RSA Ready Implementation Guide for RSA Security Analytics

Fox Technologies Server Controls 6.6

Daniel R. Pintal, RSA Partner Engineering
Last Modified: 2/29/2016

RSA READY

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	
Server Controls 6.6	
Integration package name	foxtpe.envision
Device display name within Security Analytics	foxtpe
Event source class	Security Access Controls
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
foxtpe.envision	SA package deployed to parse events from device integrations.
foxtpemsg.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
12/9/2013	Initial support for Fox Technologies Server Controls.
2/29/2016	Security Analytics 10.5 Support.

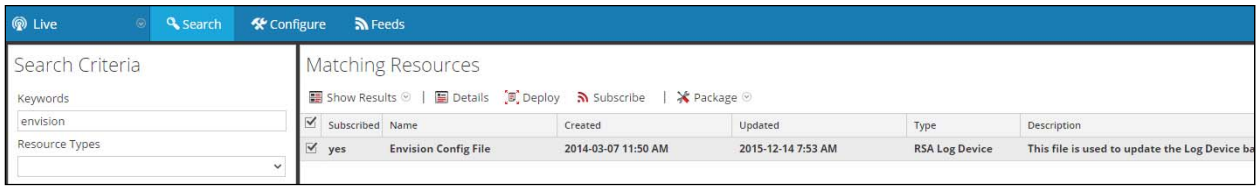
RSA Security Analytics Configuration

Deploy the enVision Config File

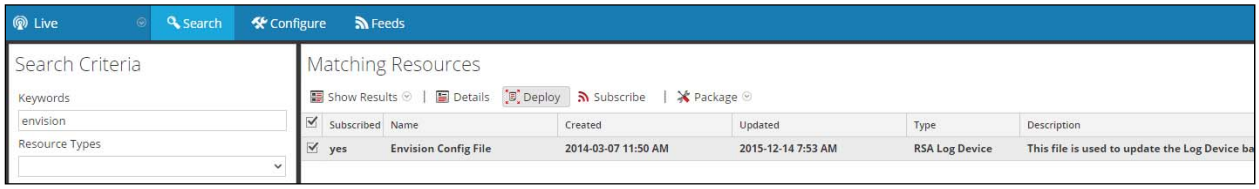
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

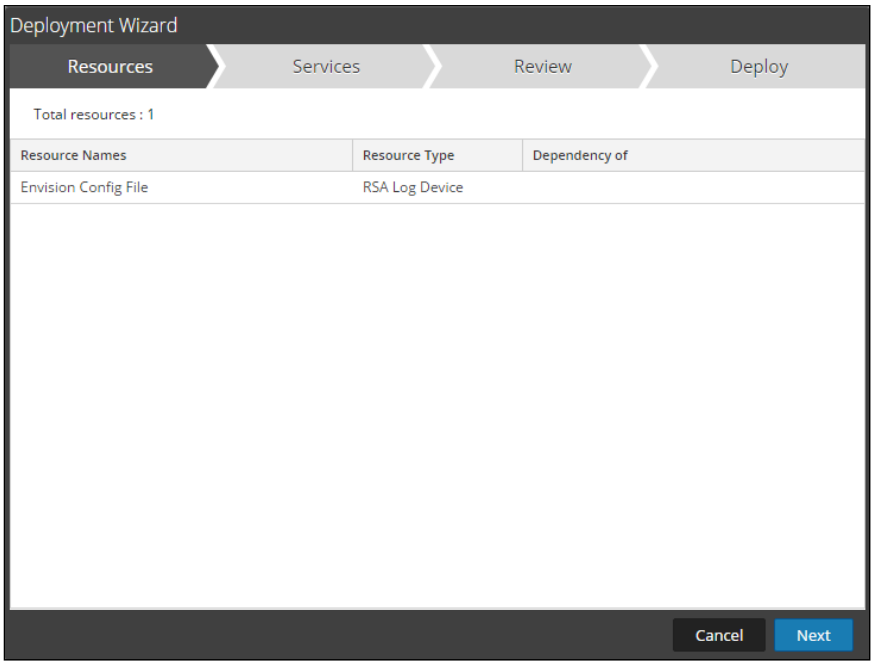
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**. Security Analytics will display the **Envision Config File** in Matching Resources.
3. Select the checkbox next to **Envision Config File**.



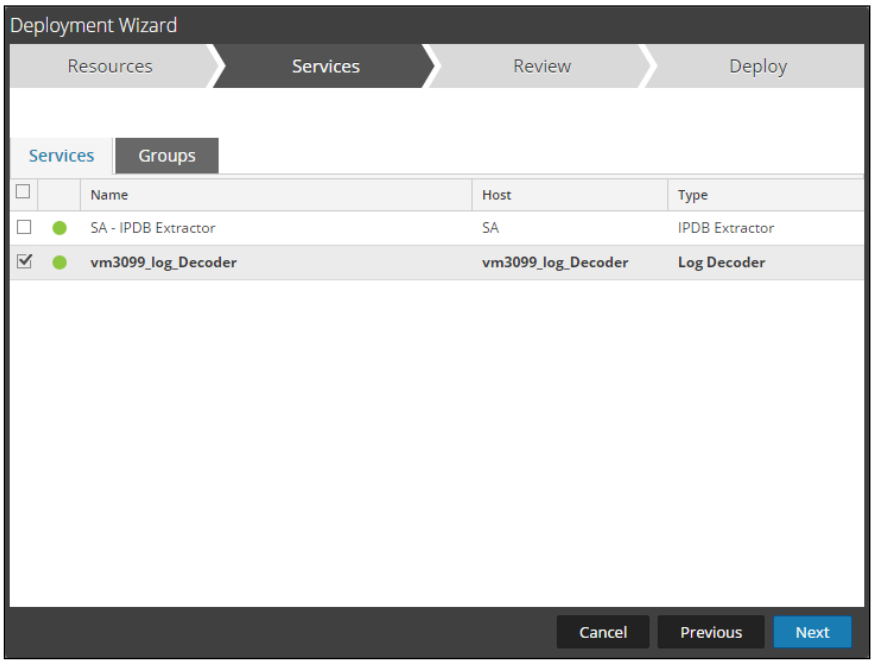
4. Click **Deploy** in the menu bar.



5. Select **Next**.

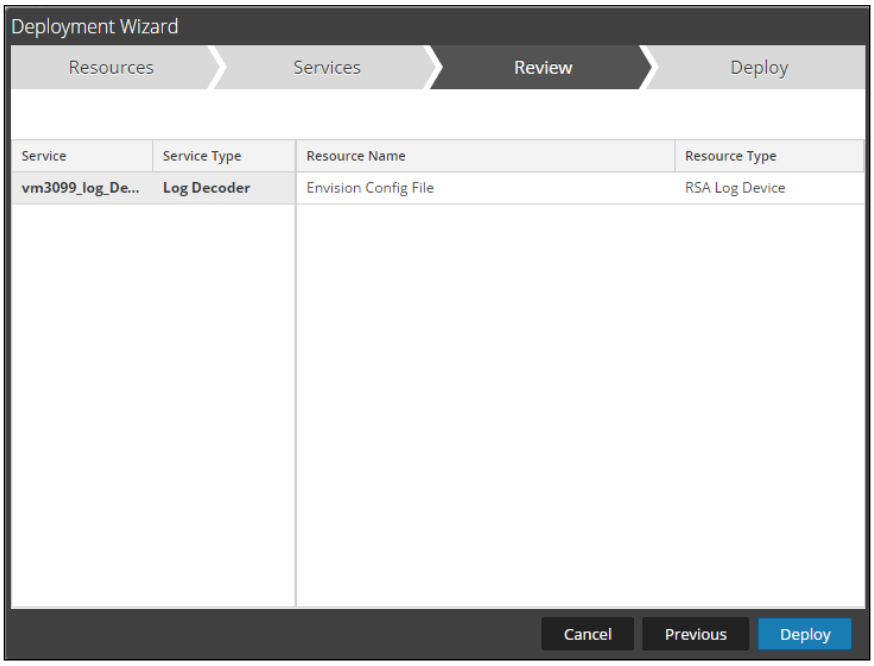


6. Select the **Log Decoder** and select **Next**.

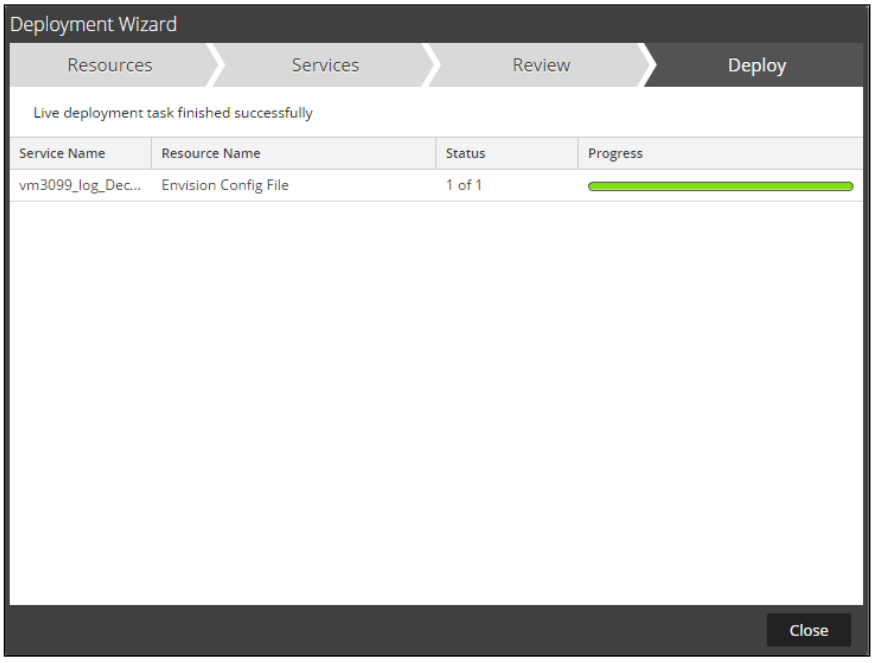


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

7. Select **Deploy**.



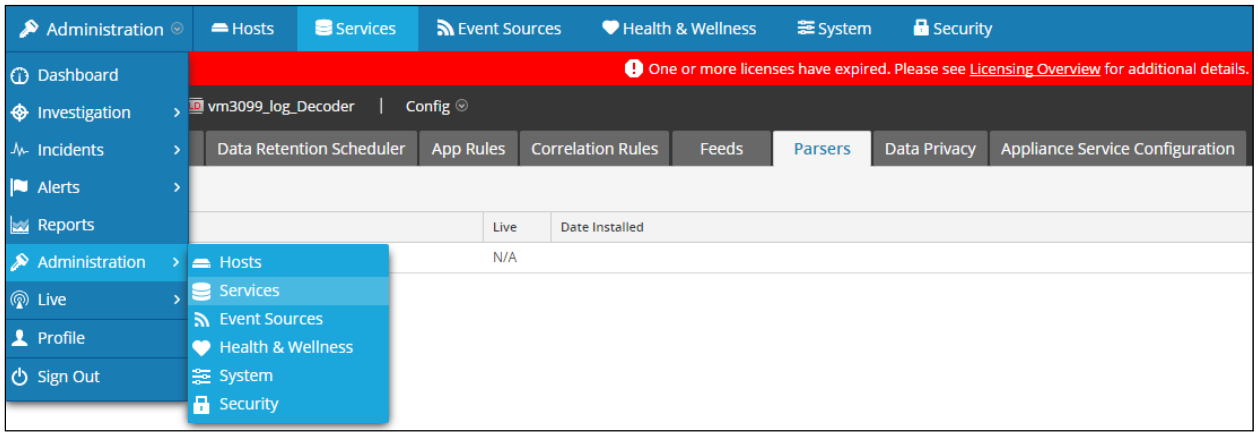
8. Select **Close**, to complete the deployment of the Envision Config file.



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.**



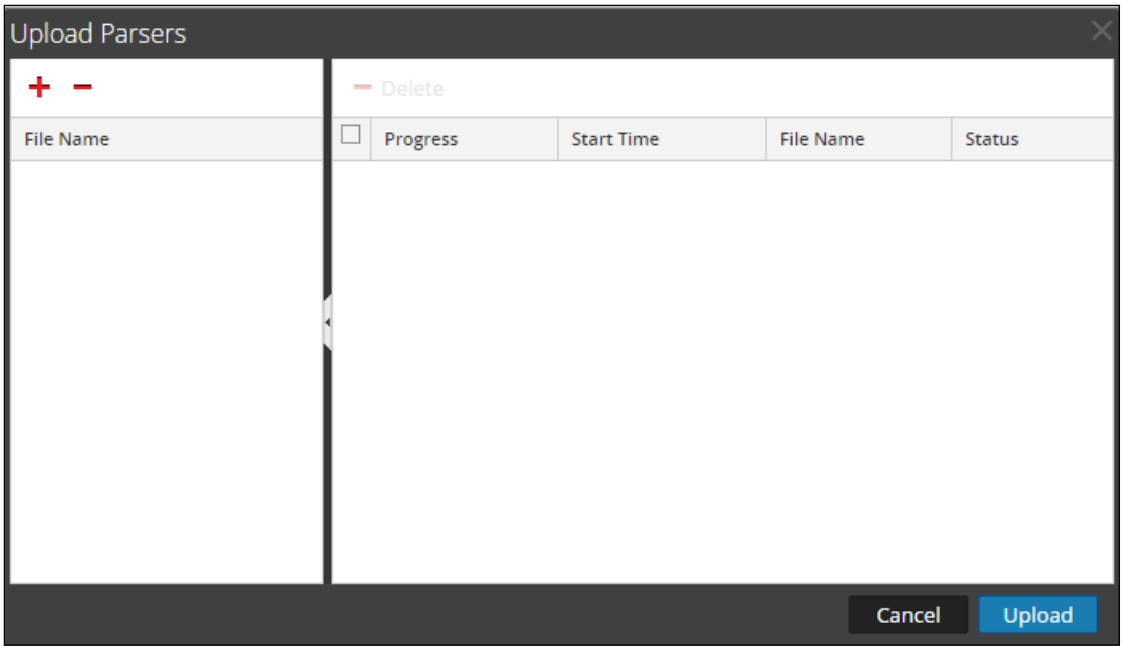
2. Select your Log Decoder from the list, select **View > Config**.

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

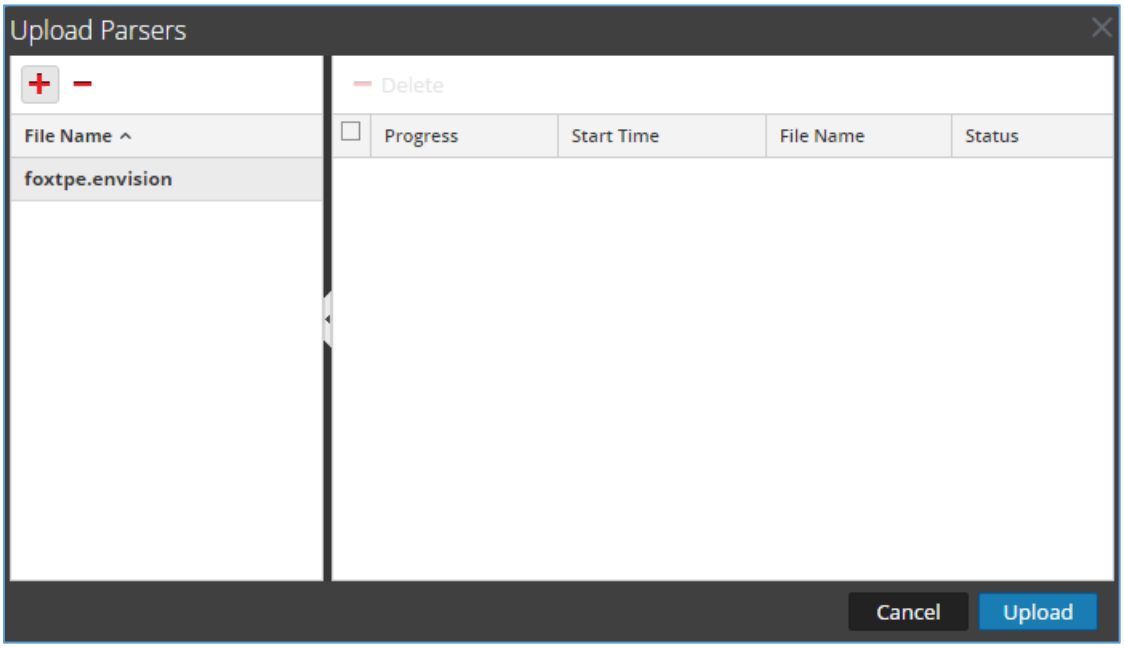
3. Next, select the **Parsers** tab and click the **Upload** button.

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

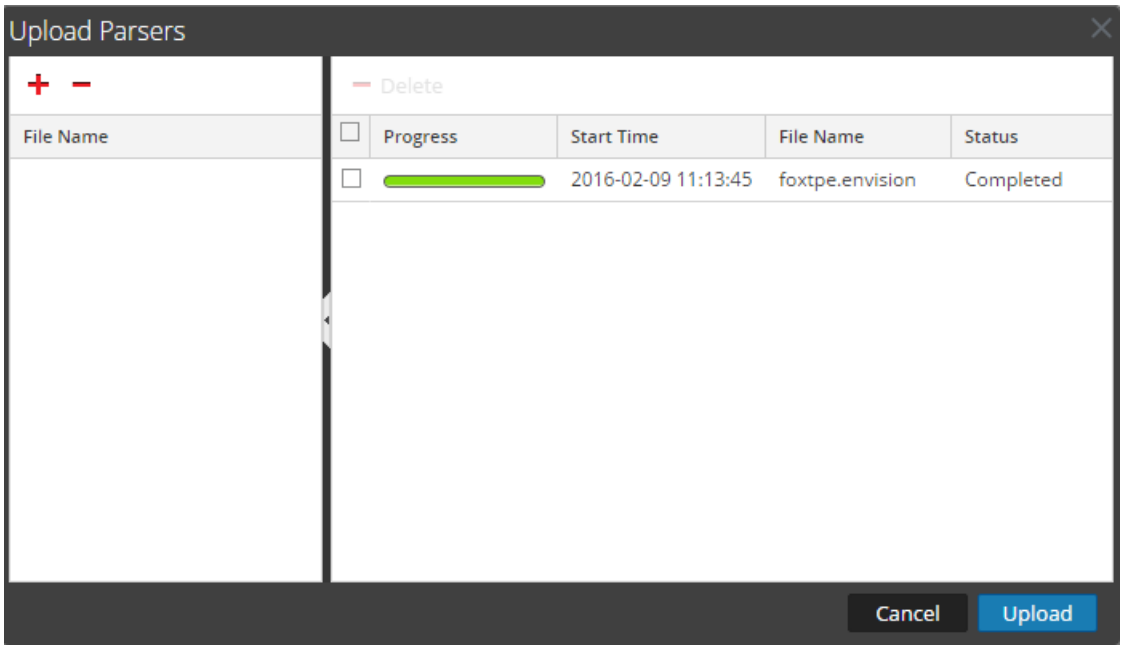
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Ready Community.**



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



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



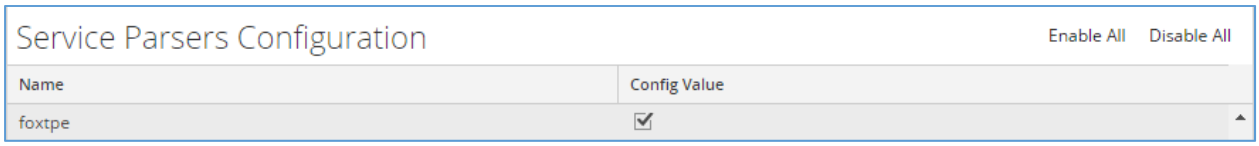
7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the table-map-custom.xml file from the contents of the .zip file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the log decoder(s), enter only the contents between the <mappings>...</mappings>.

```
<mappings>

        <mapping envisionName="severity" nwName="severity" flags="Transient" envisionDisplayName="Severity|SeverityLevel"/>
        <mapping envisionName="msg" nwName="msg" flags="Transient" format="Text" envisionDisplayName="Message"/>
        <mapping envisionName="event_time_string" nwName="event.time.str" flags="Transient" envisionDisplayName="EventTimeString"/>

</mappings>
```

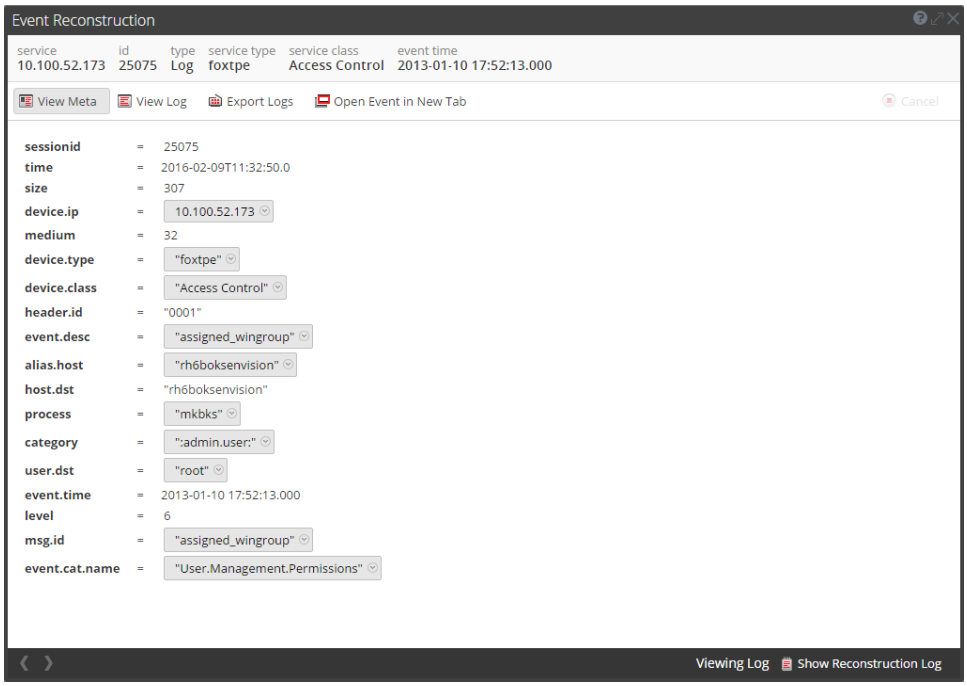
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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 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 bdcm component installed on the Master (i.e. bdcm10-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 bdcm 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:

```
#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: February 29, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
FoxT Server Controls	6.6	Microsoft Windows, UNIX, Linux

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

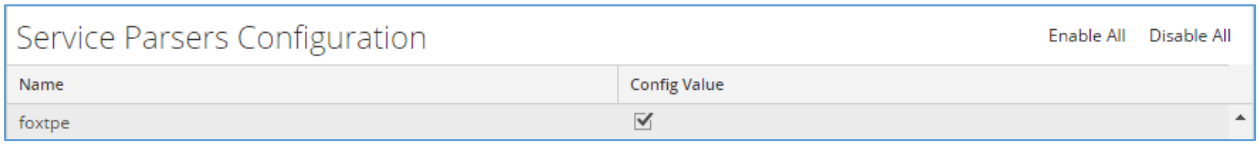
Appendix

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).