



## RSA Security Analytics Ready Implementation Guide

Last Modified: December 9, 2013

### Partner Information

---

Product Information	
Partner Name	Fox Technologies
Web Site	<a href="http://www.foxt.com">www.foxt.com</a>
Product Name	Server Control
Version & Platform	6.6
Product Description	FoxT ServerControl enables companies to centrally control access across their diverse server domains.



## Solution Summary

---

This guide provides information for configuring the FoxT Server Control for syslog-based event log integration with RSA Security Analytics.

RSA Security Analytics Features	
Fox Technologies Server Controls 6.6	
Integration package name	Foxtpe.zip
Device display name within Security Analytics	foxtpe
Event source class	Security Access Controls
Collection method	Syslog

## Release Notes

---

Release Date	What's New In This Release
12/9/2013	Initial support for Fox Technologies Server Controls.

## 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.

---

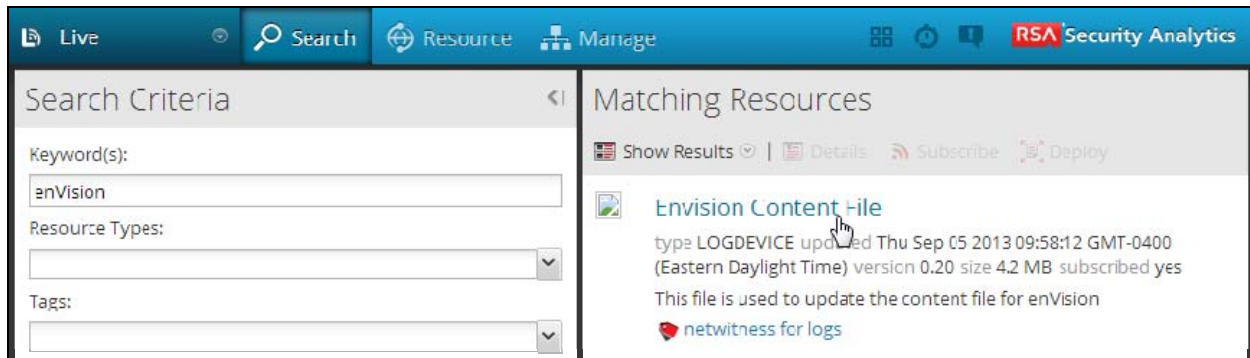
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
<b>foxtpe.envision</b>	This file is deployed during the <b>Deploy Security Analytics Integration Package</b> section in this guide.
<b>index-concentrator-custom.xml</b>	This file can be referenced for the <b>Create the index-concentrator-custom.xml</b> section.
<b>table-map.xml</b>	This file can be referenced for the <b>Modify the table-map.xml</b> section.
<b>variables.txt</b>	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 --&gt; SA variable name --&gt; SA variable type</i>

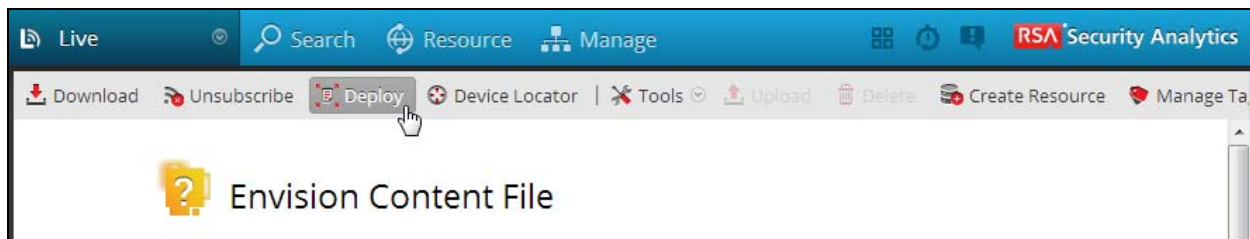
## Deploy enVision Content File

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:

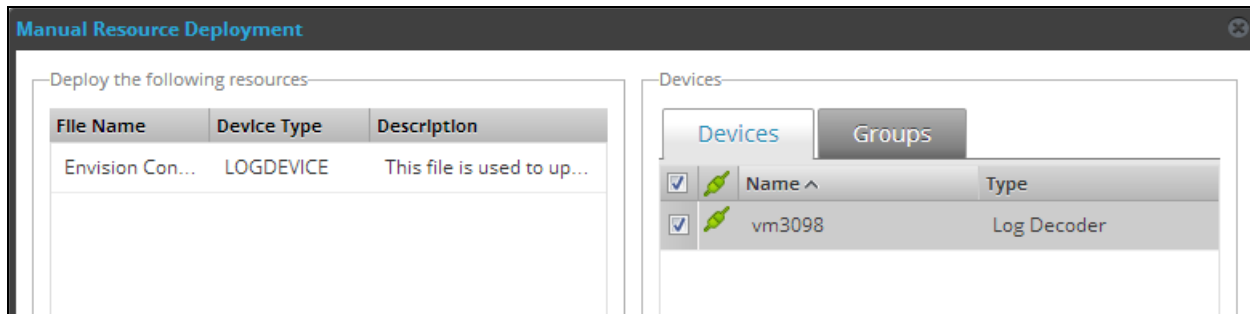
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Click on **Envision Content File**.



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**.

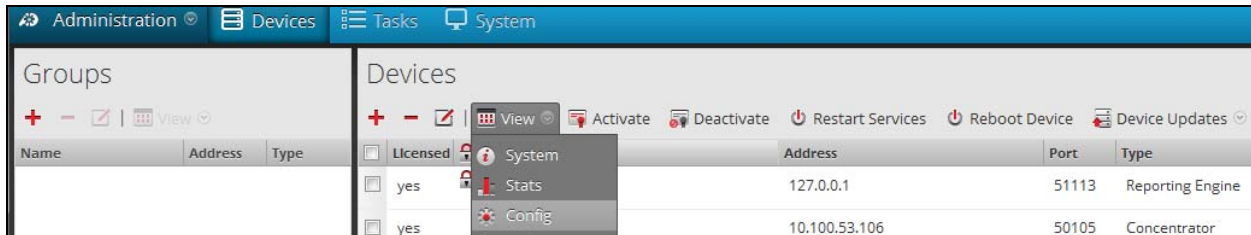
 **Note:** In an environment with multiple Log Decoders, deploy the Integration Package on each Log Decoder that will use the new device.

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**.



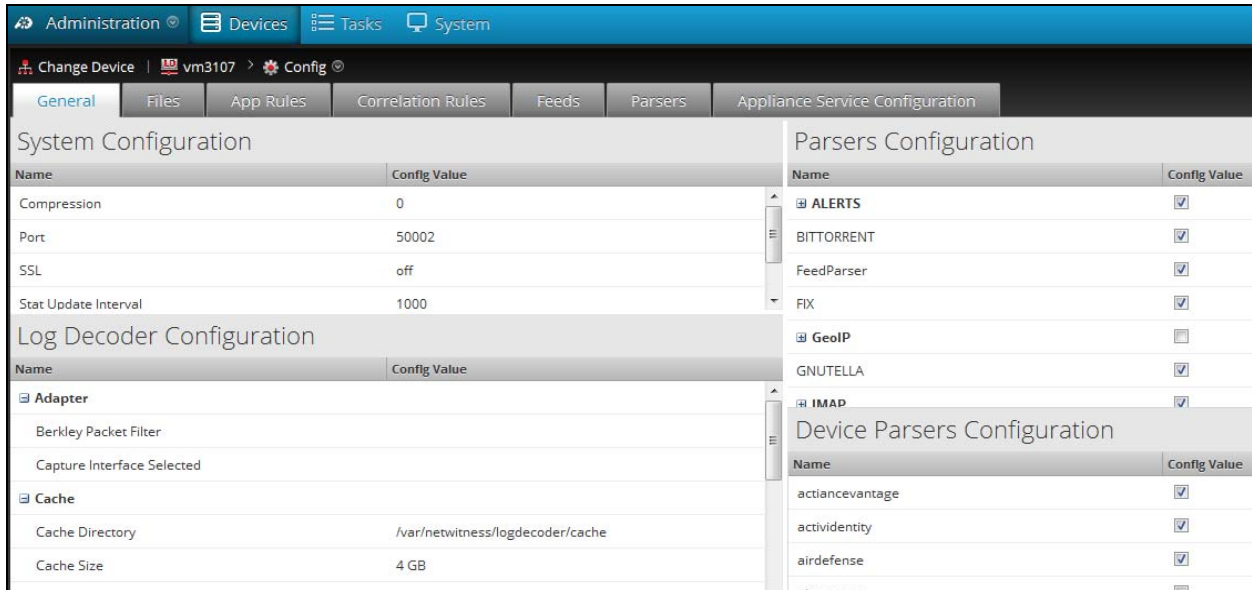
Groups		Devices					
Name	Address	Type	Licensed	Name	Address	Port	Type
			<input type="checkbox"/>	vm3105	127.0.0.1	51113	Reporting Engine
			<input type="checkbox"/>	vm3106	10.100.53.106	50105	Concentrator
			<input type="checkbox"/>	vm3107	10.100.53.107	50101	Log Collector
			<input checked="" type="checkbox"/>	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	Name	Address	Port	Type
			<input type="checkbox"/>	System	127.0.0.1	51113	Reporting Engine
			<input type="checkbox"/>	Stats	10.100.53.106	50105	Concentrator
			<input type="checkbox"/>	Config			

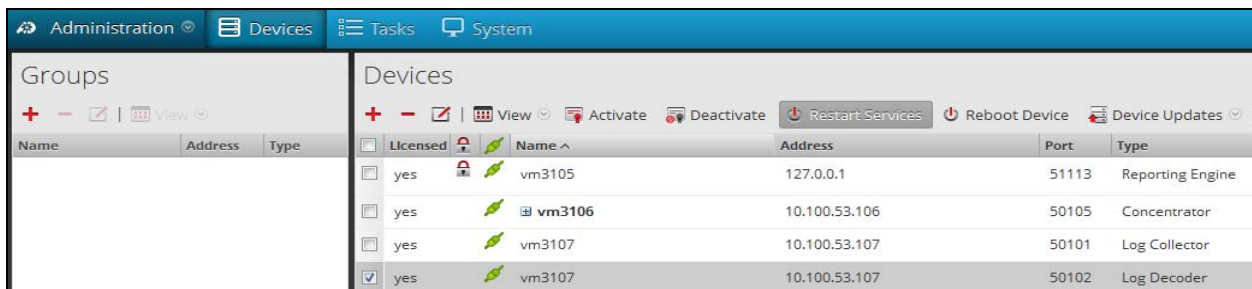
8. The new device will automatically be listed under **General > Device Parsers Configuration**.



## 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*.

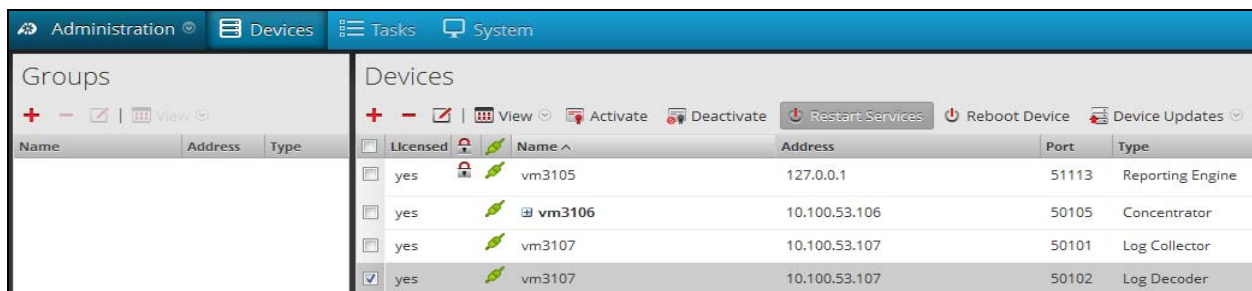
- Use the name fields in the index-concentrator-custom.xml file to determine the list of attributes which need to be modified in the table-map.xml file.
- Copy the **table.map.xml** from **/etc/netwitness/ng/envision/etc** to **/etc/netwitness/ng/envision**.
- Open **/etc/netwitness/ng/envision/table.map.xml** 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="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 Fox Technologies Server Controls 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 Fox Technologies Server Controls components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***Fox Technologies Server Controls Configuration***

#### **Prerequisites:**

- A FoxT Master running 6.5.x or later.
- A system (loghost) to perform the conversion of FoxT (BoKS) logs to standard format.
- Loghost machine must have ruby installed, version 1.8.7.
- FoxT Linux BRM package's bdcn component installed on the Master (i.e. bdcn10-linux-x86.tar.gz). This package contains only scripts and can run on any operating system, even though the file is titled Linux.
- Syslog NG version 2.0 or later installed on loghost.

#### **Install and setup:**

1. Unpack the bdcn package from FoxT Reporting Manager on the FoxT (BoKS) master and run install script. See documentation from FoxT Reporting manager for details.
2. Use rsauser as user and homedir to match existing config.cfg file. Ignore Boot request, do not reboot.
3. Edit \$BOKS\_etc/boks\_dbupdate\_reader.cfg and remove all lines.
4. Make sure BoKS sshd is running (kill system sshd and set.\$BOKS\_etc/ENV:BOKS\_SSHD=on).
5. Restart BoKS.
6. Create rsauser on loghost, homedir /home/rsauser.
7. Log in as rsauser on loghost and run ssh-keygen -t rsa.
8. Put .ssh/id\_rsa.pub in a place where you can get it from BoKS master.
9. SU to rsauser on BoKS master and go to homedir.
10. Install and setup continued:
11. Create .ssh dir, mode 700.
12. Copy in id\_rsa.pub as .ssh/authorized\_keys.
13. Activate BoKS.
14. As rsauser on loghost, ssh to BoKS master. Answer yes to trust the machine.
15. You should get in without having to give a password. If not, troubleshoot.
16. Check that you can execute /opt/boksm/lib/brmcmd -t with no issue and 0 exit status.
17. As rsauser on loghost, create directory arctmp, mode 700.
18. Unpack boks2cef.tar.gz.
19. Edit config.cfg and change the value for remote\_host (ssh\_cmd and scp\_cmd if needed). If BoKS on master is installed in a non-standard place also change brmcmd to point to have whatever \$BOKS\_lib is as path.
20. Execute ./bokslog2cef.rb config.cfg. It should produce standard log output on stdout (edit bokslog2cef.rb and change \$dodebug=false to \$dodebug=true to get some debug output on stderr if needed). If you execute it again it should produce fewer lines as output as it should remember what lines it has already processed. reset it to process all lines remove arcstate file.



21. Write a script that is executed regularly (e.g. once every 1-5 minutes or so) and calls on bokslog2cef.rb to produce a file with BoKS logs in standard format that the script then pushes into a logfile, which syslog-ng will detect and transfer to the RSA Security Analytics system. Execute the script as root, for example:
22. `#su - rsauser -c "/home/rsauser/bokslog2cef.rb /home/rsauser/config.cfg"` and redirect output to some the file being watched by syslog-ng. Remember to check exit status. The program exits with status 1 and error on stderr on configuration errors, and status 2 and error on stderr if ssh/scp fails. stderr on configuration errors, and status 2 and error on stderr if ssh/scp fails.

## Certification Checklist for RSA Security Analytics

Date Tested: December 9, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.2 SP2	Virtual Appliance
Fox Technologies Server Controls	6.6	Microsoft Windows, UNIX, Linux

Security Analytics Test Case	Result
<b>Device Administration</b>	
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"/>
<b>Investigation</b>	
Device name displays properly from Device Type	<input checked="" type="checkbox"/>
Displays Meta Data properly within Investigator	<input checked="" type="checkbox"/>

DRP / PAR

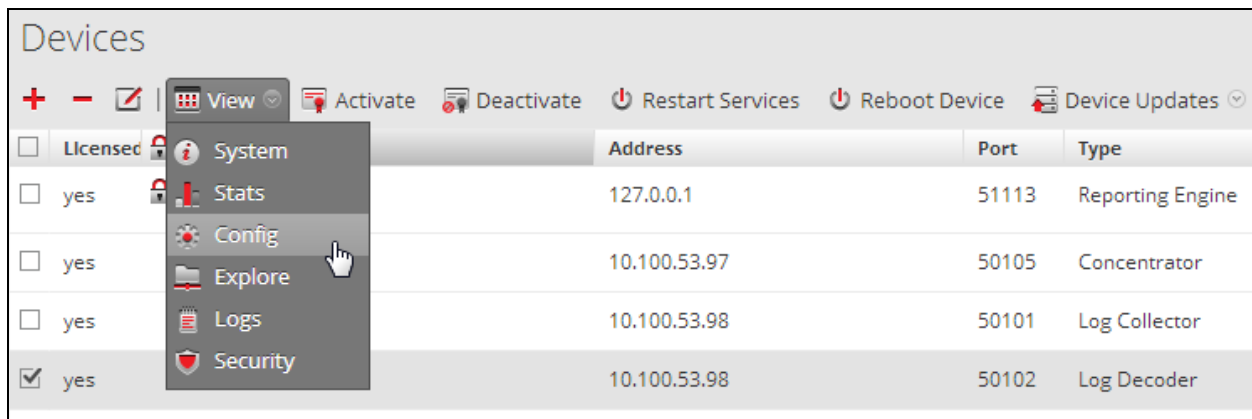
✓ = Pass ✗ = Fail N/A = Non-Available Function

## 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.