Array Networks

SPX Series Universal Access Controllers

RSA Security Analytics Ready Implementation Guide

Last Modified: December 2nd, 2013

Partner Information

Product Information	
Partner Name	Array Networks
Web Site	www.arraynetworks.net
Product Name	SPX Series Universal Access Controllers
Version & Platform	8.4.6
Product Description	Engineered from the ground up for high-performance universal secure access, Array Networks SPX Series Universal Access Controllers provide secure access to networks, applications and data for any class of user, on any device in any location. Using end-point security, server-side security and encryption for data in motion, the SPX Series holds all users to the same security standards regardless of whether they are employees, partners or visitors located inside or outside the corporate network. Whether at corporate headquarters, a branch office, home, a wireless hotspot or on the go, users can quickly and easily use PCs, laptops, smart phones and tablets to quickly and easily access email, file shares and applications.

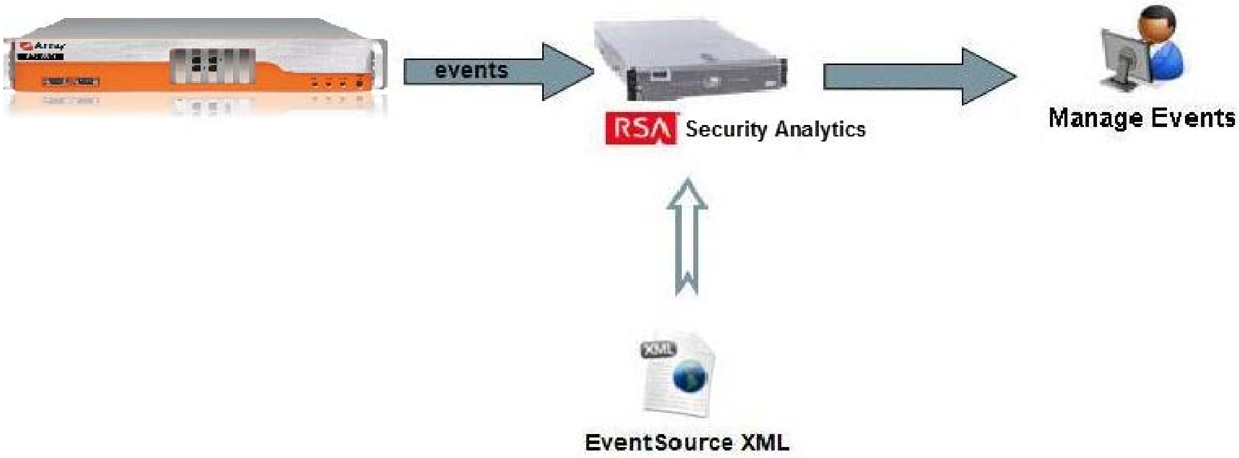
Solution Summary

Integrating Array Networks SPX Series Universal Access Controllers with RSA's enVision involves directing the SPX's logs to the Security Analytics server.

```
Format:  log host <IP_of_SA_server> <destination_port> <protocol>
Example: log host 10.10.39.60 514 udp
```

The Array Networks SPX Series Universal Access Controllers paired with RSA Security Analytics allows customers to monitor, provide compliance reports for government and industry regulations and perform forensic analysis of logs generated. Additional benefits include tracking user activity and detecting anomalous behavior.

RSA Security Analytics Features	
Array SPX 8.4.6	
Integration package name	arrayspxpe.zip
Device display name within Security Analytics	arrayspxpe
Event source class	VPN
Collection method	Syslog



Release Notes

Release Date	What's New In This Release
12/02/2013	Initial SA support for Array SPX

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 Implementation Guide.

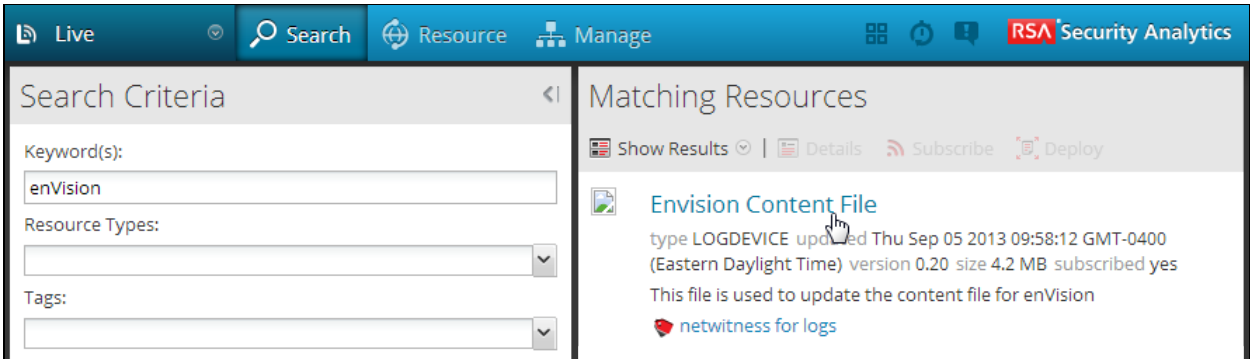
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
arrayspxpe.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**.



Keyword(s): enVision

Resource Types:

Tags:

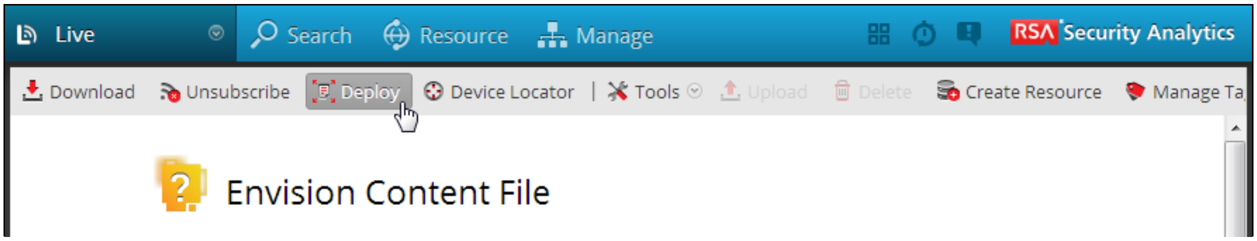
Envision Content File

type LOGDEVICE updated Thu Sep 05 2013 09:58:12 GMT-0400 (Eastern Daylight Time) version 0.20 size 4.2 MB subscribed yes

This file is used to update the content file for enVision

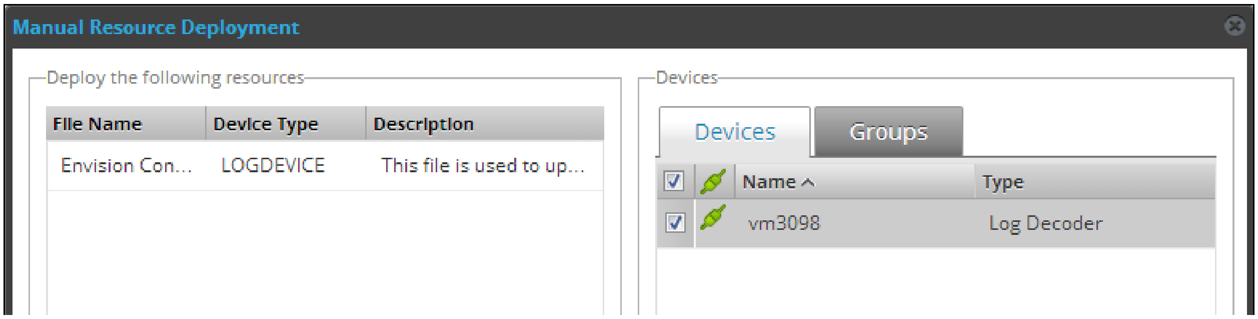
netwitness for logs

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



Envision Content File

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



File Name	Device Type	Description
Envision Con…	LOGDEVICE	This file is used to up…

☑	Name ^	Type
☑	vm3098	Log Decoder

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

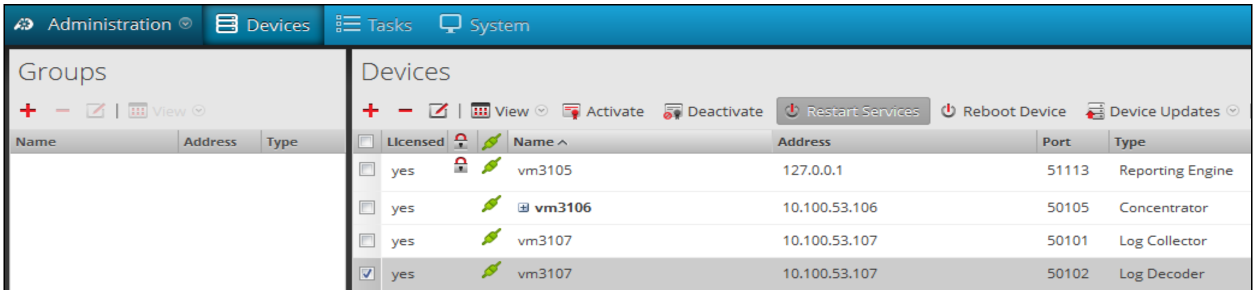
Deploy Security Analytics Integration Package

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**.

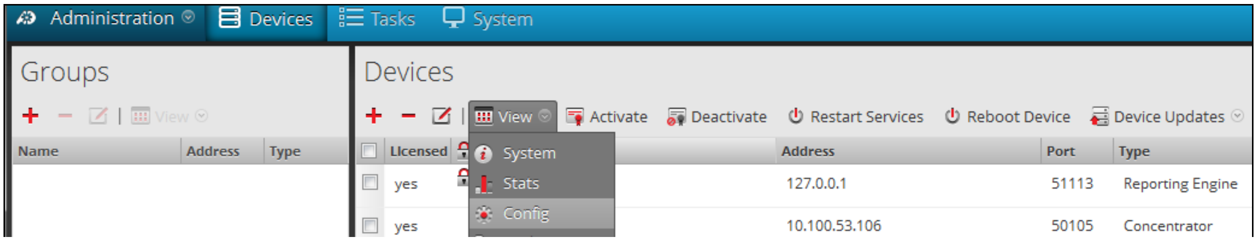
> **Note: In an environment with multiple Log Decoders, deploy the Integration Package on each Log Decoder that will use the new device.**

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.**



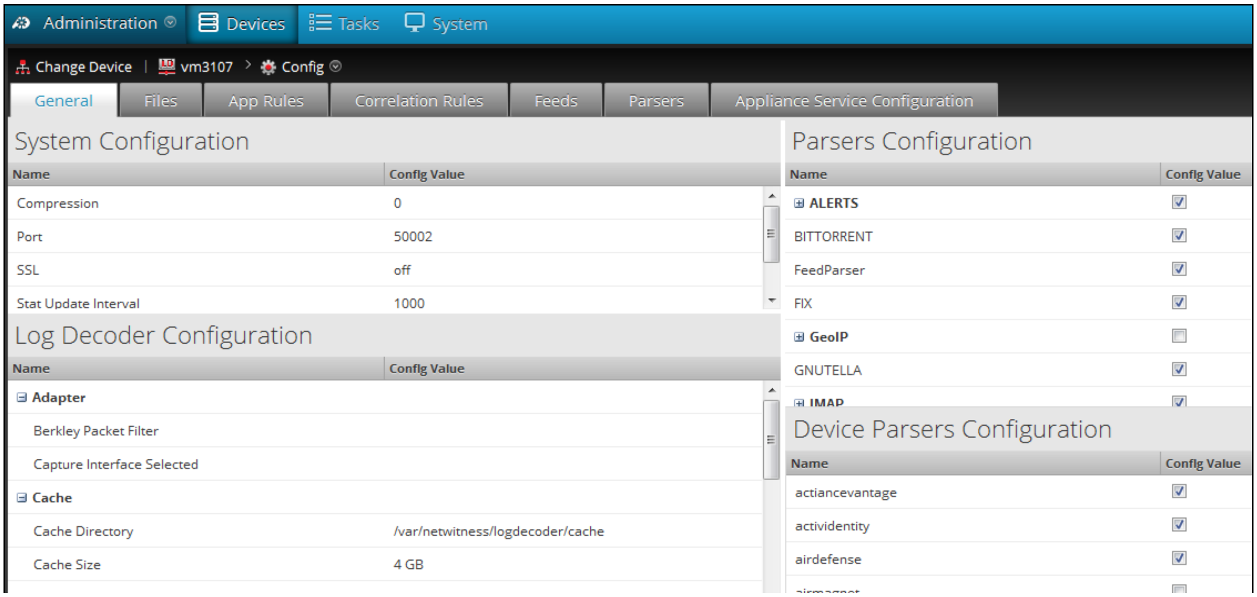
☐	Licensed	Name	Address	Port	Type
☐	yes	vm3105	127.0.0.1	51113	Reporting Engine
☐	yes	⊞ **vm3106**	10.100.53.106	50105	Concentrator
☐	yes	vm3107	10.100.53.107	50101	Log Collector
☑	yes	vm3107	10.100.53.107	50102	Log Decoder

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



☐	Licensed	Address	Port	Type
☐	yes	127.0.0.1	51113	Reporting Engine
☐	yes	10.100.53.106	50105	Concentrator

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



System Configuration

Name	Config Value
Compression	0
Port	50002
SSL	off
Stat Update Interval	1000

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkley Packet Filter	
Capture Interface Selected	
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB

Parsers Configuration

Name	Config Value
⊞ ALERTS	☑
BITTORRENT	☑
FeedParser	☑
FIX	☑
⊞ GeoIP	☐
GNUTELLA	☑
⊞ IMAP	☑

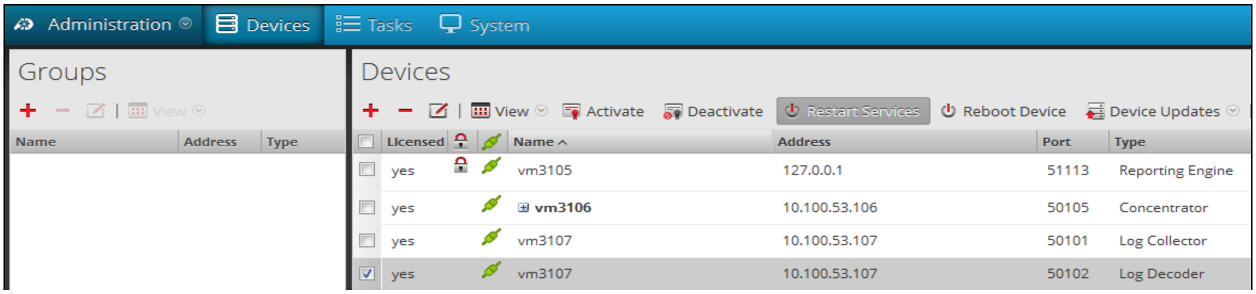
Device Parsers Configuration

Name	Config Value
actiancevantage	☑
actividentity	☑
airdefense	☑
airmagnet	☐

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.**



Groups

Name	Address	Type

Devices

☐	Licensed			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

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" />
```

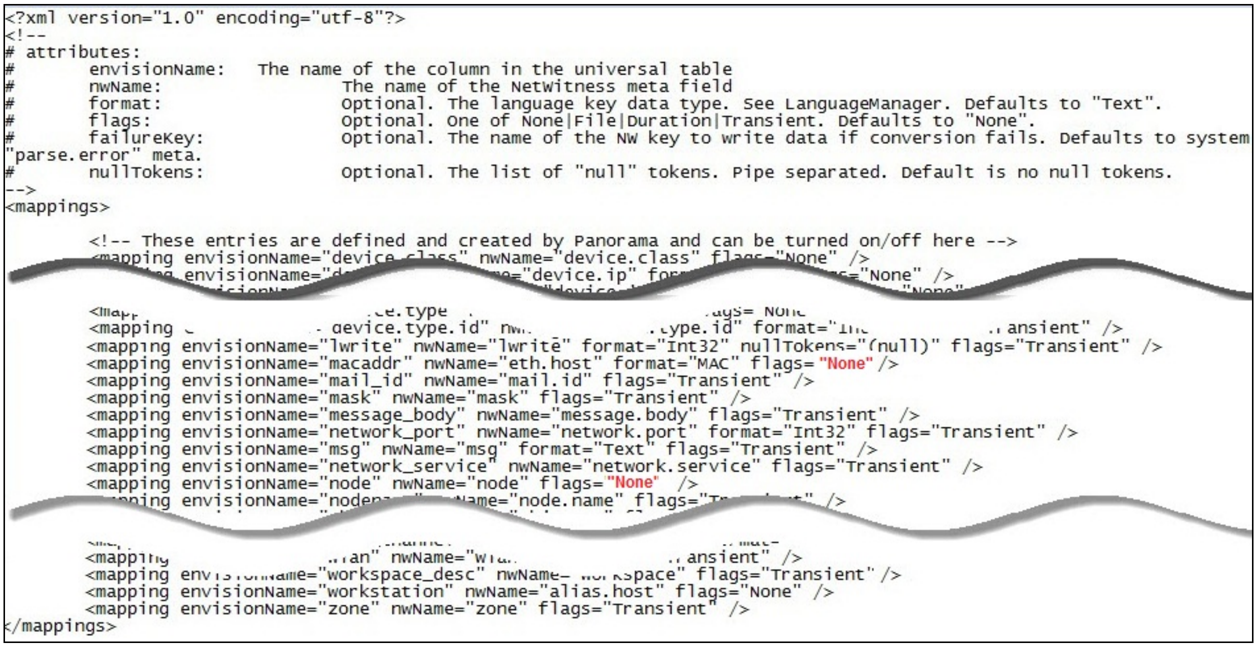
Modify the table-map.xml

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.

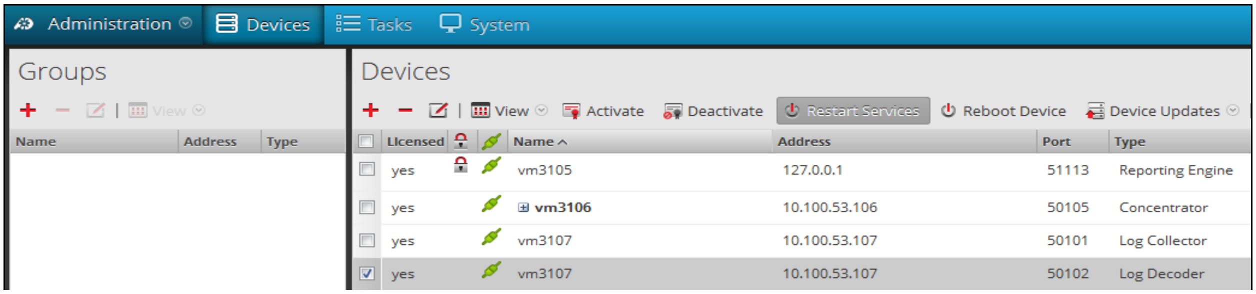
The below table-map.xml maps is an example of the enVision attribute **macaddr** and **node** mapped to the correlated NetWitness attribute, with the flag field modified to **None**.



```
<?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="d        e="device.ip" for              ="None" />
        <mapping device.type.id" nw            .type.id" format="Int        ansient" />
        <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="noden      Name="node.name" flags="T        t" />
        <mapping        an" nwName="wl             ansient" />
        <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.**



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

Partner Product Configuration

Before You Begin

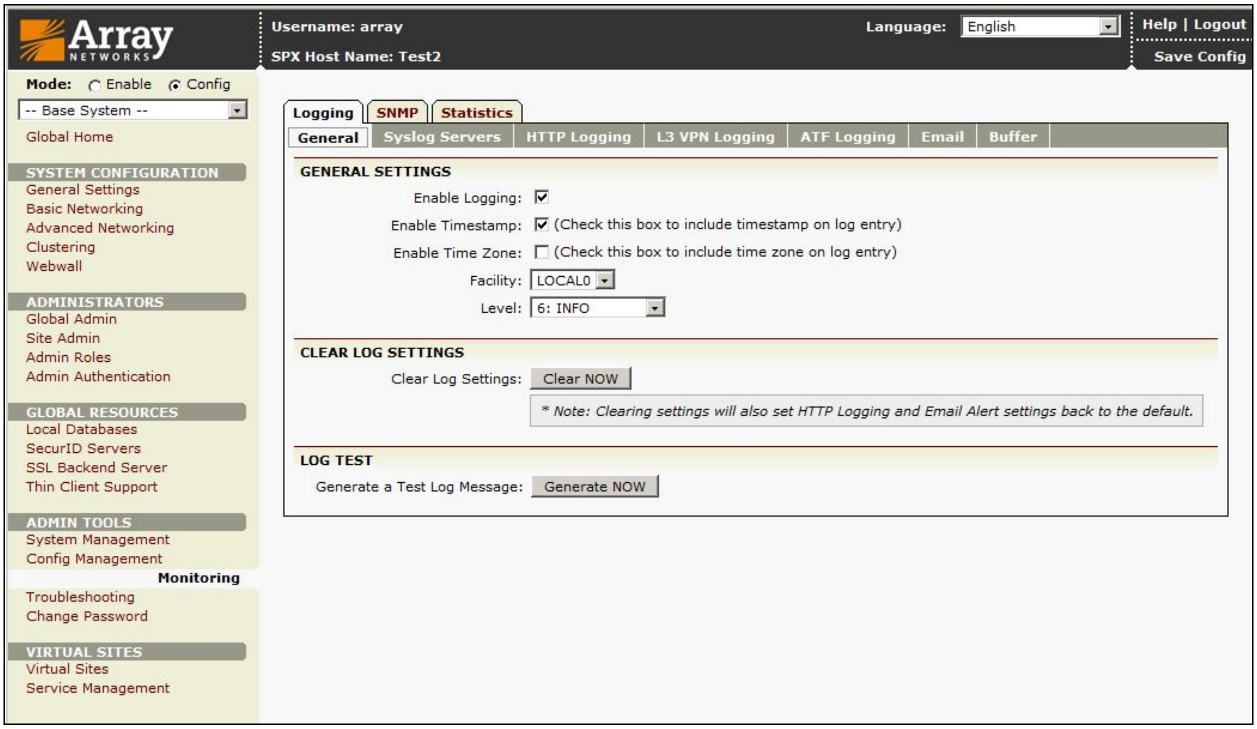
This section provides instructions for configuring the Array Networks SPX with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

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 Array Networks components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Array SPX Configuration

1. Login to the WebUI.
2. Select **Monitoring** from the column on the left.
3. Select **Enable Logging**. If the check box is grayed out, enter *Config* mode by clicking the **Config** radio button in the upper left corner.



Username: array
SPX Host Name: Test2
Language: English

Mode: ○ Enable ● Config

GENERAL SETTINGS

Enable Logging: ☑
Enable Timestamp: ☑ (Check this box to include timestamp on log entry)
Enable Time Zone: □ (Check this box to include time zone on log entry)
Facility: LOCAL0
Level: 6: INFO

CLEAR LOG SETTINGS

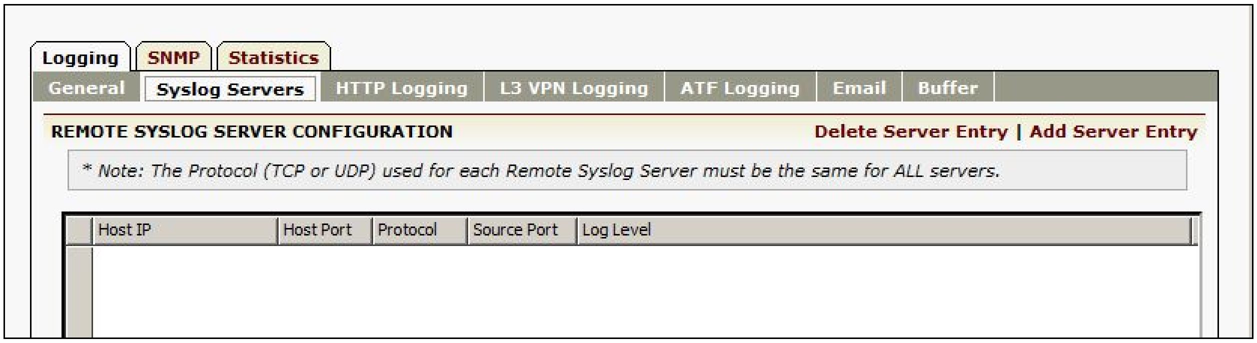
Clear Log Settings: Clear NOW

** Note: Clearing settings will also set HTTP Logging and Email Alert settings back to the default.*

LOG TEST

Generate a Test Log Message: Generate NOW

4. Navigate to **Logging > Syslog Servers** and click **Add Server Entry**.

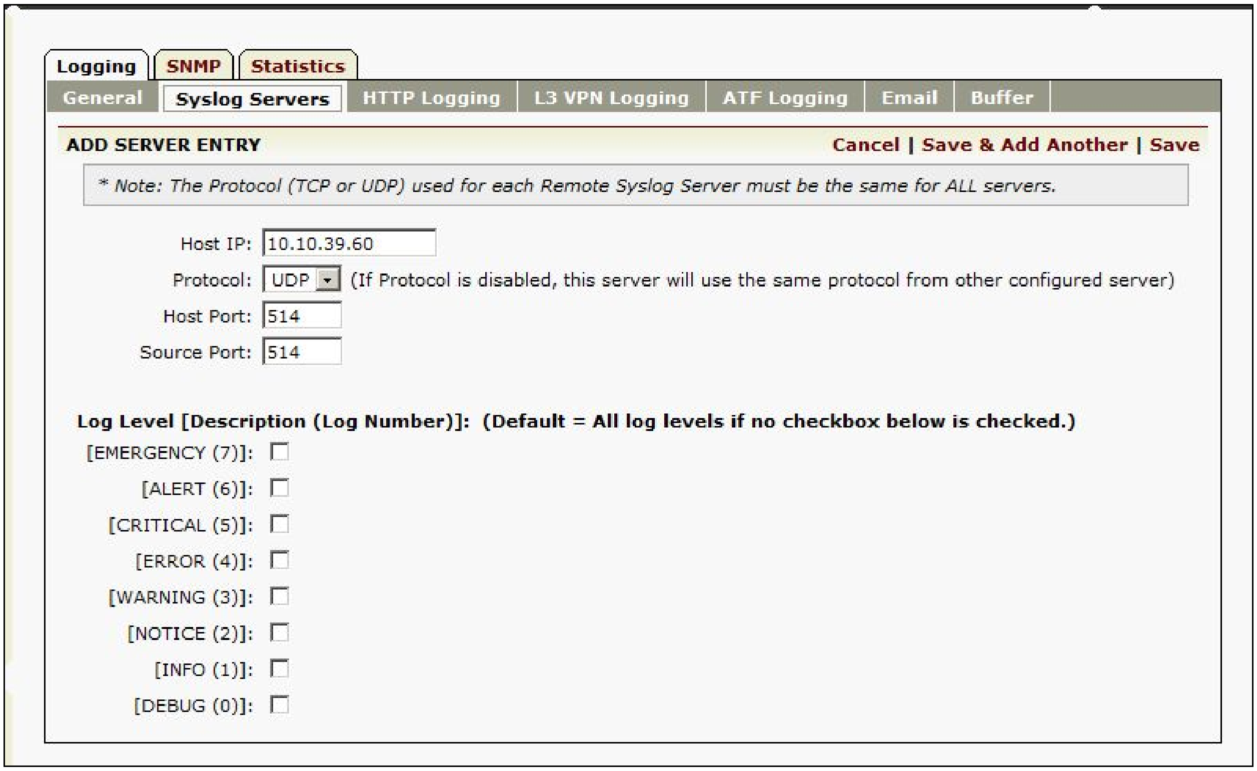


REMOTE SYSLOG SERVER CONFIGURATION

* Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.

Host IP	Host Port	Protocol	Source Port	Log Level

5. Enter the **Host IP** and **Host Port** information of the Security Analytics log server. Select the log levels or leave all the boxes unchecked to enable all log levels.



ADD SERVER ENTRY

* Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.

Host IP: 10.10.39.60

Protocol: UDP (If Protocol is disabled, this server will use the same protocol from other configured server)

Host Port: 514

Source Port: 514

Log Level [Description (Log Number)]: (Default = All log levels if no checkbox below is checked.)

[EMERGENCY (7)]: □

[ALERT (6)]: □

[CRITICAL (5)]: □

[ERROR (4)]: □

[WARNING (3)]: □

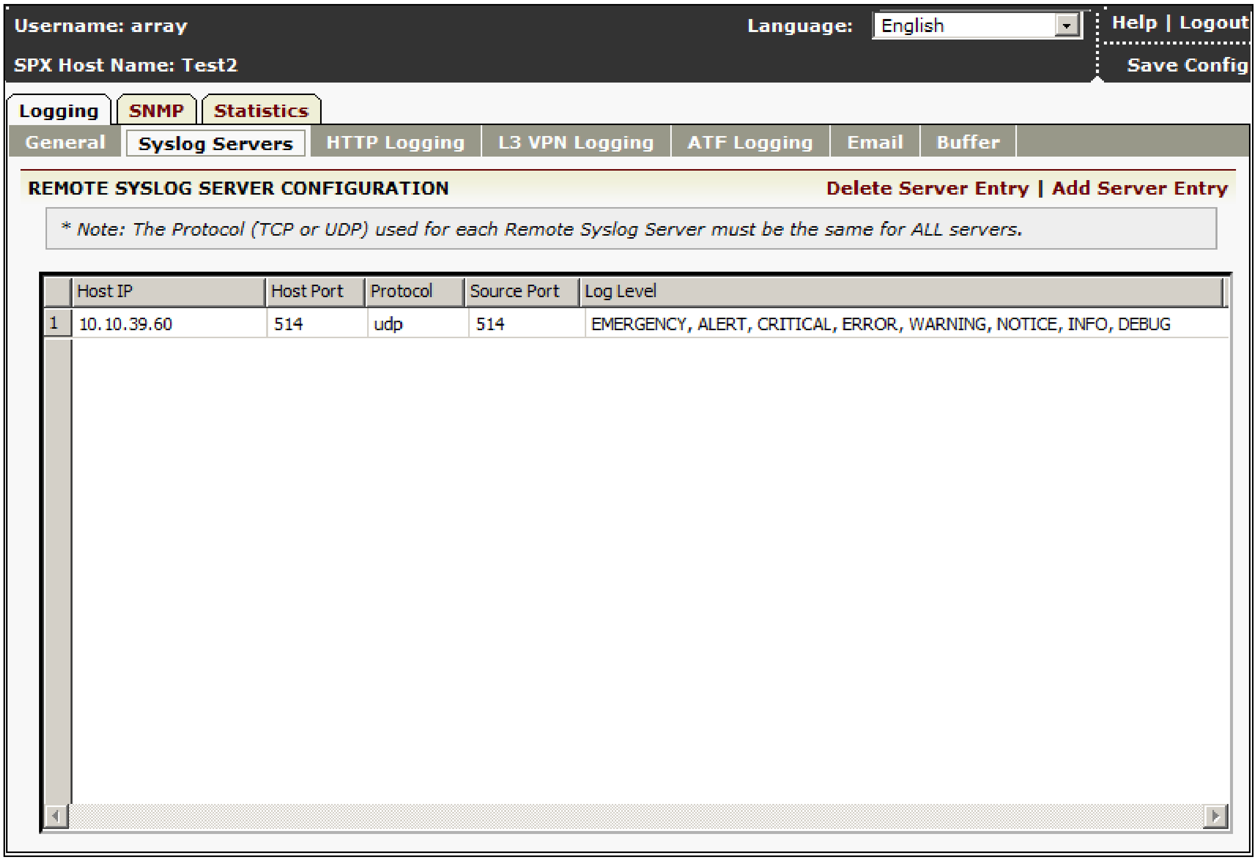
[NOTICE (2)]: □

[INFO (1)]: □

[DEBUG (0)]: □

6. Click **Save**.

7. The Security Analytics server will now appear in the list.



Username: array

SPX Host Name: Test2

Language: English

REMOTE SYSLOG SERVER CONFIGURATION

* Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.

	Host IP	Host Port	Protocol	Source Port	Log Level
1	10.10.39.60	514	udp	514	EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG

8. Click **Save Config** to commit the changes made to the configuration to memory.

Note: The previous configuration may also be configured via the Command Line Interface (CLI). Refer to Appendix A.

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
Array Network SPX Series	8.4.6	Proprietary

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	✓

JJO / PAR

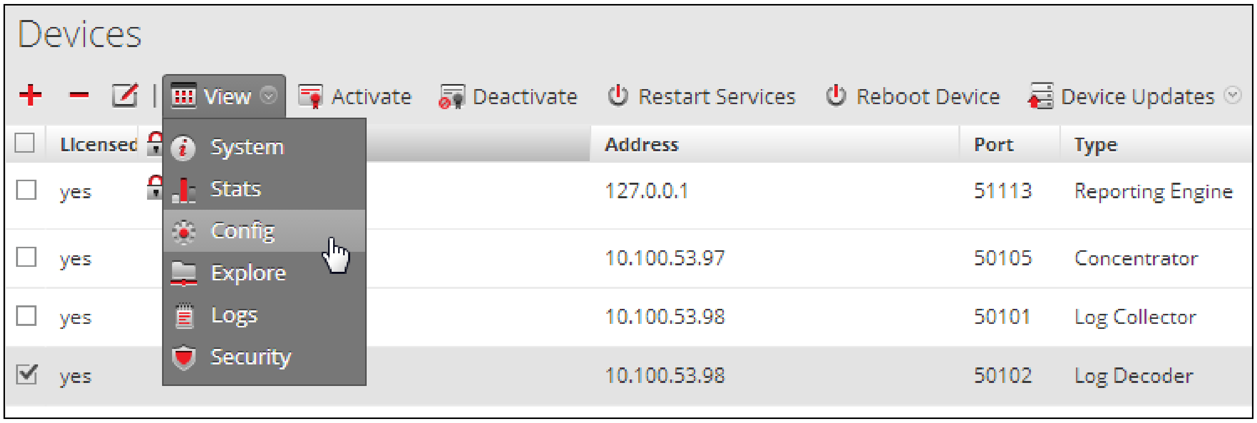
✓ = Pass ✗ = Fail N/A = Non-Available Function

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.**



Devices

□	Licensed	Address	Port	Type
□	yes	127.0.0.1	51113	Reporting Engine
□	yes	10.100.53.97	50105	Concentrator
□	yes	10.100.53.98	50101	Log Collector
☑	yes	10.100.53.98	50102	Log Decoder

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.

Appendix A

Array SPX CLI Configuration

```
Test2>enable
Test2# configure terminal
Test2(config)#log on
Test2(config)#log host 10.10.39.60 514 udp 514
Test2(config)#write memory
```