

RSA Ready Implementation Guide for **RSA** | Security Analytics

Array Networks SPX Series Universal Access Controllers 8.4.6

Daniel Pintal, RSA Partner Engineering
Last Modified: February 16, 2016

RSA
READY

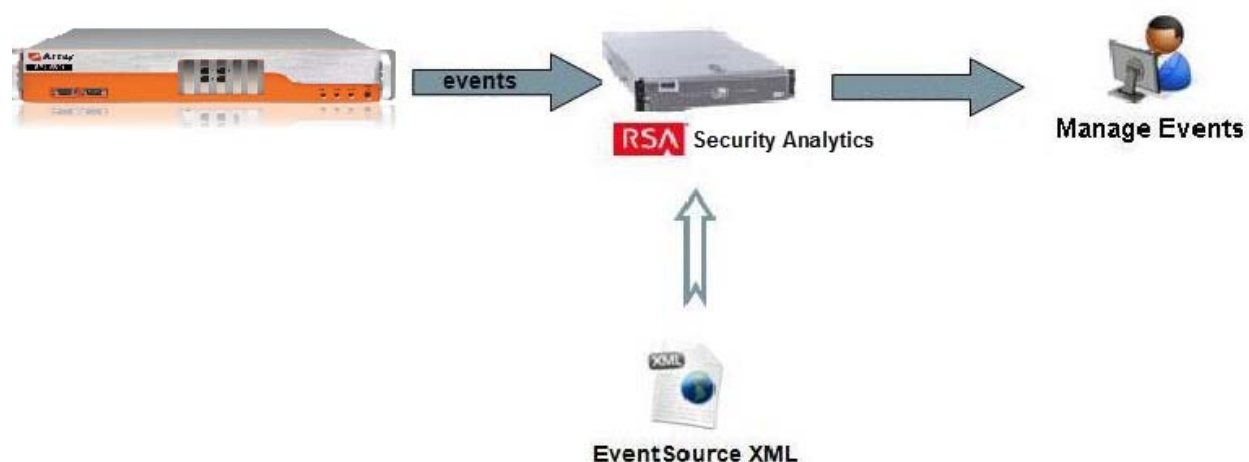
Solution Summary

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.envision |
| Device display name within Security Analytics | arrayspxpe |
| Event source class | VPN |
| 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 |
|-----------------------------|---|
| arrayspxpe.envision | SA package deployed to parse events from device integrations. |
| arrayspxpemsg.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 Array Networks. |
| 2/4/2016 | SA 10.5 support |
| | |

RSA Security Analytics 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.

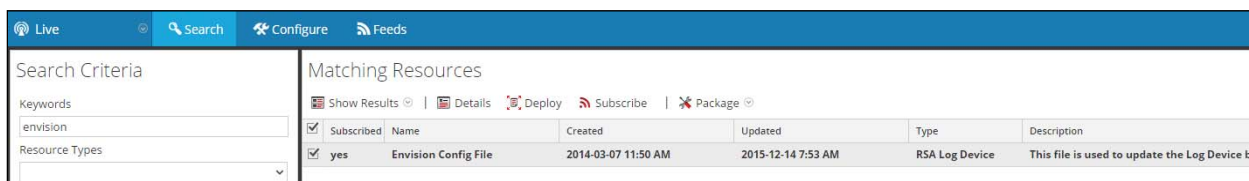
! > Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure <Partner> <Product> is properly configured and secured before deploying to a production environment.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



| Live Search Configure Feeds | | | | | | |
|-----------------------------|--|---|------------|----------------------|---|--------------------|
| Search Criteria | | Matching Resources | | | | |
| Keywords [envision] | | Show Results Details Deploy Subscribe Package | | | | |
| Resource Types [v] | | <input checked="" type="checkbox"/> | Subscribed | Name | Created | Updated |
| | | <input checked="" type="checkbox"/> | yes | Envision Config File | 2014-03-07 11:50 AM | 2015-12-14 7:53 AM |
| | | | | Type | Description | |
| | | | | RSA Log Device | This file is used to update the Log Device ba | |

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

Live

Search

Configure

Feeds

Search Criteria

Keywords
envision

Resource Types

Matching Resources

Show Results | Details **Deploy** | Subscribe | Package

| <input checked="" type="checkbox"/> | Subscribed | Name | Created | Updated | Type | Description |
|-------------------------------------|------------|----------------------|---------------------|--------------------|----------------|---|
| <input checked="" type="checkbox"/> | yes | Envision Config File | 2014-03-07 11:50 AM | 2015-12-14 7:53 AM | RSA Log Device | This file is used to update the Log Device ba |

6. Select **Next**.

Deployment Wizard

Resources

Services

Review

Deploy

Total resources : 1

| Resource Names | Resource Type | Dependency of |
|----------------------|----------------|---------------|
| Envision Config File | RSA Log Device | |

Cancel

Next

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

Deployment Wizard

Resources Services Review Deploy

Services Groups

| <input type="checkbox"/> | Name | Host | Type |
|-------------------------------------|---------------------|--------------------|----------------|
| <input type="checkbox"/> | SA - IPDB Extractor | SA | IPDB Extractor |
| <input checked="" type="checkbox"/> | vm3099_log_Decoder | vm3099_log_Decoder | Log Decoder |

Cancel Previous Next

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

8. Select **Deploy**.

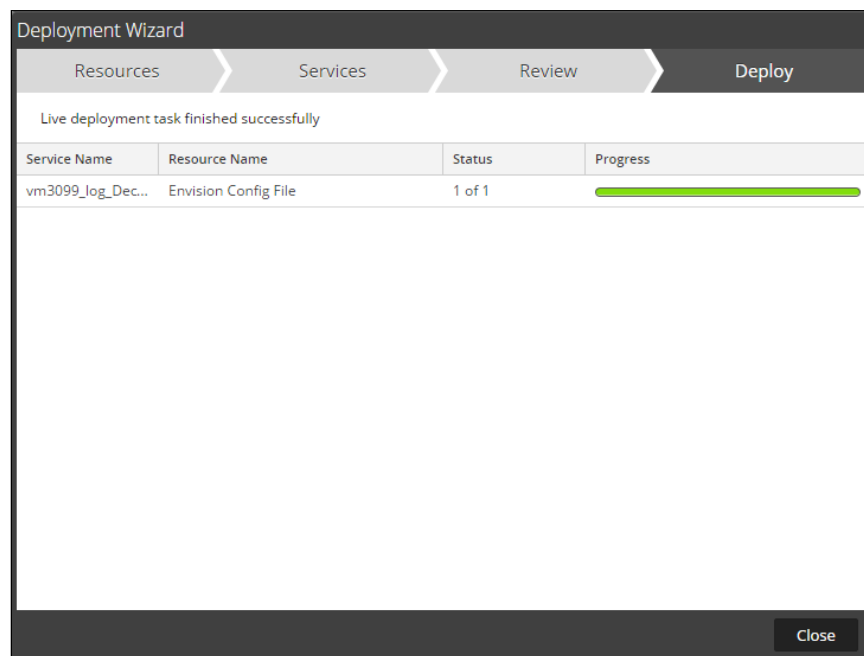
Deployment Wizard

Resources Services Review Deploy

| Service | Service Type | Resource Name | Resource Type |
|------------------|--------------|----------------------|----------------|
| vm3099_log_De... | Log Decoder | Envision Config File | RSA Log Device |

Cancel Previous Deploy

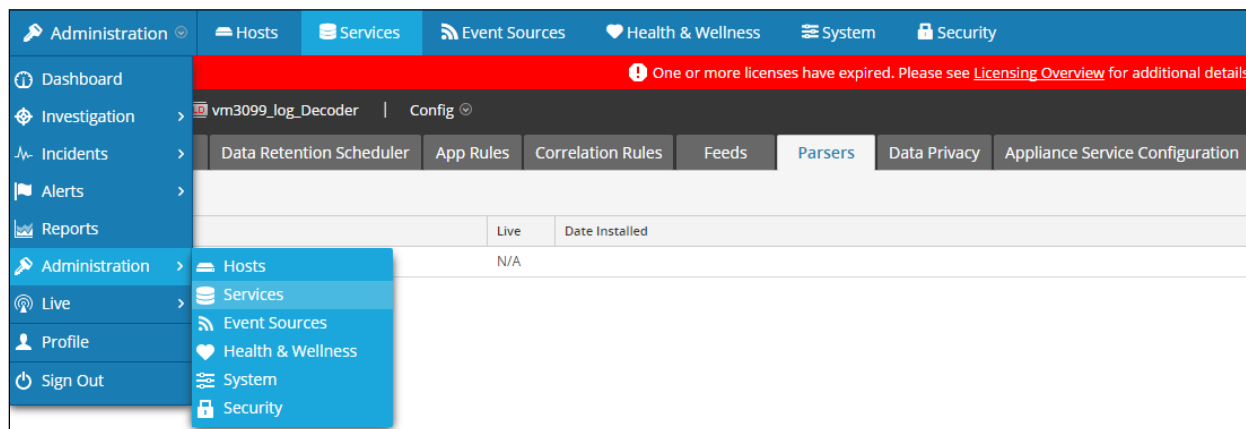
9. Select **Close**, to complete the deployment of the Envision Config file.



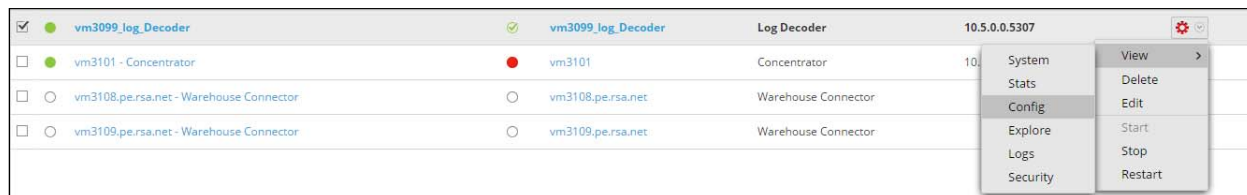
Deploy the Security Analytics Integration Package

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**.

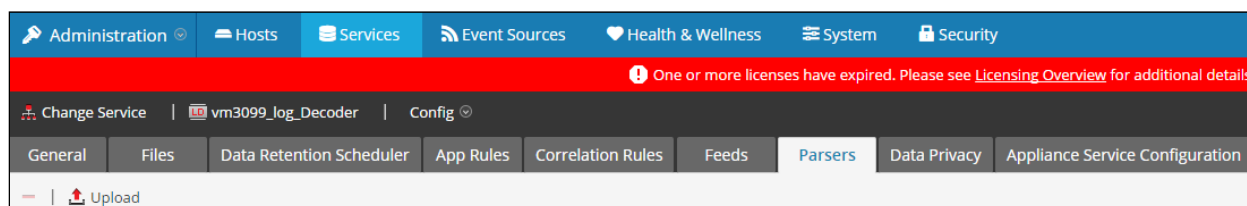


2. Select your Log Decoder from the list, select **View > Config**.



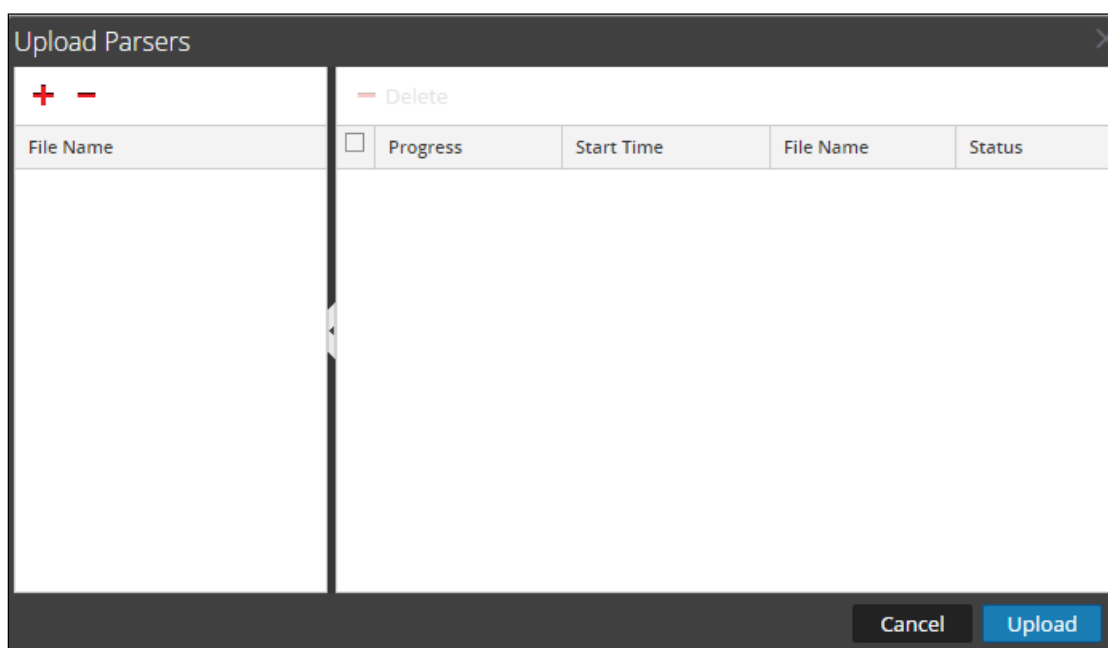
! > Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.

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

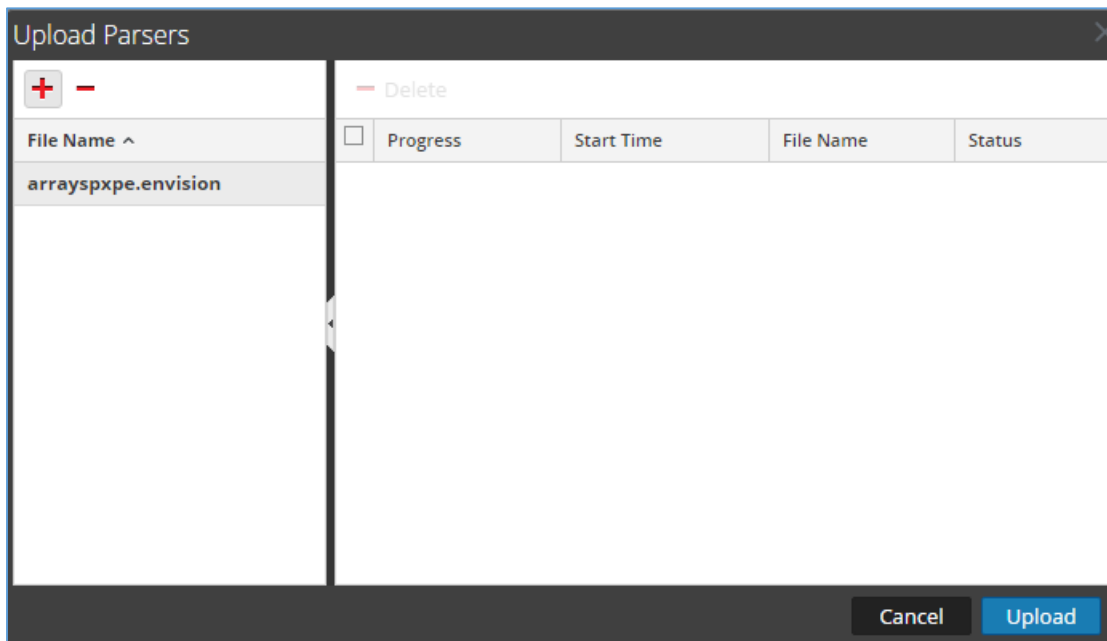


4. From the *Upload Parsers* window, click the **+** **Add** button and select the *.envision* file.

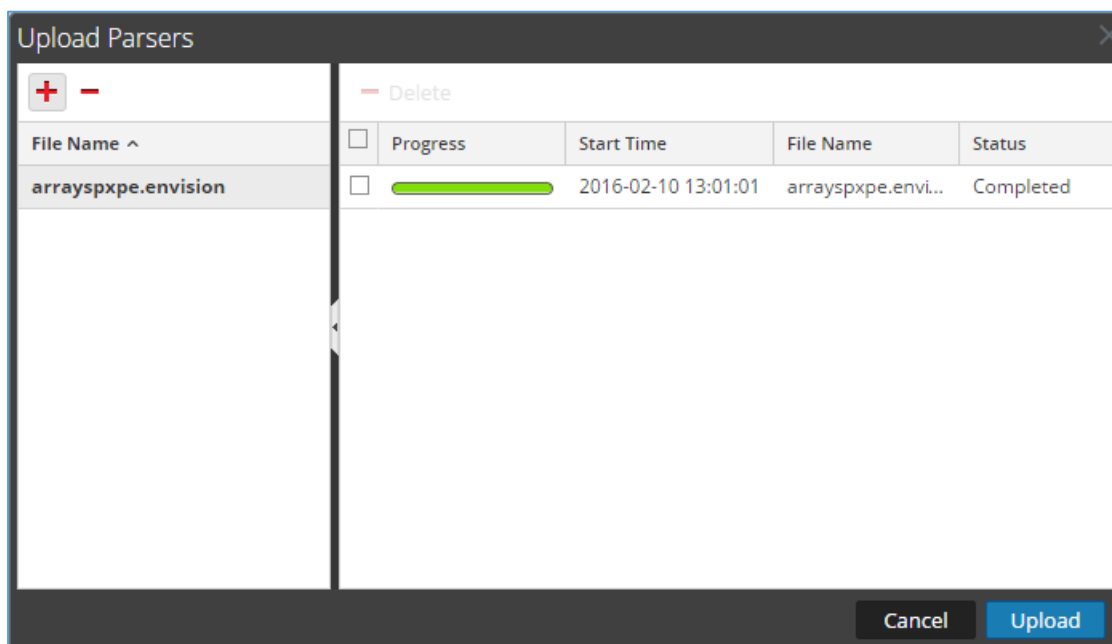
! > Important: The .envision file is contained within the .zip file downloaded from the RSA Community.



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



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



- 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="dtransaddr" nwName="dtransaddr" flags="None"/>
  <mapping envisionName="result" nwName="result" flags="None" envisionDisplayName="Result|Volume|Information|Reason|Succeed|Failed"/>
  <mapping envisionName="info" nwName="index" flags="None"/>
  <mapping envisionName="dtransport" nwName="dtransport" flags="None"/>
  <mapping envisionName="web_ref_query" nwName="web.ref.query" flags="None"/>
  <mapping envisionName="protocol" nwName="protocol" flags="None" envisionDisplayName="Protocol"/>
  <mapping envisionName="stransaddr" nwName="stransaddr" flags="None"/>
  <mapping envisionName="sport" nwName="ip.srcport" flags="None" format="UInt16" envisionDisplayName="SourcePort|LocalPort|ServerPort|src_ip|addr|src_port" nullTokens="-|(null)"/>
  <mapping envisionName="stransport" nwName="stransport" flags="None"/>
  <mapping envisionName="msg" nwName="msg" flags="None" format="Text" envisionDisplayName="Message"/>
  <mapping envisionName="url" nwName="url" flags="None" envisionDisplayName="URL"/>
  <mapping envisionName="rbytes" nwName="rbytes" flags="None" format="UInt64" nullTokens="(null)"/>
  <mapping envisionName="service" nwName="service.name" flags="None" envisionDisplayName="Service|Protocol"/>
</mappings>
```

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

| | | | | | | |
|-------------------------------------|---|-------------------------------------|--------------------|---------------------|---------------|--|
| <input checked="" type="checkbox"/> | vm3099_log_Decoder | <input checked="" type="checkbox"/> | vm3099_log_Decoder | Log Decoder | 10.5.0.0.5307 | |
| <input type="checkbox"/> | vm3101 - Concentrator | <input type="checkbox"/> | vm3101 | Concentrator | 10.5.0.0.5307 | |
| <input type="checkbox"/> | vm3108.pe.rsa.net - Warehouse Connector | <input type="checkbox"/> | vm3108.pe.rsa.net | Warehouse Connector | | |
| <input type="checkbox"/> | vm3109.pe.rsa.net - Warehouse Connector | <input type="checkbox"/> | vm3109.pe.rsa.net | Warehouse Connector | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

- Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View > Config**.

| | | | | | | |
|-------------------------------------|---|-------------------------------------|--------------------|---------------------|---------------|--|
| <input checked="" type="checkbox"/> | vm3099_log_Decoder | <input checked="" type="checkbox"/> | vm3099_log_Decoder | Log Decoder | 10.5.0.0.5307 | |
| <input type="checkbox"/> | vm3101 - Concentrator | <input type="checkbox"/> | vm3101 | Concentrator | 10.5.0.0.5307 | |
| <input type="checkbox"/> | vm3108.pe.rsa.net - Warehouse Connector | <input type="checkbox"/> | vm3108.pe.rsa.net | Warehouse Connector | | |
| <input type="checkbox"/> | vm3109.pe.rsa.net - Warehouse Connector | <input type="checkbox"/> | vm3109.pe.rsa.net | Warehouse Connector | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

- The new device is listed under the Log Decoder(s) General Tab within the Service Parsers Configuration.

| Service Parsers Configuration | | Enable All | Disable All |
|-------------------------------|-------------------------------------|------------|-------------|
| Name | Config Value | | |
| arrayspxpe | <input checked="" type="checkbox"/> | | |

! > Important: The device parser above is an example and not the actual parser for this integration.

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.

Event Reconstruction

service
10.100.52.173

id
77408

type
Log

service type
arrayspxpe

service class
VPN

View Meta

View Log

Export Logs

Open Event in New Tab

Cancel

sessionid

=

77408

time

=

2016-02-10T13:12:27.0

size

=

195

device.ip

=

10.100.52.173

medium

=

32

device.type

=

arrayspxpe

device.class

=

VPN

header.id

=

0002

ip.src

=

10.1.231.6

result

=

TCP_MISS/200

rbytes

=

12338

action

=

/js1285072889/sitewide/js/sitewide.js

web.ref.query

=

DIRECT

ip.dst

=

173.223.232.130

level

=

6

msg.id

=

AN_SQUID_LOG

event.cat.name

=

User.Activity

<

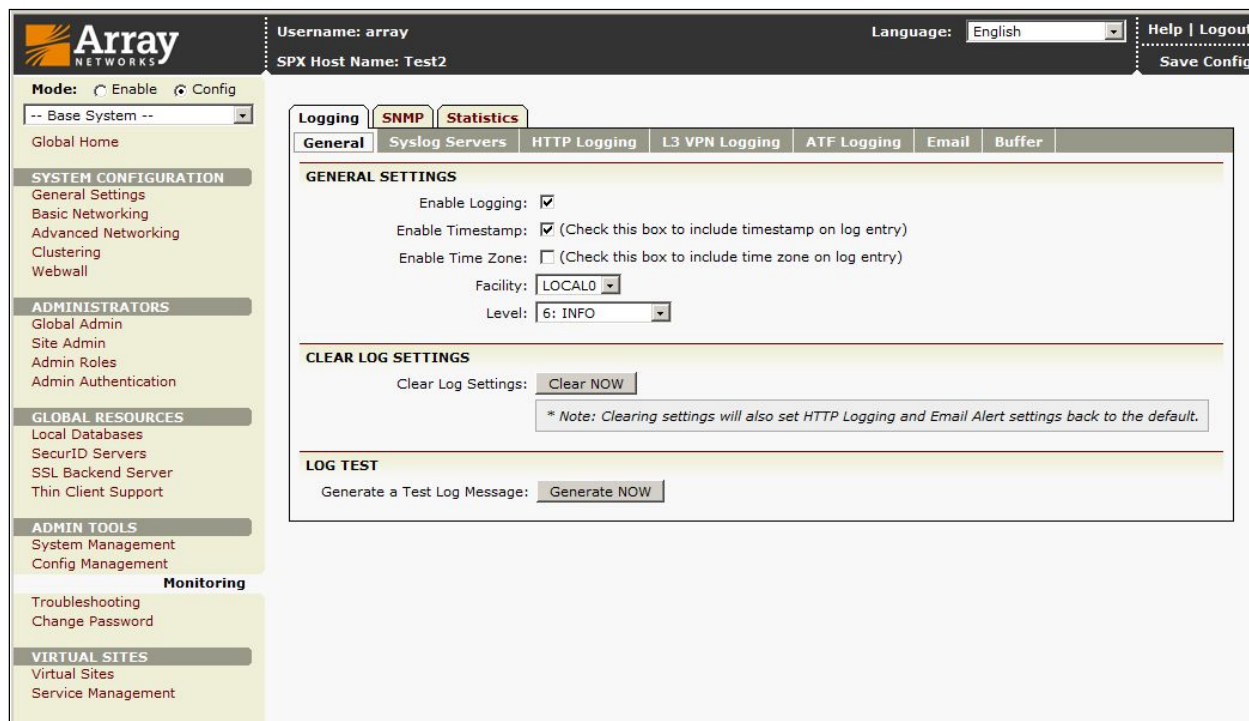
>

Viewing Log

Show Reconstruction Log

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.



Array Networks

Username: array
SPX Host Name: Test2

Language: English Help | Logout

Mode: ☐ Enable ☒ Config

-- Base System --

Global Home

SYSTEM CONFIGURATION

- General Settings
- Basic Networking
- Advanced Networking
- Clustering
- Webwall

ADMINISTRATORS

- Global Admin
- Site Admin
- Admin Roles
- Admin Authentication

GLOBAL RESOURCES

- Local Databases
- SecurID Servers
- SSL Backend Server
- Thin Client Support

ADMIN TOOLS

- System Management
- Config Management

Monitoring

- Troubleshooting
- Change Password

VIRTUAL SITES

- Virtual Sites
- Service Management

Logging **SNMP** **Statistics**

General Syslog Servers HTTP Logging L3 VPN Logging ATF Logging Email Buffer

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

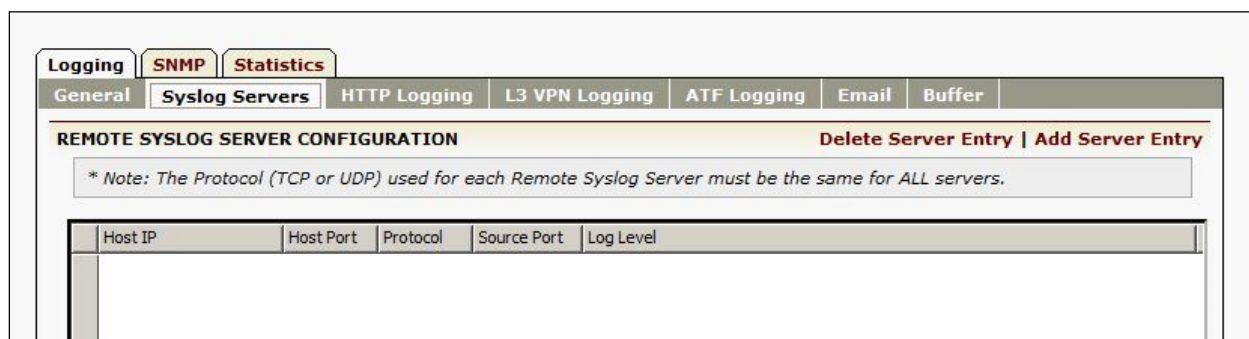
Clear Log Settings:

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

LOG TEST

Generate a Test Log Message:

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



Logging **SNMP** **Statistics**

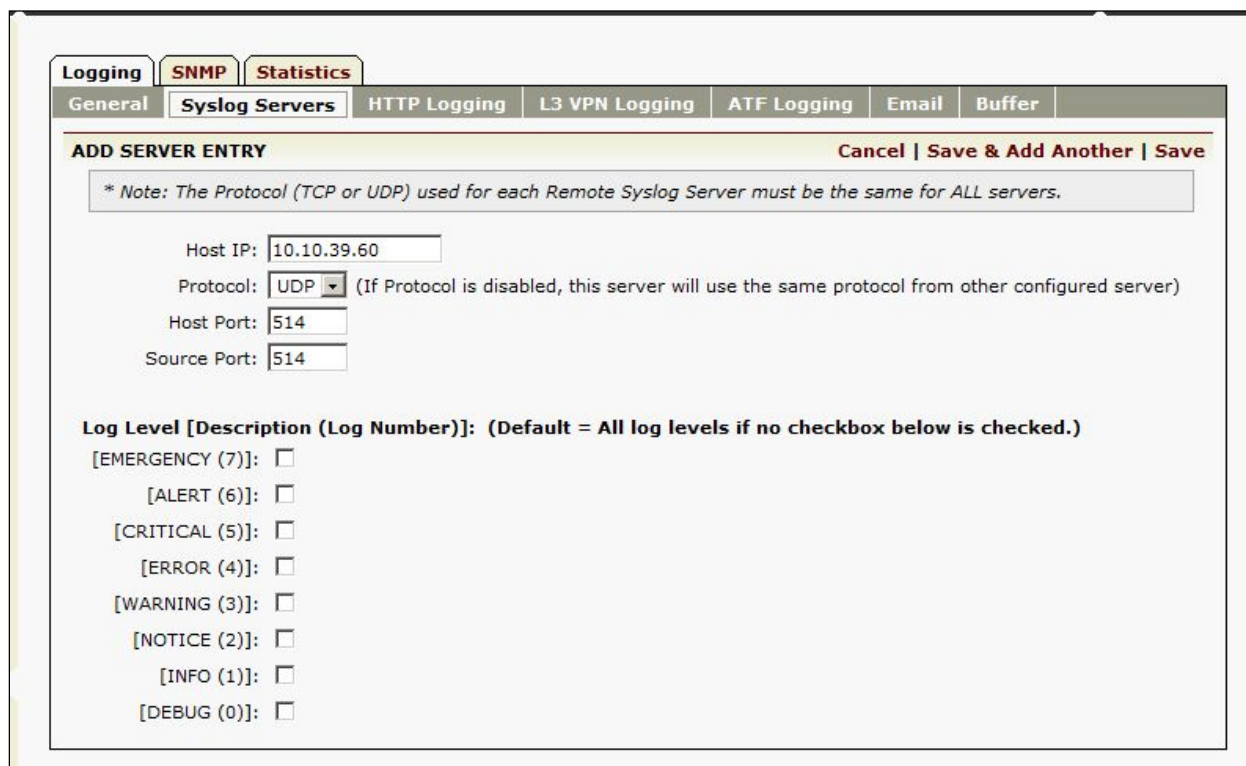
General **Syslog Servers** HTTP Logging L3 VPN Logging ATF Logging Email Buffer

REMOTE SYSLOG SERVER CONFIGURATION [Delete Server Entry](#) | [Add Server Entry](#)

* 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.



The screenshot shows the 'Syslog Servers' configuration page. At the top, there are tabs for 'Logging', 'SNMP', and 'Statistics'. Below these are sub-tabs: 'General', 'Syslog Servers' (selected), 'HTTP Logging', 'L3 VPN Logging', 'ATF Logging', 'Email', and 'Buffer'. The main section is titled 'ADD SERVER ENTRY' and includes a note: '* Note: The Protocol (TCP or UDP) used for each Remote Syslog Server must be the same for ALL servers.' Below the note, there are input fields for 'Host IP' (10.10.39.60), 'Protocol' (UDP), 'Host Port' (514), and 'Source Port' (514). A note next to the Protocol dropdown states: '(If Protocol is disabled, this server will use the same protocol from other configured server)'. At the bottom, there is a section for 'Log Level [Description (Log Number)]' with checkboxes for various levels: [EMERGENCY (7)], [ALERT (6)], [CRITICAL (5)], [ERROR (4)], [WARNING (3)], [NOTICE (2)], [INFO (1)], and [DEBUG (0)]. All checkboxes are currently unchecked.

6. Click **Save**.

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

Username: array

Language: English

Help | Logout

SPX Host Name: Test2

Save Config

Logging

SNMP

Statistics

General

Syslog Servers

HTTP Logging

L3 VPN Logging

ATF Logging

Email

Buffer


REMOTE SYSLOG SERVER CONFIGURATION

Delete Server Entry | Add Server Entry

* 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: February 4, 2016

| Certification Environment | | |
|--|---------------------|-------------------|
| Product Name | Version Information | Operating System |
| RSA Security Analytics | 10.5 | Virtual Appliance |
| Array Networks SPX Series Universal Access Controllers | 8.4.6 | Proprietary |

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

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

Appendix

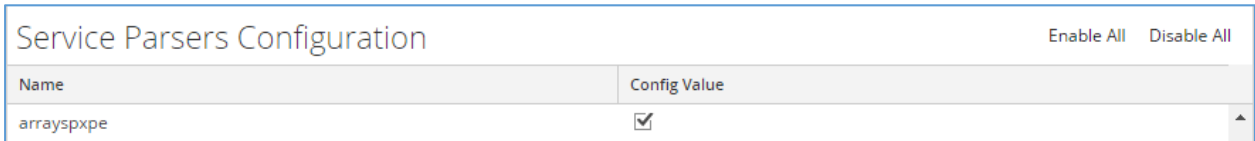
Security Analytics Disable Device Parser

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).