RSA Ready Implementation Guide for RSA Security Analytics

CounterTack Event Horizon 3.1.7

Daniel R. Pintal, RSA Partner Engineering

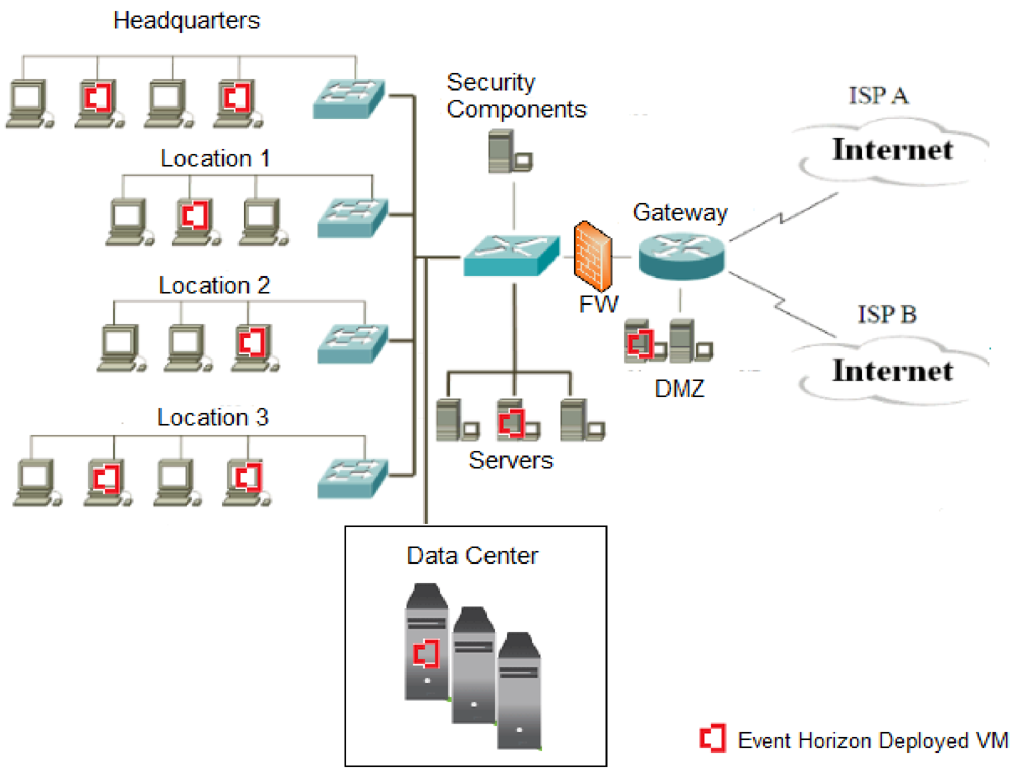
Last Modified: February 22, 2016

RSA READY

Solution Summary

The Event Horizon can be configured to send forensic information data to Syslog Event Correlation devices. By integrating with RSA Security Analytics, Event Horizon detected attack activity (file manipulation, process activity, inbound/outbound communication and registry manipulation) can be used as an effective security management solution for real-time alerting, correlation of events and scheduled reporting.

RSA Security Analytics Features	
Event Horizon 3.1.7	
Integration package name	countertackehpe.envision
Device display name within Security Analytics	countertackehpe
Event source class	Analysis
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
countertackehpe.envision	SA package deployed to parse events from device integrations.
countertackpemsg.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 support for CounterTack Event Horizon
2/22/2016	SA 10.5 support

RSA Security Analytics Configuration

Before You Begin

This section provides instructions for configuring CounterTack Event Horizon 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 CounterTack Event Horizon components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

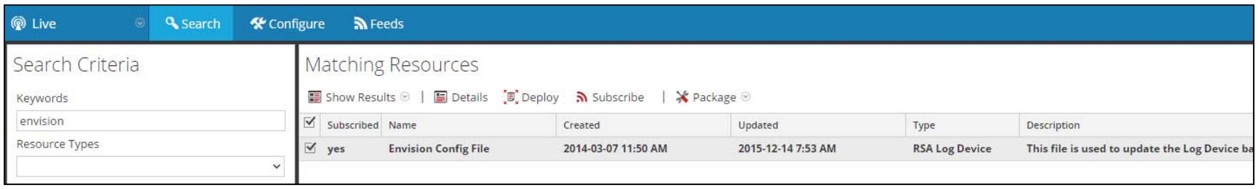
! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure CounterTack Event Horizon is properly configured and secured before deploying to a production environment. For more information, please refer to the CounterTack Event Horizon documentation or website.

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.

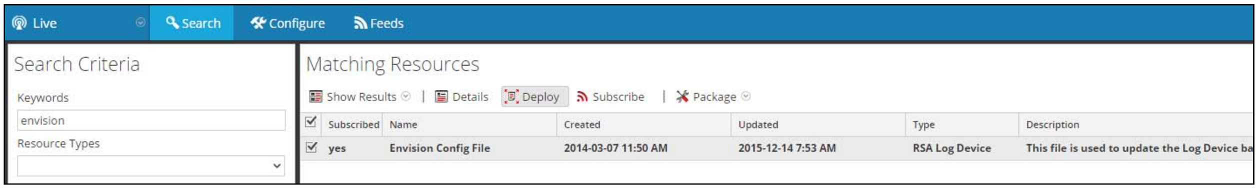
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



Keywords: envision

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

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

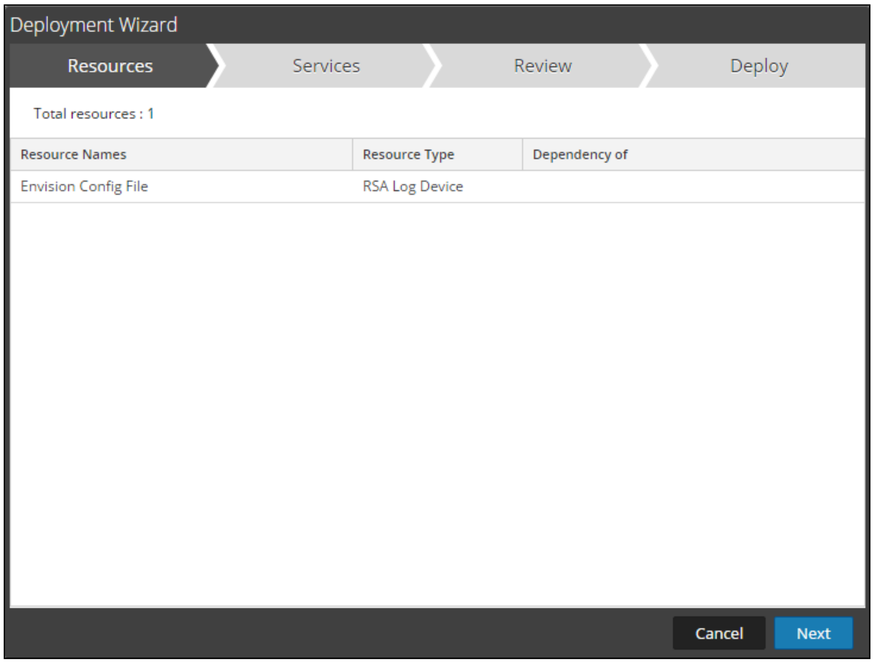


Keywords: envision

Resource Types:

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

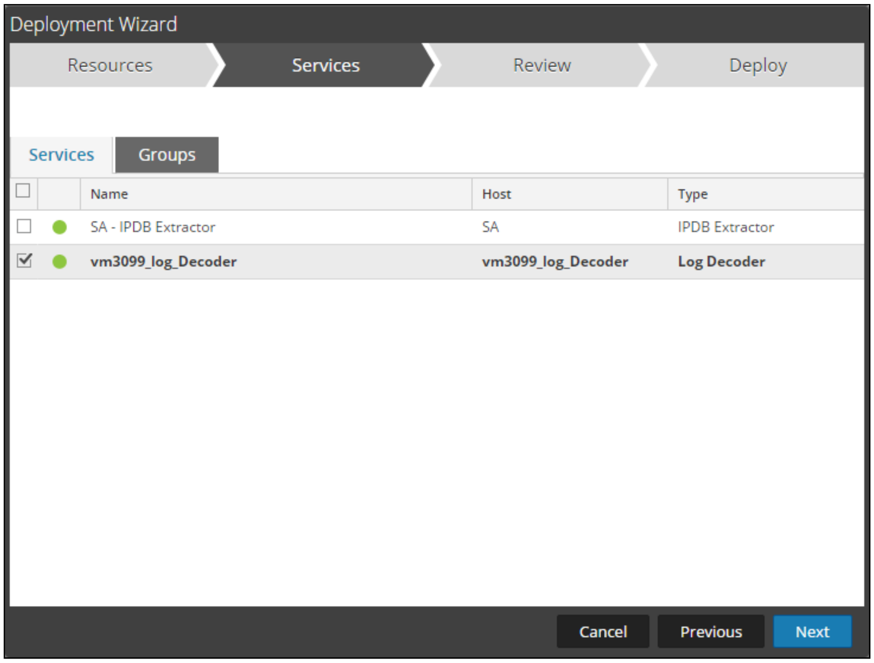
6. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency of
Envision Config File	RSA Log Device	

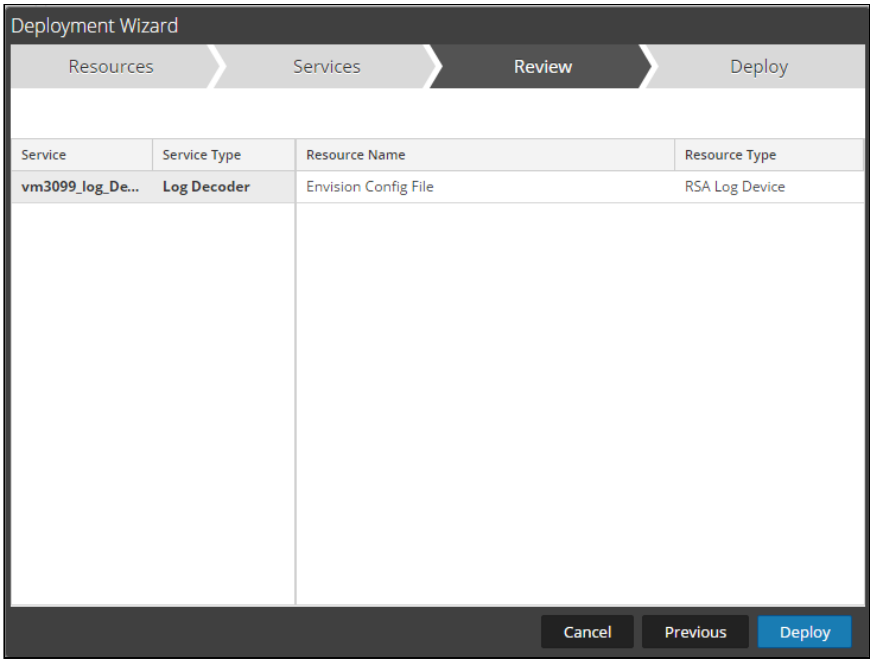
7. Select the **Log Decoder** and select **Next**.



□		Name	Host	Type
□	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	**vm3099_log_Decoder**	**vm3099_log_Decoder**	**Log Decoder**

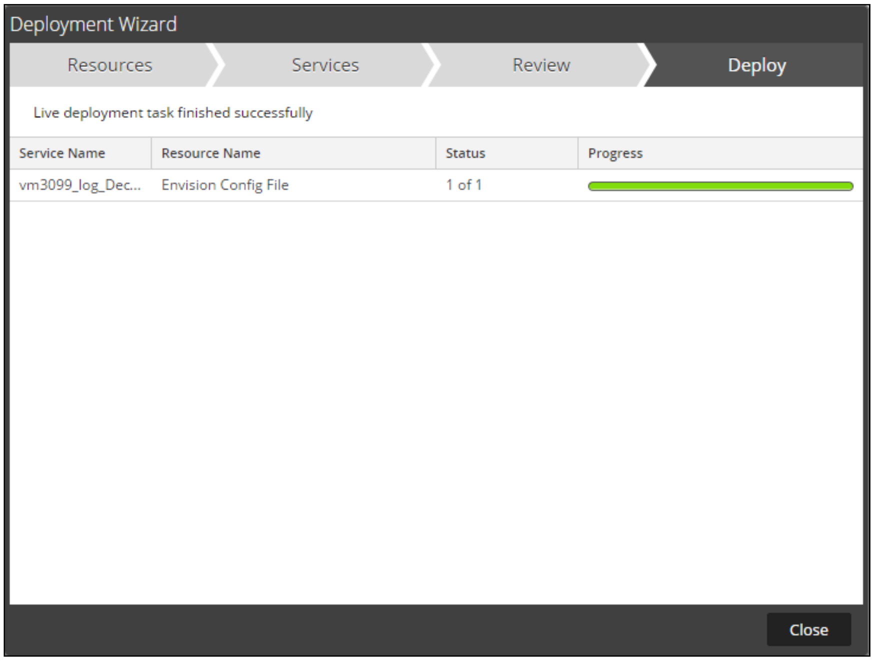
! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	**Log Decoder**	Envision Config File	RSA Log Device

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



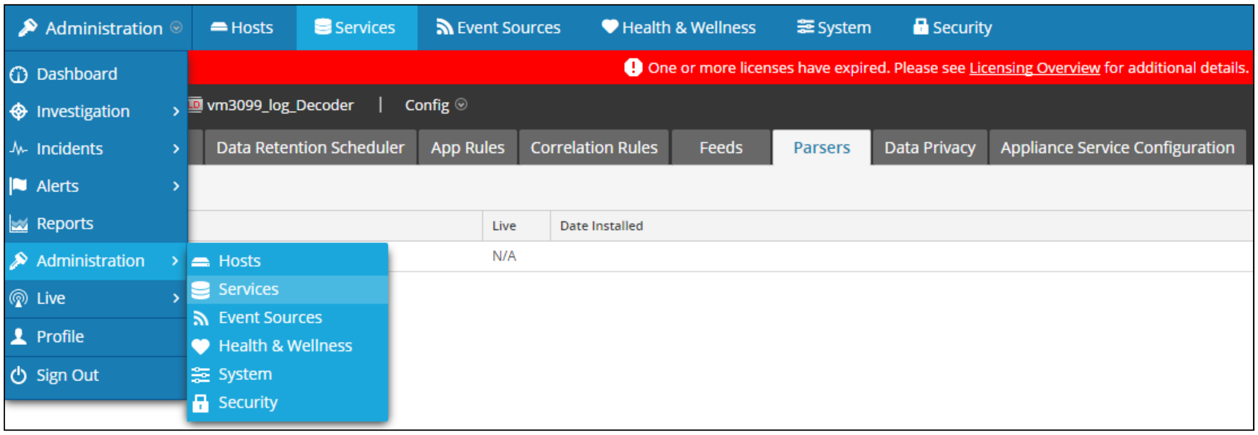
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3099_log_Dec...	Envision Config File	1 of 1	

Deploy the Security Analytics Integration Package

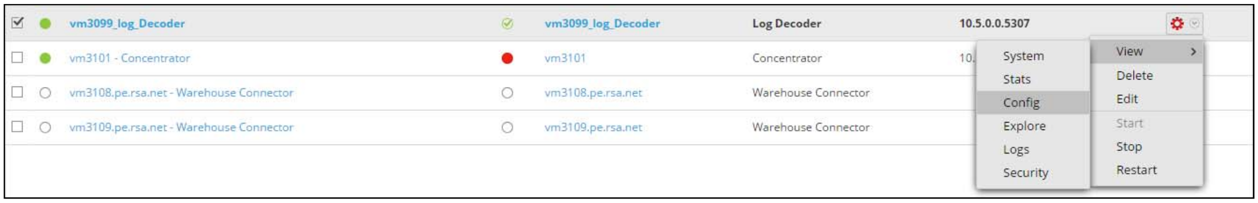
After completing the previous section, ***Deploy the enVision Config File***, you can now deploy the Security Analytics Integration Package. Download the appropriate RSA Partner Integration Package, then log into Security Analytics to perform the following actions:

1. From the Security Analytics menu, select **Administration** > **Services.**



One or more licenses have expired. Please see Licensing Overview for additional details.

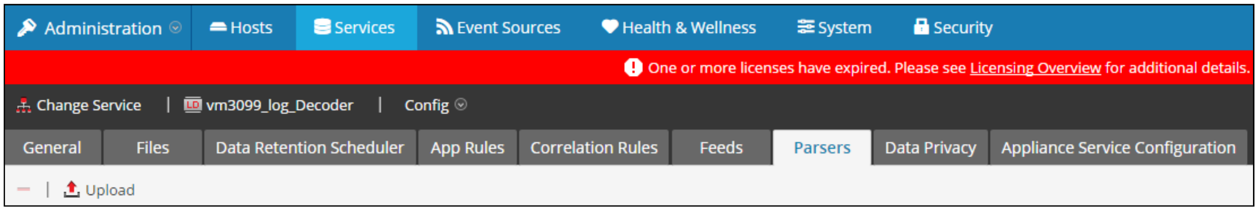
2. Select your Log Decoder from the list, select **View > Config**.



☑	●	vm3099_log_Decoder	✓	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307
□	●	vm3101 - Concentrator	●	vm3101	Concentrator	10.
□	○	vm3108.pe.rsa.net - Warehouse Connector	○	vm3108.pe.rsa.net	Warehouse Connector	
□	○	vm3109.pe.rsa.net - Warehouse Connector	○	vm3109.pe.rsa.net	Warehouse Connector	

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

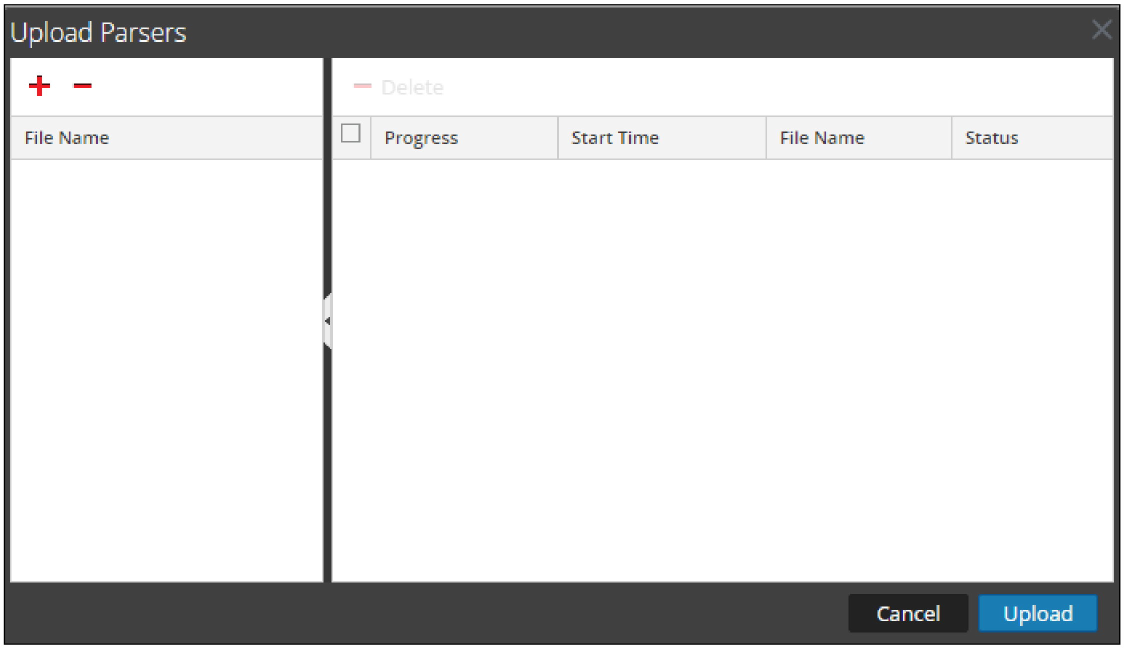
3. Next, select the **Parsers** tab and click the **Upload** button.



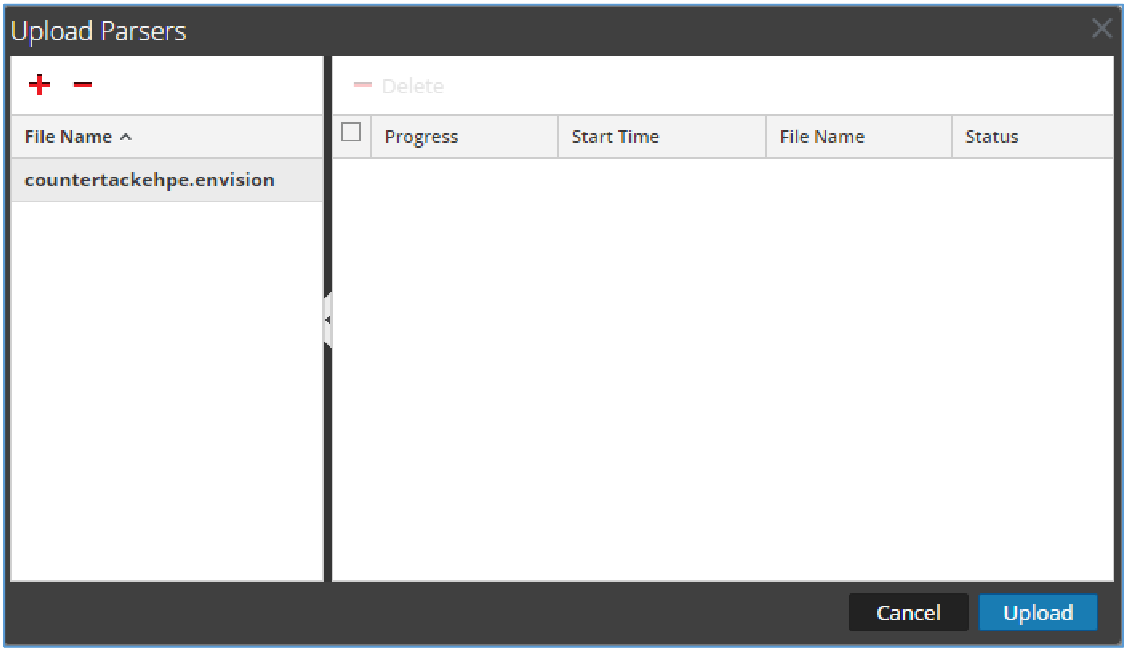
One or more licenses have expired. Please see Licensing Overview for additional details.

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.



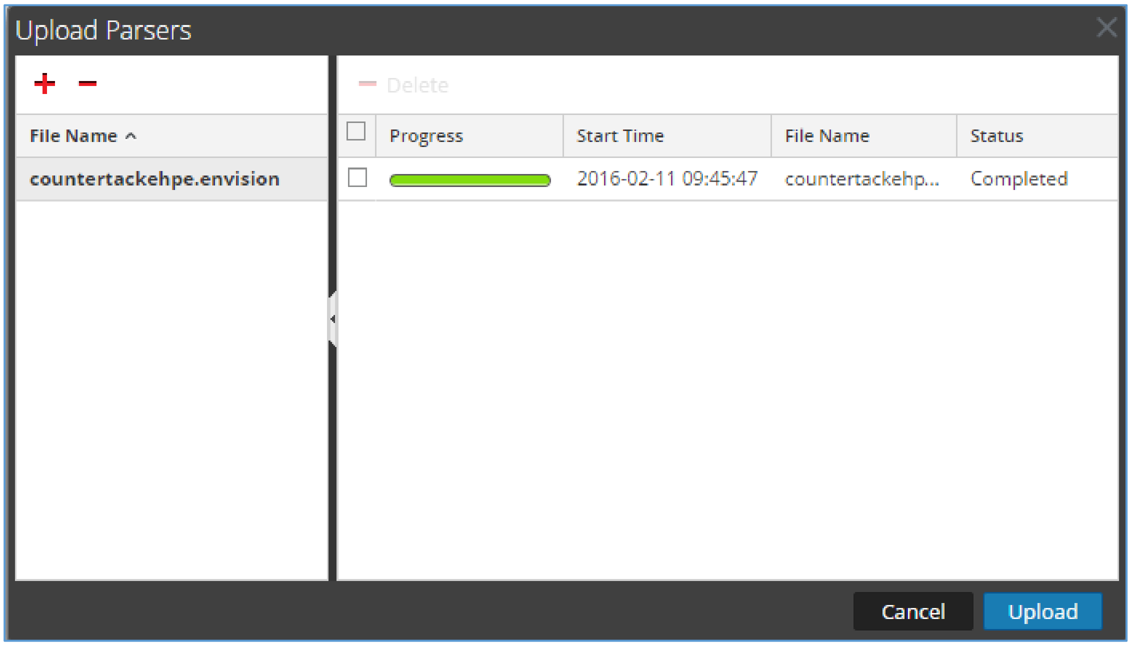
5. Under the file name column, select the integration package name and click **Upload**.



File Name ^
countertackehpe.envision

□	Progress	Start Time	File Name	Status

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



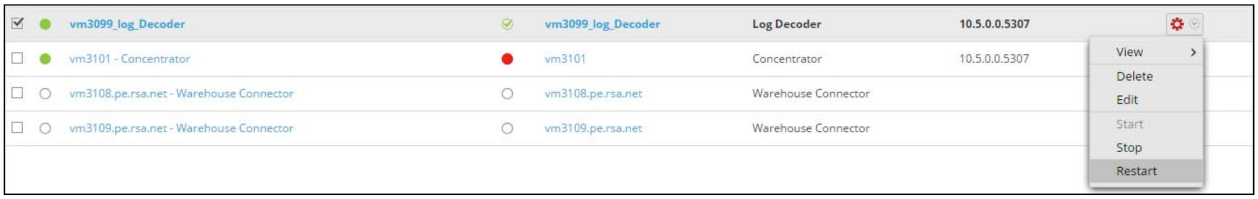
File Name ^
countertackehpe.envision

□	Progress	Start Time	File Name	Status
□	🟩	2016-02-11 09:45:47	countertackehp...	Completed

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>.

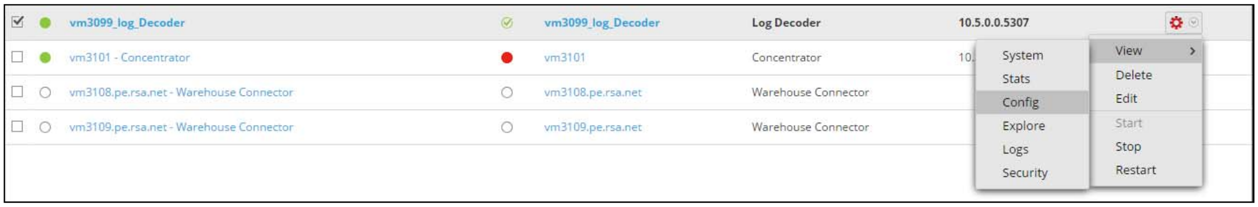
```
<mappings>

        <mapping envisionName="dinterface" nwName="dinterface" flags="Transient" envisionDisplayName="DestinationInterface"/>
        <mapping envisionName="sinterface" nwName="sinterface" flags="Transient" envisionDisplayName="SourceInterface"/>
        <mapping envisionName="info" nwName="index" flags="Transient"/>
        <mapping envisionName="inode" nwName="inode" flags="Transient" format="Int64"/>
        <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.**



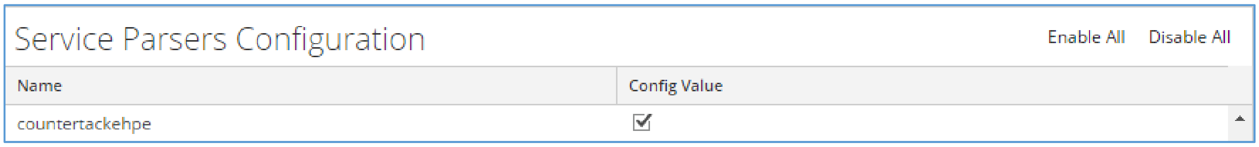
☑ ●	vm3099_log_Decoder	✓	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307
□ ●	vm3101 - Concentrator	●	vm3101	Concentrator	10.5.0.0.5307
□ ○	vm3108.pe.rsa.net - Warehouse Connector	○	vm3108.pe.rsa.net	Warehouse Connector	
□ ○	vm3109.pe.rsa.net - Warehouse Connector	○	vm3109.pe.rsa.net	Warehouse Connector	

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



☑ ●	vm3099_log_Decoder	✓	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307
□ ●	vm3101 - Concentrator	●	vm3101	Concentrator	10.
□ ○	vm3108.pe.rsa.net - Warehouse Connector	○	vm3108.pe.rsa.net	Warehouse Connector	
□ ○	vm3109.pe.rsa.net - Warehouse Connector	○	vm3109.pe.rsa.net	Warehouse Connector	

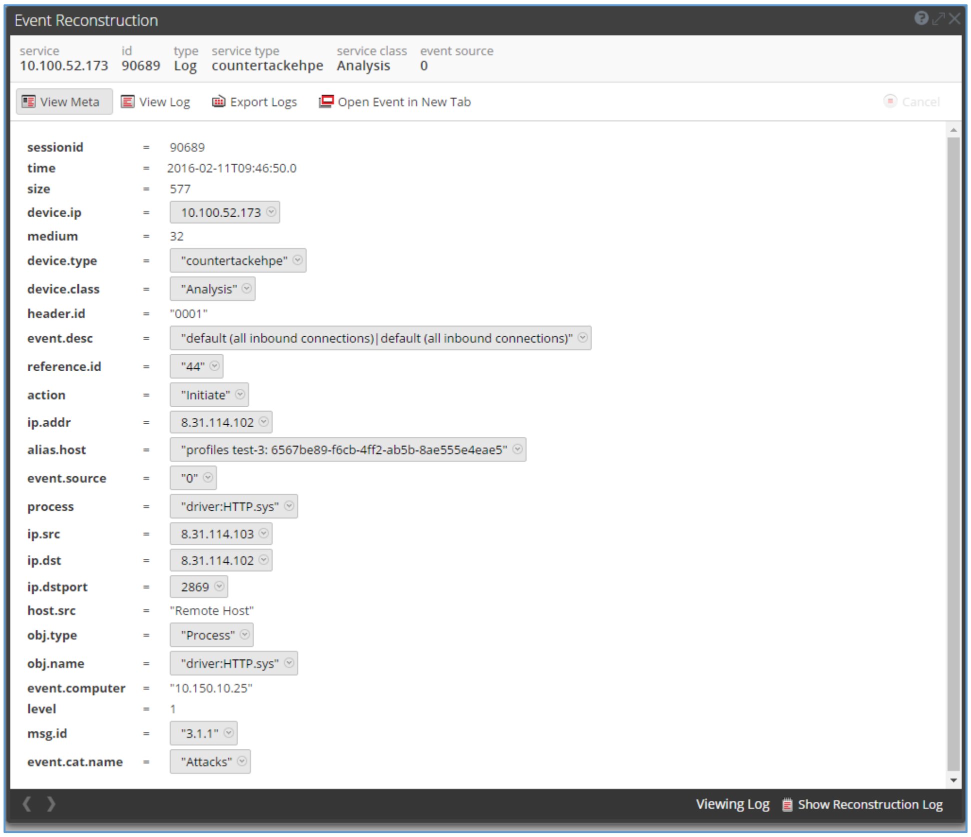
10. The new device is listed under the Log Decoder(s) General Tab within the Service Parsers Configuration.



Service Parsers Configuration

Name	Config Value
countertackehpe	☑

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.



service	id	type	service type	service class	event source
10.100.52.173	90689	Log	countertackehpe	Analysis	0

```
sessionid       =  90689
time            =  2016-02-11T09:46:50.0
size            =  577
device.ip       =  10.100.52.173
medium          =  32
device.type     =  "countertackehpe"
device.class    =  "Analysis"
header.id       =  "0001"
event.desc      =  "default (all inbound connections)|default (all inbound connections)"
reference.id    =  "44"
action          =  "Initiate"
ip.addr         =  8.31.114.102
alias.host      =  "profiles test-3: 6567be89-f6cb-4ff2-ab5b-8ae555e4eae5"
event.source    =  "0"
process         =  "driver:HTTP.sys"
ip.src          =  8.31.114.103
ip.dst          =  8.31.114.102
ip.dstport      =  2869
host.src        =  "Remote Host"
obj.type        =  "Process"
obj.name        =  "driver:HTTP.sys"
event.computer  =  "10.150.10.25"
level           =  1
msg.id          =  "3.1.1"
event.cat.name  =  "Attacks"
```

CounterTack Event Horizon Configuration

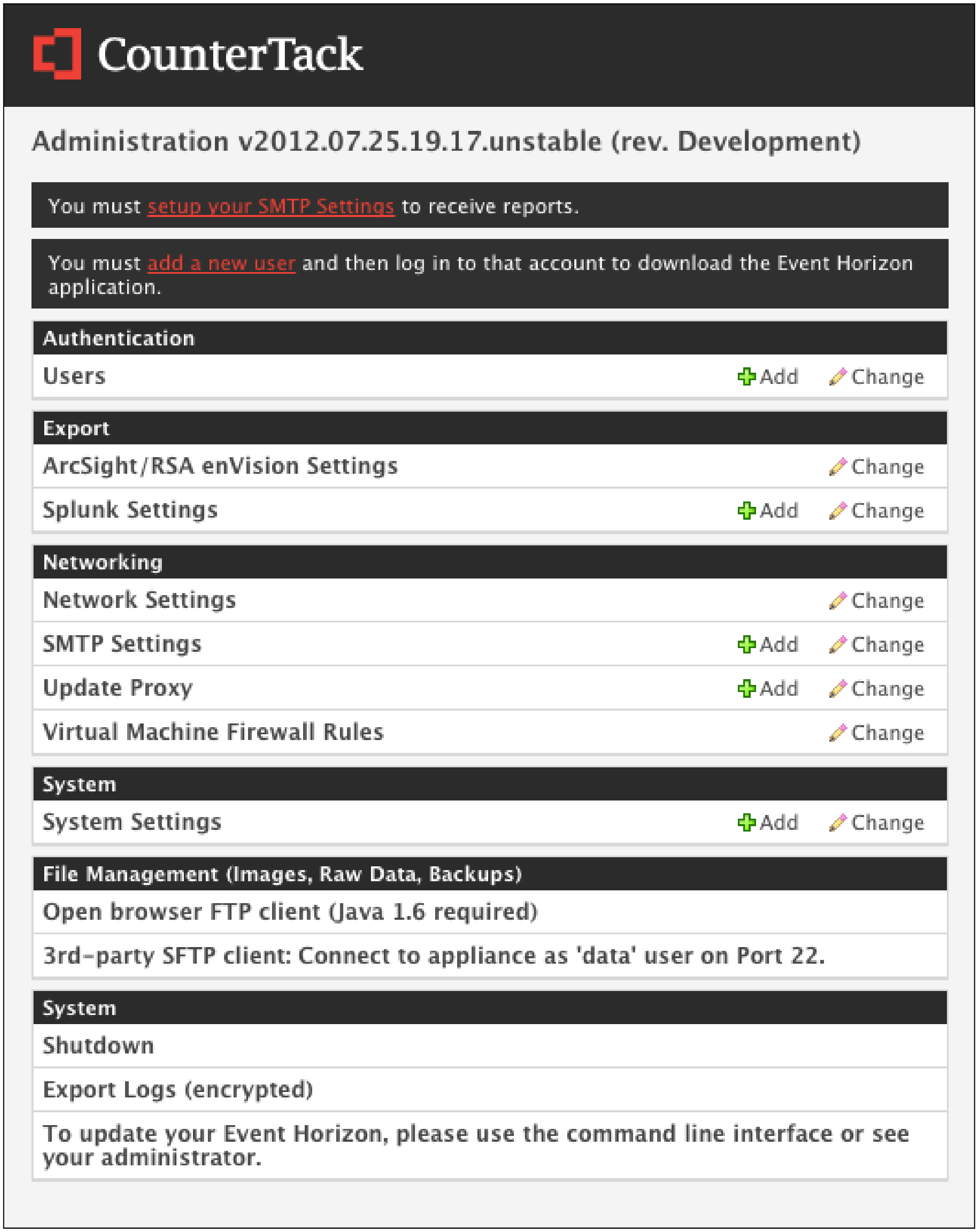
In order to export data to third-party systems, Event Horizon has an Export Options section in the main menu. Export settings are accessible from the Export section of the web-based administration application.

Event Horizon exports events to RSA Security Analytics as syslog messages over UDP. Before configuring Security Analytics export, please note the address or hostname of your SA instance and the port number on which your instance is listening for messages.

To configure Security Analytics export within Event Horizon:

1. Open your Internet browser and navigate to the IP address of your Event Horizon server: **https://Event_Horizon_Server_IP_Address**

2. From the home page, click the **ArcSight/RSA enVision Settings** link.



CounterTack

Administration v2012.07.25.19.17.unstable (rev. Development)

You must setup your SMTP Settings to receive reports.

You must add a new user and then log in to that account to download the Event Horizon application.

Authentication		
Users	Add	Change

Export		
ArcSight/RSA enVision Settings		Change
Splunk Settings	Add	Change

Networking		
Network Settings		Change
SMTP Settings	Add	Change
Update Proxy	Add	Change
Virtual Machine Firewall Rules		Change

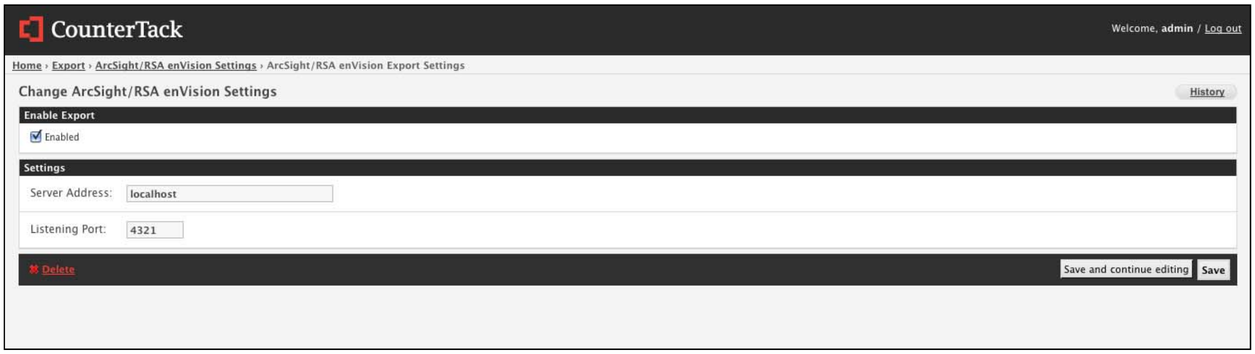
System		
System Settings	Add	Change

File Management (Images, Raw Data, Backups)
Open browser FTP client (Java 1.6 required)
3rd-party SFTP client: Connect to appliance as 'data' user on Port 22.

System
Shutdown
Export Logs (encrypted)
To update your Event Horizon, please use the command line interface or see your administrator.

3. Next, click on the **ArcSight/RSA enVision Export Settings** link.
4. Click the checkbox to **Enable ArcSight/RSA enVision**.

5. Supply the address of your enVision instance and the **Listening Port** number on which your instance will be listening for messages.



Home › Export › ArcSight/RSA enVision Settings › ArcSight/RSA enVision Export Settings

Change ArcSight/RSA enVision Settings

Enable Export

☑ Enabled

Settings

Server Address: localhost

Listening Port: 4321

6. Click **Save**.

Certification Checklist for RSA Security Analytics

Date Tested: 2/16/2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
CounterTack Event Horizon	3.1.7	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	✓

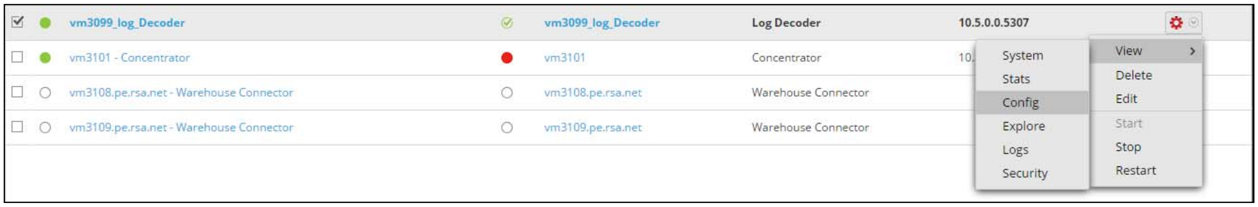
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Security Analytics Disable Device Parser

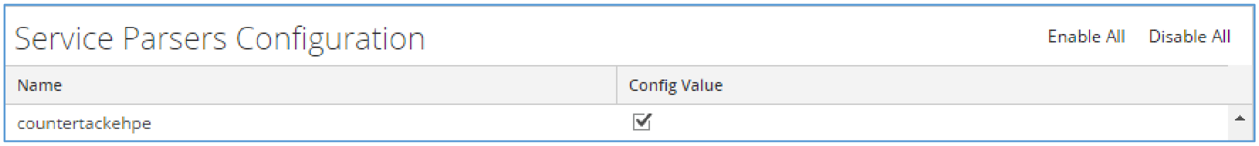
To disable the Security Analytics Integration Package but not delete the XML from the system, perform the following:

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



☑	●	vm3099_log_Decoder	✓	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307
□	●	vm3101 - Concentrator	●	vm3101	Concentrator	10.
□	○	vm3108.pe.rsa.net - Warehouse Connector	○	vm3108.pe.rsa.net	Warehouse Connector	
□	○	vm3109.pe.rsa.net - Warehouse Connector	○	vm3109.pe.rsa.net	Warehouse Connector	

2. From the **Service Parses Configuration** window, scroll down to the device you wish to disable and uncheck the Config Value checkbox.



Service Parsers Configuration

Name	Config Value
countertackehpe	☑

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).