



RSA enVision Ready Implementation Guide

Last Modified: November 10th, 2011

Partner Information

Product Information	
Partner Name	ObserveIT
Web Site	www.observeit.com
Product Name	ObserveIT
Version & Platform	5.5, Windows
Product Description	ObserveIT captures video recording and detailed audit logs of every user action on servers or desktops in RDP, SSH, Citrix, VDI or console user sessions. Including for apps that have no internal logging. ObserveIT identifies any new server session, and associates the session with a specific user. During the session, all user actions on screen are recorded for video replay. Detailed textual metadata logs list every app, resource or CLI command that the user ran. Canned compliance reports show all actions, with links to video replay for further clarification.



Solution Summary

The ObserveIT connector for RSA enVision provides three main business cases; Upload all ObserveIT video activity logging information into enVision, enables enVision to run reports on ObserveIT video logs and ObserveIT logs contains the video http link which can be copied and used from any internet browser in order to play the video.

RSA enVision Features	
ObserveIT 5.5	
EventSource Integration package name	ObserveITPE.zip
Device display name within enVision	ObserveITPE
enVision table	Access
Event source class	Access Control
Collection method	ODBC

Release Notes

Release Date	What's New In This Release
11/10/2011	Initial support for ObserveIT

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 ObserveITPE package from the Intelligence Community, the package will be deployed on all your 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)

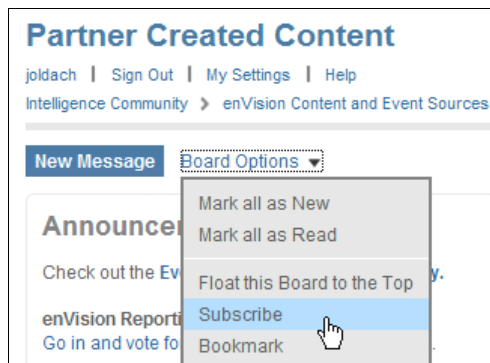
EventSource Integrator Package Notifications

An EventSource Integrator package may be updated frequently depending on the vendor or changes to the log messages of the device. To ensure you receive e-mail notifications on all new and existing RSA Partner ESI Packages, simply subscribe to the **Partner Created Content** message board within the RSA enVision Intelligence Community. To do so, perform the following steps:

1. Login to the [enVision Intelligence Community](#).
2. Scroll down and click **enVision Content and Event Sources** → **Partner Created Content**.

enVision Content and Event Sources (8 Items)			
TITLE		POSTS	NEW
 General Latest Post - SQL 2005 Trace		399	399
 Correlation Rules Latest Post - Re: When will the next series of Correlation Rules...		316	316
 Reports Latest Post - Re: enVision Reporting BASH: Comments and Question...		368	364
 ESI (and UDS) Latest Post - Re: How to Develop XML for Database using ESI		603	593
 Partner Created Content Latest Post - AirTight Networks SpectraGuard Enterprise (SGE)		9	6

- On the top menu, click **Board Options** → **Subscribe**.



 **Note:** You will now be notified via e-mail when new or existing ESI packages are updated.

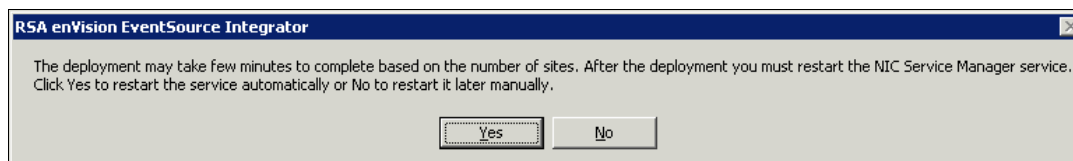
Deploying an EventSource Package

To deploy an event source package:

- 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.

- Run the script file, **DeployEventSourceSetup.vbs**.



- 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.
- Login to the enVision console to confirm the new device type is displayed under **Overview** → **System Configuration** → **Devices** → **Manage Device Types** and listed as **ObserveITPE**.

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

enVision Configuration Overview

In order for enVision to collect logs from the ObserveIT database, the NIC ODBC service must be configured.

The NIC ODBC service makes it possible for RSA enVision to collect messages from multiple ODBC definitions. The NIC ODBC service converts these messages into syslog events and sends them to the NIC Collector service.

An overview of these steps is as follows:

- Add the ODBC Data Source to the Windows System DSN tab
- Add the ODBC Device Type XML to enVision
- Add the ODBC Service within enVision

 **Note:** Refer to enVision online help documentation for more information on configuring each area.

Add the ODBC Data Source to the Windows System DSN tab

1. The first configuration step is to add the ODBC Data Source to the System DSN tab through the Window's **Control Panel** → **Administrative Tools** menu. For complete instructions, refer to the **Add Set Up ODBC Data Source** section in the enVision online help documentation.

Add the ODBC Device Type XML to enVision

The ODBC Device Type XML zip file, **ObserveIT_ODBC.zip**, is included as part of the partner package downloaded from the enVision Intelligence Community.

To add the ODBC Device Type XML to enVision, perform the following steps:

1. Extract the **ObserveIT_ODBC.zip** file directly into the **%_ENVISION%\etc\gots** directory. Do not create a subfolder when extracting the file.
2. Restart the **NIC Service Manager** from the Microsoft Services console.

After deploying the ODBC Device Type XML, the enVision console will now display the **ObserveIT** name from the **Manage ODBC Service - Add/Modify ODBC Definition** *Type* pull-down menu.

! > Important: Once the ODBC Device Type XML has been deployed DO NOT edit the XML through the enVision administration console (Overview > System Configuration > Services > Universal Device Collection > Manage ODBC Types) or the device XML will not be able to parse the data correctly.

Add the ODBC Service within enVision

1. The final configuration step is to add the ODBC Service within the enVision console. For complete instructions, refer to the **Set Up ODBC Service** section in the enVision online help documentation. The **NIC ODBC Service** will need to be restarted in order for the changes to take effect.

Certification Checklist for RSA enVision

Date Tested: November 10th, 2011

Certification Environment		
Product Name	Version Information	Operating System
RSA enVision	4.0 SP4	Microsoft Windows 2003 R2
RSA EventSource Integrator	1.2	Microsoft Windows XP
RSA Event Source Update (ESU)	20111031-165949	Microsoft Windows 2003 R2
ObserveIT	5.5	Microsoft Windows 2003 R2

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	✓

JJO / PAR

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

Appendix

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

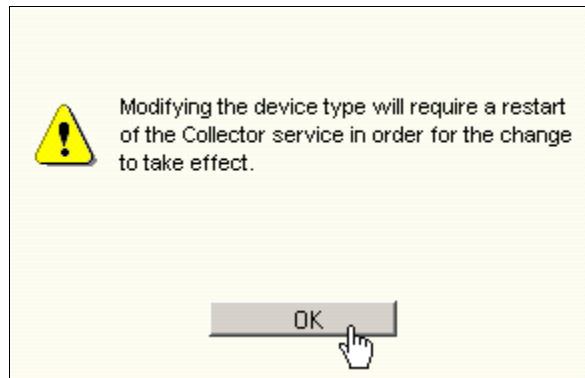
Filtered Devices: 2 Devices found

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.

- 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 IP address: 10.100.51.38
 Node: PH038-ES Device class: Security,Application Firewall
 Discovery: 2011-01-28 11:58:26.64 Device type: NewDevicePE
 Analyze: Collection: Candidate
 Multi device: Has timestamp: Candidate/Disabled
 Remove relay headers: Use timestamp: Active
 Encoding: [65001 (UTF-8)] Active/Disabled

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 IP address: 10.100.51.38
 Node: PH038-ES Device class: Security,Application Firewall
 Discovery: 2011-01-28 11:58:26.64 Device type: NewDevicePE
 Analyze: Collection: Active
 Multi device: Has timestamp:
 Remove relay headers: Use timestamp:
 Encoding: [65001 (UTF-8)]

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.
