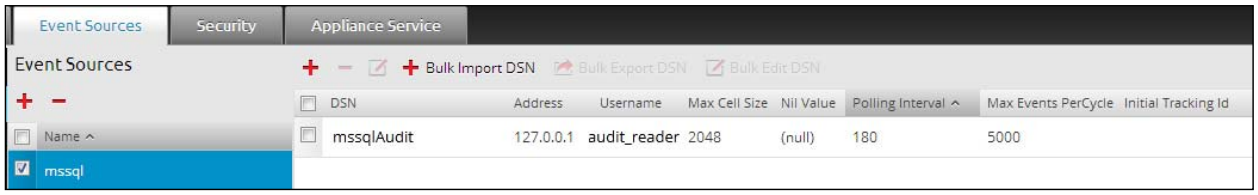
16. Under the Name column, **select** the Event Source Type that was added and click + in the DSNs pane.



17. Select the DSN you create from the drop down list, specify or modify the other parameters as required, and click **OK**.



18. The newly defined DSN is displayed in the DSNs panel.



Start the ODBC Collection Service

The final configuration step is to start the ODBC Service within Security Analytics. For complete instructions, refer to ***Configure Log Collection*** in the SA online help documentation.

Certification Checklist for RSA Security Analytics

Date Tested: 2/23/2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
ESET Remote Administrator	5.0	Microsoft Windows 2008

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

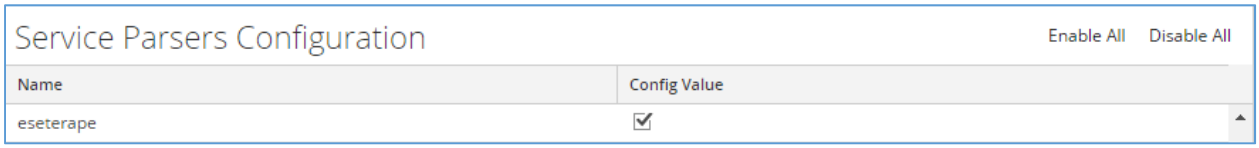
Appendix

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).