RSA Ready Implementation Guide for RSA Security Analytics

M86 Security
Secure Web Gateway 10.2

Daniel R. Pintal, RSA Partner Engineering
Last Modified: February 29, 2016

RSA READY

Solution Summary

M86 Secure Web Gateway (SWG) is a fast and accurate Web 2.0 protection system. It protects organizations from even the most complex malware while enabling productive access to Web 2.0 applications.

SWG can be deployed as a traditional appliance, virtual appliance, hybrid cloud or any combination of the three. Regardless of the type of implementation that you choose, its centralized policy control and single interface make SWG easy to implement and easy to manage.

By integrating M86 SWG with RSA Security Analytics, M86's SWG log activity can be used in an effective security log management solution for real-time alerting, correlated rules and events, and scheduled reporting.

RSA Security Analytics Features	
Secure Web Gateway 10.2	
Integration package name	m86swgpe.envision
Device display name within Security Analytics	m86swgpe
Event source class	Application 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
m86swgpe.envision	SA package deployed to parse events from device integrations.
m86swgpemsg.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
12/02/2013	Initial SA support for M86 Secure Web Gateway.
2/29/2016	RSA Security Analytics 10.5 Support.

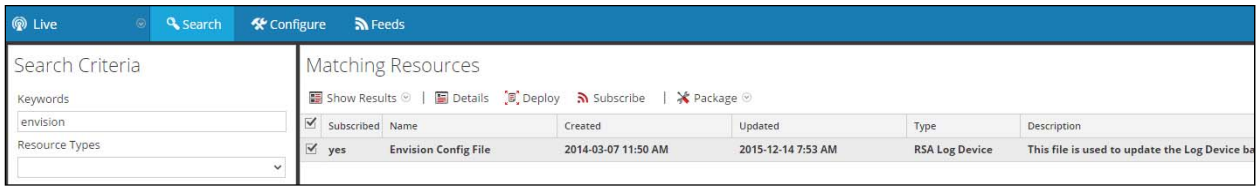
RSA Security Analytics Configuration

Deploy the enVision Config File

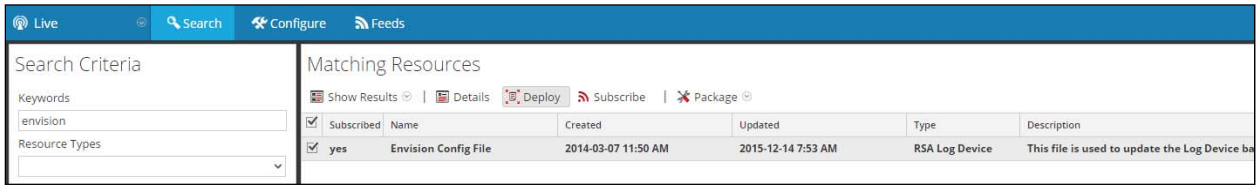
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

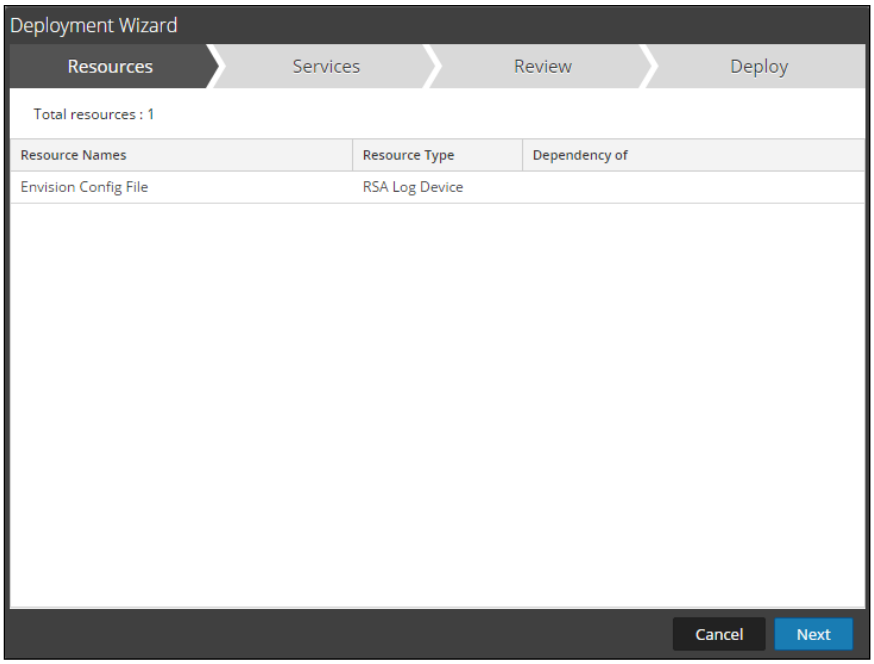
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**. Security Analytics will display the **Envision Config File** in Matching Resources.
3. Select the checkbox next to **Envision Config File**.



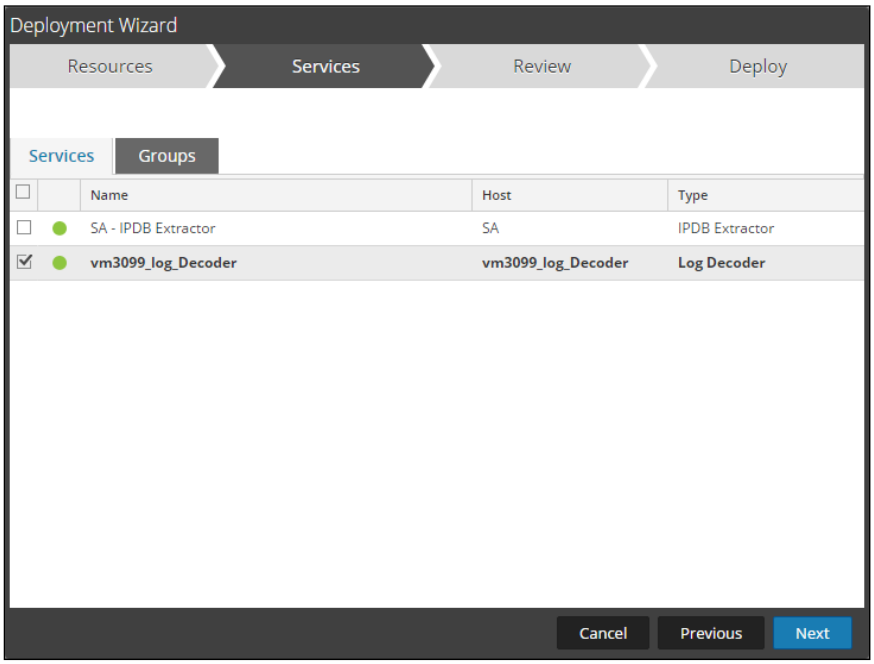
4. Click **Deploy** in the menu bar.



5. Select **Next**.

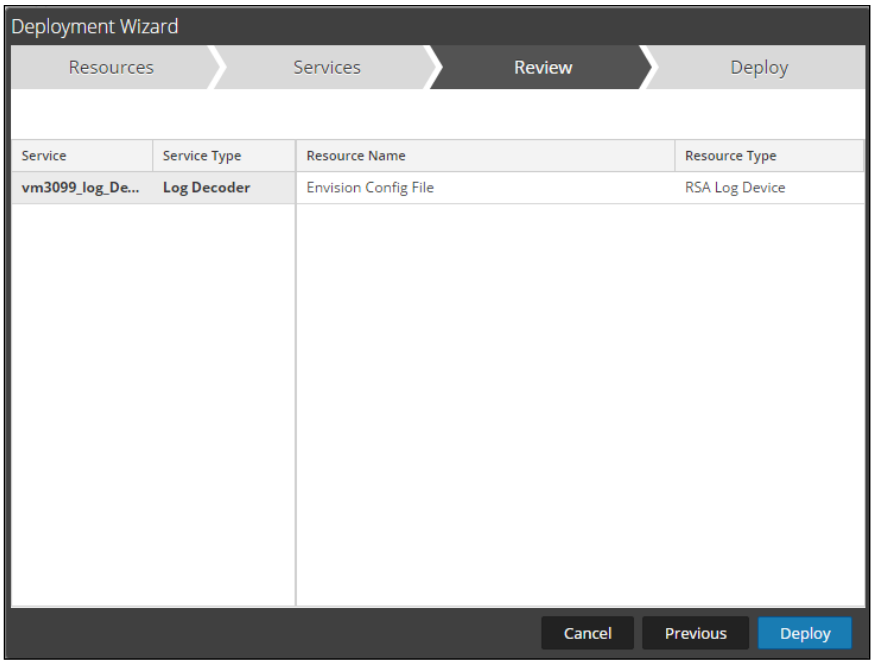


6. Select the **Log Decoder** and select **Next**.

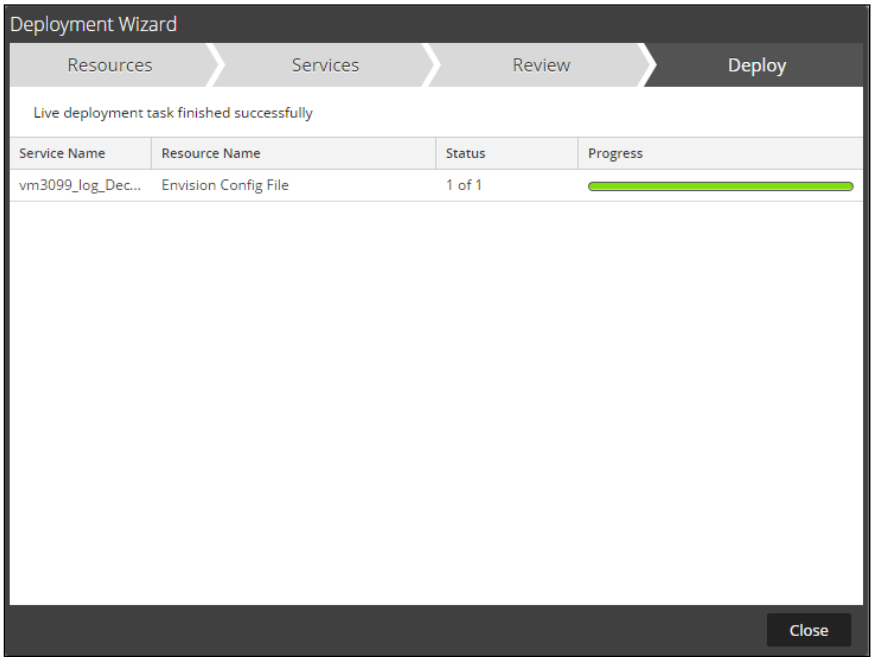


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

7. Select **Deploy**.



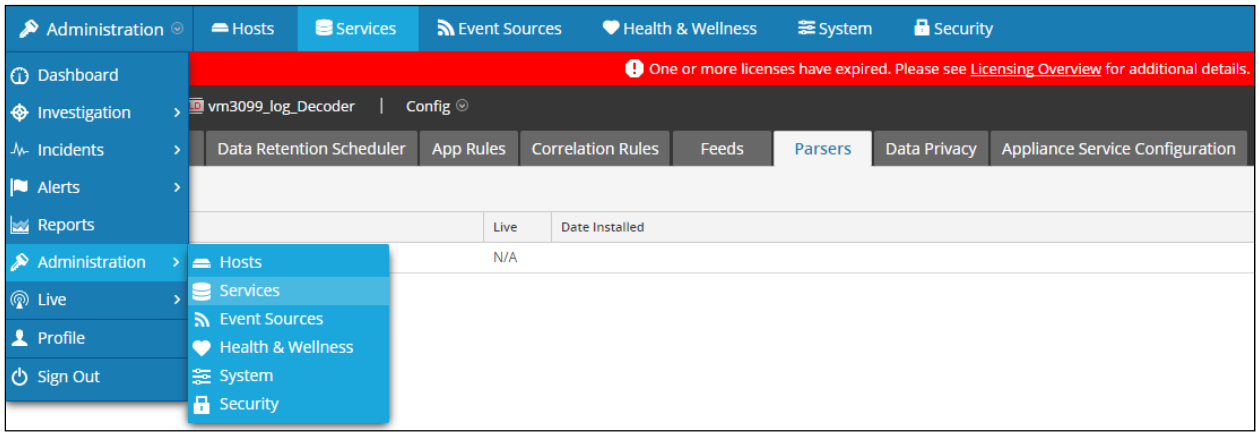
8. Select **Close**, to complete the deployment of the Envision Config file.



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.**



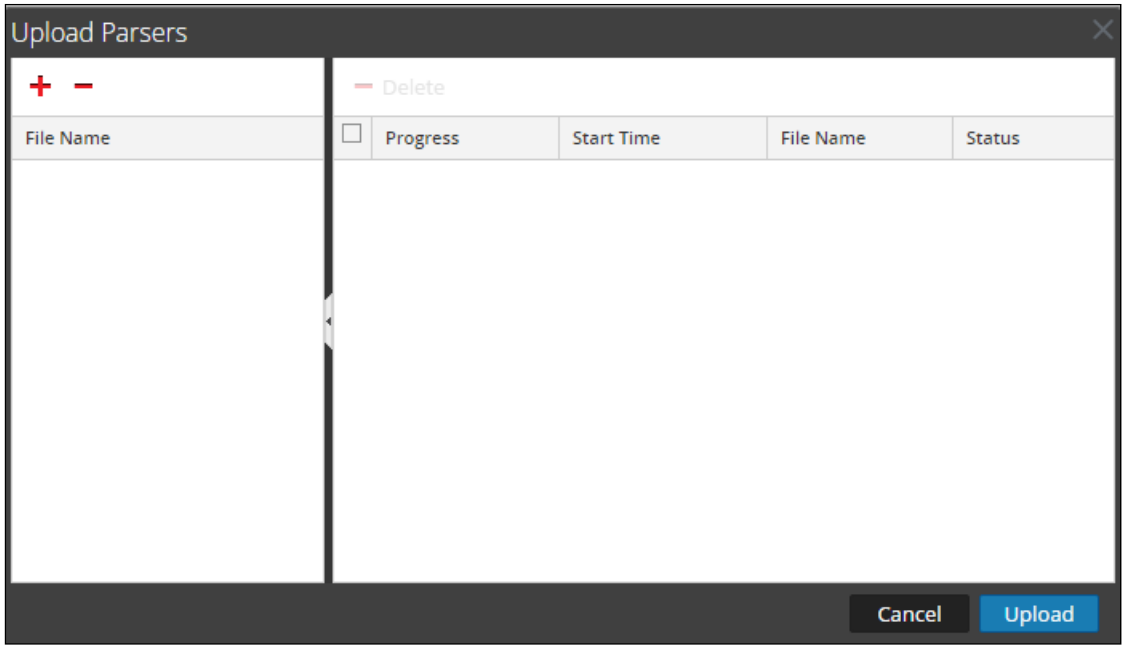
2. Select your Log Decoder from the list, select **View > Config**.

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

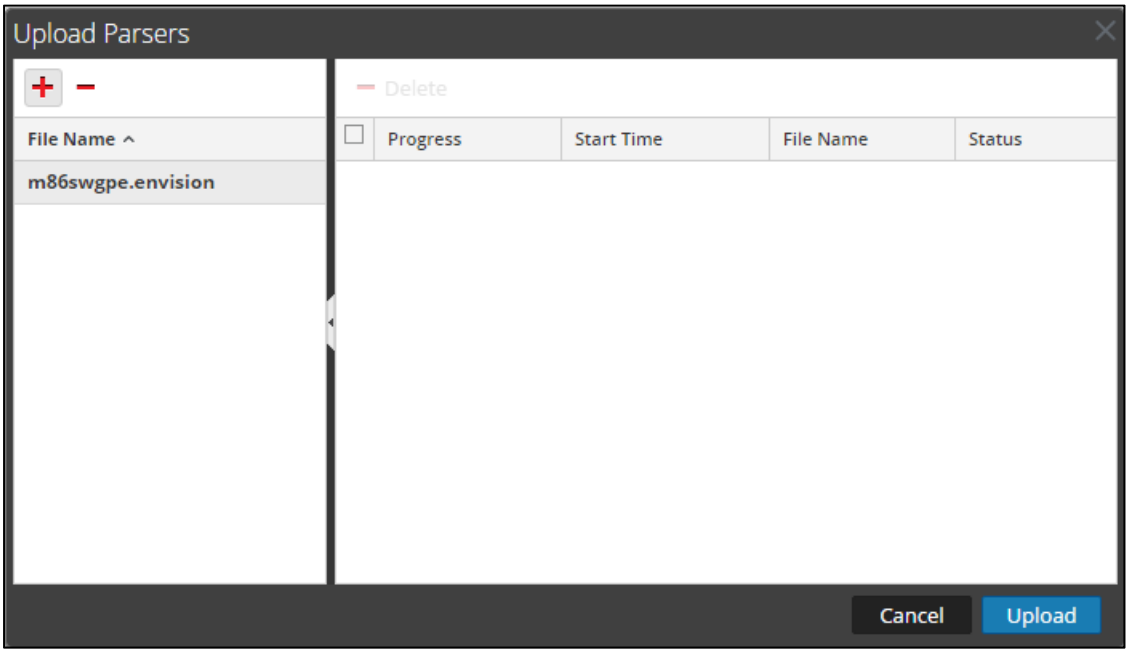
3. Next, select the **Parsers** tab and click the **Upload** button.

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

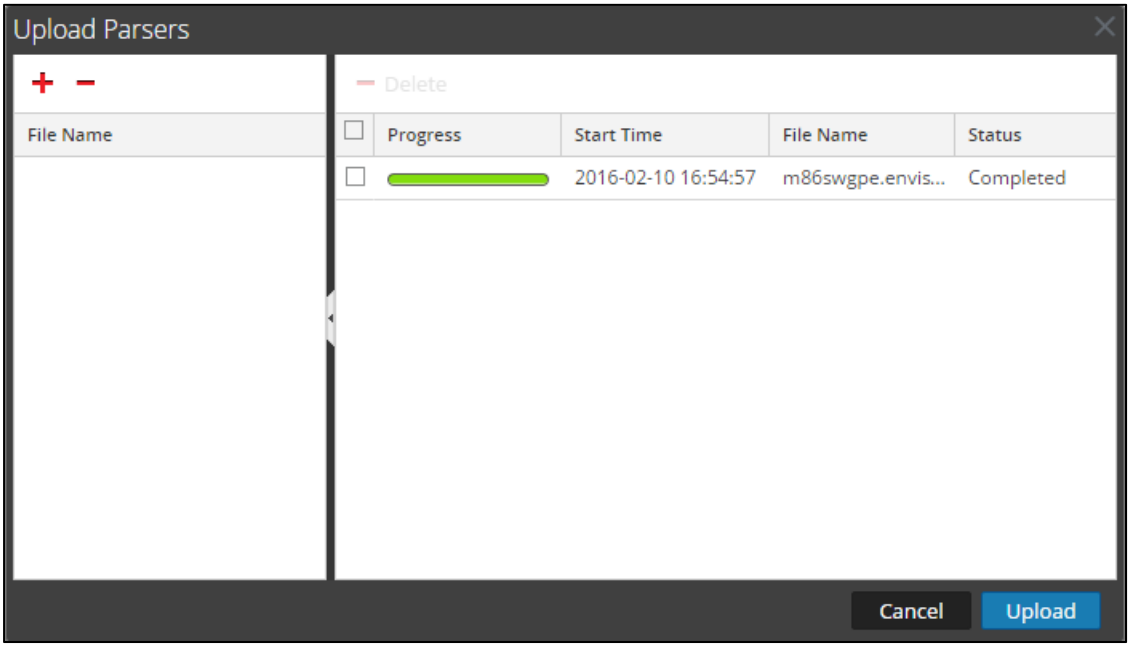
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Ready Community.**



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>.

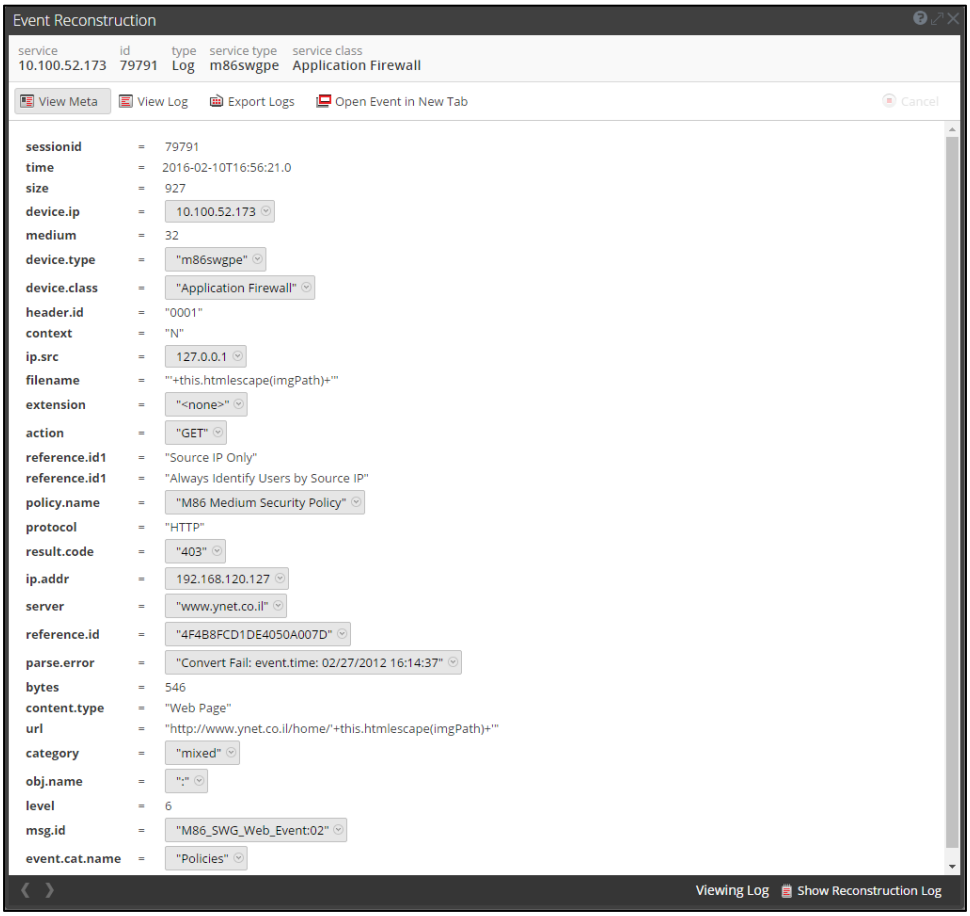
```
<mappings>

        <mapping envisionName="result" nwName="result" flags="None" envisionDisplayName="Result|Volume|Information|Reason|Succeed/Failed"/>
        <mapping envisionName="rulename" nwName="rule.name" flags="None" envisionDisplayName="Rule|RuleName"/>
        <mapping envisionName="web_referer" nwName="referer" flags="None"/>
        <mapping envisionName="info" nwName="index" flags="None"/>
        <mapping envisionName="ddomain" nwName="ddomain" flags="None"/>
        <mapping envisionName="event_counter" nwName="event.counter" flags="None" format="Int32"/>
        <mapping envisionName="rule" nwName="rule" flags="None" envisionDisplayName="Rule"/>
        <mapping envisionName="content_type" nwName="content.type" flags="None" envisionDisplayName="Content"/>
        <mapping envisionName="protocol_detail" nwName="protocol.detail" flags="None"/>
        <mapping envisionName="protocol" nwName="protocol" flags="None" envisionDisplayName="Protocol"/>
        <mapping envisionName="application" nwName="server" flags="None"/>
        <mapping envisionName="id1" nwName="reference.id1" flags="None"/>
        <mapping envisionName="id2" nwName="reference.id1" flags="None"/>
        <mapping envisionName="trigger_val" nwName="trigger.val" flags="None"/>
        <mapping envisionName="url" nwName="url" flags="None" envisionDisplayName="URL"/>
        <mapping envisionName="context" nwName="context" 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 the M86 Security Secure Web Gateway (SWG) 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 M86 Security 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 M86 Security Secure Web Gateway is properly configured and secured before deploying to a production environment. For more information, please refer to the M86 Security Secure Web Gateway documentation or website.**

M86 Security Secure Web Gateway Configuration

Overview

Within the M86 administrator's console, the Log Server can send the following types of log information to designated syslog server facilities such as RSA Security Analytics:

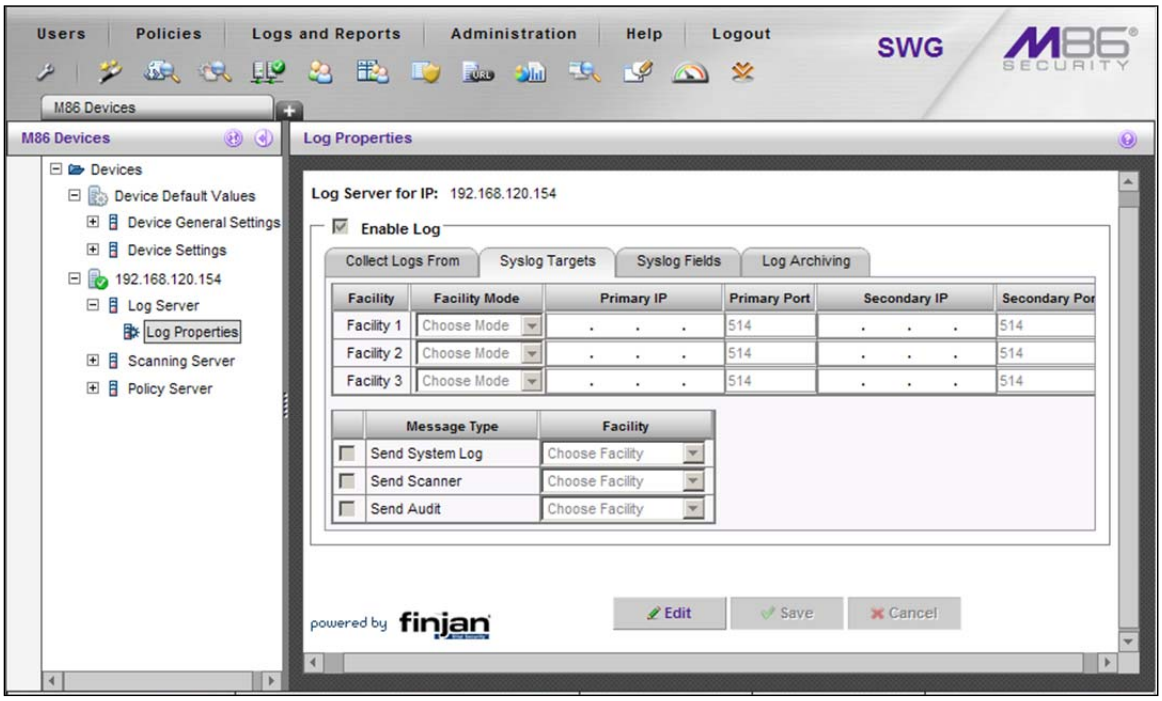
- System Log Messages
- Scanning Server (Web) Messages
- Audit messages (of all changes made or actions taken from the Management Console)

To implement this functionality, the Log Server must be configured with several parameters, including the syslog file locations which are described in the following sections.

Configuring Syslog

1. Using a web browser, login to the **Secure Web Gateway Management Console**.
2. Select **Administration** > **System Settings** > **M86 Devices**.
3. In the Device tree, under the policy server device, select **Log Server** > **Log Properties**.
4. In the Log Server Properties screen, click **Edit**.

5. In the **Syslog Target** tab, for each message type (System Log, Scanner, and/or Audit) that will be sent to RSA Security Analytics, define a facility as follows:

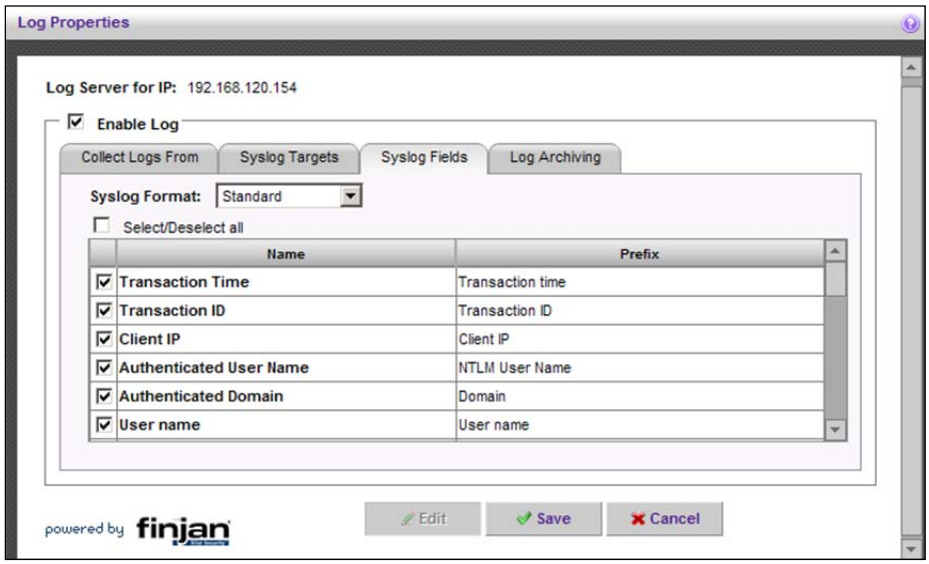


For each syslog target, edit the Facility line (beginning with Facility1) in the top set of entry fields as follows:

a. In the **Facility Mode** field, select a mode label — use this label to differentiate M86 logs from each other and from other platforms' logs on the remote syslog server.
b. In the **Primary IP** field, specify the IP address for the RSA Security Analytics Log Decoder server.
c. In the **Primary Port** field, specify the Primary port for the RSA Security Analytics Log Decoder server (default port is **514**).
d. Optionally, in the **Secondary IP** and **Secondary Port** fields, specify (respectively) a secondary syslog Server target address and the secondary port to which the logs will be sent.

6. In the bottom set of entry fields, for each message type being sent to RSA Security Analytics, click the checkbox and select the facility for which it is defined.

7. If Scanning Server messages are to be sent to RSA Security Analytics, define the configuration options for those messages in the **Syslog Fields** tab as follows:



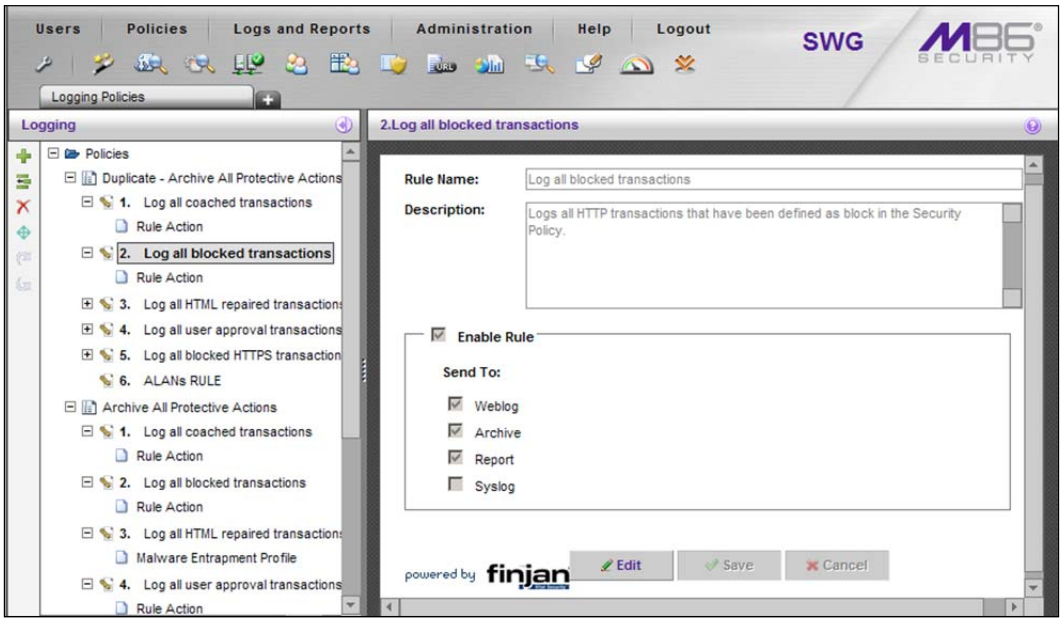
   a. In the **Syslog Format** field, select **Standard**. RSA Security Analytics only supports **Standard** format.
   b. Select the transaction fields that should be logged. See note below.

> **Important: You must either select ALL fields or leave the default fields checked. Do not make any other changes or Security Analytics will not be able to parse the logs correctly. For reference, the following are the default fields: Transaction Time, Transaction ID, Client IP, Authenticated User Name, Authenticated Domain, User Name, URL, Action, Block Reason, and X-Ray Mode.**

8. Click **Save**.
9. Set the appropriate settings in those Logging Policy rules whose logging information should be sent to RSA Security Analytics, otherwise the information will not be sent. For instructions, see the next section titled, **Setting Logging Policy Rules to Send Logging Information to Syslog**.
10. Click  to commit the change.

Setting Logging Policy Rules to Send Logging Information to Syslog

Important: Pre-supplied M86 Logging Policy rules cannot be edited. To change the settings of a Logging Policy's rules, duplicate the policy, and then edit the duplicate policy's rules or alternatively, create a new policy.



For each Logging Policy rule whose logging information should be sent to RSA Security Analytics, perform the following:

1. Select **Policies → Logging**.
2. In the Logging Policies tree, expand the Logging Policy to display its rules.
3. For each rule whose logging information should be sent to syslog:
   a. Select the rule.
   b. In the Rule definition screen, click **Edit**.
   c. Ensure that the **Enable Rule** checkbox is checked.
   d. In the **Send To** section, check the **Syslog** checkbox. Other checkboxes can remain as is.
   e. Click **Save**.

When the rule settings are complete, click  to commit the changes.

Certification Checklist for RSA Security Analytics

Date Tested: February 29, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
M86 Secure Web Gateway	10.2	Linux Appliance

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).