Enforcive
Enterprise Security

RSA Security Analytics Ready Implementation Guide

Last Modified: December 9, 2013

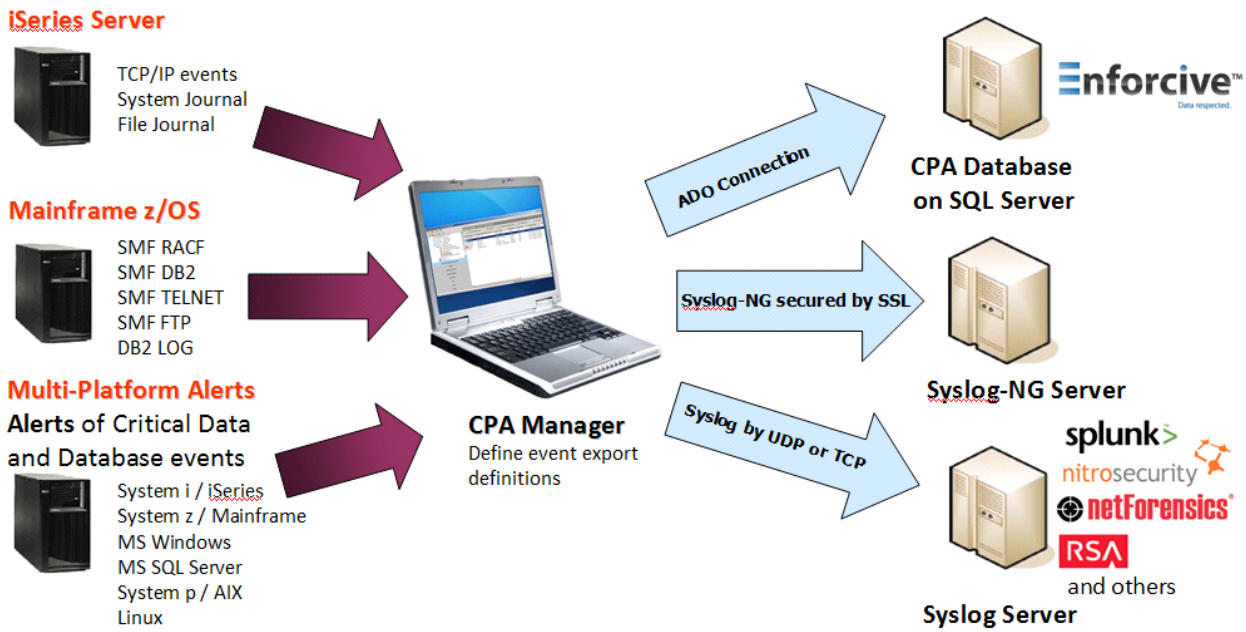
Partner Information

Product Information	
Partner Name	Enforcive
Web Site	www.enforcive.com
Product Name	Enforcive Enterprise Security
Version & Platform	Version: 7.2.1 Platforms: IBM z (Mainframe), IBM i (AS/400), Windows, Linux, AIX, SQL Server
Product Description	Enforcive Enterprise Security is a suite of solutions designed for the securing, monitoring, auditing and management of IBM i, IBM z, Windows, SQL Server, Unix and other platforms. It is aimed at organizations running systems on single or multiple platforms.

Solution Summary

The integration of the Enforcive Enterprise Security solutions suite with RSA Security Analytics provides customers with the ability to monitor and audit user and network activity as well system, file and database changes on multiple platforms, including the complex IBM z (Mainframe). This provides centralization of the log management and ability to correlate events from different systems which becomes a critical part of the organization's IT security program.

RSA Security Analytics Features	
Enforcive Enterprise Security 7.2.1	
Integration package name	enforcivepe.zip
Device display name within Security Analytics	enforcivepe
Event source class	Access
Collection method	Syslog



Release Notes

Release Date	What's New In This Release
12/9/2013	Initial support for Enforcive Enterprise Security.

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.

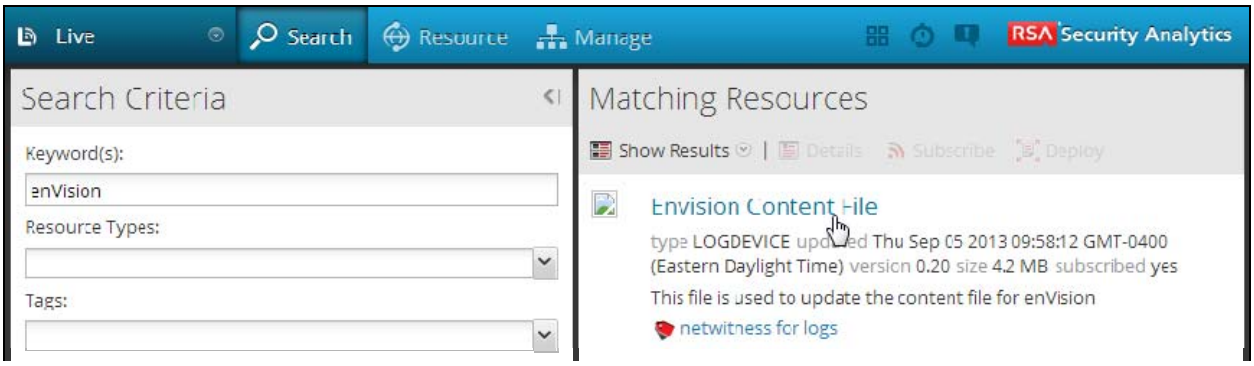
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
enforiceivepe.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: ***enVision variable name --> SA variable name --> SA variable type***

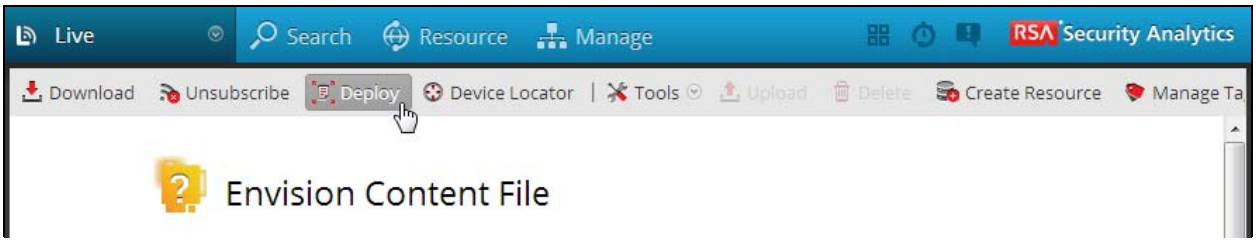
Deploy enVision Content File

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:

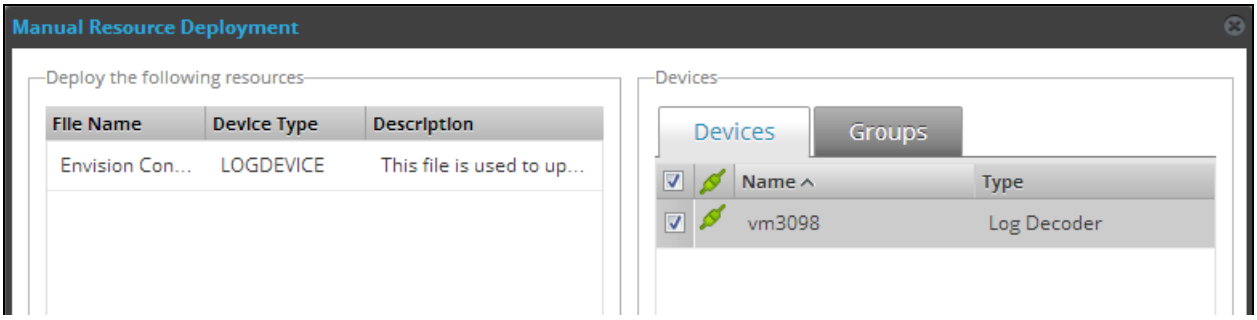
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Click on **Envision Content File**.



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.

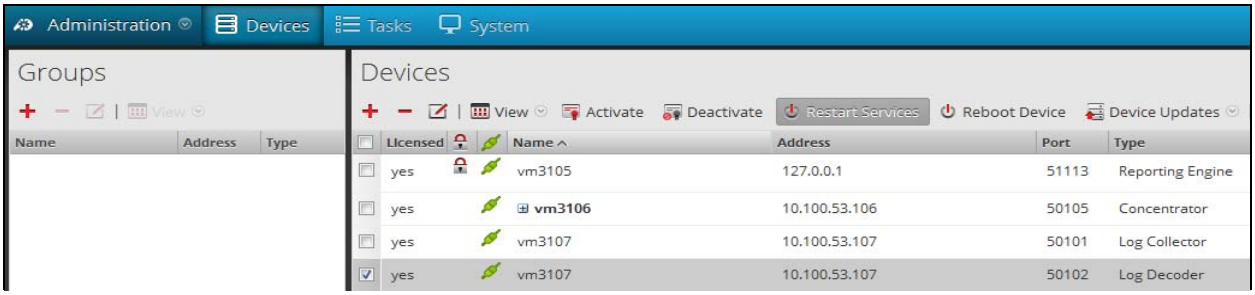
Deploy Security Analytics Integration Package

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:

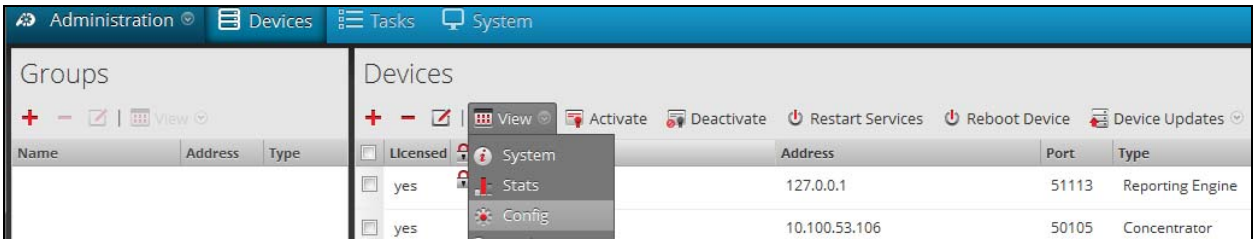
1. From the Security Analytics menu, select **Administration > Devices.**
2. Select your Log Decoder from the list, select **View > Config**.

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

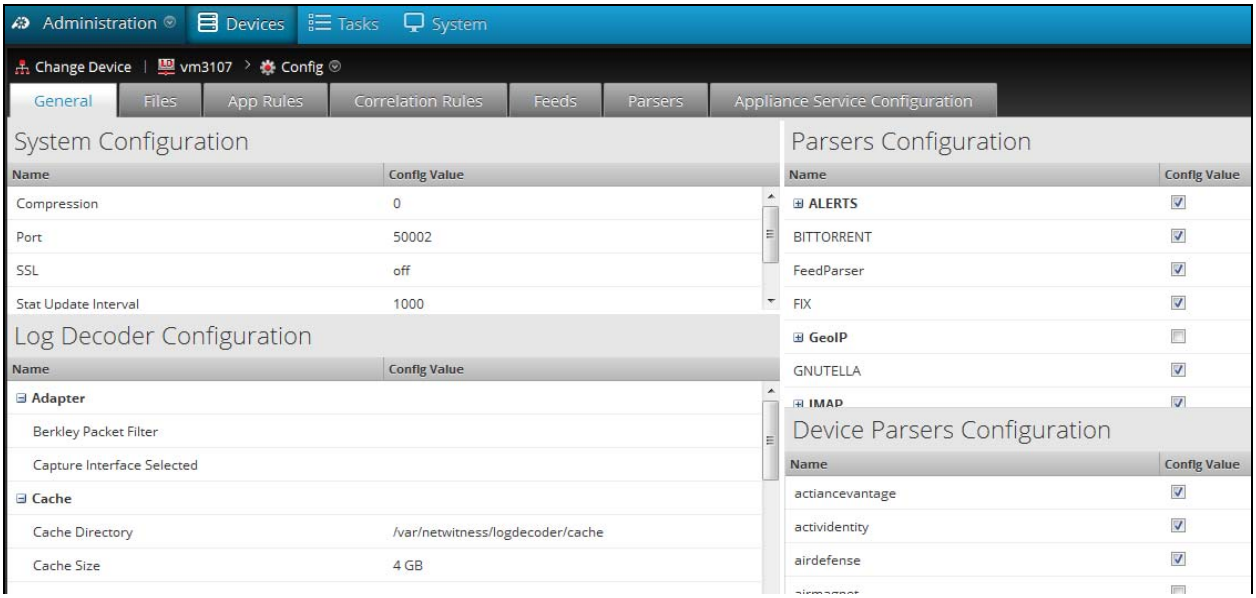
3. Next, select the **Parsers** tab and click the **Upload** button.
4. From the *Upload Parsers* window, click the **Add** button and select the *.envision* file.
5. Under the file name column, select the integration package name and click **Upload**.
6. Navigate to **Administration > Devices** and check the **Log Decoder** than click **Restart Services.**



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



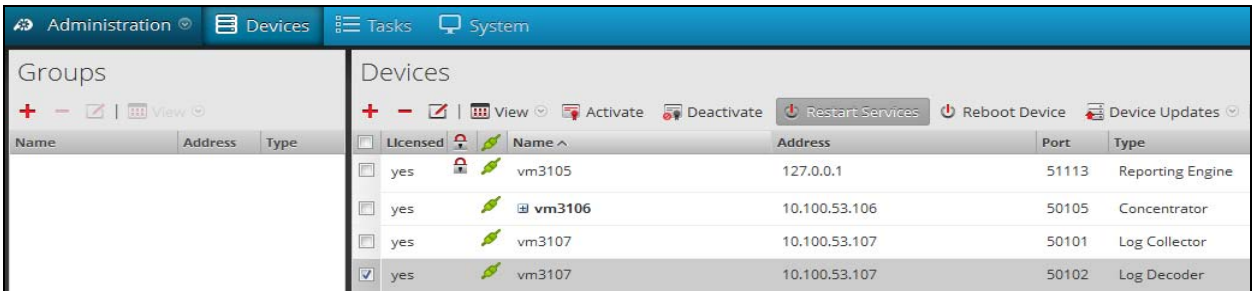
8. The new device will automatically be listed under **General > Device Parsers Configuration**.



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-customer.xml** file does not exist, copy the index-concentrator-custom.xml from the Integration zip file to this directory.
   If the index-concentator-custom.xml file already exists then append the content to the existing file.
4. Navigate to **Administration > Devices** and check the **Log Decoder** than 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**.

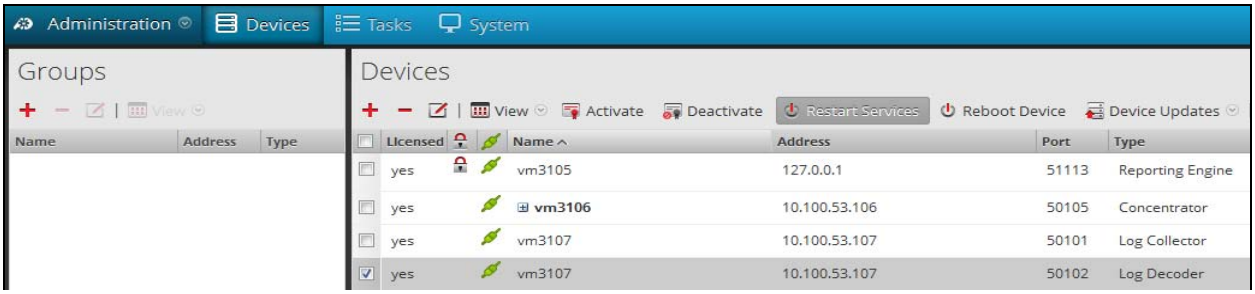
3. Use the name fields in the index-concentrator-custom.xml file to determine the list of attributes which need to be modified in the table-map.xml file.
4. Copy the **table.map.xml** from**/etc/netwitness/ng/envision/etc** to **/etc/netwitness/ng/envision**.
5. Open **/etc/netwitness/ng/envision/table.map.xml** 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" format="IPv4" flags="None" />
        <mapping envisionName="device.type" nwName="device.type" flags="None" />
        <mapping envisionName="device.type.id" nwName="device.type.id" format="Int32" 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="wrap" nwName="wrap" 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>
```

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



7. 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 Enforcive Enterprise Security with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

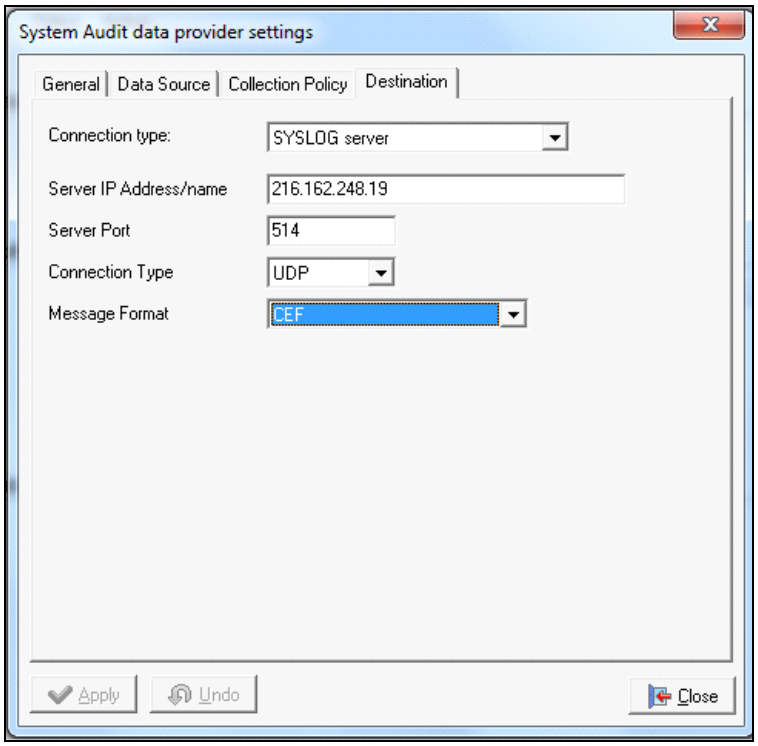
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Enforcive Enterprise Security components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Enforcive Enterprise Security Configuration

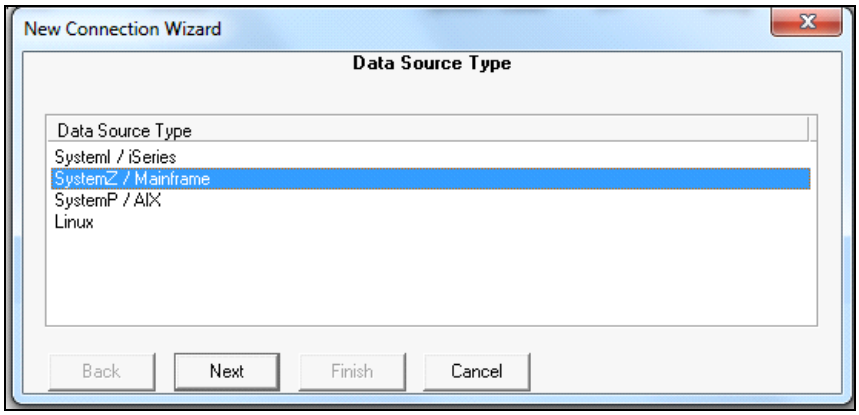
IBM i (AS/400) data providers

1. After logging in to Enforcive Enterprise Security Manager on the System i, enter the System i Data Providers module. Choose a data provider type and click **Change settings**.
2. On the **Destination** tab, define the required SYSLOG server details.

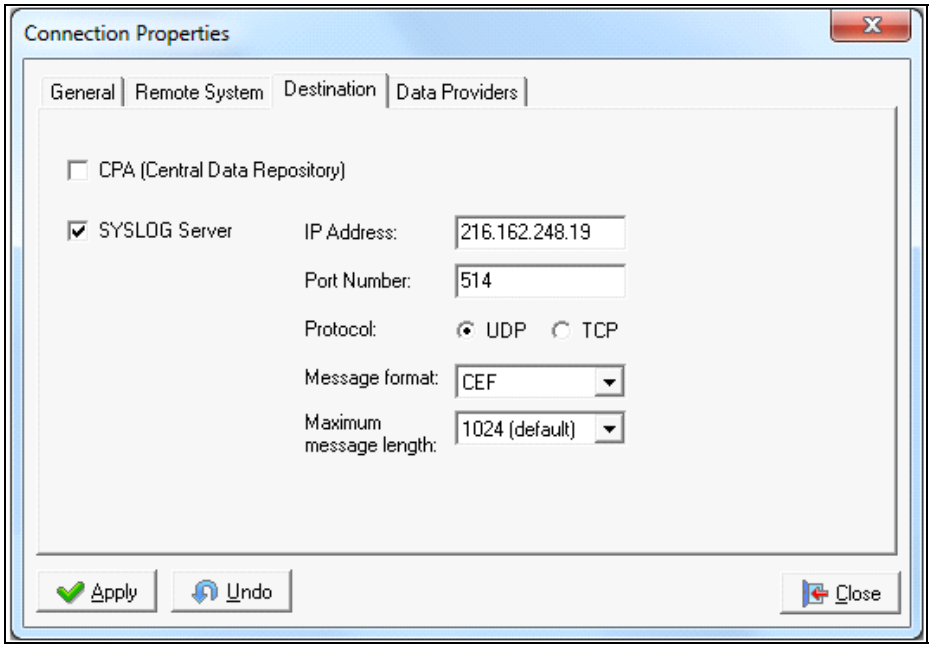


IBM z (Mainframe) Remote Collection Service

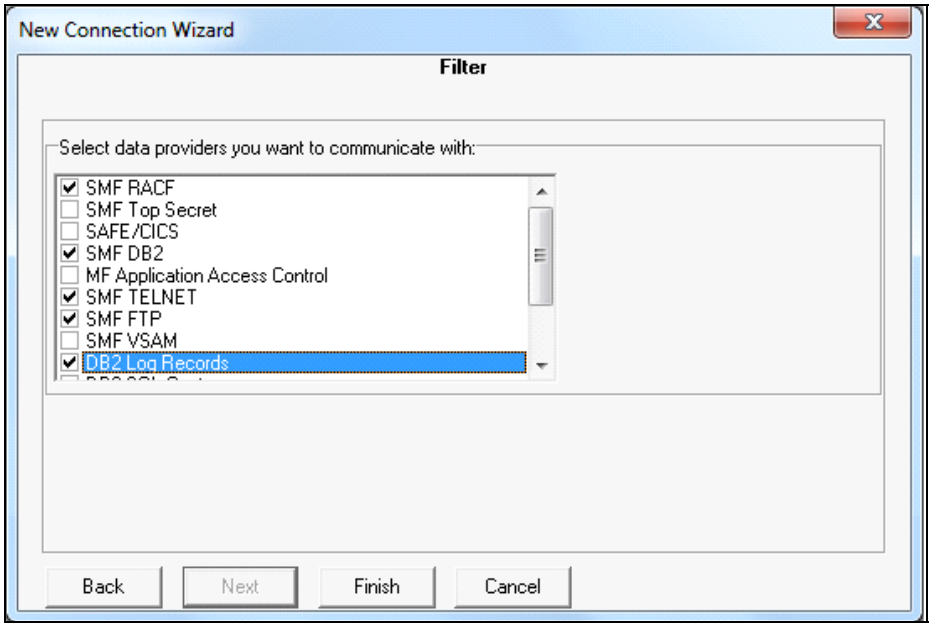
3. After logging in to Central Management System, select **Cross Platform Audit** module and then choose **Remote Collection Service.** Click **Add Connection**, choose **SystemZ / Mainframe** from the Data Source Type list and click **Next** to continue the wizard.



4. After choosing a specific remote system, continue the wizard until you get to the Destination window. Check the SYSLOG Server option and enter the required SYSLOG server definitions. Click **Next** to continue.

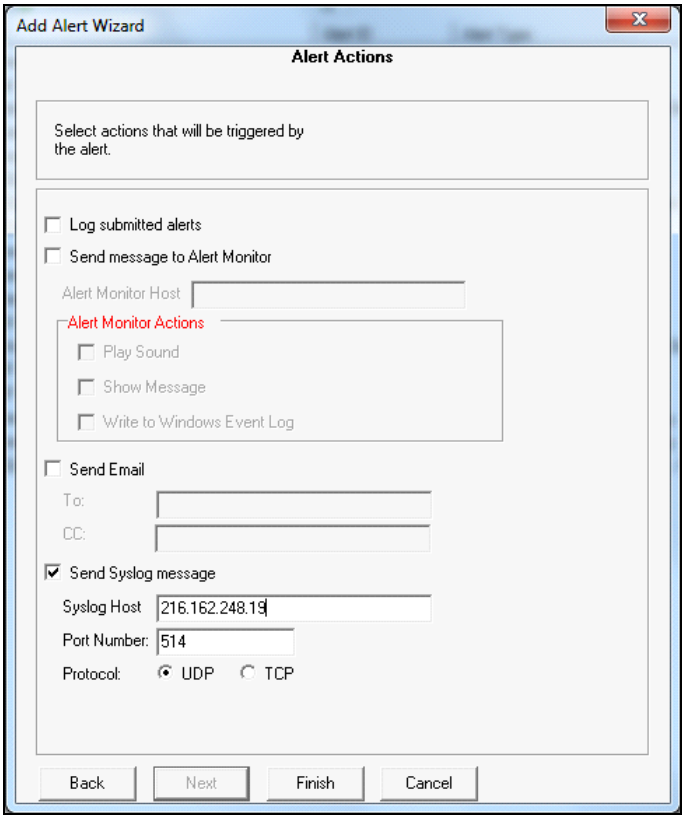


5. On the Filter window, choose one or more of the following applications to be sent to your SYSLOG server.



Multi-system Alerts

6. After logging in to the Central Management System, select **Cross Platform Audit** module and then choose **CPA Alerts**. Click **Add Alert**, choose an alert type and click **Next** to continue the wizard.



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
Enforcive Enterprise Security	7.2	IBM z (Mainframe), IBM i (AS/400), Windows, Linux, AIX, SQL Server

Security Analytics Test Case	Result
Device Administration	
Partners 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	✓

DRP / PAR

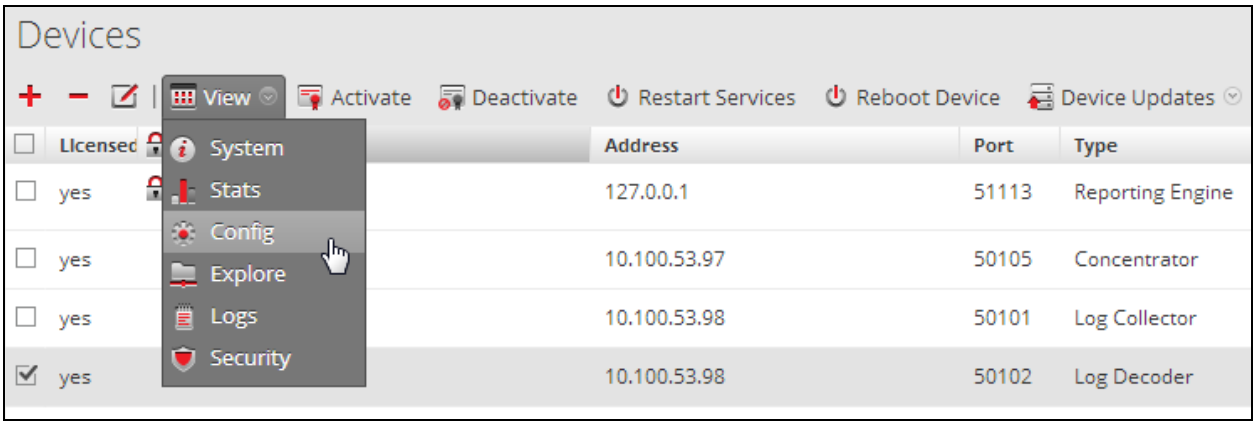
✓ = Pass ✗ = Fail N/A = Non-Available Function

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.