



RSA Security Analytics Ready Implementation Guide

Last Modified: December 2, 2013

Partner Information

Product Information	
Partner Name	Raz-Lee Security
Web Site	www.razlee.com
Product Name	iSecurity for IBM-i
Version & Platform	Raz-Lee 11.4, IBM-i OS/400 V5R3 7.1
Product Description	Raz-Lee's iSecurity suite of products is a comprehensive, user-friendly auditing, compliance and security solution for IBM i (AS/400) environments. iSecurity products address insider threats, external security risks, and the need to monitor business-critical application.



Solution Summary

Raz-Lee iSecurity for IBM i triggers real-time Syslog and SNMP:

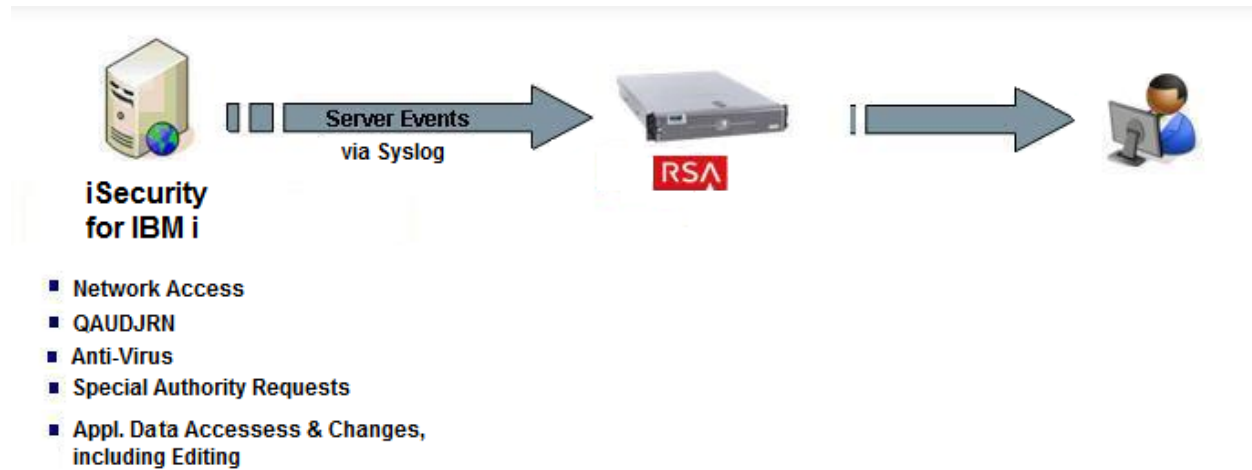
- Security alerts when a potential security breach has been detected.
- Event messages when a site-defined event has occurred; messages can be of varying severity levels, from Informational through Emergency.

Pertinent Syslog definitions are defined to iSecurity only once, and thereafter are invoked when triggered.

Providing real-time alerts and event messages, and integrating this information within the larger context of RSA Security Analytics monitoring and reporting, will provide multi-platform customers the ability to add previously unsupported IBM i security-related events into their overall system.

)

RSA Security Analytics Features	
Raz-Lee 11.4	
Integration package name	razleepe
Device display name within Security Analytics	razleepe
Event source class	Application Firewall
Collection method	Syslog



Release Notes

Release Date	What's New In This Release
12/02/2013	Initial support for Raz-Lee iSecurity for IBM-i.

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 Guide.

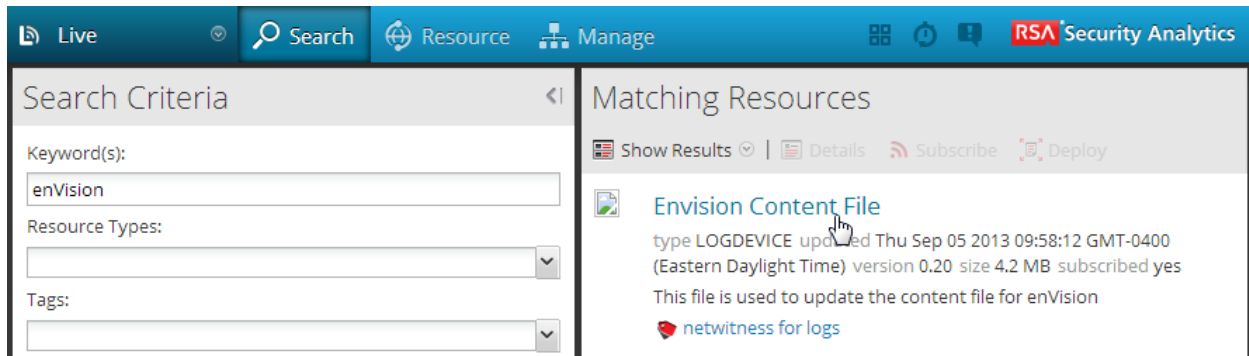
An overview of the RSA Security Analytics package consists of the following files:

Filename	File Function
razleepe.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: <i>enVision variable name --> SA variable name --> SA variable type</i>

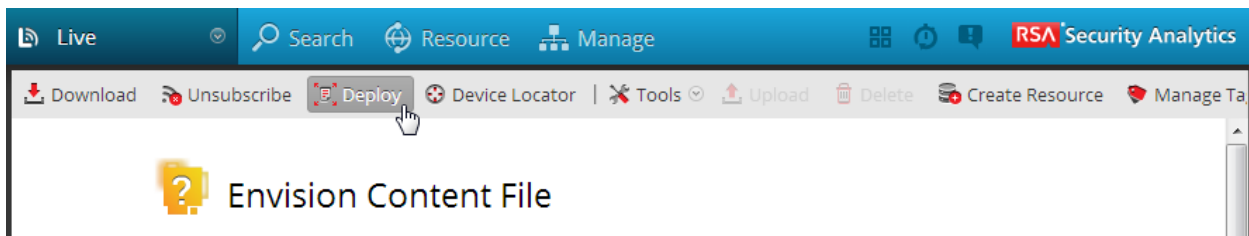
Deploy enVision Content File

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:

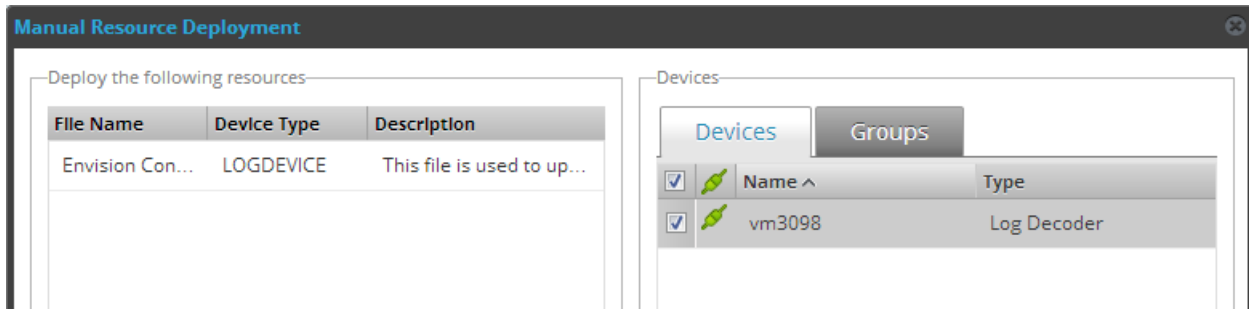
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Content File** in Matching Resources.
4. Click on **Envision Content File**.



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



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



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

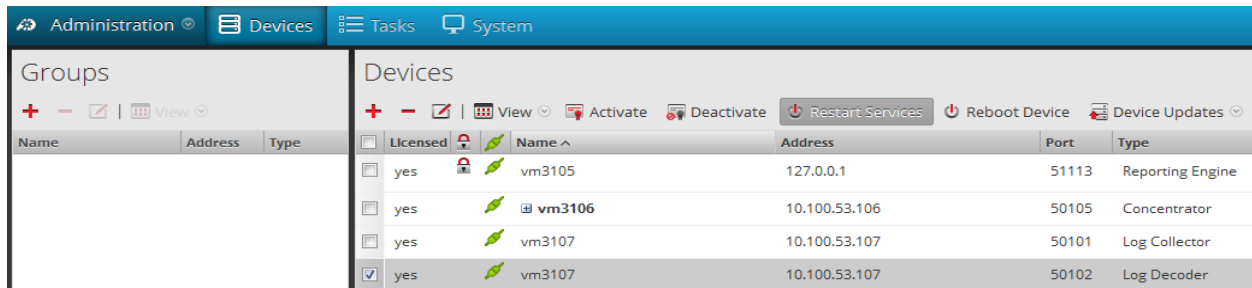
Deploy Security Analytics Integration Package

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**.

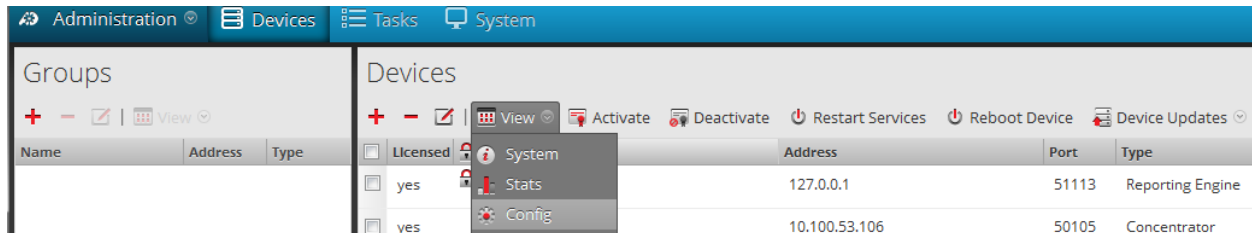
 **Note:** In an environment with multiple Log Decoders, deploy the Integration Package on each Log Decoder that will use the new device.

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** then 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	Name	Address	Port	Type
yes	System	127.0.0.1	51113	Reporting Engine
yes	vm3106	10.100.53.106	50105	Concentrator

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

The screenshot shows the NetWitness configuration interface. The top navigation bar includes Administration, Devices, Tasks, and System. The main content area is divided into three sections:

- System Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
Compression	0
Port	50002
SSL	off
Stat Update Interval	1000
- Log Decoder Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
Adapter	
Berkley Packet Filter	
Capture Interface Selected	
Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB
- Device Parsers Configuration:** A table with columns 'Name' and 'Config Value'.

Name	Config Value
ALERTS	<input checked="" type="checkbox"/>
BITTORRENT	<input checked="" type="checkbox"/>
FeedParser	<input checked="" type="checkbox"/>
FIX	<input checked="" type="checkbox"/>
GeoIP	<input type="checkbox"/>
GNUTELLA	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>

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-custom.xml` file does not exist, copy the `index-concentrator-custom.xml` from the Integration zip file to this directory.
If the `index-concentrator-custom.xml` file already exists then append the content to the existing file.
4. Navigate to **Administration > Devices** and check the **Log Decoder** then click **Restart Services**.

The screenshot shows the NetWitness 'Devices' page. It features a table with columns: Licensed, Name, Address, Port, and Type. The 'Restart Services' button is highlighted.

Licensed	Name	Address	Port	Type
<input type="checkbox"/>	vm3105	127.0.0.1	51113	Reporting Engine
<input type="checkbox"/>	vm3106	10.100.53.106	50105	Concentrator
<input type="checkbox"/>	vm3107	10.100.53.107	50101	Log Collector
<input checked="" type="checkbox"/>	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.

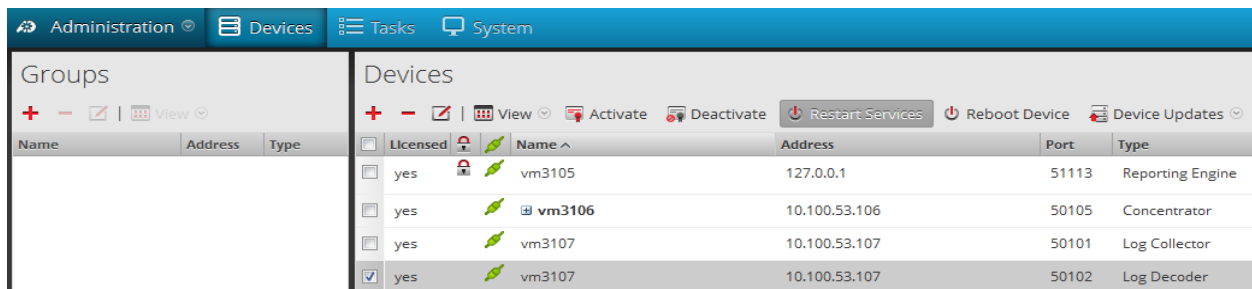
1. Log into the Log Decoder via console or SSH.
2. On the Log Decoder, go to `/etc/netwitness/ng/envision/etc`.
3. Use the name fields in the *index-concentrator-custom.xml* file to determine the list of attributes which need to be modified in the *table-map.xml* file.

- Copy the `table.map.xml` from `/etc/netwitness/ng/envision/etc` to `/etc/netwitness/ng/envision`.
- 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="device_ip" nwName="device.ip" format="Text" flags="None" />
  <mapping envisionName="device_name" nwName="device.name" flags="None" />
  <mapping envisionName="device_type" nwName="device.type" flags="None" />
  <mapping envisionName="device_type_id" nwName="device.type.id" format="Int" flags="Transient" />
  <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="node_name" nwName="node.name" flags="Transient" />
  <mapping envisionName="workspace_desc" nwName="workspace" flags="Transient" />
  <mapping envisionName="workstation" nwName="alias.host" flags="None" />
  <mapping envisionName="zone" nwName="zone" flags="Transient" />
</mappings>
```

- Navigate to **Administration > Devices** and check the **Log Decoder** than click **Restart Services**.



- 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 Raz-Lee iSecurity 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 Raz-Lee iSecurity components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

SIEM Syslog Configuration

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems; web-based alerts are supported using Twitter www.twitter.com (can transmit up to 1000 lines per second). Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, malicious network access to the IBM i and more.

Use iSecurity Audit to set SIEM general alert definitions and use iSecurity Action to determine if SIEM alerts will be generated in individual cases.

The iSecurity SIEM Syslog feature sends event alerts from various IBM i facilities (such as logs and message systems) to a remote RSA Security Analytics server within a range of severities such as Emergency, Alert, Critical, Error, Warning and more.

1. Type **STRAUD** on the IBM i command line; the iSecurity Audit main menu appears. Select option **81. System Configuration**.

```
AUAUDMN                               Audit                               iSecurity/Audit
                                      System: S520

Settings
  1. OS/400 Audit Features
  2. Activation

Real-Time Detection Rules
  11. Real-Time Auditing
  12. Firewall/Screen
  13. Status & Active Job (SysCtl)
  14. Message Queue (SysCtl)

Definitions
  31. Time Groups
  32. General Groups

Selection or command
===> █

Analysis
  41. Queries and Reports
  42. Display Log

Related Modules/Options
  61. Work With Actions
  62. User Management
  63. Display Action Log
  65. Action Main Menu
  66. Native Object Security
  67. User, Pwd, SysVal Replication
  68. Audit for Cross Platform

General
  81. System Configuration
  82. Maintenance Menu
  83. Central Administration
  84. Compliance Evaluator

F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=AS/400 main menu
```


- From the iSecurity/Base System Configuration menu, select option 31. Syslog Definitions.

```

iSecurity/Base System Configuration

Select one of the following:

Audit
  1. General Definitions
  5. Auto start activities in ZAUDIT
  9. Log & Journal Retention
  Action *FYI* Mode Active
  11. General Definitions
  12. SMS Definitions
  13. E-Mail Definitions

Central Administration
  31. Syslog Definitions
  32. SNMP Definitions
  33. Twitter Definitions

Security Event Manager (SEM/SIEM)
  21. QSYSOPR and other message queues
  22. QAUDJRN Type/Sub Severity Setting

Authentication
  71. Setup

General
  91. Language Support
  99. Copyright Notice

Selection ==> █

Release ID . . . . . 11.5 11-01-27 44DE466 520 7459
Authorization code . . . . . ----- 1 1
Authorization code - Native Security . -----
F3=Exit F22=Enter Authorization Code
  
```

- In the **SYSLOG Definitions** screen define whether to send Syslog messages and if so to which IP address, from which facility (list of optional facilities below), in what range of severity (list below) and the format of the message.

```

SYSLOG Definitions

SYSLOG Support
Send SYSLOG messages . . . . .  Y=Yes, N=No, A=Action only
Destination address . . . . . 216.162.248.19

"Facility" to use . . . . . 9 CLOCK DAEMON
"Severity" range to auto send . 0 - 7 Emergency - DEBUG
Sends QAUDJRN edited messages. Use F22 to set.
Send all or after filter . . . . . N A=All, F=After filter
Convert data to CCSID . . . . . 0 0=Default, 65535=No conversion
Maximum length . . . . . 1024 128-9800
Message structure . . . . . &4 iSecurity/ &5 : &3 &1

Mix Variables and constants (except &, %) to compose message:
&1=First level msg &3=Msg Id. &4=System &5=Module
&6=Prod Id. &7=Audit type &8=Host name &9=User
&H=Hour &M=Minute &S=Second &X=Time
&d=Day in month &m=Month (mm) &y=Year (yy) &x=Date
&a/&A=Weekday (abbr/full) &b/&B=Month name (abbr/full)

F3=Exit F12=Cancel F22=Set SYSLOG handling per audit sub-type
  
```

- By using iSecurity Firewall -> 81. System Configuration -> 8. SYSLOG, a user can decide whether they want the SYSLOG to contain all Firewall events (2=All), Rejects only (1) or none (0).

- To prompt and receive alerts, define an **Alert Message** in **Action** (STRACT → 31. **Work with Actions**).

```

Work with Actions
Position to: _____
Type options, press Enter.
  1=Select  3=Copy  4=Delete  5=Run Action  7=Rename  8=Where used

Opt Action      Description
█ *FORGOT      Keep user FORGOT always *ENABLED
- QSEC111955   Created by ActionZ
- QSEC114512   Created by Action 2
- QSEC120754   Created by Action
- QSEC121040   Created by Action
- QSEC122323   Created by Action
- QSEC122533   Created by Action
- QSEC170020   Created by Action

F3=Exit  F6=Add new  F8=Print  F12=Cancel

Bottom
  
```

- Type 1 to select an Action to modify or press F6 to add a new Action. Follow the definitions screens to define pre-defined message text and one or more recipient addresses. You may prefer to have the system send a default message or you may select a pre-defined message. Finally, specify how to send the alert using the screen below.

```

*FYI* Mode Active      Modify Alert Message
Type choices, press Enter.

Action Name . . . . . ACT001
Description . . . . . █

Define alert message recipients
1=E-mail  2=Message Queue  3=User  4=Remote User  5=LAN user  6=SMS  7=Special
8=Syslog  9=SNMP          T=Twitter
Message ID . . . . . *AUTO          *AUTO, Message ID

Type  Recipient address, *USER, *DEV, *JOB, *SYSTEM
 1    MARKETING@RAZLEE.COM
 2    QSECOFR
 8
 9
-
More...

F3=Exit  F4=Prompt          F12=Cancel
  
```

Modify Alert Message

Your rule may send alert messages to designated personnel via one or more of the following methods:

- E-mail
- Local workstation message queue using the *SENDMSG TOMSGQ* command
- Local user message queue using the *SENDMSG TOUSER* command
- Remote user on another System over the SNADS network using the *SENDNETMSG* command
- SMS to a cellular telephone
- SYSLOG
- SNMP

Certification Checklist for RSA Security Analytics

Date Tested: December 2, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.2SP2	Virtual Appliance
IBM-i	7.1	OS/400 V5R3 or higher
Raz-Lee iSecurity	11.4	IBM-i

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	✓

GLS / PAR

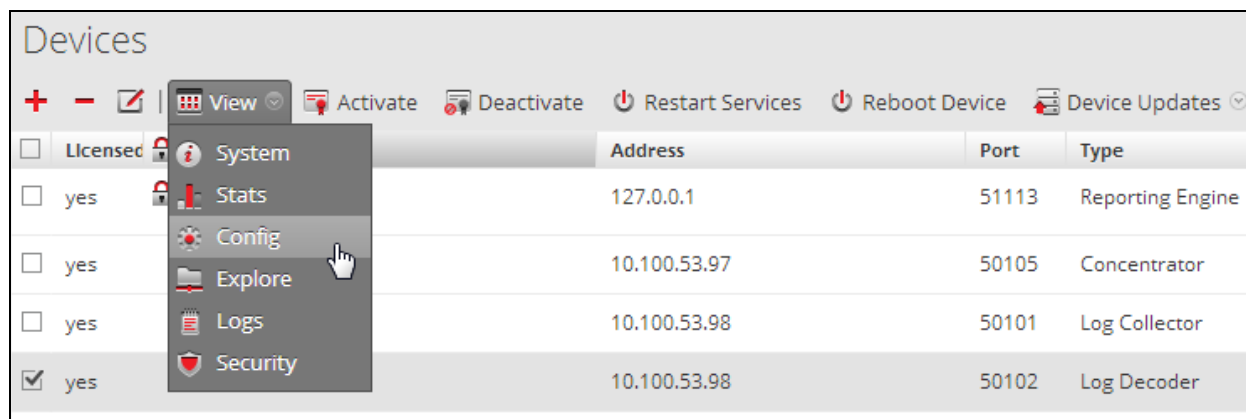
✓ = Pass ✗ = Fail N/A = Non-Available Function

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**.



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.