# RSA Ready Implementation Guide for RSA Security Analytics

NetClarity NACwall 8.0.6

Daniel R. Pintal, RSA Partner Engineering Last Modified: February 29, 2016





## **Solution Summary**

Among the NACwall appliance's capabilities are the ability to manage network access control, perform regulatory audits and identify zero day malware. The NACwall appliance logs events regarding almost every activity which takes place on the appliance. By integrating with RSA Security Analytics, users can get a clear picture of their network activity and network asset status.

NACwall 8.0.6								
Integration package name	netclaritype.envision							
Device display name within Security Analytics	netclaritype							
Event source class	Access Control							
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 <u>Appendix</u> of this Guide.

The RSA Security Analytics package consists of the following files:

Filename	File Function
netclaritype.envision	SA package deployed to parse events from device integrations.
netclaritypemsg. 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
11/27/2013	Initial support for NetClarity NACwall.
2/29/2016	RSA Security Analytics 10.5 Support.



## **RSA Security Analytics Configuration**

#### 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	🛠 Confi	gure 🔊 Fo	eeds				
Search Criteria		Matching	g Resources				
Keywords		E Show Rest	ults 🌝 🕴 🧮 Details 🛛 🐻 D	Deploy 🔊 Subscribe   💥 Pa	ackage ତ		
envision		Subscribed	Name	Created	Updated	Туре	Description
Resource Types		🗹 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 Devi					
	~						

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

	Search	🛠 Configu	ire 🔊 Fe	eds				
Search Criteria		Ţ	Matching	g Resources				
Keywords			🗑 Show Resu	ilts 🛛   🔚 Details [ 🗊 🕻	Deploy 🔊 Subscribe   💥 Pa	ackage 🛞		
envision		E	Subscribed	Name	Created	Updated	Туре	Description
Resource Types		5	🗹 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 De					
		~						





6. Select Next.

Deployment Wizard						
Resources	Services	s	Re	view		Deploy
Total resources : 1						
Resource Names		Resource Type		Dependency of		
Envision Config File		RSA Log Device				
					Can	cel Next

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

Deployn	nent Wizard			
R	esources	Services	Review	Deploy
Servic	es Groups			
	Name		Host	Туре
	SA - IPDB Extractor		SA	IPDB Extractor
<b>I</b>	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 Wiza	ard			
Resources		Services	Review	Deploy
Service	Service Type	Resource Name		Resource Type
vm3099_log_De	Log Decoder	Envision Config File		RSA Log Device
			Cancel F	Previous Deploy

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

Deployment Wiz	ard					
Resources	5	Services		Review		Deploy
Live deployment	task finished success	sfully				
Service Name	Resource Name		Status		Progress	
vm3099_log_Dec	Envision Config File	e	1 of 1			
						Close



#### NetClarity NACwall 8.0.6

### Deploy the Security Analytics Integration Package

After completing the previous section, <u>Deploy the enVision Config File</u>, 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.** 

Administration	ı ©	🚍 Hosts	Services	🔊 Event Sou	ırces 🔍 Heal	th & Wellness	🞏 System	📇 Security	/
① Dashboard					. e	ne or more licer	nses have expire	ed. Please see <u>Lic</u>	ensing Overview for additional details.
Investigation		🔟 vm3099_log_	Decoder   C	Config 😔					
-∿- Incidents		Data Reter	ntion Scheduler	App Rules	Correlation Rules	Feeds	Parsers	Data Privacy	Appliance Service Configuration
🍽 Alerts									
🕁 Reports				Live	Date Installed				
🔊 Administration		🚔 Hosts		N/A					
🖗 Live		Services							
👤 Profile		<ul> <li>Event Sour</li> <li>Health &amp; V</li> </ul>	rces Vellness						
🖰 Sign Out		æ System ₽ Security							

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

<b>I</b>	vm3099_log_Decoder	0	vm3099_log_Decoder	Log Decoder	10.5.0	0.0.5307	۲
	vm3101 - Concentrator	• vm3101 Concentrator 10		101 Concentrator 10. System		System	View >
00	vm3108.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector		Sta <mark>t</mark> s Config	Edit
0	vm3109.pe.rsa.net - Warehouse Connector	ursalnet - Warehouse Connector O vm3109.pe.rsalnet Warehouse Connector			Explore Logs Security	Start Stop Restart	

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.

🔎 Admini	stration $\odot$	🖴 Hosts	Services	Sevent So	ources 🔍 Hea	Health & Wellness		n 📑 Securit	y		
						One or more licer	ises have expii	red. Please see <u>Lic</u>	ensing Overview for additional details.		
🚠 Change Se	ervice   🛄	vm3099_log_	Decoder   C	onfig 👳							
General	Files	Data Reten	tion Scheduler	App Rules	Correlation Rule	Feeds	Parsers	Data Privacy	Appliance Service Configuration		
—   🏦 Up	-   1 Upload										



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 Ready Community.

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

Upload Parsers					×
+ -	- 0				
File Name 🔨	F	Progress	Start Time	File Name	Status
netclaritype.envision					
	4				
	2			Cancel	Upload



- NetClarity NACwall 8.0.6
  - 6. Upon completion of the upload click **Cancel**.

Upload Parsers					×
+ -	-	Delete			
File Name		Progress	Start Time	File Name	Status
			2016-02-09 15:44:16	netclaritype.env	Completed
				Cancel	Upload

 Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the table-mapcustom.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="macaddr" nwName="eth.host" flags="None" format="MAC" envisionDisplayName="DeviceMacAddress"/> <mapping envisionName="node" nwName="node" flags="None" envisionDisplayName="NodeName"/> <mapping envisionName="process\_id" nwName="process.id" flags="None" format="Int64" nullTokens="(null)|-"/> <mapping envisionName="info" nwName="index" flags="None"/>

</mappings>

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

2		vm3099_log_Decoder	0	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307	<b>\$</b> (9)
		vm3101 - Concentrator	•	vm3101	Concentrator	10.5.0.0.5307	View >
□ c	2	vm3108.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector		Delete Edit
D C	)	vm3109.pe.rsa.net - Warehouse Connector	0	vm3109.pe.rsa.net	Warehouse Connector		Start
							Stop
							Restart





#### NetClarity NACwall 8.0.6

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

🗹 😑 vm309	99_log_Decoder	0	vm3099_log_Decoder	Log Decoder	10.5.	0.0.5307	<b>\$</b> ()	
🗆 😑 vm310	11 - Concentrator	•	vm3101	Concentrator	10.	System	View >	
□ ○ vm310	18.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector		Stats Config	Delete Edit	
□ ○ vm310	19. pe.rsa.net - Warehouse Connector	0	vm3109.pe.rsa.net	Warehouse Connector	_	Explore Logs Security	Start Stop Restart	

10. 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		
netclaritype	$\checkmark$		•

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.





## **Partner Product Configuration**

#### Before You Begin

This section provides instructions for configuring the NACwall 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 NACwall 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 NetClarity NACwall is properly configured and secured before deploying to a production environment. For more information, please refer to the NetClarity NACwall documentation or website.

#### NACwall Configuration

- 1. Log into NACwall with Administrator privileges.
- 2. Navigate to Setup | Syslog / SNMP Traps.



3. Under Syslog Message Setup enter the RSA Security Analytics information in the **RSA enVision** Server or Syslog Port Number and **RSA enVision Server or Syslog Server IP Address** fields.

Syslog Message	Setup
RSA enVision Server or Syslog Port Number RSA enVision Server or Syslog Server IP Address	514       192     . 168     . 254     . 220

All events generated by the NACwall will now be sent to the RSA Security Analytics on the designated port.



## **Certification Checklist for RSA Security Analytics**

Date Tested: February 29, 2016

Certification Environment							
Version Information	Operating System						
10.5	Virtual Appliance						
8.0.6	Hardened Linux, Red Hat 9						
	Certification Environment           Version Information           10.5           8.0.6						

Security Analytics Test Case	Result
Device Administration	
Partner's device name appears in Device Parsers Configuration	<b></b>
Device can be enabled from Device Parsers Configuration	<b></b>
Device can be disabled from Device Parsers Configuration	<b></b>
Device can be removed from Device Parsers Configuration	$\checkmark$
Investigation	
Device name displays properly from Device Type	<b></b>
Displays Meta Data properly within Investigator	

 $\checkmark$  = Pass  $\times$  = 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.

<b>1</b>	vm3099_log_Decoder	9	vm3099_log_Decoder	Log Decoder	10.5.	0.0.5307	<b>\$</b> 9	
	vm3101 - Concentrator	٠	vm3101	Concentrator	10.	System	View >	
	ym3108.pe.rsa.net - Warehouse Connector	0	vm3108.pe.rsa.net	Warehouse Connector		Stats Config	Delete Edit	
00	vm3109,pe.rsa.net - Warehouse Connector O vm3109,pe.rsa.net Warehouse Connector		-	Explore Logs Security	Start Stop Restart			

2. From the **Service Parses Configuration** window, scroll down to the device you wish to disable and uncheck the Config Value checkbox.

Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
netclaritype	$\checkmark$		-

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 **tablemap-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).