RSA Ready Implementation Guide for RSA Security Analytics

CoreTrace Bouncer 6

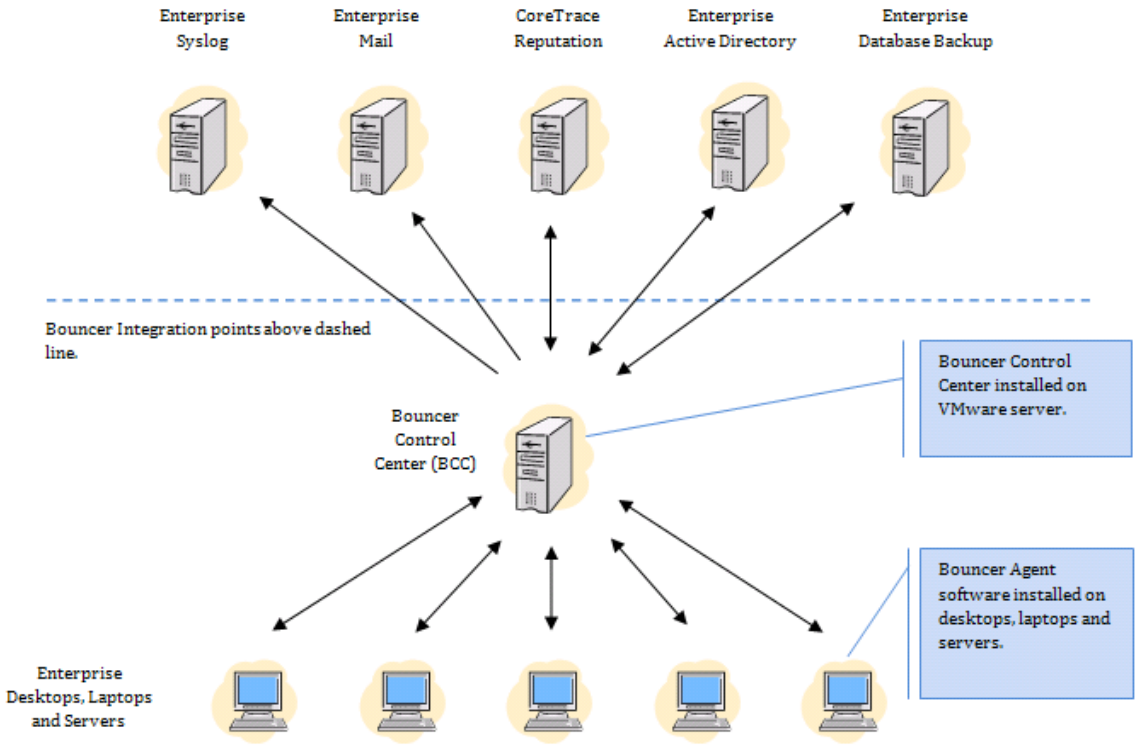
Daniel R. Pintal, RSA Partner Engineering
Last Modified: February 22, 2016

RSA READY

Solution Summary

The Bouncer Control Center can be configured to send syslog data to one or more Syslog Event Correlation devices. By integrating with RSA Security Analytics, Bouncer's log activity can be used in an effective security log management solution for real-time alerting, correlated rules and events, and scheduled reporting.

RSA Security Analytics Features	
Bouncer 6	
Integration package name	coretracebouncerpe.envision
Device display name within Security Analytics	coretracebouncerpe
Event source class	Application Firewall
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
coretracebouncerpe.envision	SA package deployed to parse events from device integrations.
coretracebouncerpemsg.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 CoreTrace Bouncer 6.
2/22/2016	SA 10.5 support

RSA Security Analytics Configuration

Before You Begin

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

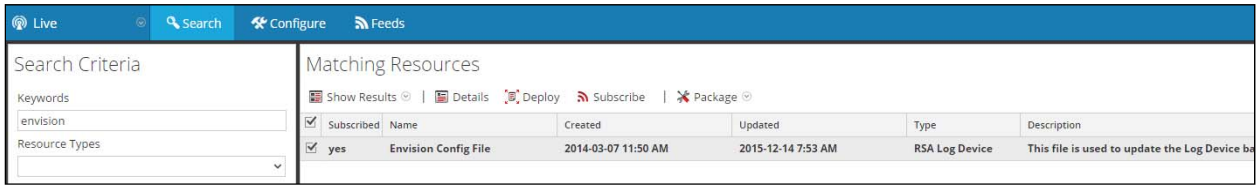
> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure CoreTrace Bouncer is properly configured and secured before deploying to a production environment.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

Deploy the enVision Config File

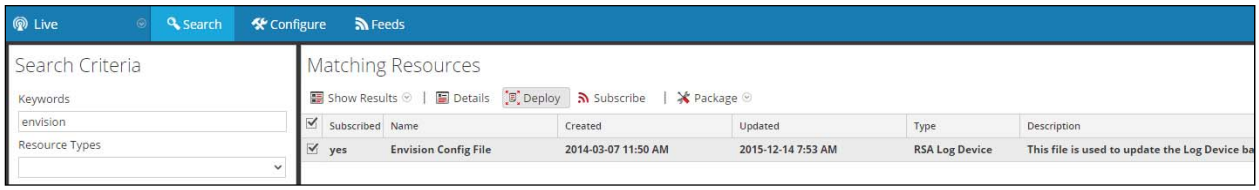
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

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

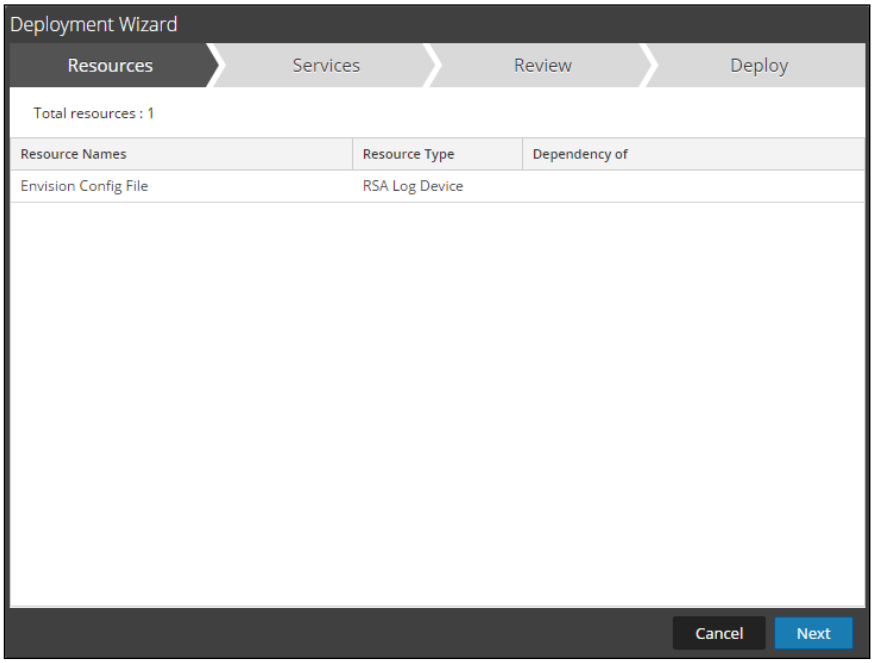
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



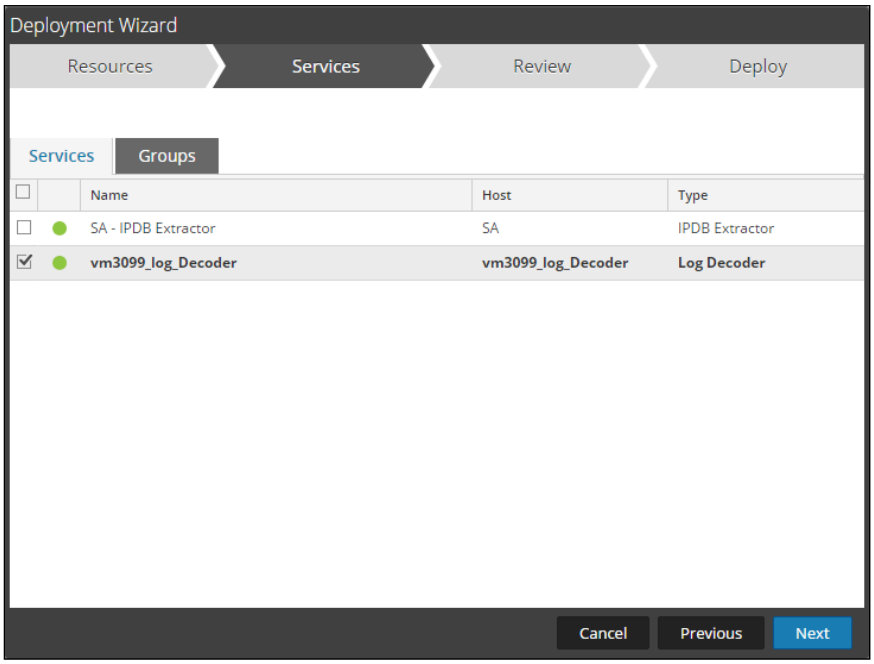
5. Click **Deploy** in the menu bar.



6. Select **Next**.

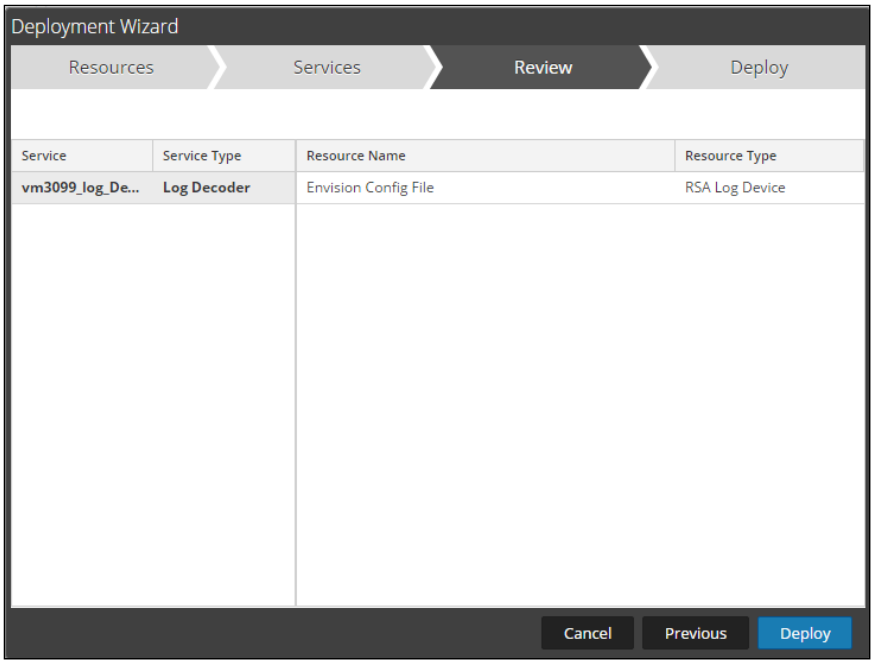


7. Select the **Log Decoder** and select **Next**.

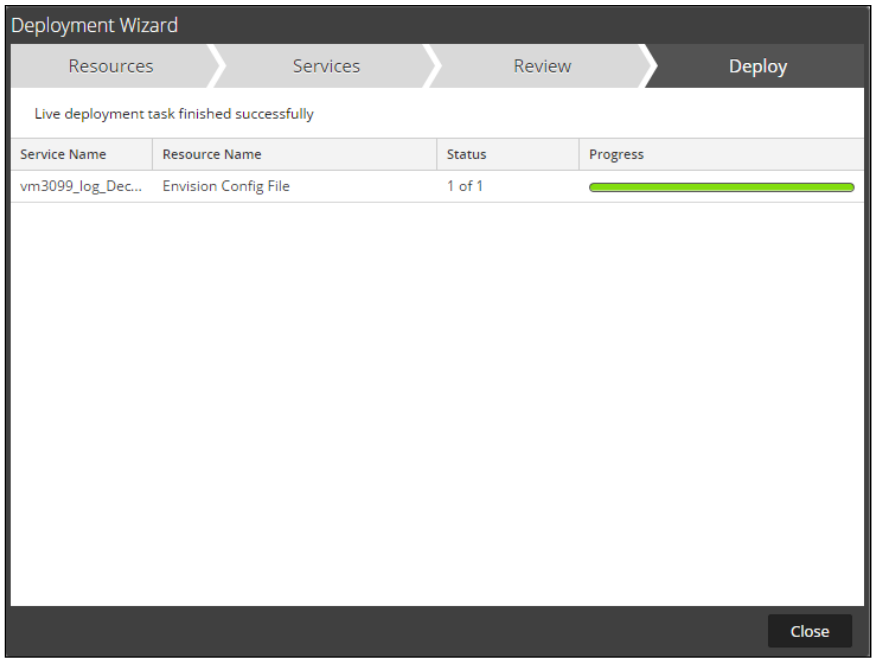


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



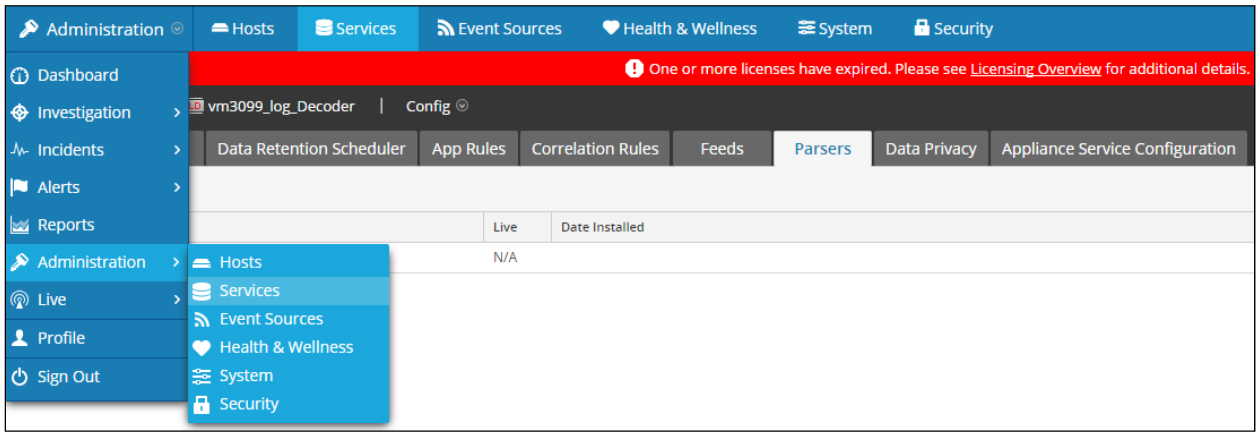
9. Select **Close**, to complete the deployment of the Envision Config file.



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.**



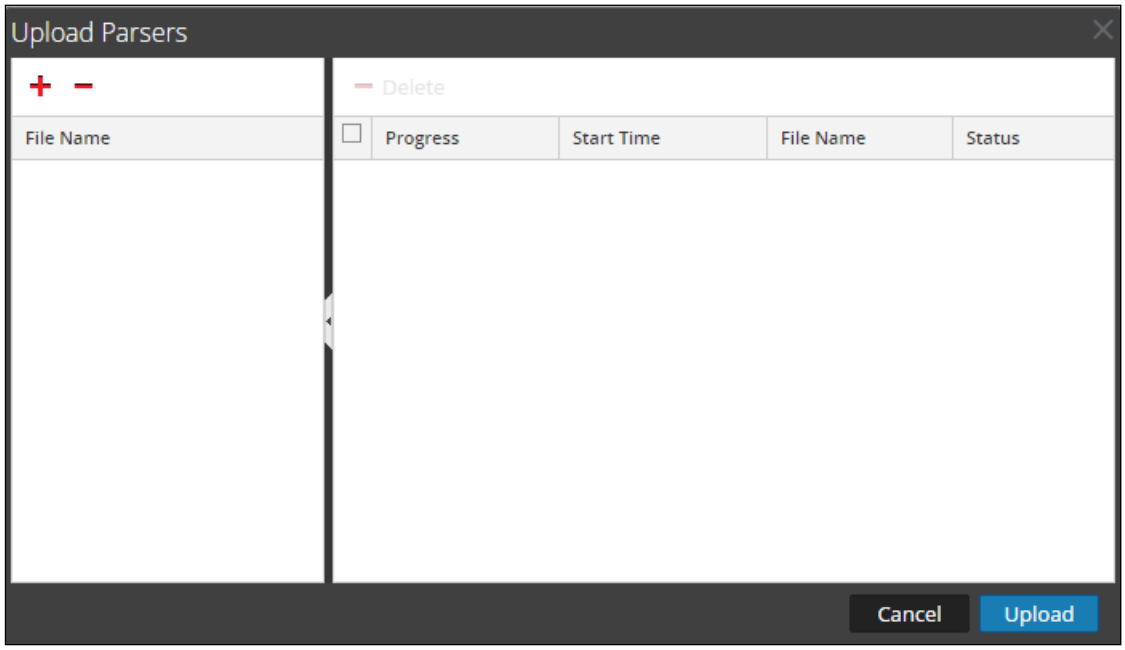
2. Select your Log Decoder from the list, select **View > Config**.

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

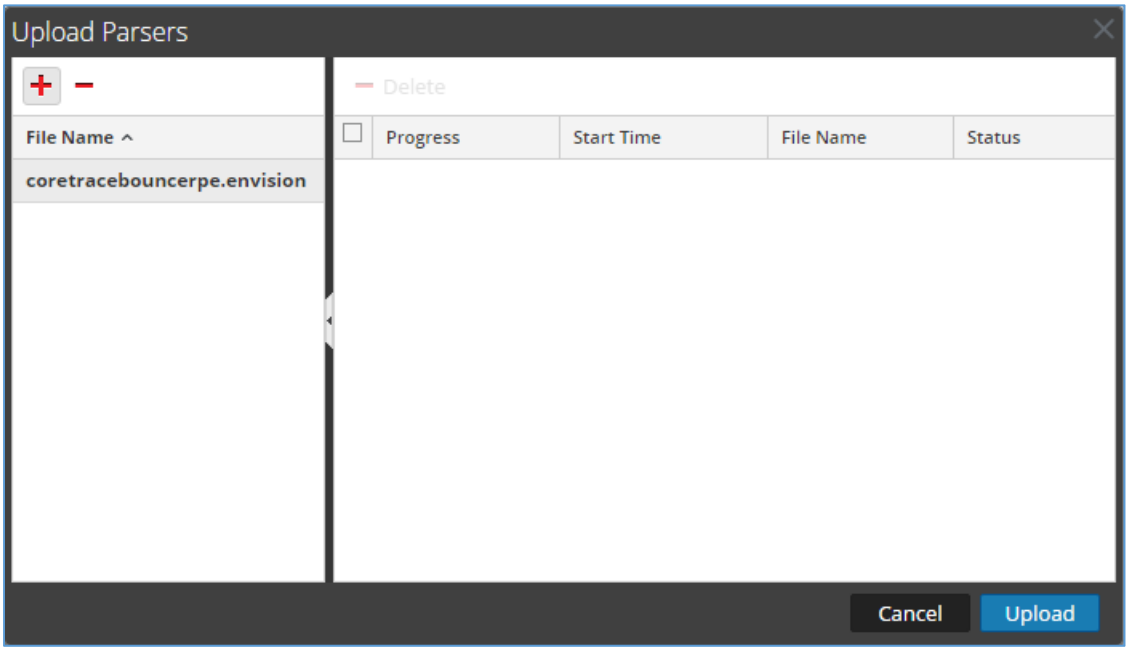
3. Next, select the **Parsers** tab and click the **Upload** button.

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

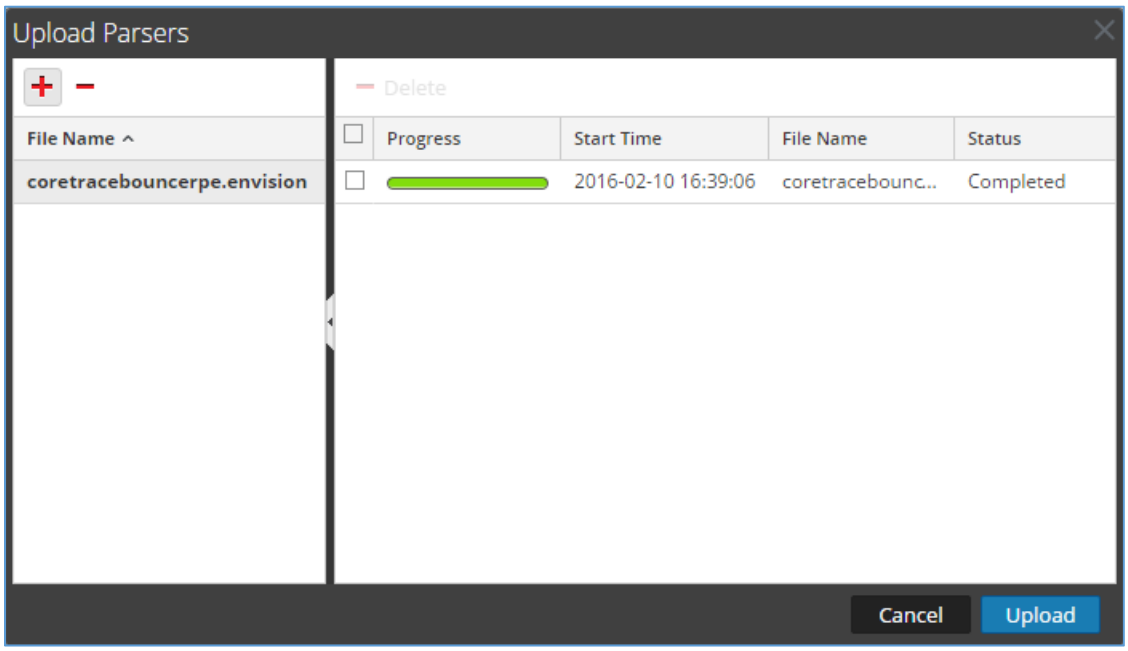
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**



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



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



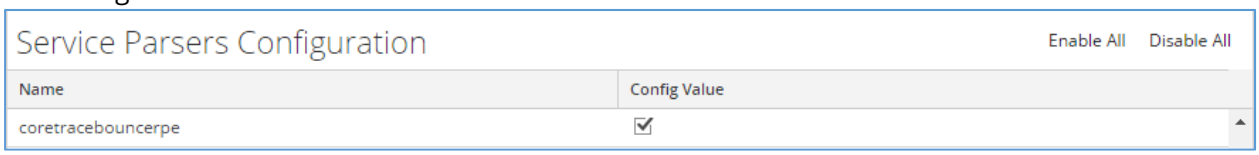
7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the table-map-custom.xml file from the contents of the .zip file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the log decoder(s), enter only the contents between the <mappings>…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

```
<mappings>

        <mapping envisionName="trigger_desc" nwName="trigger.desc" flags="Transient"/>
        <mapping envisionName="info" nwName="index" flags="Transient"/>
        <mapping envisionName="version" nwName="version" flags="Transient"/>
        <mapping envisionName="disposition" nwName="disposition" flags="Transient" envisionDisplayName="Disposition"/>
        <mapping envisionName="application" nwName="server" flags="Transient"/>
        <mapping envisionName="trigger_val" nwName="trigger.val" flags="Transient"/>
        <mapping envisionName="context" nwName="context" flags="Transient"/>

</mappings>
```

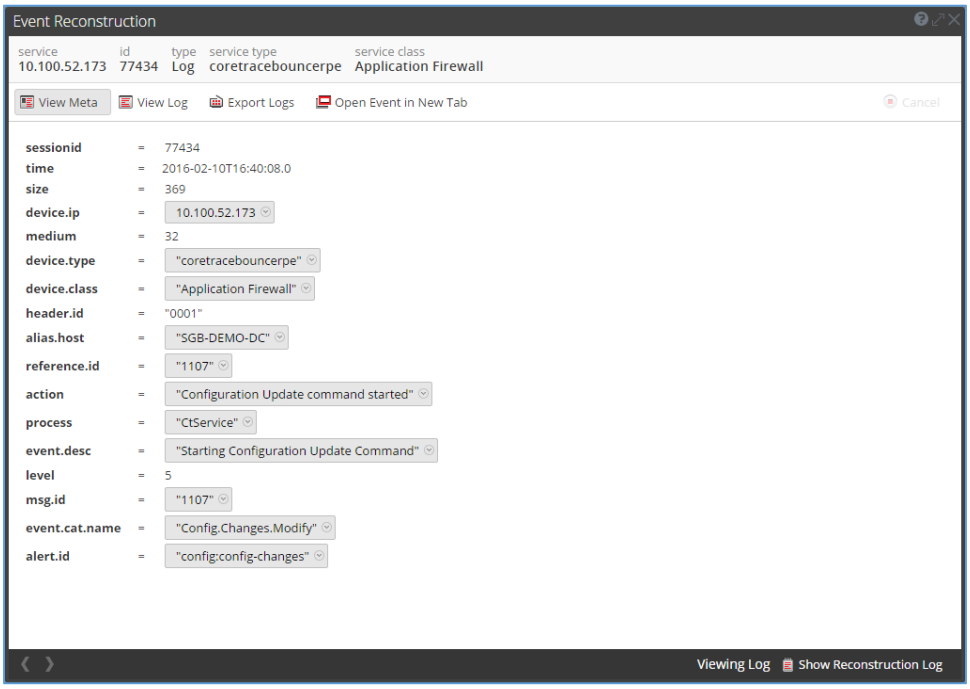
8. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **Restart.**

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.



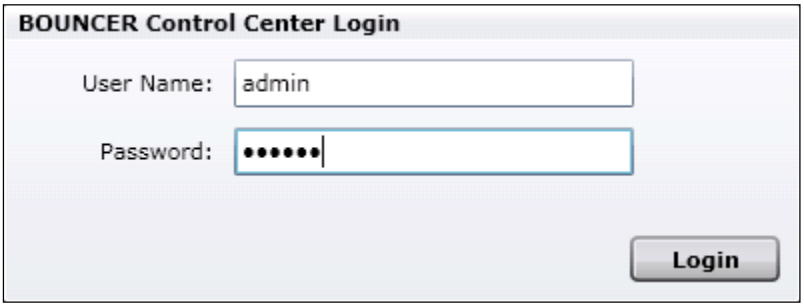
11. The Log Decoder is now ready to parse events for this device. Below is an example of the RSA SA metadata collected from an Absolute DDS logfile.



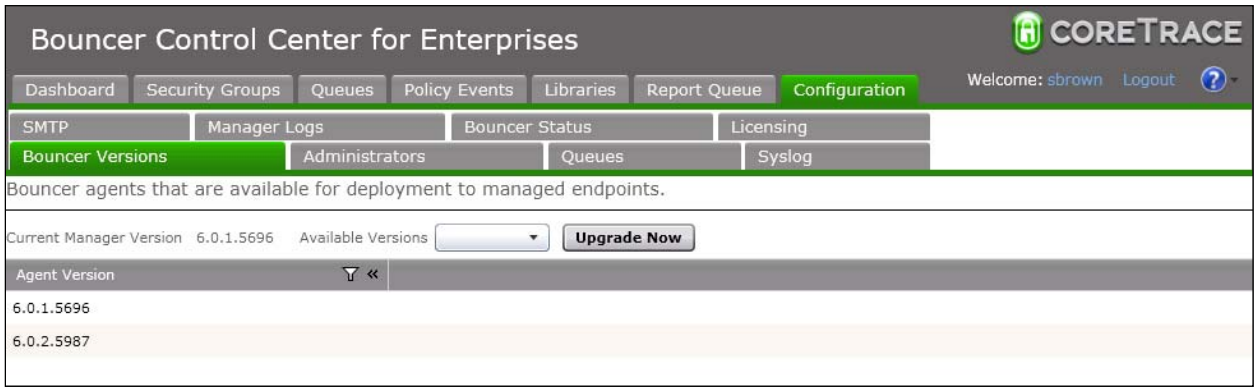
CoreTrace Bouncer Configuration

To configure Bouncer Control Center to send syslog data to Security Analytics, perform the following steps:

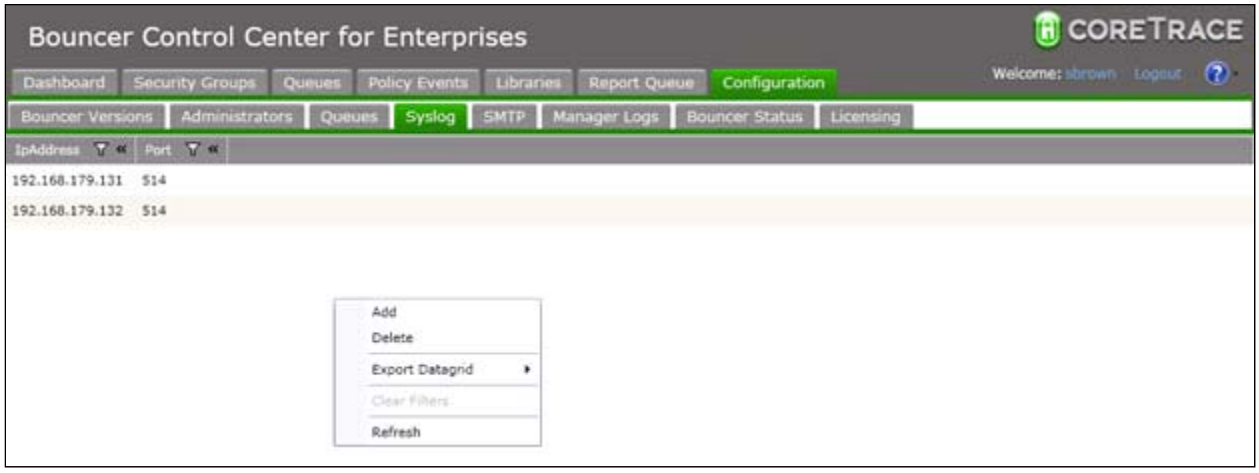
1. Log in to the Bouncer Control Center.



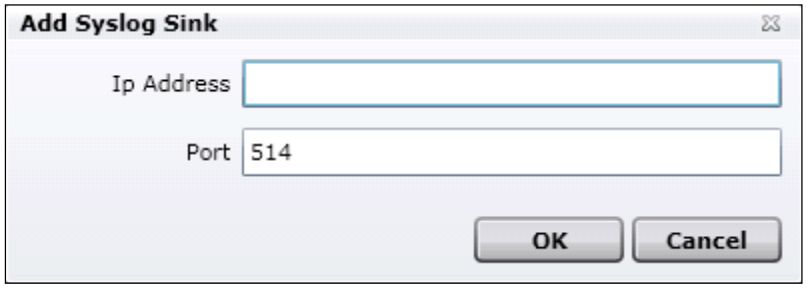
2. Select the **Configuration** tab.



3. Select the **Syslog** sub-tab.
4. Right-click into the whitespace on the page.
5. Select **Add**.



6. Enter the **IP Address** and **Port** number of the SA server. Click **OK**.



7. Click **Save**.

Certification Checklist for RSA Security Analytics

Date Tested: 2/22/2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
CoreTrace Bouncer	6.0.1.5696	Microsoft Windows 2003

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

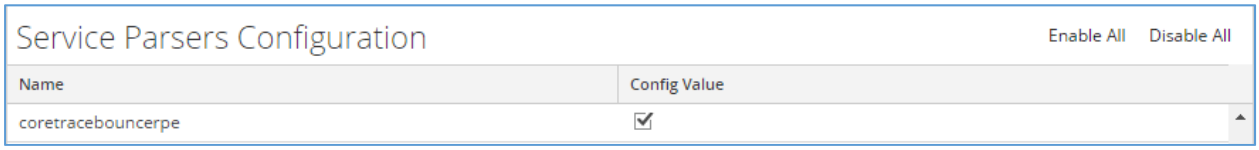
Appendix

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).