RSA Ready Implementation Guide for RSA Security Analytics

StoneSoft Stonegate 5.3

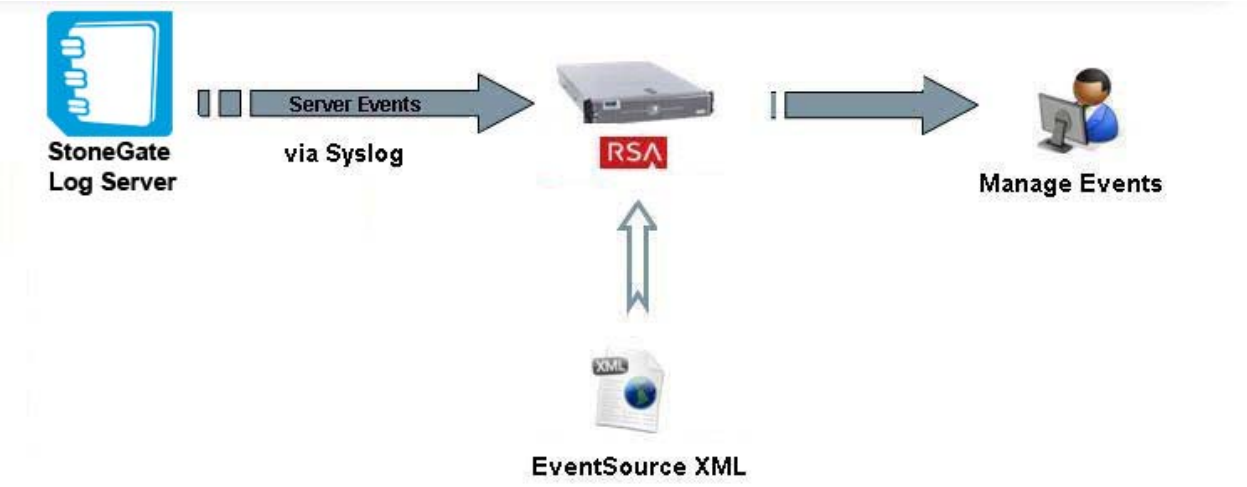
Daniel R. Pintal, RSA Partner Engineering
Last Modified: March 1, 2016

RSA READY

Solution Summary

StoneGate security engines send their logs to a StoneGate Log Server (part of the StoneGate Management Center). The log entries can then be exported from a Log Server to an external RSA Security Analytics server via Syslog.

RSA Security Analytics Features	
Stonegate 5.3	
Integration package name	stonesoftsgpe.envision
Device display name within Security Analytics	stonesoftsgpe
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
stonesoftsgpe.envision	SA package deployed to parse events from device integrations.
stonesoftsgpemsg.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
12/3/2013	Support for RSA Security Analytics
3/1/2016	RSA Security Analytics 10.5 Support

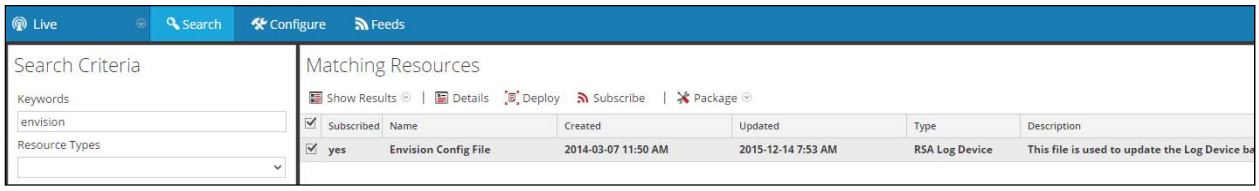
RSA Security Analytics Configuration

Deploy the enVision Config File

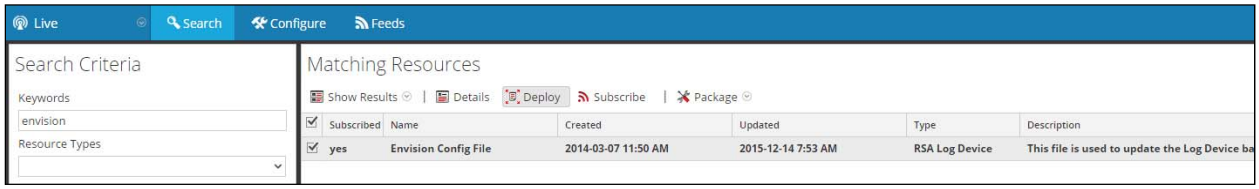
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

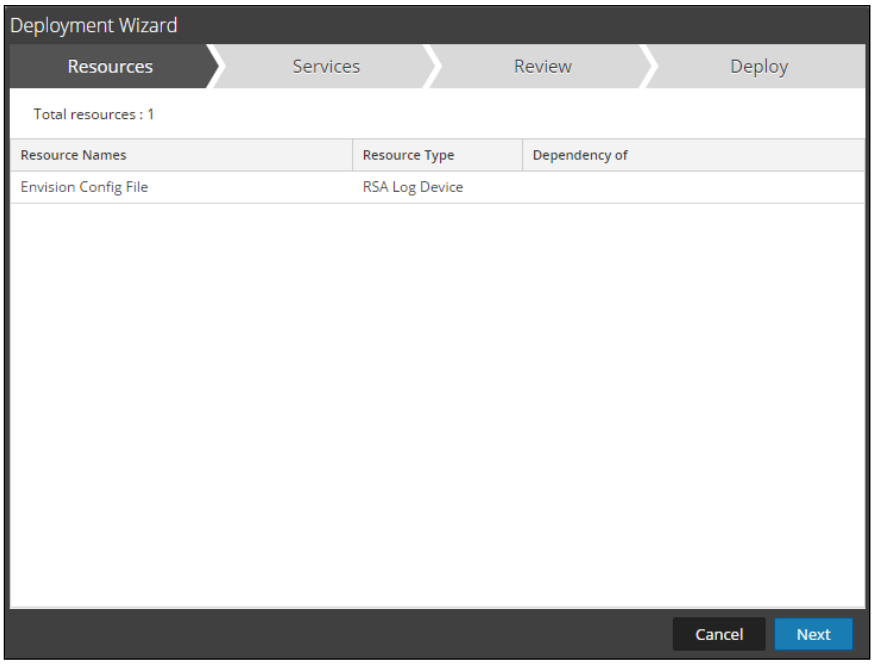
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



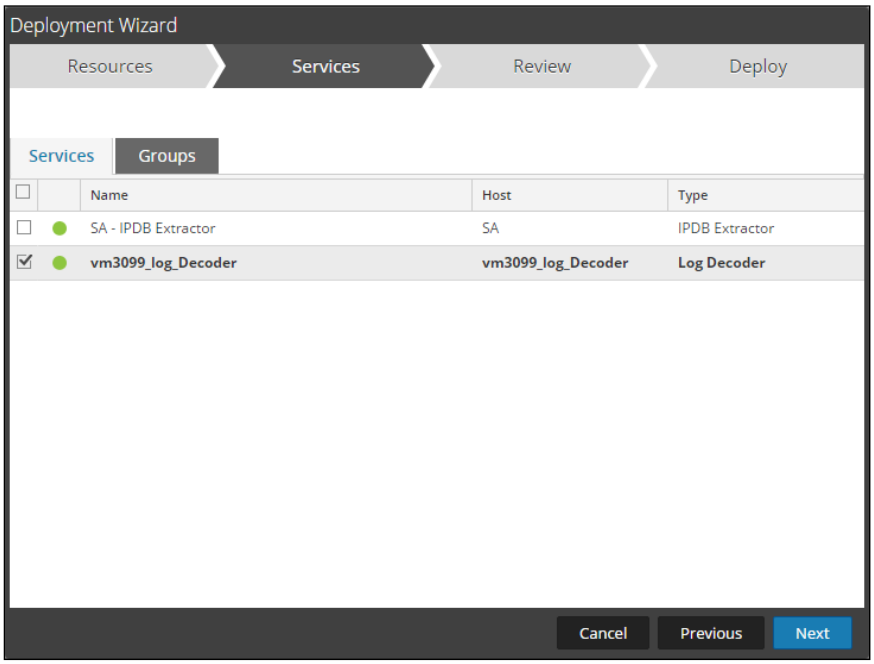
5. Click **Deploy** in the menu bar.



6. Select **Next**.

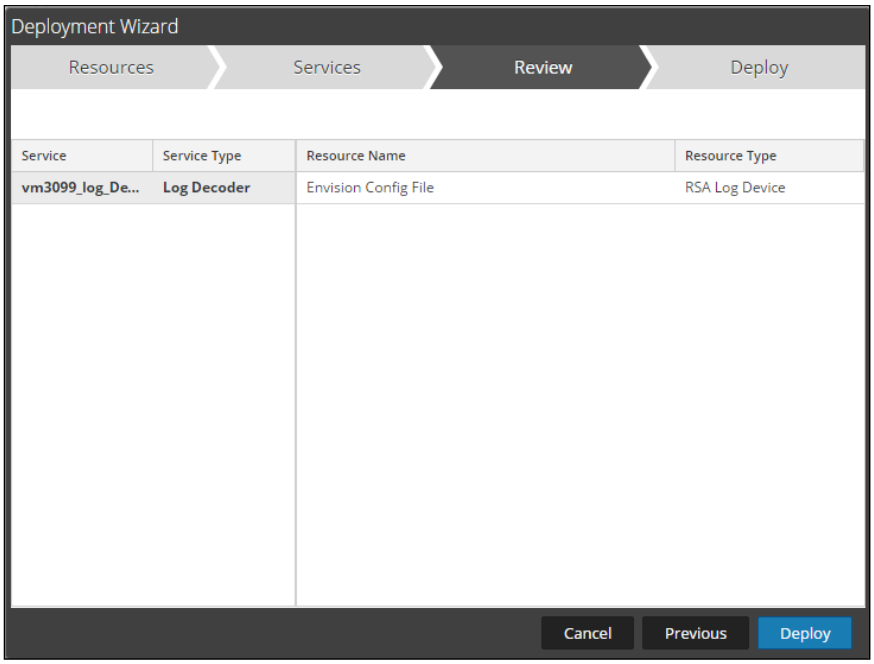


7. Select the **Log Decoder** and select **Next**.

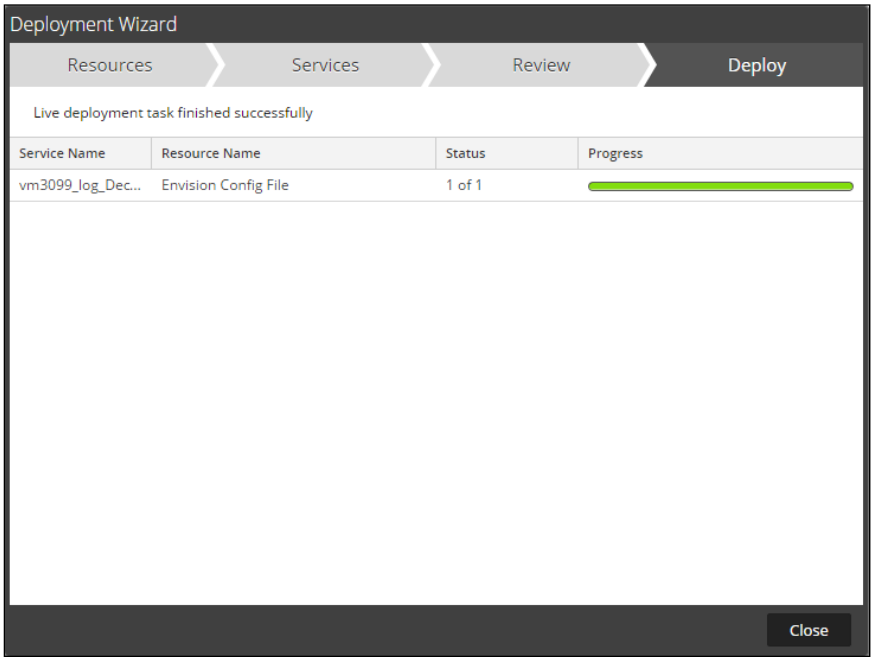


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



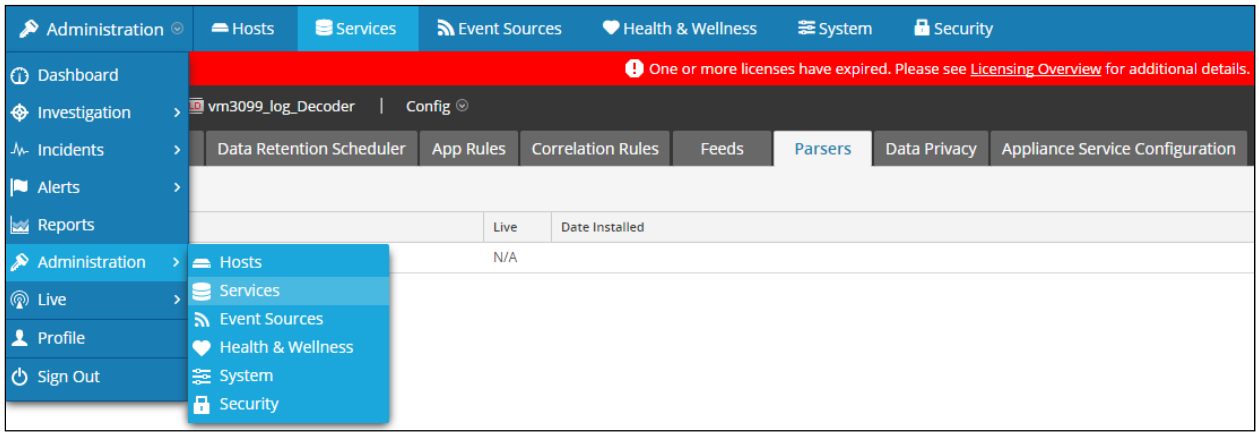
9. Select **Close**, to complete the deployment of the Envision Config file.



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.**



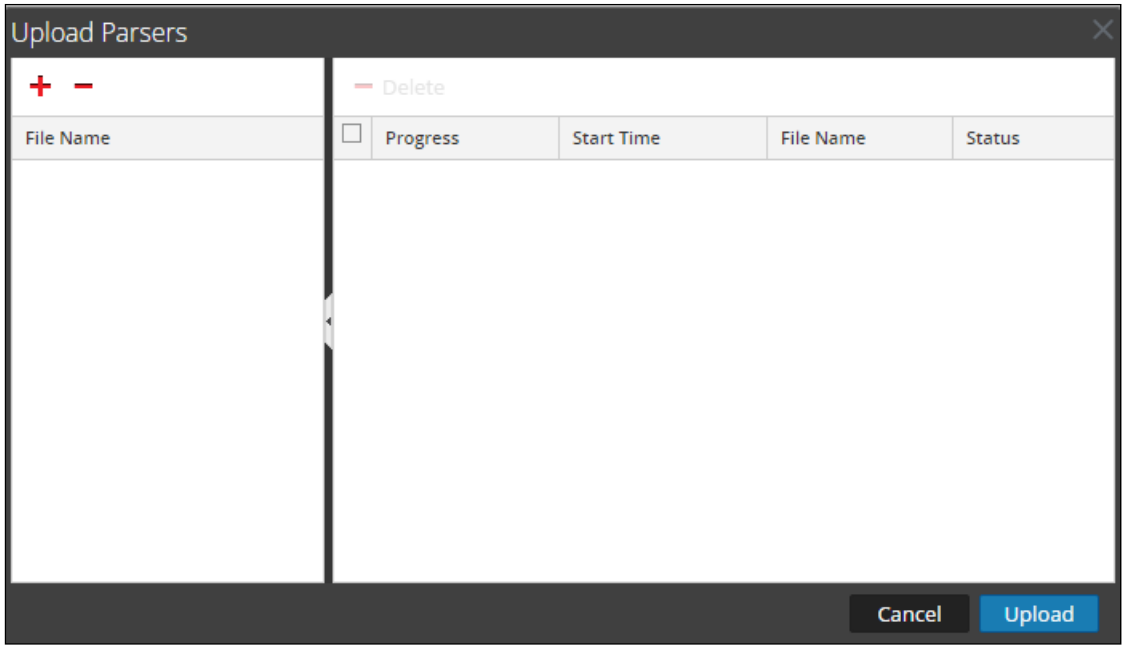
2. Select your Log Decoder from the list, select **View > Config**.

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

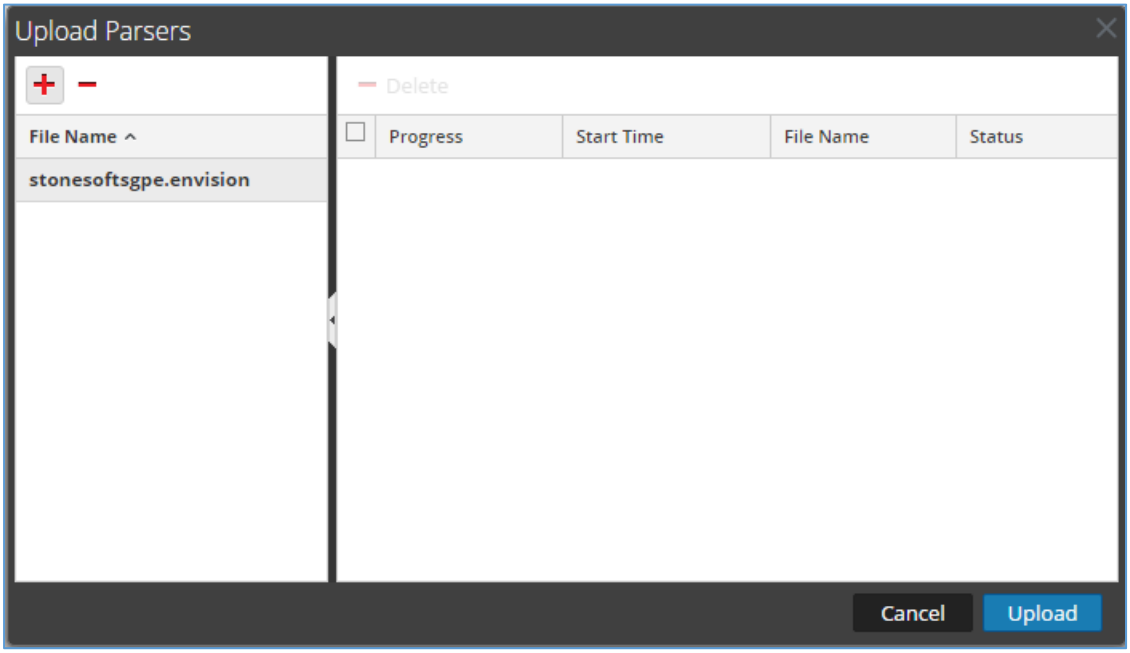
3. Next, select the **Parsers** tab and click the **Upload** button.

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

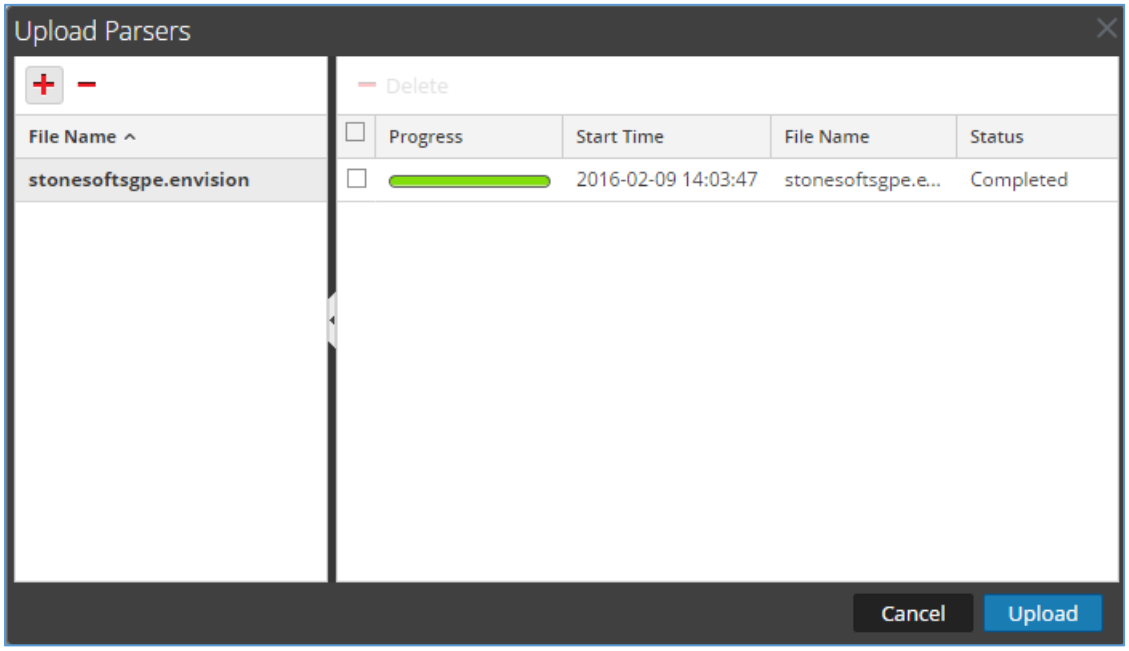
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**



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



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



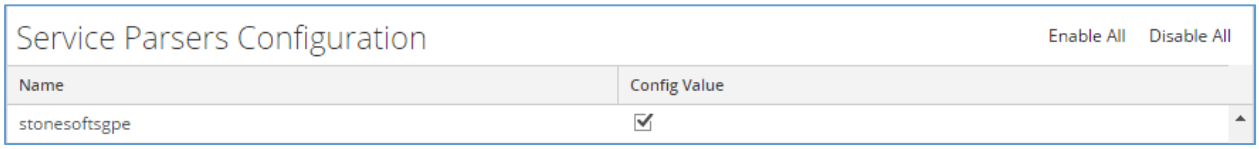
7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the *table-map-custom.xml* file from the contents of the .zip file to the */etc/netwitness/ng/envision/etc* folder. If the *table-map-custom.xml* file already exists on the log decoder(s), enter only the contents between the *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

```
<mappings>

        <mapping envisionName="dtransaddr" nwName="dtransaddr" flags="None"/>
        <mapping envisionName="version" nwName="version" flags="None"/>
        <mapping envisionName="network_service" nwName="network.service" flags="None" envisionDisplayName="NetworkServiceName"/>
        <mapping envisionName="event_counter" nwName="event.counter" flags="None" format="Int32"/>
        <mapping envisionName="dtransport" nwName="dtransport" flags="None"/>
        <mapping envisionName="protocol" nwName="protocol" flags="None" envisionDisplayName="Protocol"/>
        <mapping envisionName="stransaddr" nwName="stransaddr" flags="None"/>
        <mapping envisionName="icmpcode" nwName="icmp.code" flags="None" format="UInt32"/>
        <mapping envisionName="sport" nwName="ip.srcport" flags="None" format="UInt16" envisionDisplayName="SourcePort|LocalPort|ServerPort" nullTokens="-|(null)"/>
        <mapping envisionName="severity" nwName="severity" flags="None" envisionDisplayName="Severity|SeverityLevel"/>
        <mapping envisionName="stransport" nwName="stransport" flags="None"/>
        <mapping envisionName="interface" nwName="interface" flags="None" envisionDisplayName="Interface"/>
        <mapping envisionName="msg" nwName="msg" flags="None" format="Text" envisionDisplayName="Message"/>
        <mapping envisionName="rule_uid" nwName="rule.uid" flags="None"/>
        <mapping envisionName="sigtype" nwName="sig.type" flags="None" envisionDisplayName="SignatureType"/>
        <mapping envisionName="webpage" nwName="web.page" flags="None" envisionDisplayName="WebPage"/>
        <mapping envisionName="rbytes" nwName="rbytes" flags="None" format="UInt64" nullTokens="(null)|-"/>
        <mapping envisionName="src_spi" nwName="spi.src" flags="None"/>
        <mapping envisionName="context" nwName="context" flags="None"/>
        <mapping envisionName="listnum" nwName="listnum" flags="None"/>

</mappings>
```

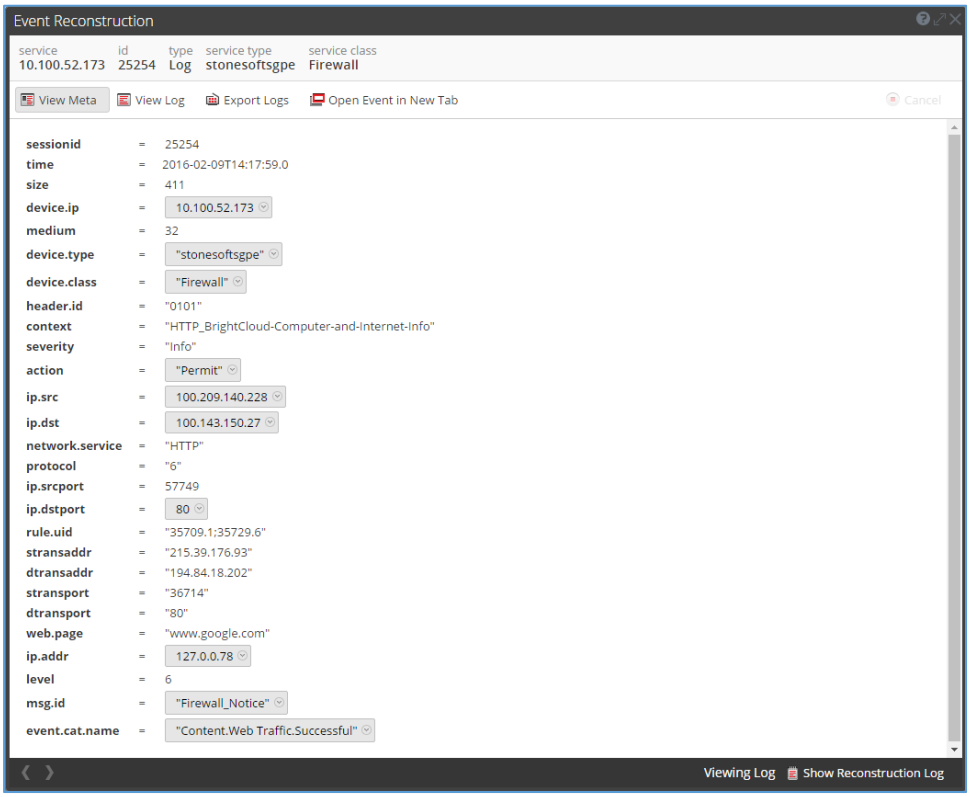
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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 Stonesoft StoneGate 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 Stonesoft StoneGate 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 StoneSoft Stonegate is properly configured and secured before deploying to a production environment. For more information, please refer to the StoneSoft Stonegate documentation or website.**

StoneGate Log Server Configuration

This section explains the general steps needed for sending log data in CSV format to RSA SA servers. For detailed instructions, see the *StoneGate Administrator's Guide* available at **http://www.stonesoft.com/en/support/technical_support_and_documents/manuals/current/**.

1. Install the StoneGate Management Center software as a typical installation, or install the StoneGate Management Center as a custom installation according to your environment. For detailed installation instructions, see the StoneGate Management Center Installation Guide available at **http://www.stonesoft.com/en/support/technical_support_and_documents/manuals/current/**
2. Configure the syslog settings of the Log Server as explained in

3. **Defining General Syslog** Settings below.
4. (*Optional*) Filter the data sent to the RSA SA server as explained in section **Exporting Log Filters for Syslog Sending**.
5. Modify your policy to allow the traffic from the Log Server to the RSA SA server to pass through the firewall as explained in **Creating a Rule Allowing Traffic to the RSA Security Analytics Server.**

Defining General Syslog Settings

To define general Syslog settings:

1. Retrieve the *RSAenvision_syslog_conf.xml* file from Stonesoft website at https://my.stonesoft.com/support/document.do?product=StoneGate&docid=6804.
2. Transfer the RSAenvision_syslog_conf.xml file to the ***<installation directory>*/data/fields/syslog_templates** directory on the Log Server computer.
3. Stop the Log Server.
4. If you have defined the Log Server as a service in Windows, you may stop the Log Server in the Windows Services list. Alternatively, you can run ***<installation directory>*/bin/sgStopLogSrv.bat**.
5. In Linux, run **<installation directory>/bin/sgStopLogSrv.sh**.
6. Modify the *LogServerConfiguration.txt* file as shown in the table below. The file is located in ***<installation directory>*/data/**.

Parameter	Value	Description
SYSLOG_CONF_FILE	SYSLOG_CONF_FILE=${SG_ROOT_DIR}/ data/fields/syslog_templates/ RSAenvision_syslog_conf.xml	The path to the syslog template file you transferred to the Log Server in step **Error! Reference source not found.**.
SYSLOG_EXPORT_FORMAT	CSV	Defines CSV as the file format used for syslog exporting.
SYSLOG_EXPORT_ALERT	YES | NO	Defines whether to export Alert entries to the RSA SA server.
SYSLOG_EXPORT_FW	YES | NO	Defines whether to export StoneGate Firewall/VPN logs to the RSA SA server.
SYSLOG__EXPORT_IPS	YES | NO	Defines whether to export StoneGate IPS logs to the RSA SA server.

Parameter	Value	Description
SYSLOG_FILTER_MATCH	ALL | ONE | NONE	If you filter the data sent to the RSA SA server, define how you want the filter match to be applied: • **ALL**: The log is exported if it matches all filters. • **ONE**: The log is exported if it matches at least one filter. • **NONE**: The log is exported if it does not match any of the filters. **Important: If you do not use filters, remove this parameter from the LogServerConfiguration.txt file.**
SYSLOG_FILTER_TYPE	KEEP | DISCARD	If you filter the data sent to the RSA SA server, define the action for logs that match the filter: • **KEEP**: The matching logs are sent to the RSA SA server. • **DISCARD**: The matching logs are not sent to the RSA SA server. **Important: If you do not use filters, remove this parameter from the LogServerConfiguration.txt file.**
SYSLOG_MESSAGE_PRIORITY	6	The priority of the syslog message is included at the beginning of each UDP packet as defined in RFC 3164 http://www.ietf.org/rfc/rfc3164.txt

Parameter	Value	Description
SYSLOG_PORT	514	The target UDP port for sending events to syslog. The default port is 514.
SYSLOG_SERVER_ADDRESS	<RSA Security Analytics server IPv4 address>	The IPv4 address of the RSA SA server for syslog sending over UDP. If left empty, transfers are not made.
SYSLOG_USE_DELIMITER	ALWAYS	Enables the use of double quotes (") to delimit all field values, including null strings, in syslog messages. **Important: The RSA SA server requires null strings to be sent with quotes. Specify ALWAYS as the value of this parameter to ensure that null strings are sent correctly.**

7. Save the file and restart the Log Server.
8. Proceed to the next relevant section:
   - If you want to filter the data sent to the RSA SA server, continue to **Exporting Log Filters for Syslog Sending**.
   - If you do not want to use filters, continue to **Creating a Rule Allowing Traffic to the RSA Security Analytics Server**.

Exporting Log Filters for Syslog Sending

You can use filters to select the data sent from the Log Server to the RSA SA server. First create the filter(s) as instructed in the section titled **Filtering Data** in the *StoneGate Administrator's Guide* or the Management Client *Online Help*. You can then export and apply the filters to firewall logs and IPS logs separately.

To export log filters for syslog sending:

1. Select **Configuration→Configuration→Monitoring** from the menu.
2. Expand the **Other Elements** tree.
3. Browse to **Filters→All Filters** or **Filters→By Filter Tag** in the left panel.
4. Right-click the filter you want to export and select **Tools→Save for Command Line Tools** from the menu. The Save Filter dialog opens.

5. Select **Local Workstation** and click **Browse** to select where the filter is exported. The Export Data dialog opens.
   - To use the filter for filtering firewall logs, select ***<installation directory>*/data/syslog/Firewall** as the directory.
   - To use the filter for filtering IPS logs, select ***<installation directory>*/data/syslog/IPS** as the directory.

> **Important: If you cannot export the filter directly to these directories, export the filter (.flp file) to another location and then copy the filter manually to the <installation directory>/data/syslog/Firewall or <installation directory>/data/syslog/IPS directory.**

6. Give the export file a name and click **OK** to export the filter.

Creating a Rule Allowing Traffic to the RSA Security Analytics Server

You must modify your firewall policy to allow the traffic from the Log Server to the RSA SA server to pass through the firewall. This may also require defining an appropriate NAT rule.

To create a rule allowing traffic to the RSA Security Analytics:

1. Select **Configuration→Configuration→Firewall** from the menu. The Firewall Configuration view or IPS Configuration view opens.
2. Select **Firewall Policies**, right-click the policy and select **Edit Firewall Policy**.
3. Add an IPv4 Access rule with the following values:
   - **Source**: your Log Server
   - **Destination**: the RSA SA server
   - **Service**: Syslog (UDP)
   - **Action**: Allow

Logging: In most cases, we recommend setting the logging to **None**, since logging syslog connections can create a loop (a log entry is sent to the RSA SA, creating a log entry that is sent to the RSA SA, creating a new log entry, and so on). If you want to log the syslog connections, make sure they are filtered out from syslog sending as explained in Error! Reference source not found.. Make sure the filter accounts for error conditions, for example, the ICMP “Destination unreachable” messages that are generated if the syslog destination server goes down.

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
StoneGate Management Center	5.3	Windows or Linux

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

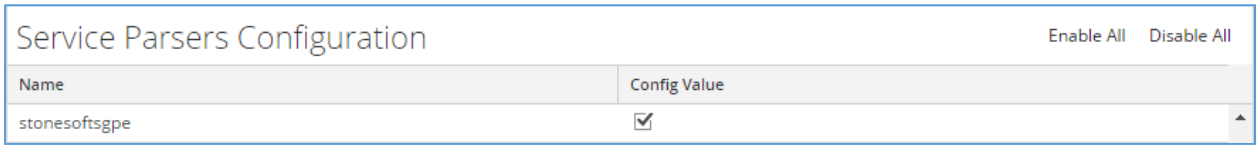
Appendix

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).