



RSA enVision Ready Implementation Guide

Last Modified: April 6, 2011

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

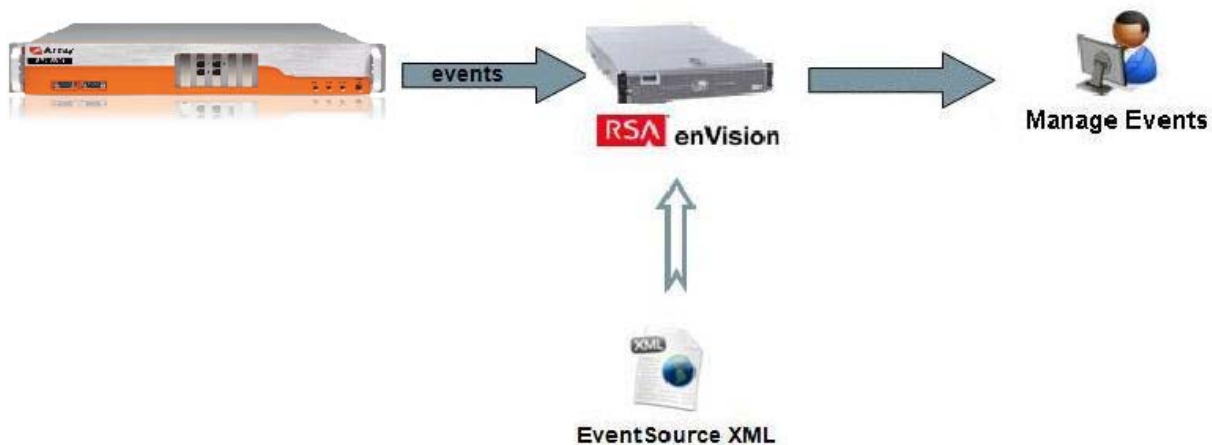
Integrating Array Networks SPX Series Universal Access Controllers with RSA's enVision involves directing the SPX's logs to the enVision server.

Format: log host <ip of enVision server> <destination port> <protocol>

Example: log host 10.10.10.10 514 udp

The Array Networks SPX Series Universal Access Controllers paired with RSA enVision 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 enVision Features	
Array SPX 8.4.6	
EventSource Integration package name	ArraySPXPE.zip
Device display name within enVision	ArraySPXPE
Collection method	Syslog





EventSource Integrator Package

The RSA enVision Intelligence 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 EventSource Integrator Package for this guide. All enVision customers and partners are invited to register and participate in the Intelligence Community: <https://rsaenvision.lithium.com>.

Once you have downloaded the ArraySPXPE.zip package from the Intelligence Community, you must deploy the package on all enVision appliances in your environment as described in the following table.

RSA enVision Site	Where to Deploy the Event Source XML Package
Single appliance site	On the appliance
Multiple appliance site	On all components: <ul style="list-style-type: none">• Application Servers (A-SRVs)• Database Servers (D-SRVs)• Local Collectors (LCs)• Remote Collectors (RCs)
Multiple appliance site with Enhanced Availability	On all components: <ul style="list-style-type: none">• Application Servers (A-SRVs)• Database Servers (D-SRVs)• Cluster Appliances (CAs)

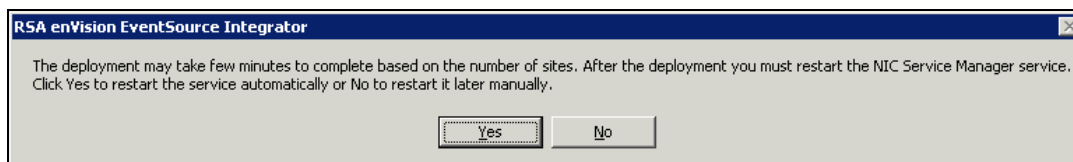
Deploying an EventSource Package

To deploy an event source package:

1. Extract the EventSource Package directly into the following folder: `%_ENVISION%\update`.

! Important: Do not create a subfolder within the `%_ENVISION%\update` directory when extracting the package.

2. Run the script file, `DeployEventSourceSetup.vbs`.



3. The RSA enVision EventSource Integrator box will appear. If you wish to have the NIC Service Manager service restart on all of your sites after the install, click **Yes**. If you plan to manually restart the services later, click **No**. The time the script file takes to run depends on the number of event source XML files that need to be verified. If you are deploying a new event source, the script assigns an event source type ID to the event source. If you are updating an existing event source, the event source XML file is updated.
4. Login to the enVision console to confirm the new device type is displayed under **Overview → System Configuration → Devices → Manage Device Types** and listed as ArraySPXPE.

! Important: The new device will not be displayed in the enVision console until the NIC Service Manager service has been restarted.





Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Array SPX with RSA enVision. 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 SPX 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.

The screenshot displays the Array Networks WebUI interface. At the top, the user is logged in as 'array' with the SPX Host Name 'Test2'. The language is set to English. The main navigation menu on the left includes sections for Mode (Enable/Config), Base System, System Configuration, Administrators, Global Resources, Admin Tools, Monitoring, and Virtual Sites. The 'Logging' tab is selected, showing 'GENERAL SETTINGS' for 'LOCAL0' at 'INFO' level. Options for 'Enable Logging', 'Enable Timestamp', and 'Enable Time Zone' are checked. A 'Clear Log Settings' button is visible, along with a note that clearing settings will reset HTTP Logging and Email Alert settings. A 'Generate NOW' button is also present for testing log messages.





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

Host IP	Host Port	Protocol	Source Port	Log Level
---------	-----------	----------	-------------	-----------

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

Host IP:

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

Host Port:

Source Port:

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 enVision 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 enVision

Date Tested: April 6, 2011

Certification Environment		
Product Name	Version Information	Operating System
RSA enVision	4.0SP3	Microsoft Windows XP
RSA EventSource Integrator	1.1.1	Microsoft Windows XP
RSA Event Source Update (ESU)	20110106-120053	Microsoft Windows XP
Array Network SPX Series	8.4.6	Proprietary

enVision Test Case	Result
Device Management	
Device discovers properly under Manage Monitored Devices	✓
Vendor name appears in enVision GUI correctly	✓
Device can be deleted from Manage Monitored Devices	✓
Device can be disabled from Manage Device Types	✓
Device Class type is correct under Manage Device Types	✓
Device displays properly under Manage Messages to Parse	✓
Message Management	
Disabled device creates unknown device in monitored device list	✓
Temporary nugget files are removed	✓
Queries / Reports	
Messages for device populate the table columns correctly	✓
Ad Hoc report populates variables correctly	✓

GLS / PAR

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



The Security Division of EMC



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
```

Appendix B.

Resolving Unknown Device Type

In certain cases after deploying the ESI Package, the device may come into enVision as an Unknown device type. To resolve this issue, complete the following steps.

1. In the enVision GUI, select **Overview** → **System Configuration** → **Devices** → **Managed Monitor Devices**, then click on the IP Address of the Unknown device.

Use this window to display the list of devices being monitored.

Manage Monitored Devices

Filter: WHERE Site Name IN 'PH038'

Delete	Operator	Attribute	Comparison	Criteria
<input type="checkbox"/>	WHERE	NIC Properties / Site Name	IN	PH038

Group By: None

Apply Add Delete

Filtered Devices: 2 Devices found

Select	IP Address	Name	Device Type	Site/Node	Status	
<input type="checkbox"/>	10.100.51.68	PH038-ES.PH038.nic	Unknown	PH038 / PH038-ES	Candidate	<input type="checkbox"/>
<input type="checkbox"/>	10.100.51.38	PH038-ES.PH038.nic	NIC System	PH038 / PH038-ES	Active	<input checked="" type="checkbox"/>

Add Modify Delete Analyze Report





- From the Device Type pull-down menu, select the correct **device type**. For the name of the device as it appears in enVision, refer to the above section *RSA enVision Features*, page 2.

Manage Monitored Devices - Add/Modify Device

Site: PH038	IP address: 10.100.51.38
Node: PH038-ES	Device class: Unknown
Discovery: 2011-01-28 11:58:26.64	Device type: Unknown
Analyze: <input type="checkbox"/>	Collection: [Dropdown menu open showing: Intel VPN, Juniper DX, Microsoft Exchange, NIC System, NewDevicePE, Secure Computing Sidewinder G2, Sonicwall-FW, Symantec Enterprise Firewall, Tipping Point, UNDX Solaris, Unknown]
Multi device: <input type="checkbox"/>	Has timestamp: <input type="checkbox"/>
Remove relay headers: <input type="checkbox"/>	Use timestamp: <input type="checkbox"/>
Encoding: [65001 (UTF-8)]	

Properties: ResolvedName = PH038-ES,PH038.nic

Location: [Field]

Organization: [Field]

Owner: [Field]

Physical: [Field]

Function: [Field]

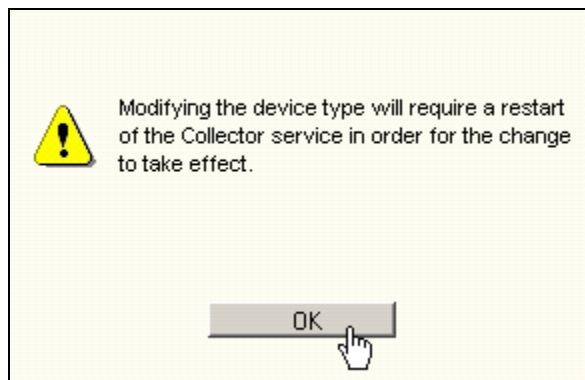
Importance: Value = 1

Vulnerability: Value = 1

Zone: [Field]

SystemInformation: [Field]

- Select **OK** to the information dialog box shown below.





4. From the Collection pull-down menu, select **Active**.

Manage Monitored Devices - Add/Modify Device

Site: PH038
Node: PH038-ES
Discovery: 2011-01-28 11:58:26.64
Analyze:
Multi device:
Remove relay headers:
Encoding: 65001 (UTF-8)

IP address: 10.100.51.38
Device class: Security Application Firewall
Device type: NewDevicePE
Collection: Candidate
Has timestamp:
Use timestamp:

Properties: ResolvedName = PH038-ES.PH038.nic
Location:
Organization:
Owner:
Physical:
Function:
Importance: Value = 1
Vulnerability: Value = 1
Zone:
SystemInformation:

5. Select the **Analyze** radio button.

Manage Monitored Devices - Add/Modify Device

Site: PH038
Node: PH038-ES
Discovery: 2011-01-28 11:58:26.64
Analyze:
Multi device:
Remove relay headers:
Encoding: 65001 (UTF-8)

IP address: 10.100.51.38
Device class: Security Application Firewall
Device type: NewDevicePE
Collection: Active
Has timestamp:
Use timestamp:

Properties: ResolvedName = PH038-ES.PH038.nic
Location:
Organization:
Owner:
Physical:
Function:
Importance: Value = 1
Vulnerability: Value = 1
Zone:
SystemInformation:

6. Click **Apply**.

! Important: You must restart the enVision NIC Collector windows service for your changes to take effect.
