

RSA Ready Implementation Guide for
RSA | Security Analytics

Lieberman Software
Enterprise Random Password Manager
(ERPM) 4.83.6

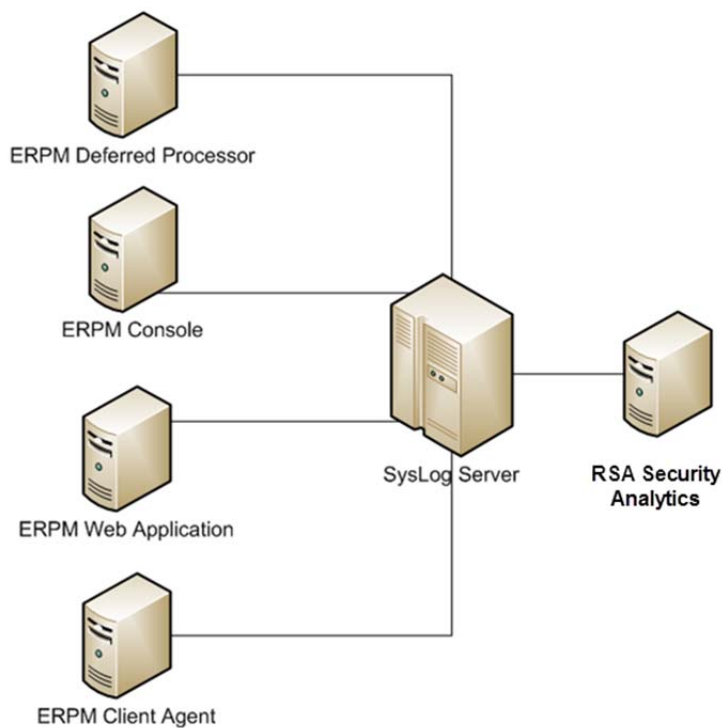
Daniel R. Pintal, RSA Partner Engineering
Last Modified: February 29, 2016

RSA
READY

Solution Summary

Each component of Enterprise Random Password Manager (ERPM) can be individually configured to report its events to RSA Security Analytics. Configuration for each event are sent as SysLog messages and configured through the ERPM console application. If desired, events can also be sent to multiple event log servers for redundancy.

| RSA Security Analytics Features | |
|---|-------------------------|
| Enterprise Random Password Manager 4.83.6 | |
| Integration package name | liebsofterpmpe.envision |
| Device display name within Security Analytics | liebsofterpmpe |
| Event source class | Applicatin Servers |
| 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 |
|--------------------------------|---|
| liebsofterpmpe envision | SA package deployed to parse events from device integrations. |
| liebsofterpmpemsg.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 ERPM. |
| 2/29/2016 | RSA Security Analytics 10.5 Support. |
| | |

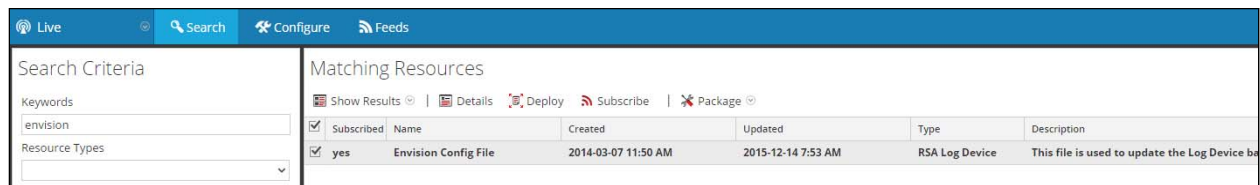
RSA Security Analytics Configuration

Deploy the *enVision Config File*

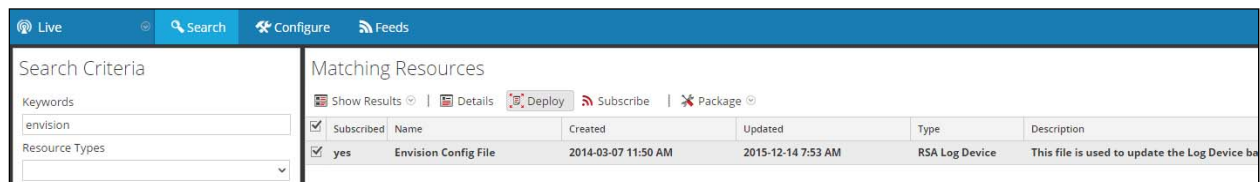
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

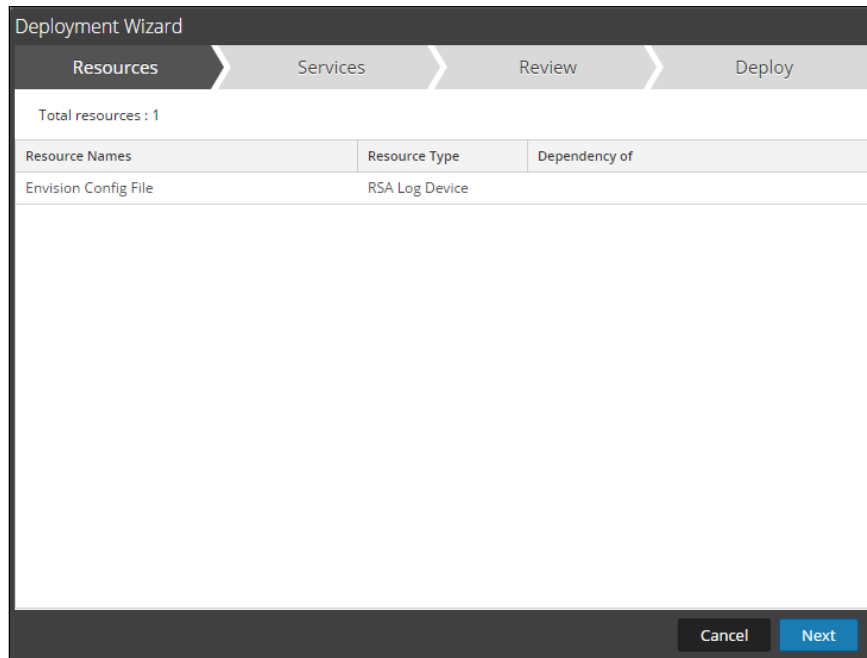
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**. Security Analytics will display the **Envision Config File** in Matching Resources.
3. Select the checkbox next to **Envision Config File**.



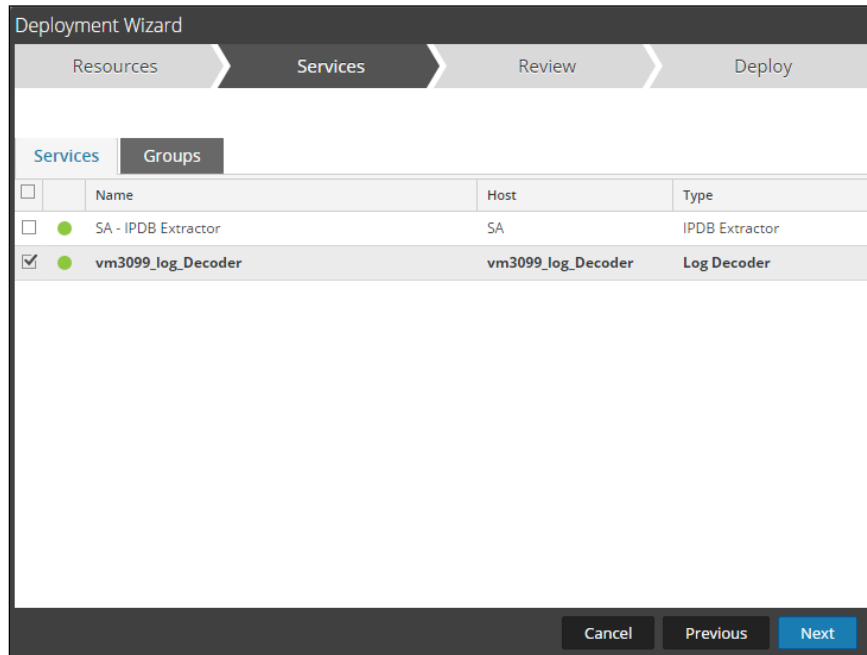
4. Click **Deploy** in the menu bar.



5. Select **Next**.

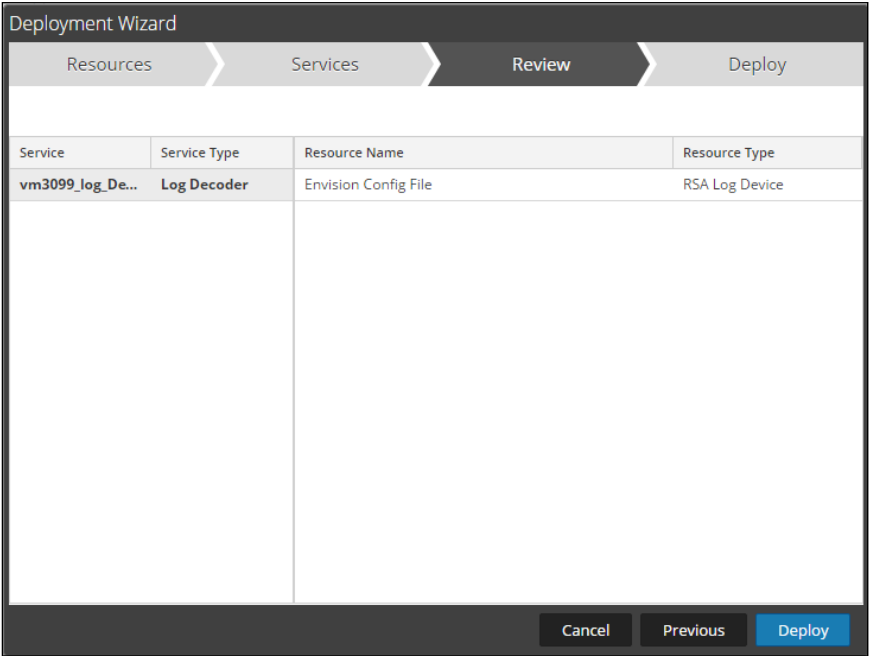


6. Select the **Log Decoder** and select **Next**.

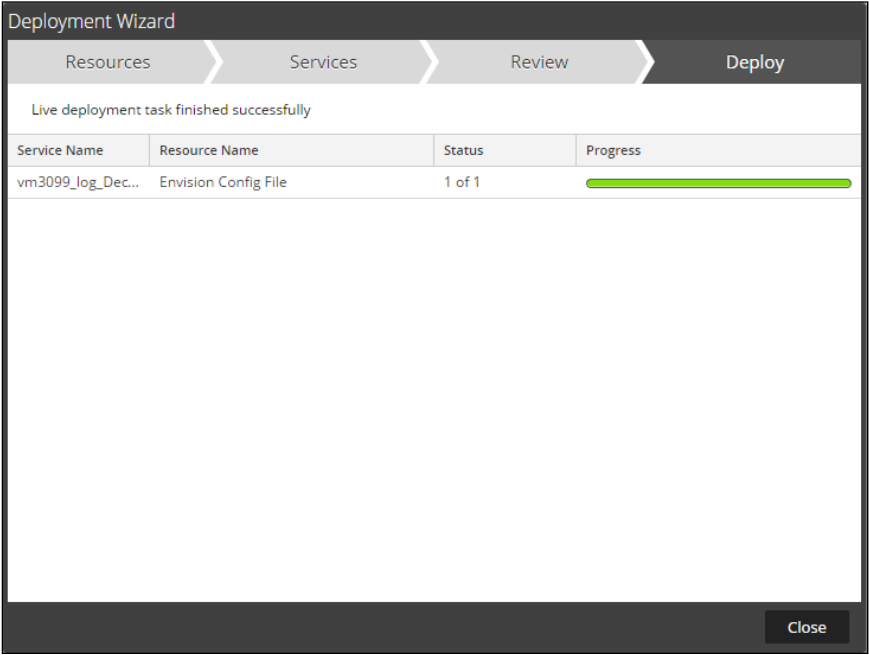


! > Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

7. Select **Deploy**.



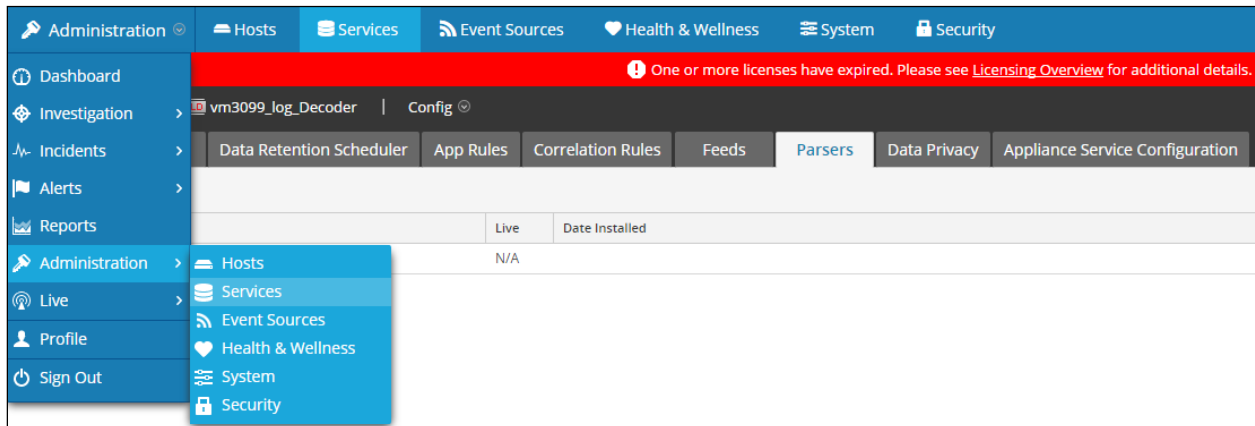
8. Select **Close**, to complete the deployment of the Envision Config file.



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**.

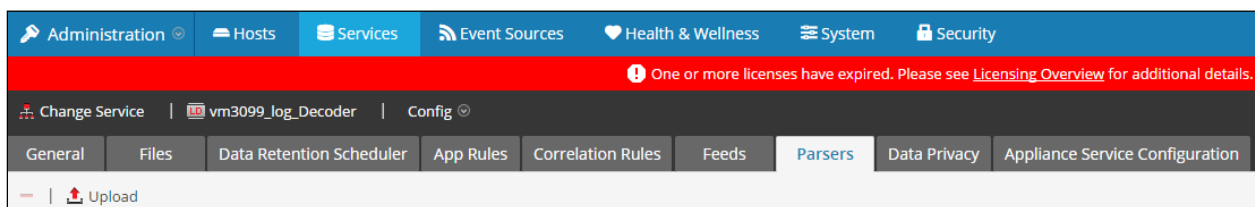


2. Select your Log Decoder from the list, select **View > Config**.



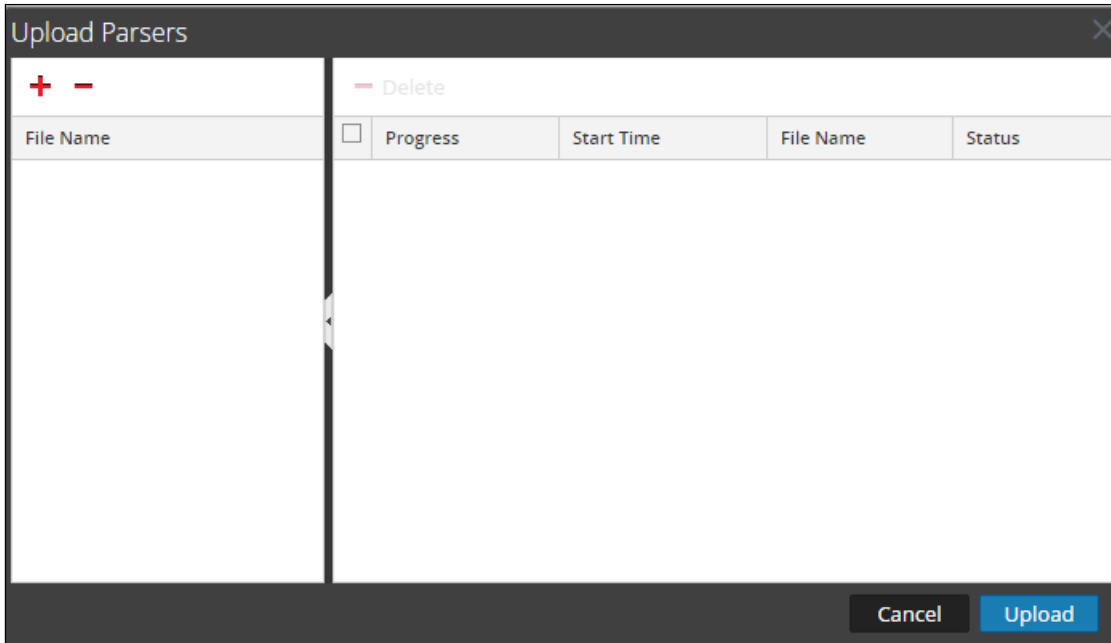
! > Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.

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

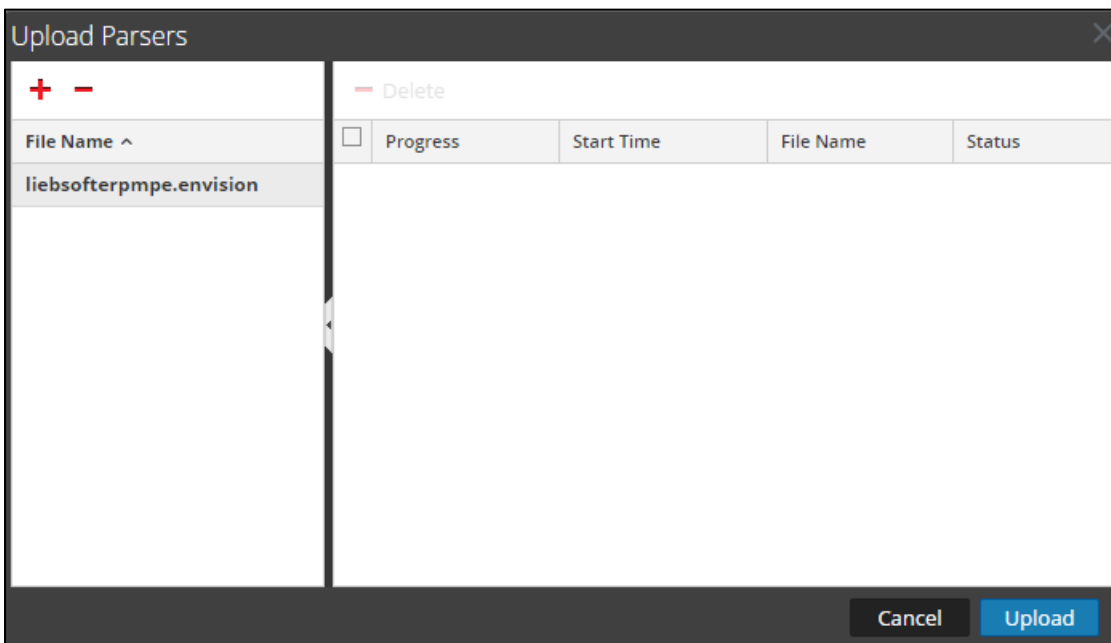


4. From the *Upload Parsers* window, click the **+** **Add** button and select the *.envision* file.

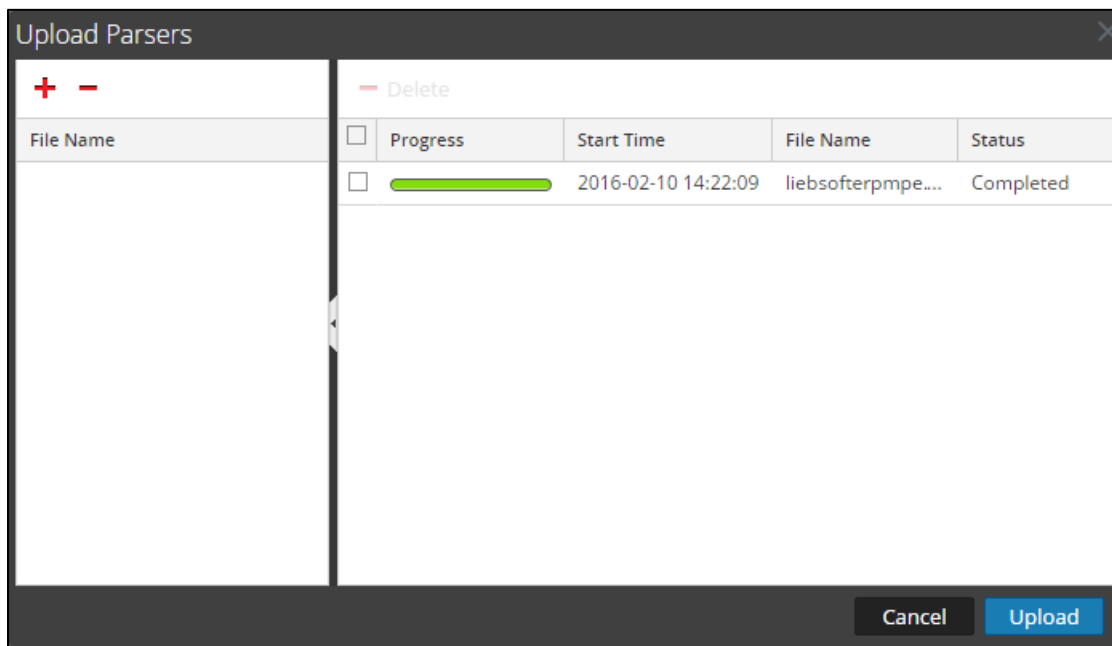
!> Important: The .envision file is contained within the .zip file downloaded from the RSA Ready Community.



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



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



- 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="application" nwName="server" flags="None" />
    < mapping envisionName="event_time_string" nwName="event.time.str" flags="None" envisionDisplayName="EventTimeString" />
    < mapping envisionName="domain" nwName="domain" flags="None" envisionDisplayName="DomainName" />
    < mapping envisionName="user_agent" nwName="user.agent" flags="None" />
    < mapping envisionName="info" nwName="index" flags="None" />
</ mappings >
    
```

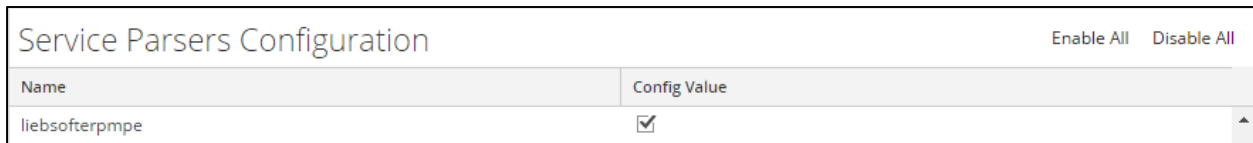
- Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart**.



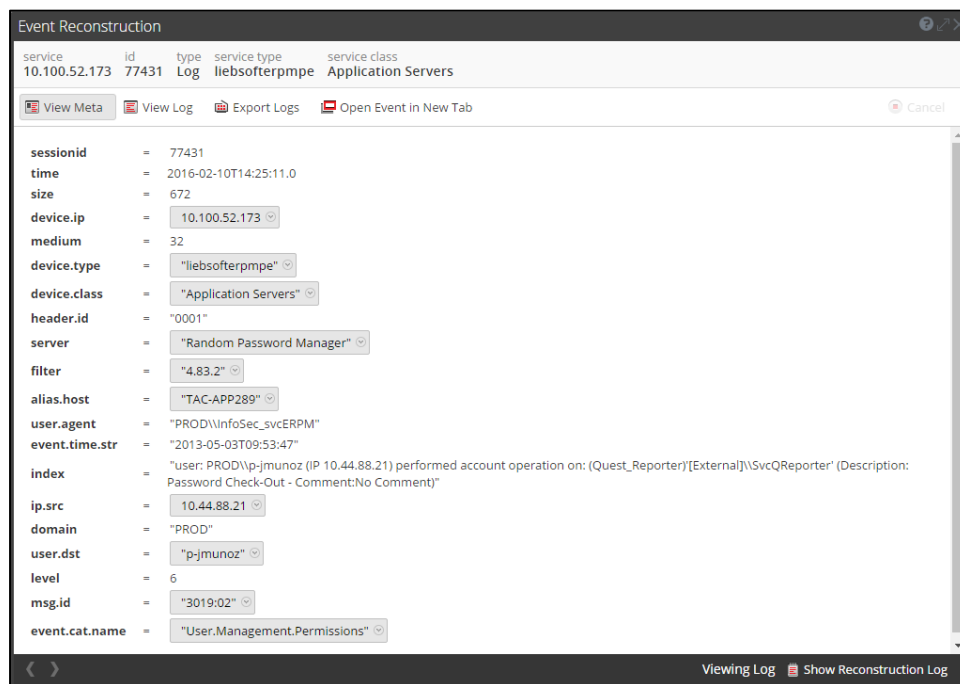
9. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View > Config**.



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 Lieberman Enterprise Random Password Manager 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.

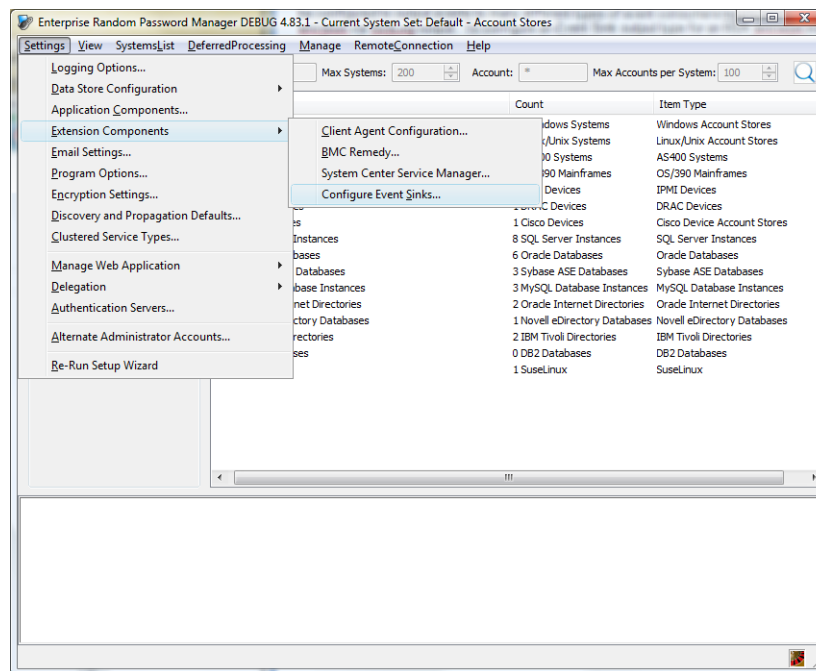
All Lieberman components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Enterprise Random Password Manager Configuration

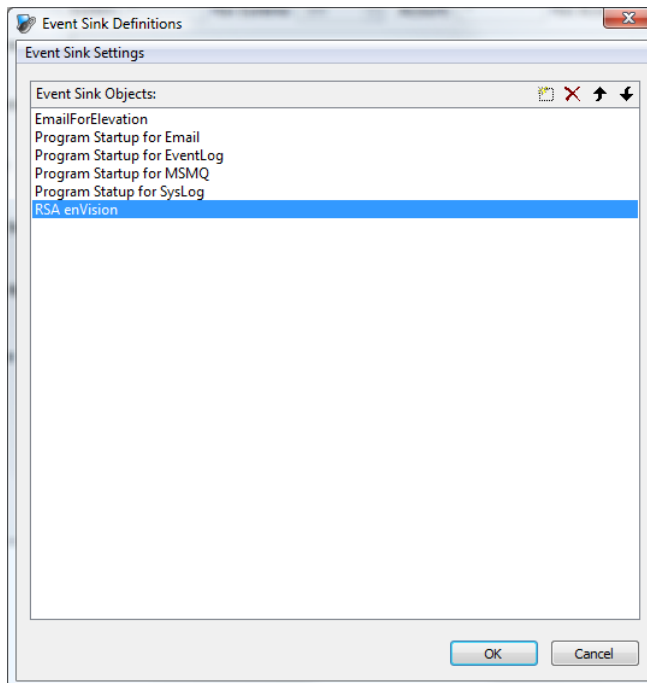
In addition to maintaining its own internal log of operations, Enterprise Random Password Manager can be configured to output events to many different types of event consumers/aggregators including RSA Security Analytics via SysLog output.

To configure an Event Sink Output Type for an RSA Security Analytics instance perform the following actions.

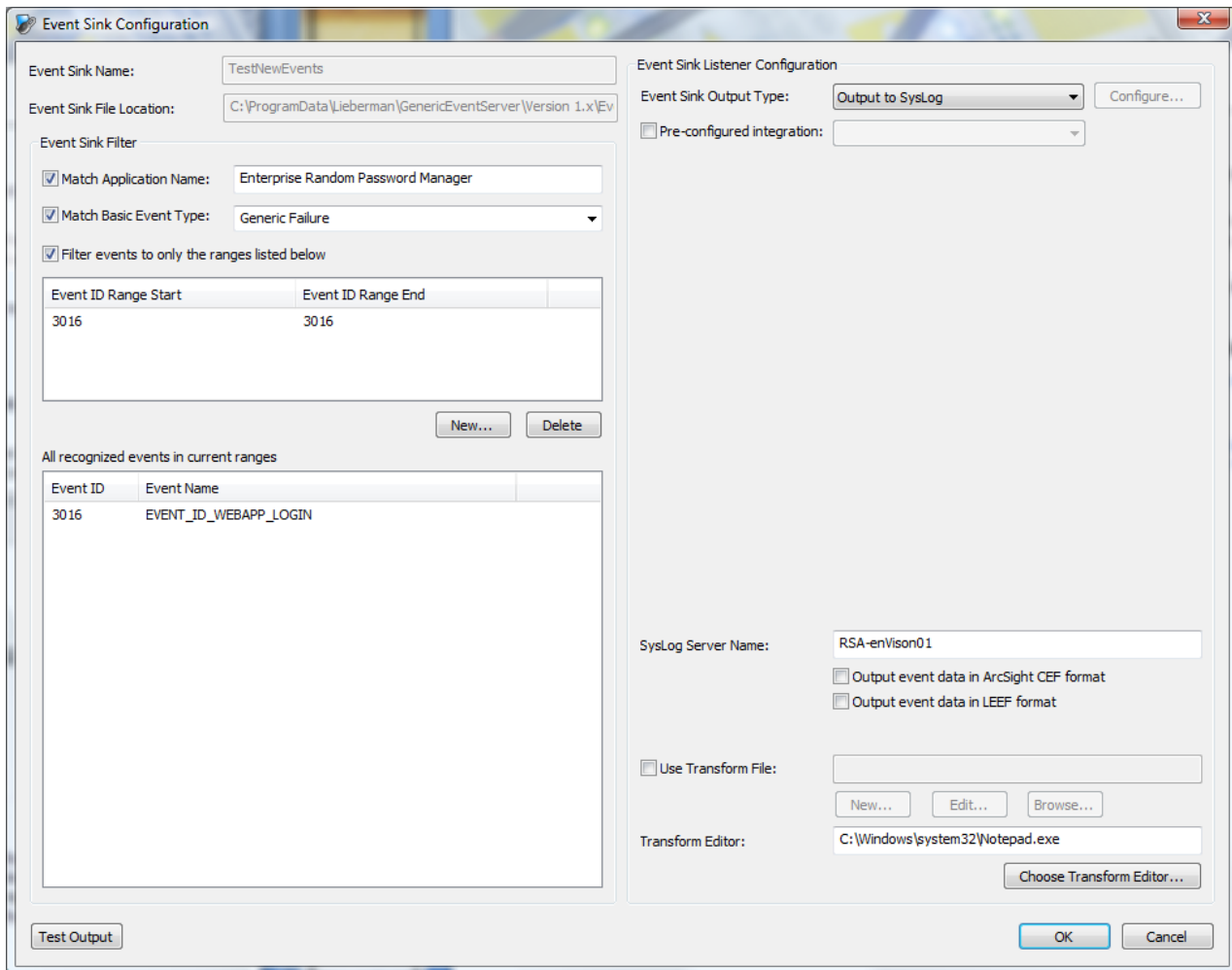
1. Open the Event Sink Configuration dialog box within the ERPM console.
2. Create a new Event Sink entry for RSA Security Analytics by selecting **Settings → Extension Components → Configure Event Sinks...**



3. From the Event Sink Definitions dialog box select **RSA enVision** (if there is a *RSA Security Analytics* option from the menu, select that) then select **OK**.



- Using the Event Sink Configuration dialog box, specify the range(s) of events you want to send to RSA Security Analytics via SysLog by selecting **New...** and entering the **Event ID Range Start** and **Event ID Range End** values.
- Select **Output to SysLog** from the **Event Sink Output Type** drop-down menu.
- Specify the name of the RSA Security Analytics device in the **SysLog Server Name** field. You can specify the name of the machine as a simple hostname, IP Address, or FQDN as long as DNS resolves the system correctly from each location where an event message generating component is located.
- Select **OK**.



The Event Sink Configuration dialog box is shown with the following settings:

- Event Sink Name: TestNewEvents
- Event Sink File Location: C:\ProgramData\Lieberman\GenericEventServer\Version 1.x\Ev
- Event Sink Filter:
 - Match Application Name: Enterprise Random Password Manager
 - Match Basic Event Type: Generic Failure
 - Filter events to only the ranges listed below
- Event ID Range Start: 3016
- Event ID Range End: 3016
- All recognized events in current ranges:

| Event ID | Event Name |
|----------|-----------------------|
| 3016 | EVENT_ID_WEBAPP_LOGIN |
- Event Sink Listener Configuration:
 - Event Sink Output Type: Output to SysLog
 - Pre-configured integration: (empty)
 - SysLog Server Name: RSA-enVison01
 - Output event data in ArcSight CEF format
 - Output event data in LEEF format
 - Use Transform File: (empty)
 - Transform Editor: C:\Windows\system32\notepad.exe

Buttons: Test Output, New..., Delete, Configure..., Choose Transform Editor..., OK, Cancel.

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 |
| Lieberman ERPM | 4.83.6 | Microsoft Windows XP |

| 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

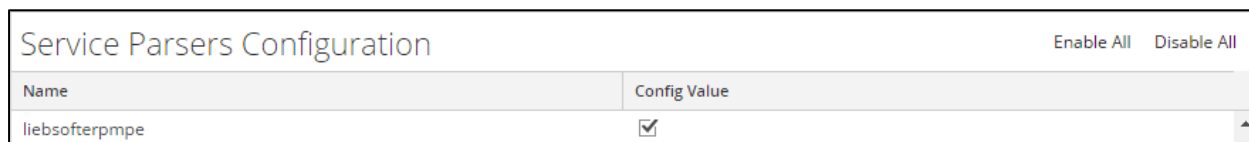
Security Analytics Disable Device Parser

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).