RSA Ready Implementation Guide for RSA Security Analytics

Stealthbits Technologies Inc.
StealthINTERCEPT 3.3

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

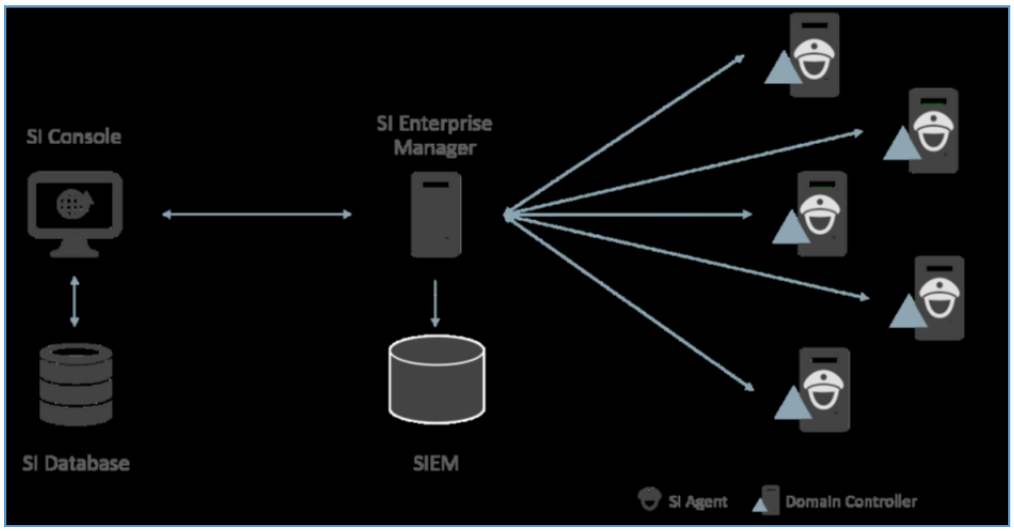
RSA READY

Solution Summary

RSA Security Analytics provides security operations teams with robust capabilities to detect, investigate, and take targeted action against advanced attacks before they can impact the business. When combined with StealthINTERCEPT (SI) Active Directory firewall technology, Security Analytics is enriched with streamlined, expedited, and enhanced visibility into security incidences occurring within Active Directory and its connected infrastructure. Eliminating any reliance on native Windows logging in order to obtain security intelligence, StealthINTERCEPT feeds RSA Security Analytics high-quality, highly-contextual data in real-time, reducing the burden on both SIEM and SIEM administrators to make sense of incomplete, insufficient data generated by Microsoft logs.

The vast majority of most organization's IT infrastructure is Windows-based, controlled and managed by Active Directory – the authentication and authorization hub of any Microsoft environment. 80% of breaches involving hacking leverage authentication-based attack techniques against Active Directory to obtain legitimate, yet unauthorized access to systems, applications, and data. Using native logging facilities, these attacks go largely undetected. But with StealthINTERCEPT and Security Analytics, organizations are now able to obtain instantaneous insight into authentication-based attacks and unauthorized changes as they're happening, so nefarious activities can be stopped in their tracks before they ever become headline news.

RSA Security Analytics Features	
StealthINTERCEPT 3.3	
Integration package name	stealthbits.envision
Device display name within Security Analytics	stealthinterceptpe
Event source class	Access Control
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
stealthbits.envision	SA package deployed to parse events from device integrations.
stealthinterceptpe.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
04/08/2015	Initial support for StealthINTERCEPT.
3/1/2016	RSA Security Analytics 10.5 Support

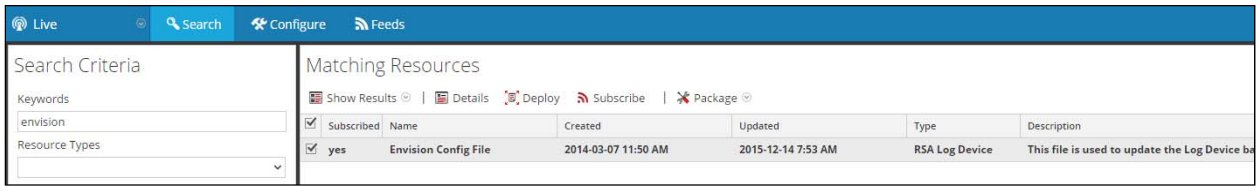
RSA Security Analytics Configuration

Deploy the enVision Config File

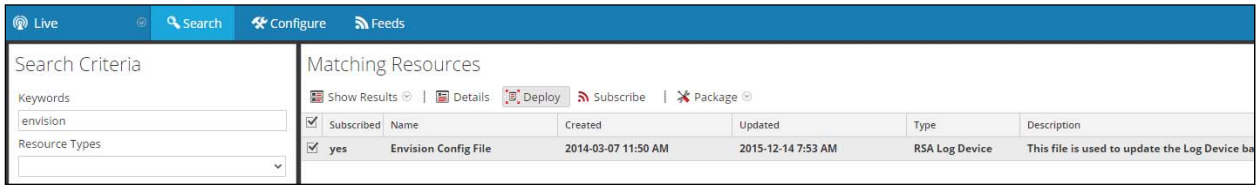
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

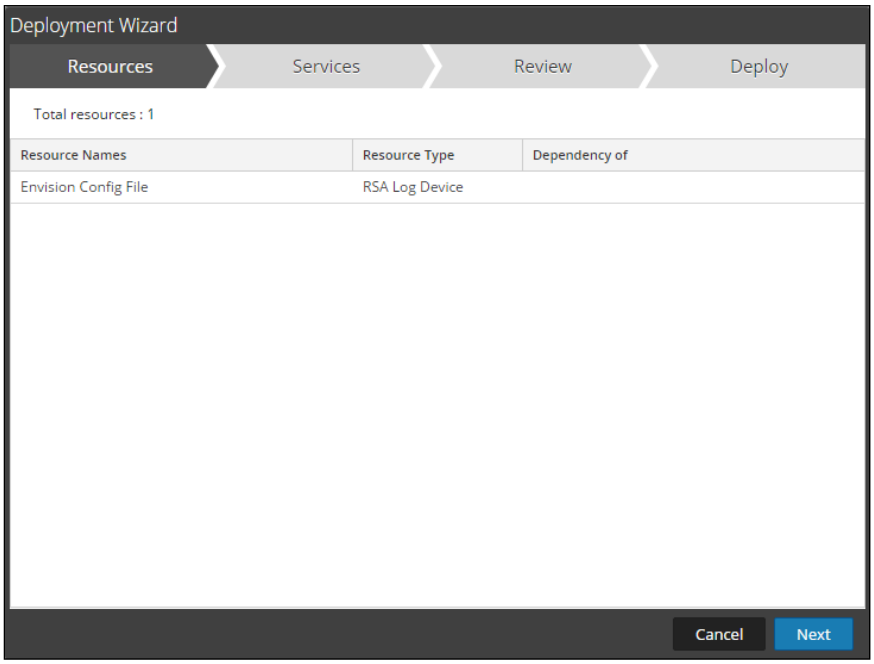
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



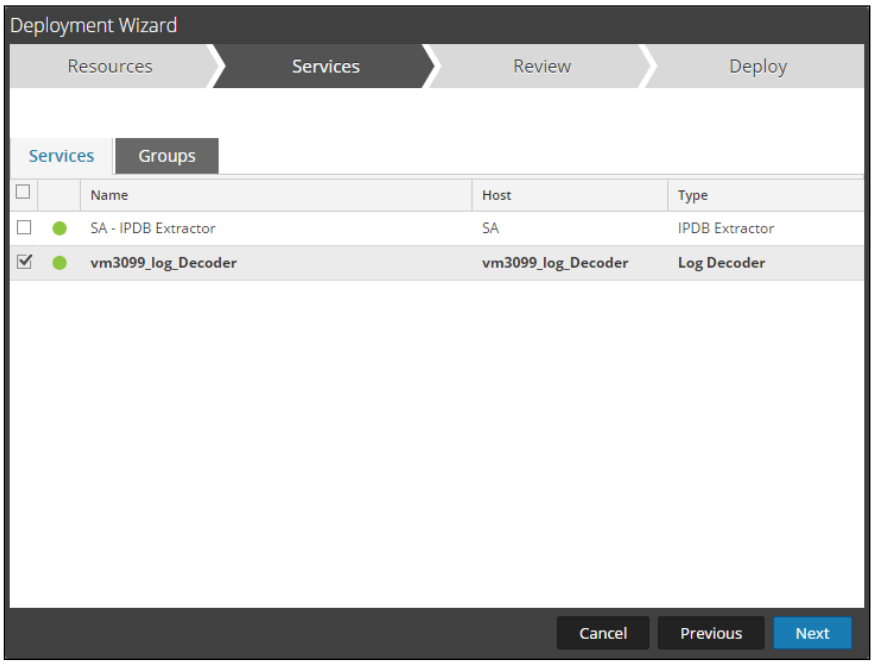
5. Click **Deploy** in the menu bar.



6. Select **Next**.

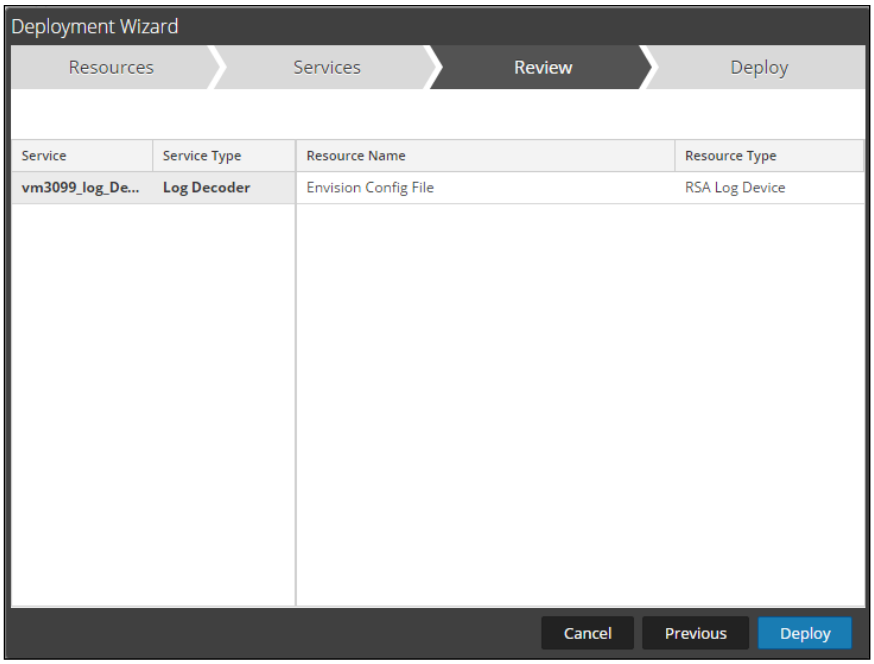


7. Select the **Log Decoder** and select **Next**.

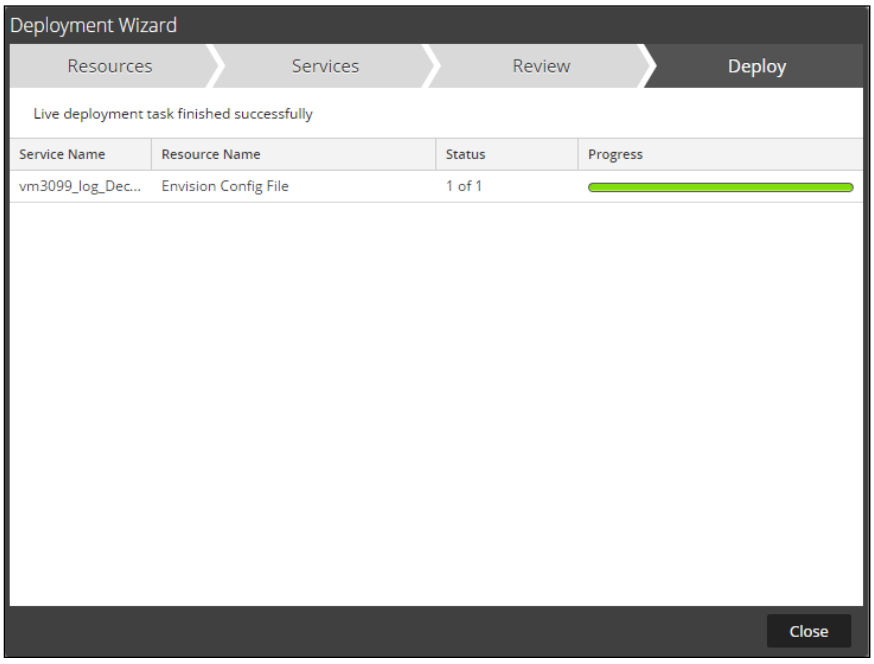


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



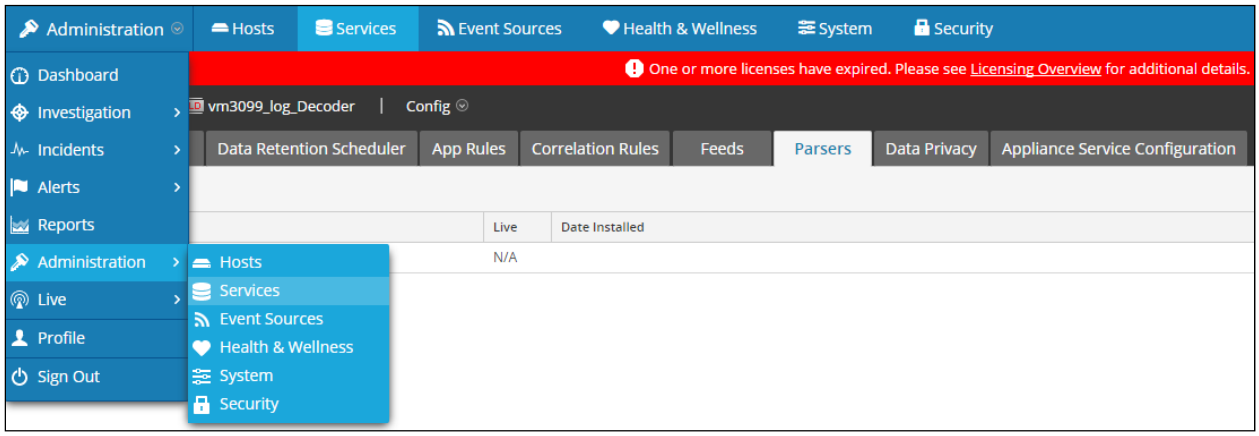
9. Select **Close**, to complete the deployment of the Envision Config file.



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.**



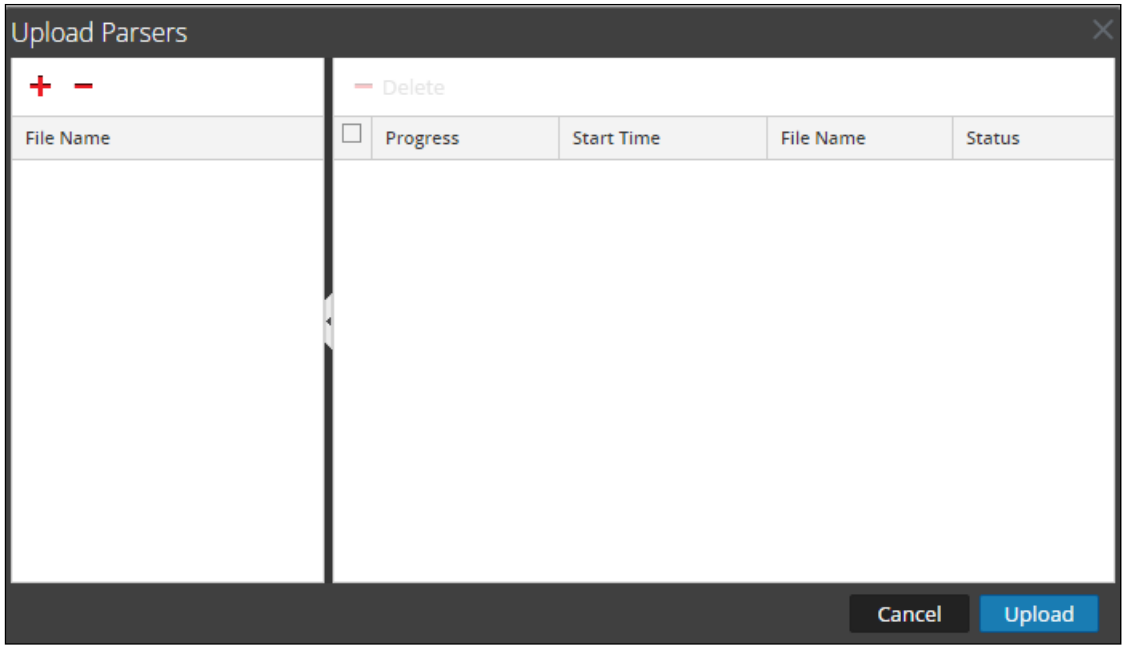
2. Select your Log Decoder from the list, select **View > Config**.

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

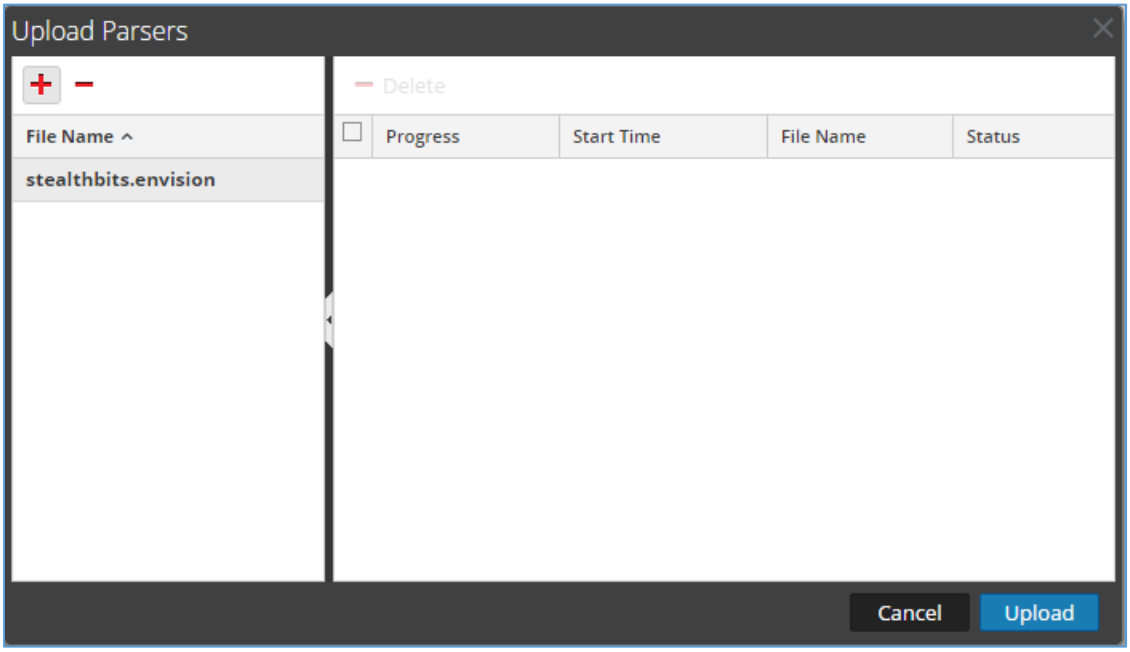
3. Next, select the **Parsers** tab and click the **Upload** button.

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

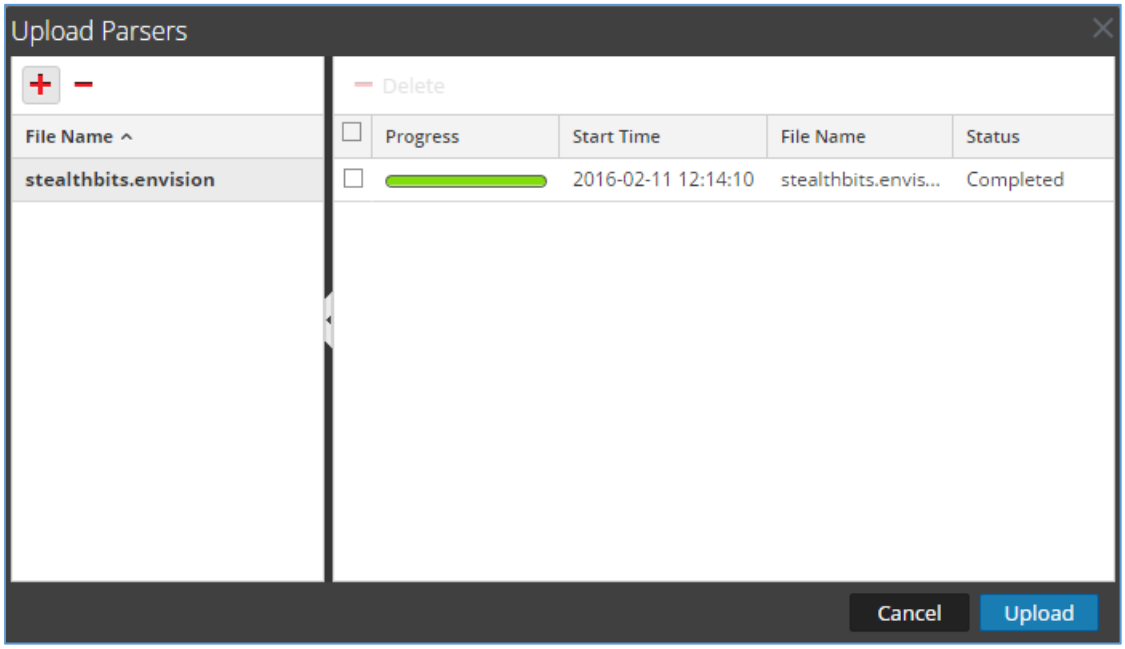
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**



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



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



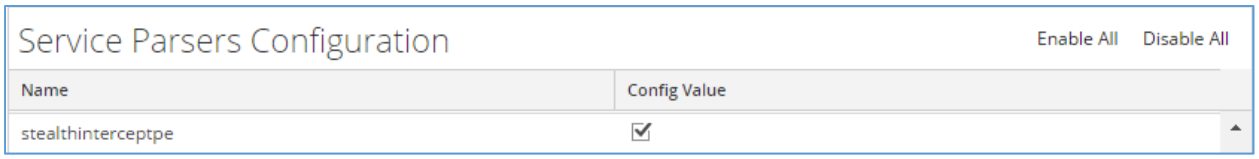
7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the *table-map-custom.xml* file from the contents of the .zip file to the */etc/netwitness/ng/envision/etc* folder. If the *table-map-custom.xml* file already exists on the log decoder(s), enter only the contents between the 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

```
<mappings>

        <mapping envisionName="change_new" nwName="change.new" flags="None" envisionDisplayName="ChangeNewValue"/>
        <mapping envisionName="change_old" nwName="change.old" flags="None" envisionDisplayName="ChangeOldValue"/>
        <mapping envisionName="component_version" nwName="comp.version" flags="None"/>
        <mapping envisionName="context" nwName="context" flags="None"/>
        <mapping envisionName="dn" nwName="dn" flags="None"/>
        <mapping envisionName="domain" nwName="domain" flags="None" envisionDisplayName="DomainName"/>
        <mapping envisionName="endtime" nwName="endtime" flags="None" format="TimeT" envisionDisplayName="EndTime"/>
        <mapping envisionName="hcategory" nwName="category" flags="None" envisionDisplayName="CallType|hcategory"/>
        <mapping envisionName="severity" nwName="severity" flags="None" envisionDisplayName="Severity|SeverityLevel"/>
        <mapping envisionName="src_dn" nwName="dn.src" flags="Transient"/>
        <mapping envisionName="starttime" nwName="starttime" flags="Transient" format="TimeT" envisionDisplayName="StartTime"/>
        <mapping envisionName="blockedevent" nwName="blockedevent" flags="None"/>
        <mapping envisionName="sucessfulchange" nwName="sucessfulchange" flags="None"/>

</mappings>
```

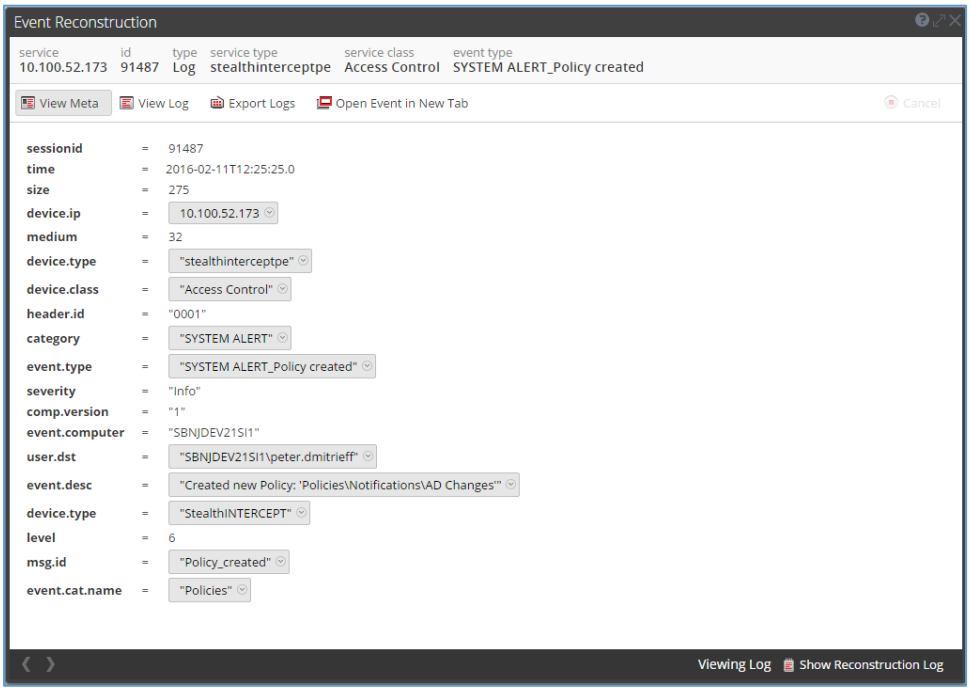
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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 StealthINTERCEPT 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.

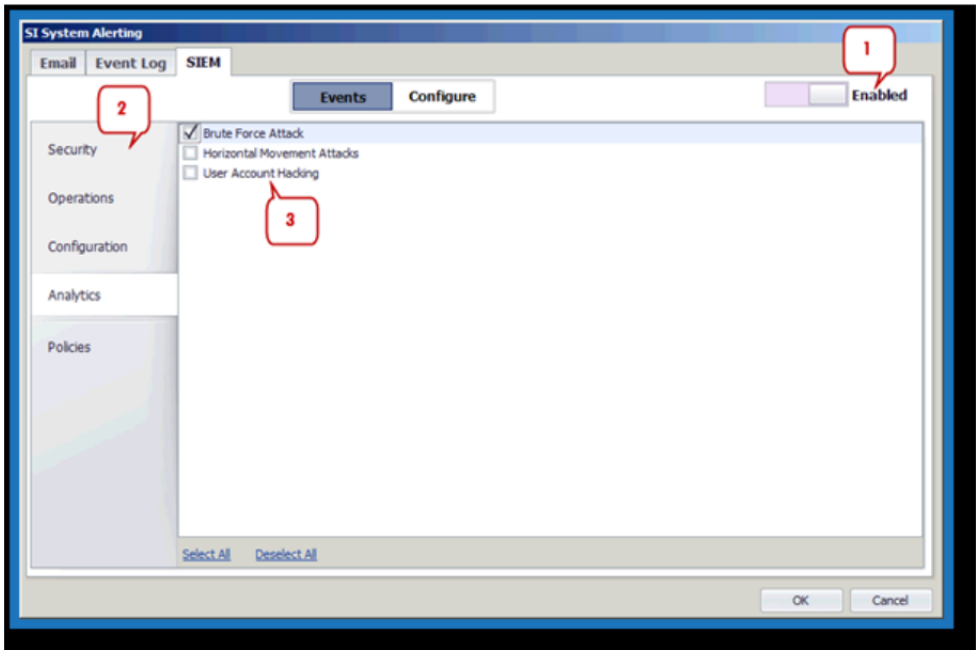
All StealthINTERCEPT components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

> **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 Stealthbits StealthINTERCEPT is properly configured and secured before deploying to a production environment. For more information, please refer to the Stealthbits StealthINTERCEPT documentation or website.**

StealthINTERCEPT Configuration

Before SIEM alerting can be enabled, the SIEM server information must be configured. This is done through the Configure section of the SIEM Tab.

When the configuration is complete, it is time to decide what events will receive notification. This can be done through the Events section of the SIEM Tab.



1. Click the button in front of **Disabled** to toggle the setting to **Enabled**.
2. Select the event category (Security, Operations, Configuration, Analytics, Policies) from the list on the left.

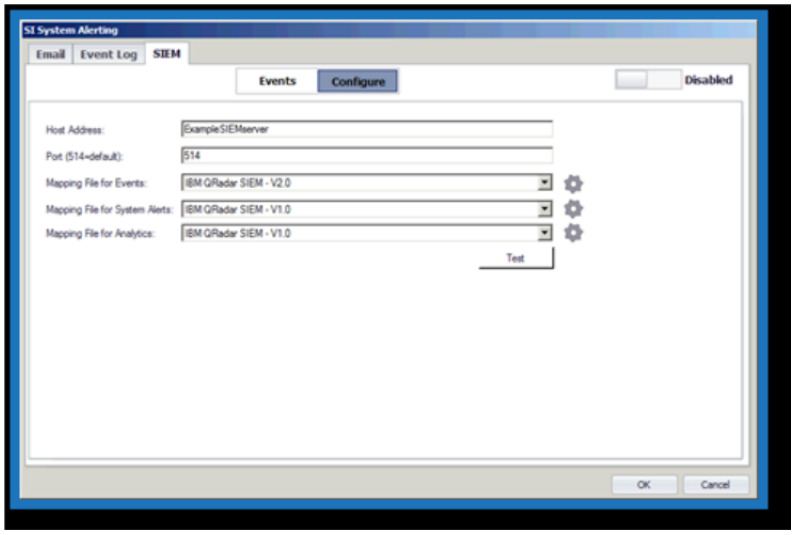
> **Important: The Configure SIEM Server options allow SI Administrators to set a SIEM Mapping File for each type of event category.**

3. Check the event(s) that will trigger SIEM notifications from the list in the center.

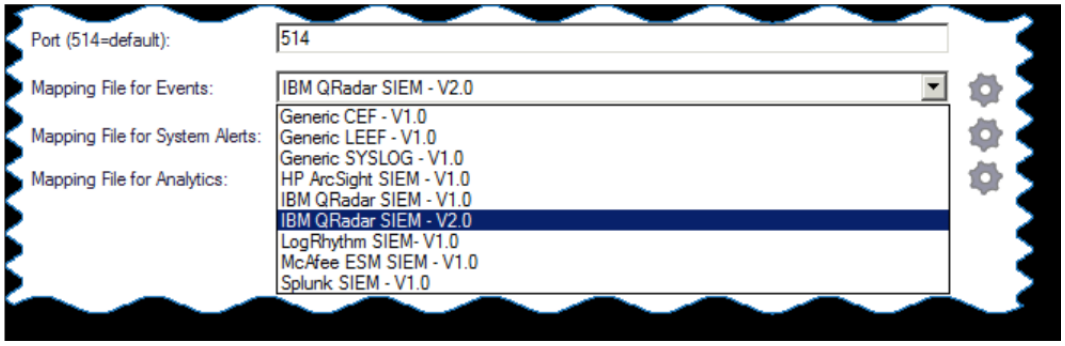
The SI Admin Console will now send SIEM notifications for the selected events/incidents/policies.

Configure SIEM Server

Follow these directions to configure the SIEM server for alerting.



1. On the SIEM Tab, select **Configure**.
2. For the Host Address box provide either an IP address or server name for the SIEM server.
3. For the Port box provide the appropriate port number to communicate with the SIEM server.



For the Mapping File for Events box, use the drop-down menu to select the SIEM product which will be receiving policy event notifications. The gear icon to the right of the drop-down arrow allows SI Administrators to import a custom mapping file. These mapping file formats are specifically designed for policy events.

For the Mapping File for System Alerts box, use the drop-down menu to select the SIEM product which will be receiving SI Security, SI Operations, and SI Configuration event alerts. The gear icon to the right of the drop-down arrow allows SI Administrators to import a custom mapping file. These mapping file formats are specifically designed for SI system events.

For the Mapping File for Analytics box, use the drop-down menu to select the SIEM product which will be receiving Analytics incident alerts. The gear icon to the right of the drop-down arrow allows SI Administrators to import a custom mapping file. These mapping file formats are specifically designed for Analytics incidents.

4. OPTIONAL: Use the Test button to confirm the configuration settings.

Now that the SIEM server has been configured, it is time to assign events to send alerts. Events can be assigned through the SI System Alerting Window's SIEM Tab or assigned to a policy on the Actions Tab of the Policy Configuration.

Certification Checklist for RSA Security Analytics

Date Tested: March 1, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
StealthINTERCEPT	3.3	Windows Server

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

Known Issues

Known Issues

Use the following guide of commonly used variables to determine which variables to use when creating custom rules and charts in Security Analytics. Use msg.id to get unique events from each category.

System Events:

event.computer: the host referenced in the event
event.desc: the full text of the event

AD Policies:

event.computer: the host referenced in the event
usr.dst: the user that triggers the event
ip.src: the IP address of the host that triggers the event
obj.name: name of the object referenced in the event
dn: the distinguished name of the event object
change.old: old value of the object
change.new: new value of the object

GPO Policies:

event.computer: the host referenced in the event
dn: the distinguished name of the GPO property changed

Authentication Policies:

ip.dst: the IP address of the host that is being logged into
host.dst: hostname of the computer being logged into

File Monitoring Policies:

ip.addr: the IP address of the host that triggers the event
dn: the distinguished name of the file that is accessed

Exchange Policies:

event.computer: the host referenced in the event
usr.dst: the user that triggers the event
ip.src: the IP address of the host that triggers the event
context: the attribute that is changed in the event

Analytics:

ip.dst: the IP address of the host that is being attacked
host.dst: hostname of the computer being attacked
ip.src: the IP address of the attacking host
host.src: hostname of the attacking computer
event.desc: full description of the event

Refer to the XML for the msg.id that refers to the events in each category.

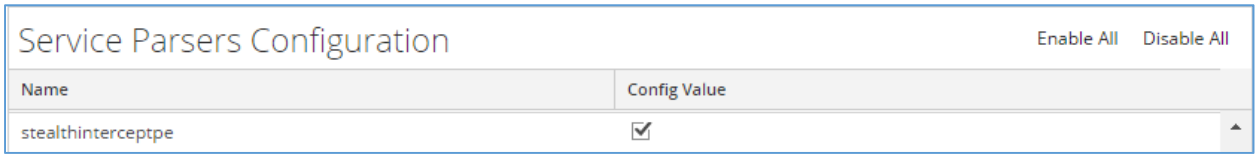
Appendix

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).