



RSA Security Analytics Ready Implementation Guide

Last Modified: December 2nd, 2013

Partner Information

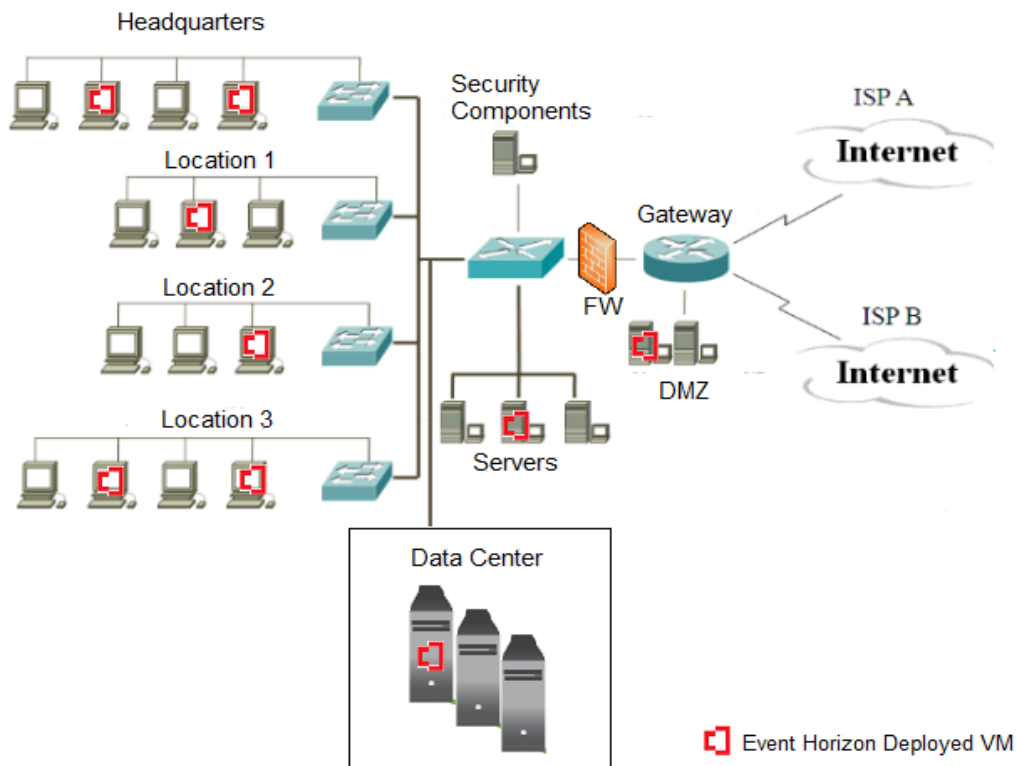
Product Information	
Partner Name	CounterTack
Web Site	www.countertack.com
Product Name	Event Horizon
Version & Platform	3.1
Product Description	CounterTack's Event Horizon® is an active monitoring, detection, and intelligence platform that enables organizations to identify, disrupt and respond to an in-progress cyber attack. It is the world's first commercially available security solution utilizing virtual machine introspection to help enterprise and government organizations defend themselves from the devastation caused by advanced, targeted threats.



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	
Integration package name	countertackehpe.zip
Device display name within Security Analytics	countertackehpe
Event source class	Analysis
Collection method	Syslog



Release Notes

Release Date	What's New In This Release
12/02/2013	Initial SA support for CounterTack Event Horizon.

Security Analytics Integration Package

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 package from the Security Analytics Community, the next steps are to deploy this on all log decoders. Follow the rest of this Implementation Guide to proceed.

 **Note:** For steps to disable or remove the Security Analytics Integration Package, please refer to the Appendix of this Guide.

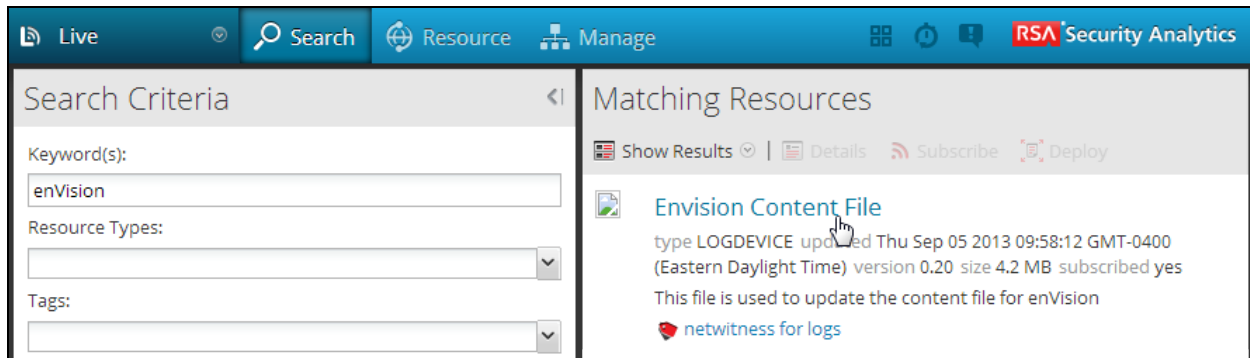
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
countertackehpe.envision	This file is deployed during the Deploy Security Analytics Integration Package section in this guide.
index-concentrator-custom.xml	This file can be referenced for the Create the index-concentrator-custom.xml section.
table-map.xml	This file can be referenced for the Modify the table-map.xml section.
variables.txt	This file can be used to determine which variables are used within the parser/XML. The format of the file consists of: <i>enVision variable name --> SA variable name --> SA variable type</i>

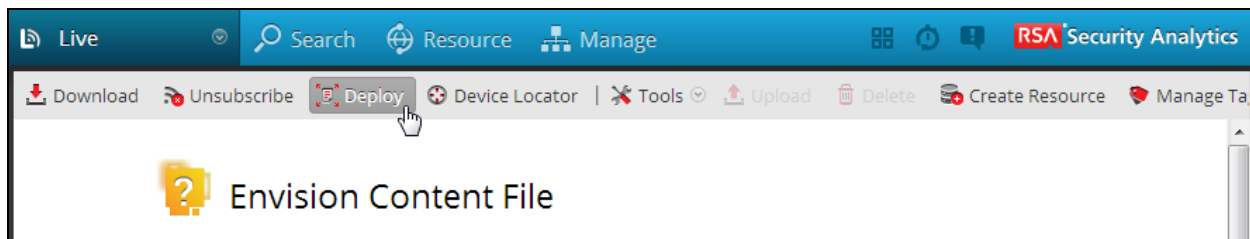
Deploy enVision Content File

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

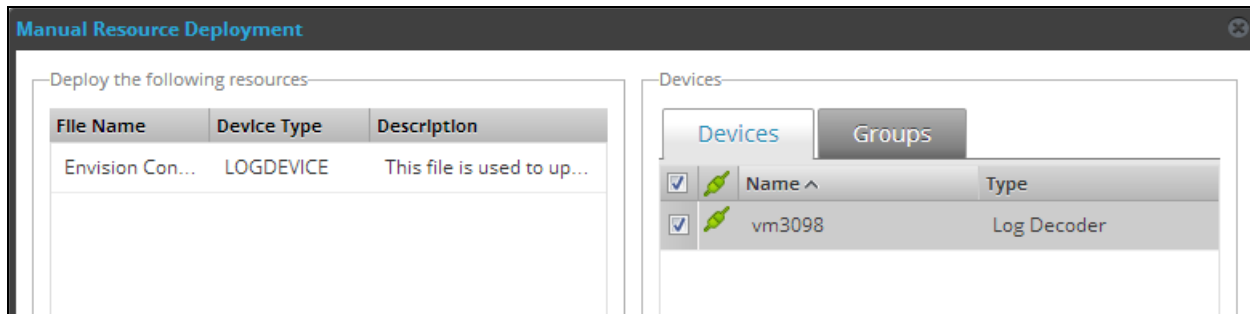
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Click on **Envision Content File**.



5. Next click **Deploy** in the menu bar.



6. Check your **Log Decoder(s)** in Devices tab and then click **Push**.



7. Once deployed, you will receive a **COMPLETE** message in the Deployment Job Progress window.

Deploy Security Analytics Integration Package

After completing the previous section, *Deploy enVision Content 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 > Devices**.
2. Select your Log Decoder from the list, select **View > Config**.

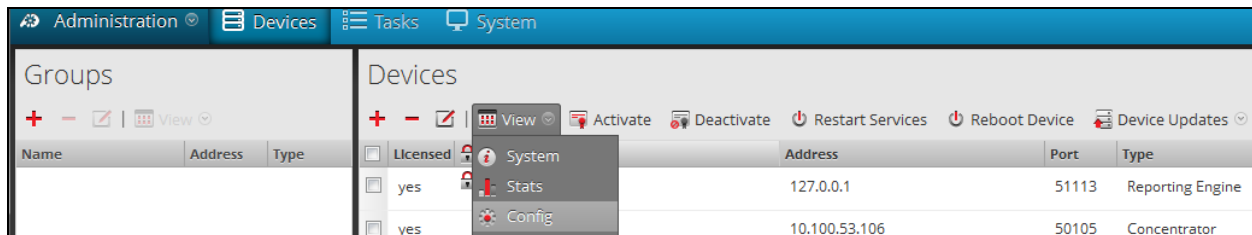
 **Note: In an environment with multiple Log Decoders, deploy the Integration Package on each Log Decoder that will use the new device.**

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.
5. Under the file name column, select the integration package name and click **Upload**.
6. Navigate to **Administration > Devices** and check the **Log Decoder** then click **Restart Services**.



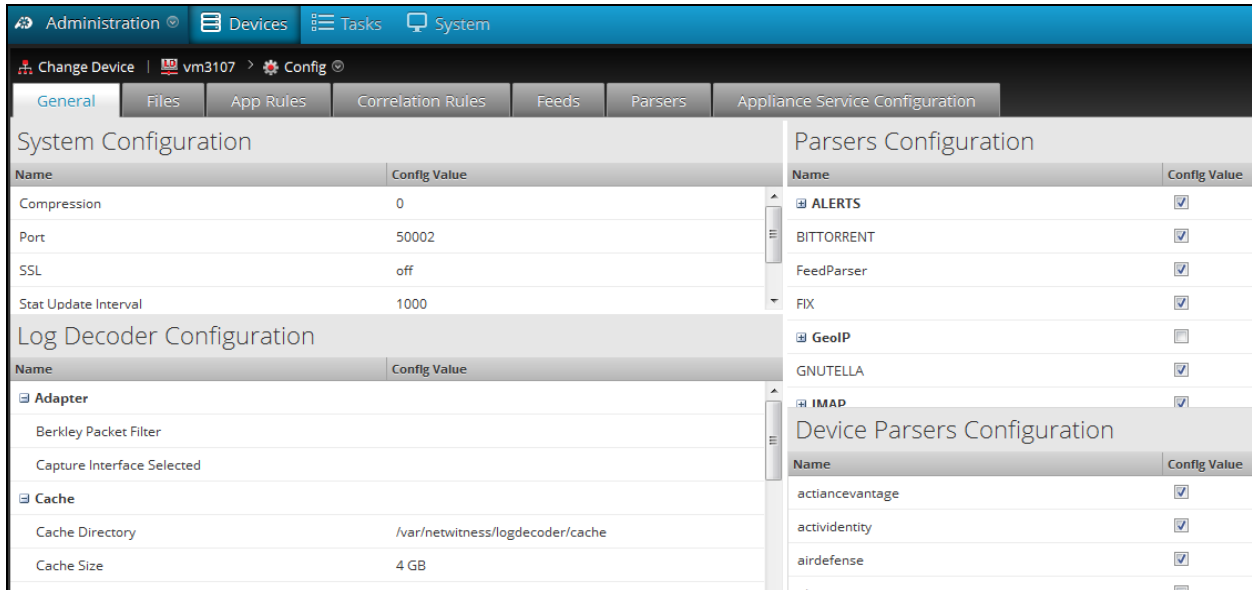
Groups		Devices						
Name	Address	Type	Licensed	System	Name	Address	Port	Type
			yes		vm3105	127.0.0.1	51113	Reporting Engine
			yes		vm3106	10.100.53.106	50105	Concentrator
			yes		vm3107	10.100.53.107	50101	Log Collector
			yes		vm3107	10.100.53.107	50102	Log Decoder

7. From the **Administration > Device** screen check **Log Decoder** and select **View > Config**.



Groups		Devices						
Name	Address	Type	Licensed	System	Name	Address	Port	Type
			yes		System	127.0.0.1	51113	Reporting Engine
			yes		Stats	10.100.53.106	50105	Concentrator
			yes		Config			

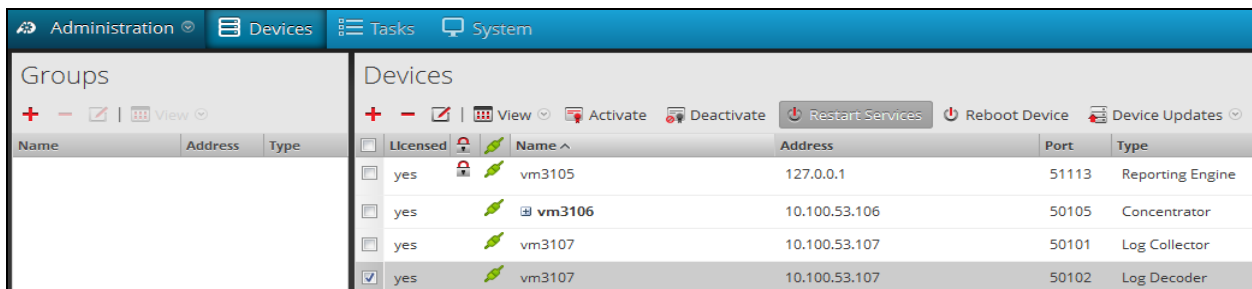
8. The new device will automatically be listed under **General > Device Parsers Configuration**.



Create the *index-concentrator-custom.xml*

Modify the *index-concentrator-custom.xml* file to retrieve meta details from log collections.

1. Log into the log decoder via console or SSH.
2. On the log decoder, go to the */etc/netwitness/ng/envision* directory.
3. If the *index-concentrator-custom.xml* file does not exist, copy the *index-concentrator-custom.xml* from the Integration zip file to this directory.
If the *index-concentrator-custom.xml* file already exists then append the content to the existing file.
4. Navigate to **Administration > Devices** and check the **Log Decoder** then click **Restart Services**.



Below is an example of the *index-concentrator-custom.xml* for the enVision attributes **macaddr** and **node**.

```
<key description="macaddr" level="Indexvalues" name="eth.host" format="Text" valueMax="100000" />
<key description="node" level="Indexvalues" name="node" format="Text" valueMax="100000" />
```

Modify the *table-map.xml*

The *table-map.xml* file contains the enVision to NetWitness meta map.

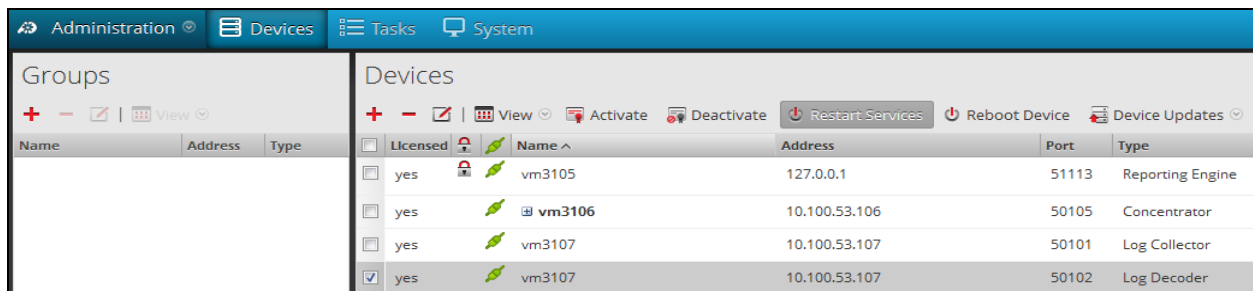
1. Log into the Log Decoder via console or SSH.
2. On the Log Decoder, go to */etc/netwitness/ng/envision/etc*.
3. Use the name fields in the *index-concentrator-custom.xml* file to determine the list of attributes which need to be modified in the *table-map.xml* file.

- Copy the **table.map.xml** from **/etc/netwitness/ng/envision/etc** to **/etc/netwitness/ng/envision**.
- Open **/etc/netwitness/ng/envision/table.map.xml** file and modify the field **flags=Transient** to **flags=None** for only the attributes that exist in the name field of the index-concentrator-custom.xml file.

The below table-map.xml maps is an example of the enVision attribute **macaddr** and **node** mapped to the correlated NetWitness attribute, with the flag field modified to **None**.

```
<?xml version="1.0" encoding="utf-8"?>
<!--
# attributes:
#   envisionName:  The name of the column in the universal table
#   nwName:       The name of the NetWitness meta field
#   format:       Optional. The language key data type. See LanguageManager. Defaults to "Text".
#   flags:        Optional. One of None|File|Duration|Transient. Defaults to "None".
#   failureKey:   Optional. The name of the NW key to write data if conversion fails. Defaults to system
#   parse.error meta.
#   nullTokens:   optional. The list of "null" tokens. Pipe separated. Default is no null tokens.
-->
<mappings>
  <!-- These entries are defined and created by Panorama and can be turned on/off here -->
  <mapping envisionName="device_class" nwName="device.class" flags="None" />
  <mapping envisionName="device_ip" nwName="device.ip" format="Text" flags="None" />
  <mapping envisionName="device_name" nwName="device.name" flags="None" />
  <mapping envisionName="device_type" nwName="device.type" flags="None" />
  <mapping envisionName="device_type_id" nwName="device.type.id" format="Int32" nullTokens="(null)" flags="Transient" />
  <mapping envisionName="lwrite" nwName="lwrite" format="Int32" nullTokens="(null)" flags="Transient" />
  <mapping envisionName="macaddr" nwName="eth.host" format="MAC" flags="None" />
  <mapping envisionName="mail_id" nwName="mail.id" flags="Transient" />
  <mapping envisionName="mask" nwName="mask" flags="Transient" />
  <mapping envisionName="message_body" nwName="message.body" flags="Transient" />
  <mapping envisionName="network_port" nwName="network.port" format="Int32" flags="Transient" />
  <mapping envisionName="msg" nwName="msg" format="Text" flags="Transient" />
  <mapping envisionName="network_service" nwName="network.service" flags="Transient" />
  <mapping envisionName="node" nwName="node" flags="None" />
  <mapping envisionName="node_name" nwName="node.name" flags="Transient" />
  <mapping envisionName="workspace_desc" nwName="workspace" flags="Transient" />
  <mapping envisionName="workstation" nwName="alias.host" flags="None" />
  <mapping envisionName="zone" nwName="zone" flags="Transient" />
</mappings>
```

- Navigate to **Administration > Devices** and check the **Log Decoder** than click **Restart Services**.



- The Log Decoder is now ready to parse events for this device.

Partner Product Configuration

Before You Begin

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

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`

- 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.

- Next, click on the **ArcSight/RSA enVision Export Settings** link.
- 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.



The screenshot shows the CounterTack web interface. At the top left is the CounterTack logo. The top right corner says "Welcome, admin / Log out". Below the navigation bar, the breadcrumb trail is "Home > Export > ArcSight/RSA enVision Settings > ArcSight/RSA enVision Export Settings". The main heading is "Change ArcSight/RSA enVision Settings" with a "History" button to its right. Under the heading, there is a section "Enable Export" with a checked checkbox labeled "Enabled". Below that is a "Settings" section with two input fields: "Server Address" containing "localhost" and "Listening Port" containing "4321". At the bottom of the settings area, there are three buttons: a red "Delete" button, a "Save and continue editing" button, and a "Save" button.

6. Click **Save**.

Certification Checklist for RSA Security Analytics

Date Tested: December 2nd, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.2 SP2	Virtual Appliance
CounterTack Event Horizon	3.1.7	Appliance

Security Analytics Test Case	Result
Device Administration	
Partners device name appears in Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be enabled from Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be disabled from Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be removed from Device Parsers Configuration	<input checked="" type="checkbox"/>
Investigation	
Device name displays properly from Device Type	<input checked="" type="checkbox"/>
Displays Meta Data properly within Investigator	<input checked="" type="checkbox"/>

JJO / PAR

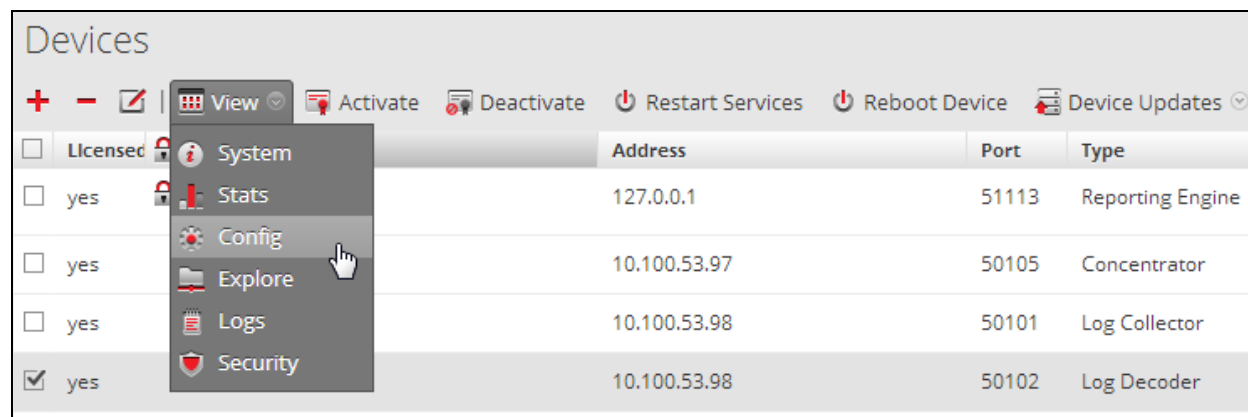
✓ = Pass ✗ = Fail N/A = Non-Available Function

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. From the Security Analytics menu, select **Administration > Devices**.
2. Check your Log Decoder from the **Devices** list and then select **View > Config**.



3. From the **Device Parses Configuration** window, scroll down to the device you wish to disable and uncheck the box.
4. 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 additional changes to the **table-map.xml** and **index-concentrator-custom.xml** files. To identify which variables were added locate the zip file downloaded from the RSA Website and open the **index-concentrator-custom.xml** contained within.
4. Edit **index-concentrator-custom.xml** on the SA server, removing only the lines present in the **index-concentrator-custom.xml** extracted from the zip.