Secude

Halocore for SAP NetWeaver

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: January 26, 2016

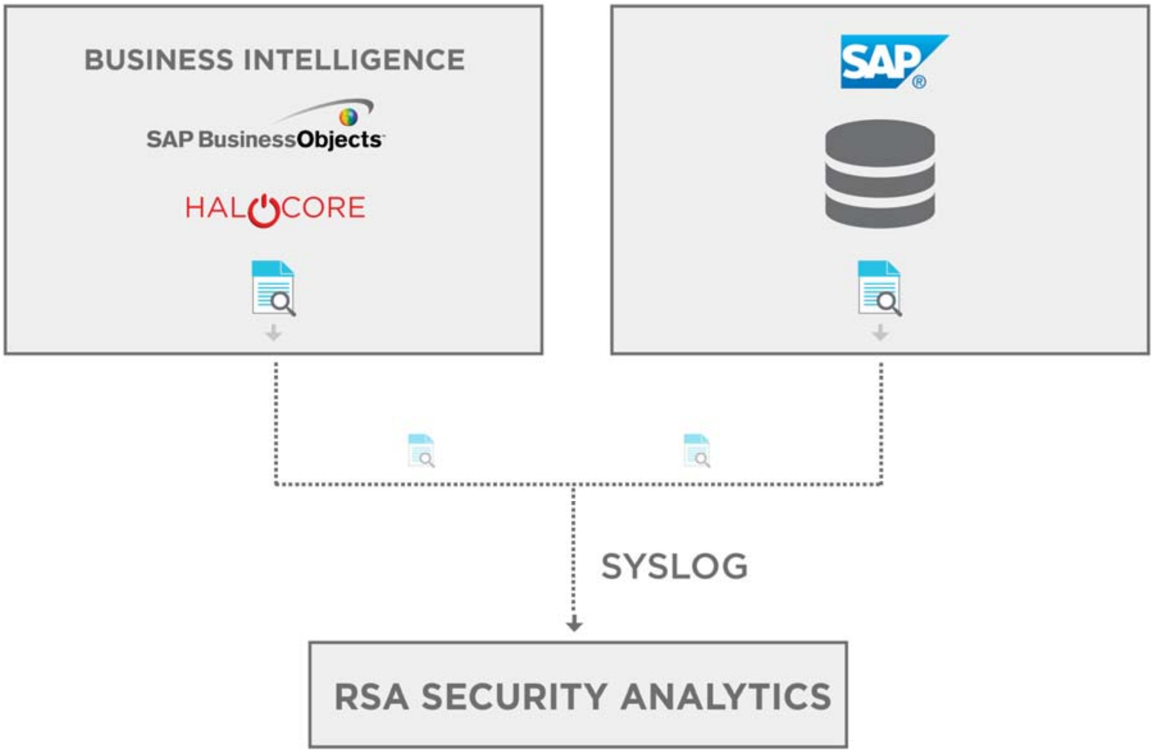
Partner Information

Product Information	
Partner Name	Secude
Web Site	www.secude.com
Product Name	Halocore
Version & Platform	Halocore v3.8/ BI Launchpad 4.1 minimum SP2.
Product Description	Halocore is an SAP data security solution that identifies sensitive data with context-aware classification, prevents potential data loss by blocking the export of highly confidential information out of SAP, persistently protects exported data with Rights Management policies, and logs data movement for auditing purposes.

Solution Summary

Halocore captures information surrounding all data exported from SAP from various exit points including the Business Intelligence Launchpad 4.1. The information collected in SAP & BO includes key insightful attributes such as file name, size, type, source and destination IP, event type, and so on and is valuable in assessing risk, maintaining compliance, or to track the movement of highly confidential data. By integrating these Halocore's Activity Logs with RSA's Security Analytics, the enterprise now has a broad overview of enterprise information and events which includes export behavior of sensitive SAP data from Crystal Reports and Web Intelligence modules. Halocore pushes the events as they occur within SAP to the RSA server and these SAP events are tagged for easy identification.

RSA Security Analytics Features	
Halocore for SAP NetWeaver	
Integration package name	Common Event Format
Device display name within Security Analytics	secude_halocore
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. All Security Analytics customers and partners are invited to register and participate in the **RSA Security Analytics Community**.

Release Notes

Release Date	What's New In This Release
1-26-2016	Initial support for Secude Halocore for SAP Netweaver.

! ▸ Important: The RSA SA CEF parser is dependent on the integrating partner adhering to the CEF Rules outlined in the Arcsite guidelines document for CEF Header Information. A copy of the Common Event Format guide can be found on http://protect724.hp.com/**.**

Eg. Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

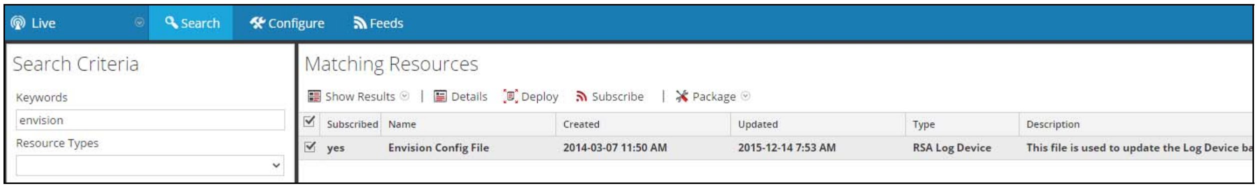
! ▸ Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.

Deploy 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:

Note: 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**.

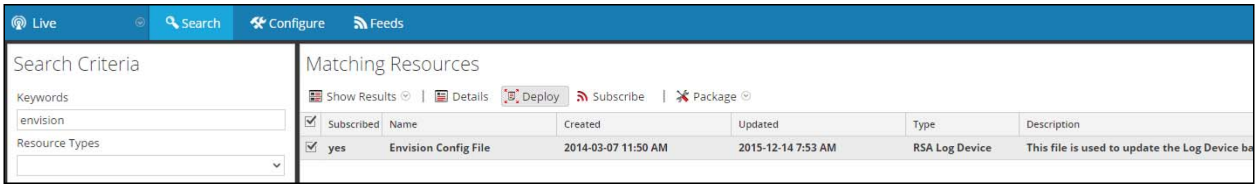


Keywords: envision

Resource Types:

☑	Subscribed	Name	Created	Updated	Type	Description
☑	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

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

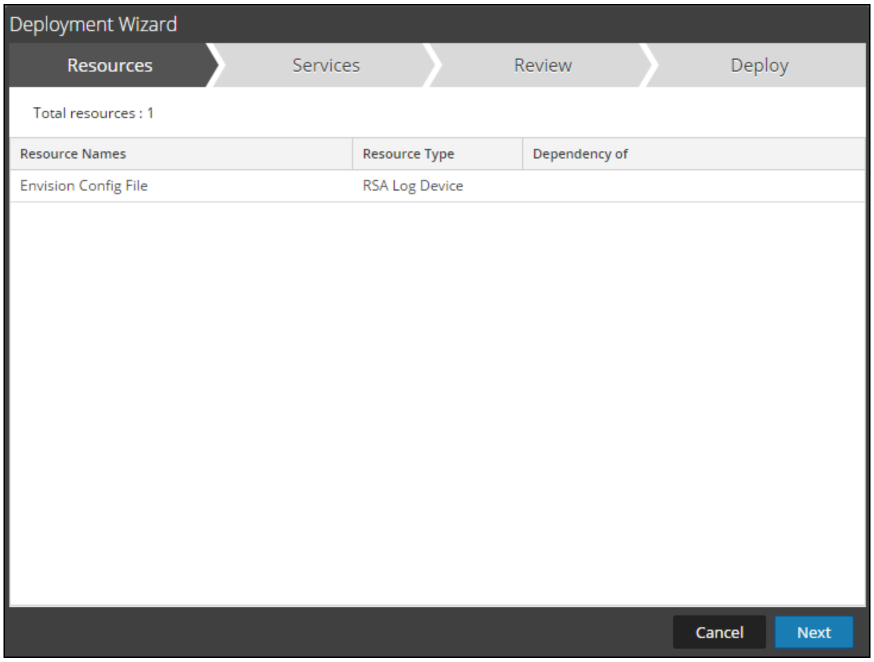


Keywords: envision

Resource Types:

☑	Subscribed	Name	Created	Updated	Type	Description
☑	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**.

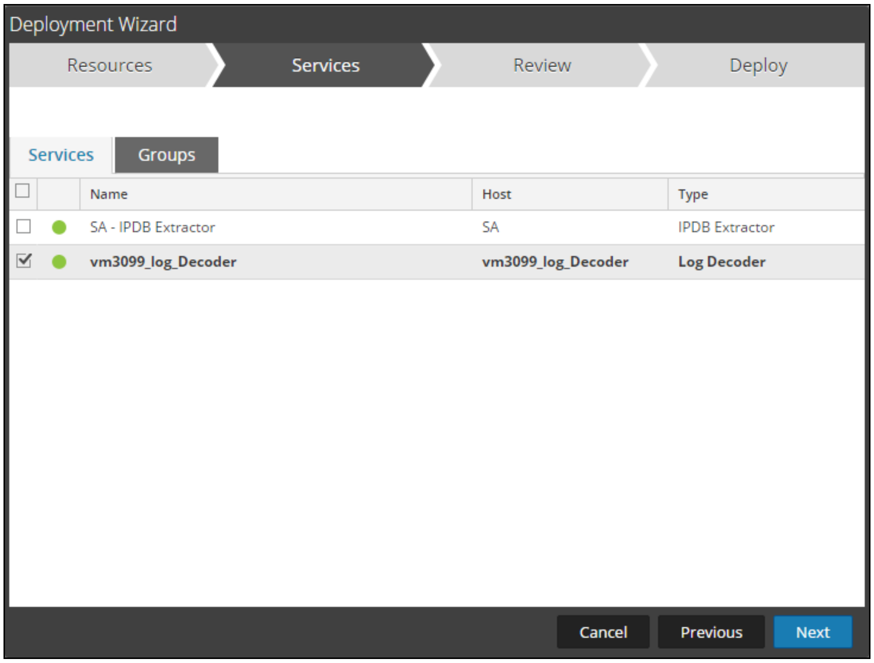


Deployment Wizard

Total resources : 1

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

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

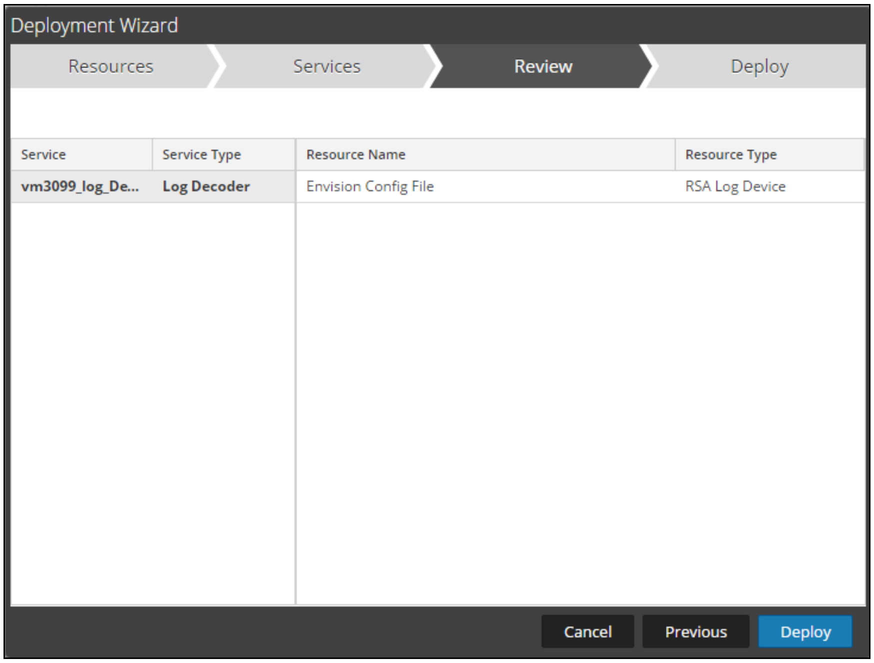


Deployment Wizard

□		Name	Host	Type
□	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	vm3099_log_Decoder	vm3099_log_Decoder	Log Decoder

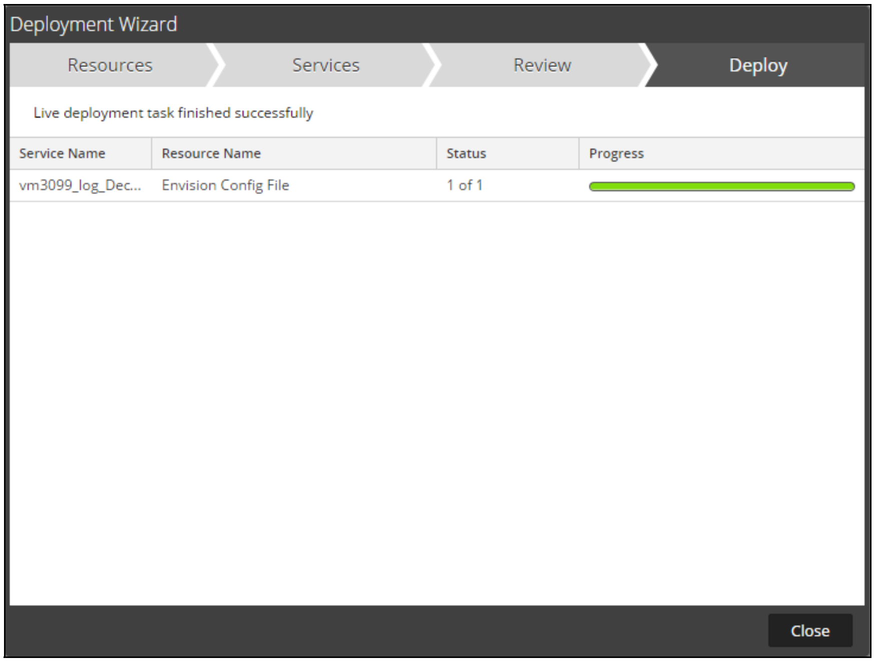
Note: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



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

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



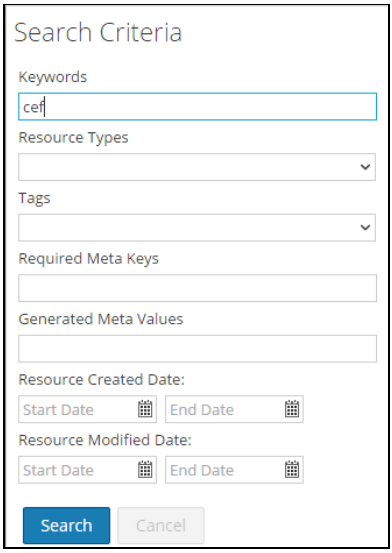
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3099_log_Dec...	Envision Config File	1 of 1	

Deploy Common Event Format

In order to use RSA Partner created content, you must first deploy the *Common Event Format file* from the **Security Analytics Live** module. Log into Security Analytics and perform the following actions:

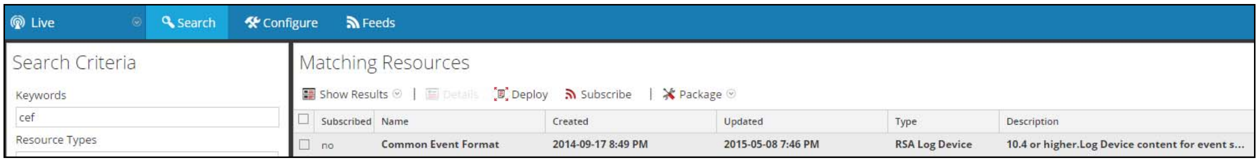
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **CEF**



Search Criteria

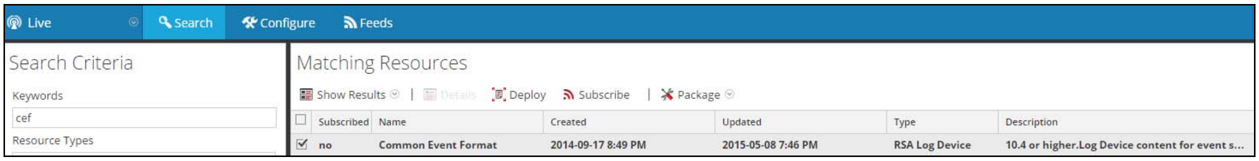
Keywords: cef

3. Security Analytics will display the **Common Event Format** in Matching Resources.



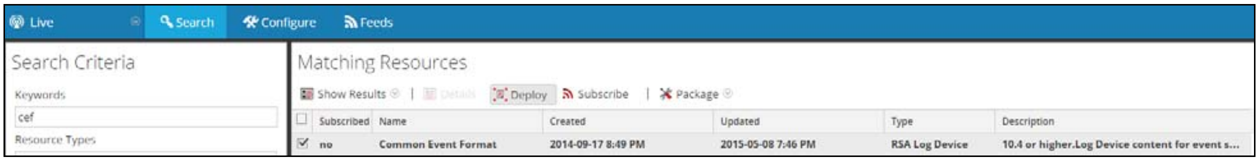
□	Subscribed	Name	Created	Updated	Type	Description
□	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

4. Select the checkbox next to **Common Event Format**.



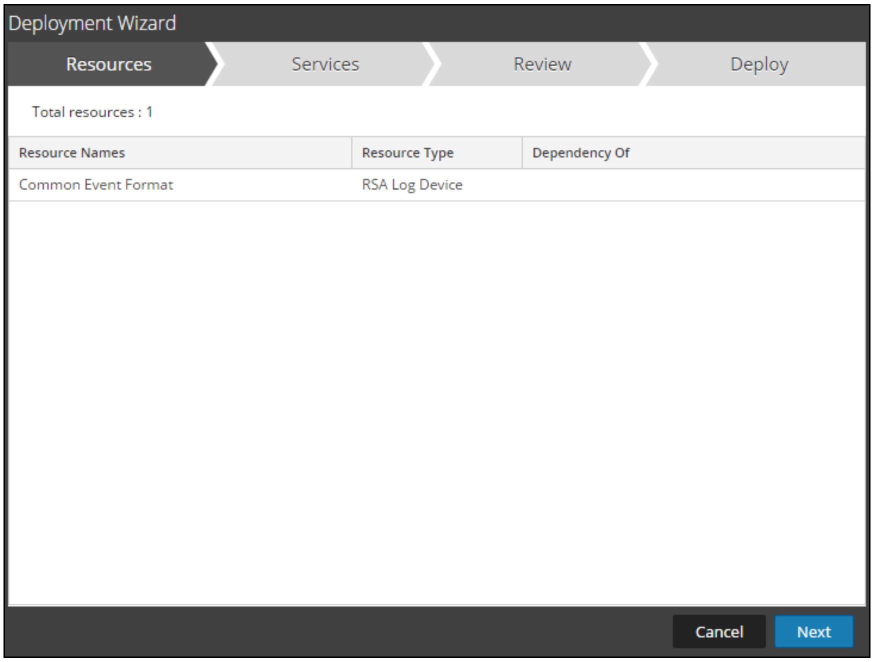
□	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

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



□	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

6. Select **Next**.

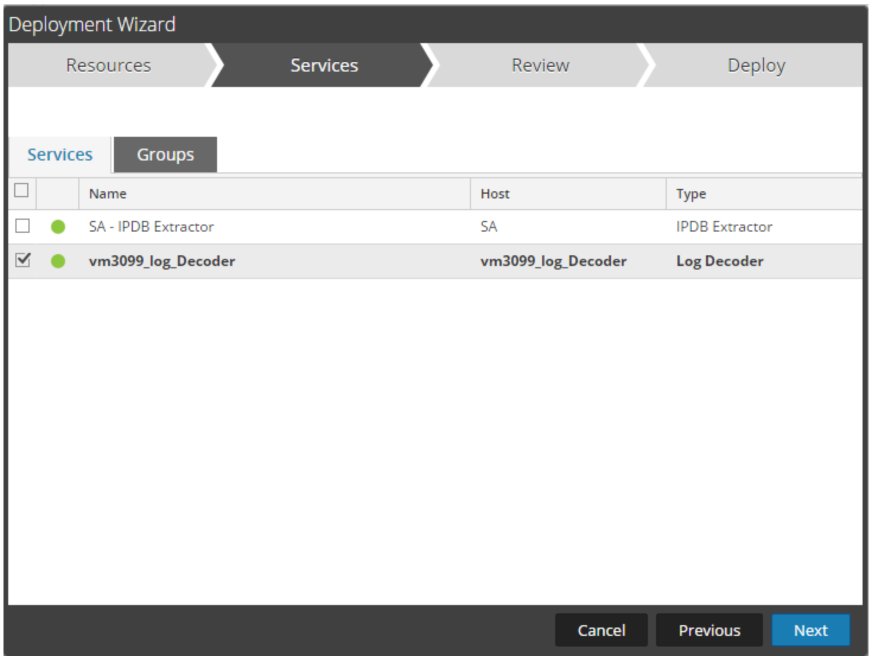


Deployment Wizard

Total resources : 1

Resource Names	Resource Type	Dependency Of
Common Event Format	RSA Log Device	

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

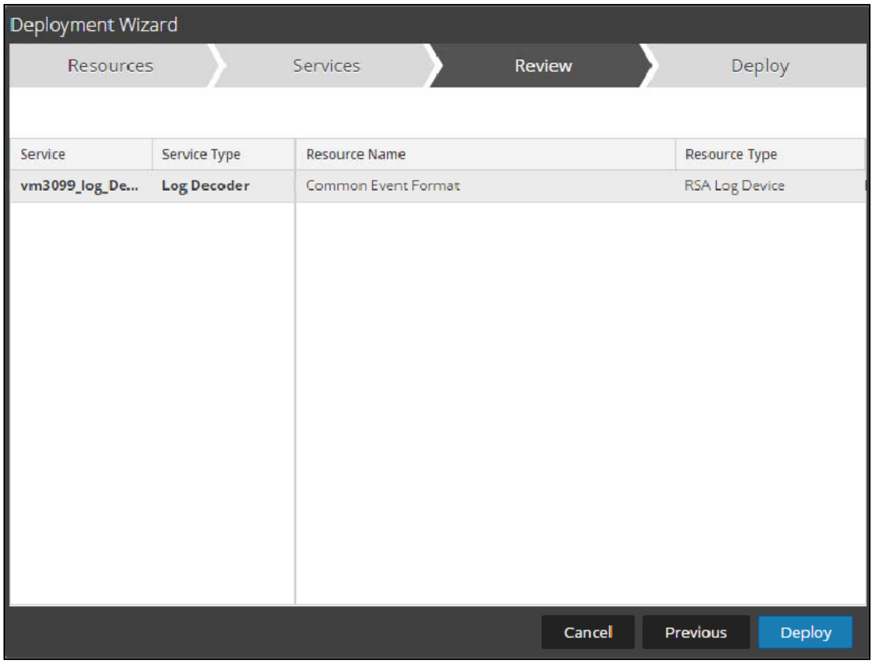


Deployment Wizard

☐		Name	Host	Type
☐	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	**vm3099_log_Decoder**	**vm3099_log_Decoder**	**Log Decoder**

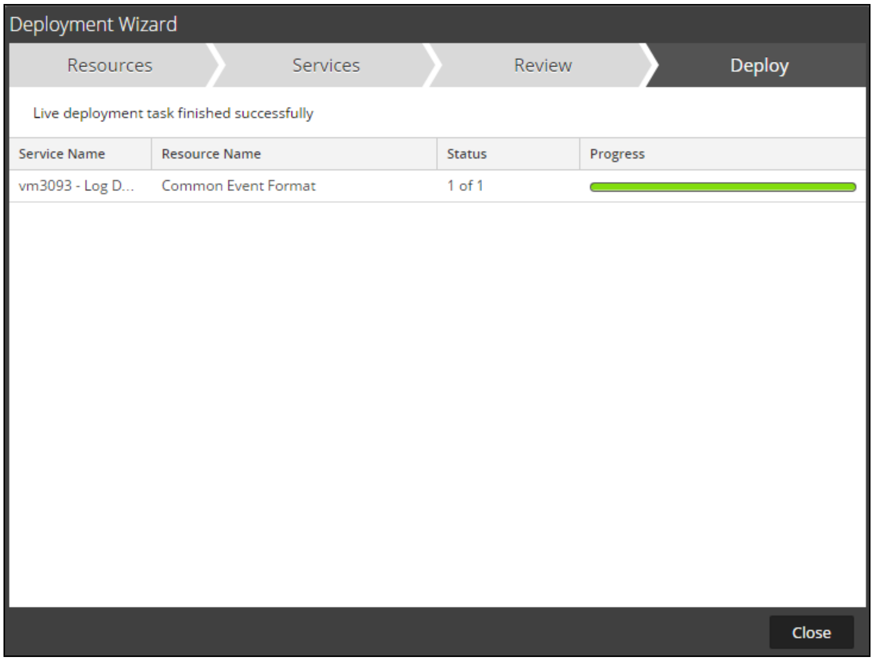
Note: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	Log Decoder	Common Event Format	RSA Log Device

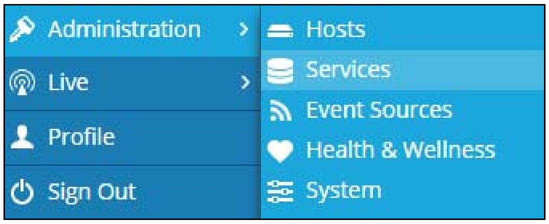
9. Select **Close**, to complete the deployment of the Common Event Format.



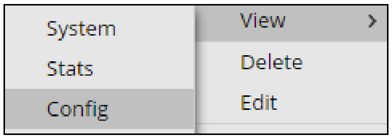
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3093 - Log D...	Common Event Format	1 of 1	🟩

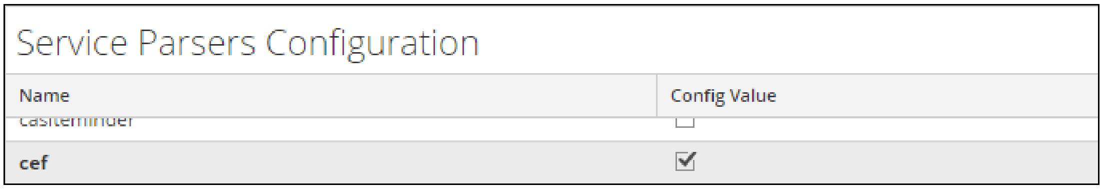
10. Insure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the SA Dashboard.



11. Locate the Log_Decoder and click the gear ⚙ to the right and select **View, Config**.



12. **Check** the box next to the CEF Parser within the Service Parsers Configuration and select **Apply**.



Service Parsers Configuration

Name	Config Value
casiteminder	☐
cef	☑

13. Restart the **Log Decoder services**.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Secude Halocore 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 Secude Halocore components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Filename	File Function
Common Event Format	SA Live package deployed to parse events from device integrations.

Secude Halocore Configuration

After completing the previous section, *Deploy Common Event Format Content File*, you can now collect events from most sources supporting the Common Event Format (CEF).

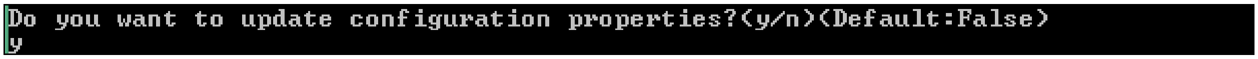
Create an overview of the steps that will be taken to provide interoperability. Use the overview steps as headings for each section as you document the integration.

Administrative Software

- halocore-tools-3.8.X.X.jar

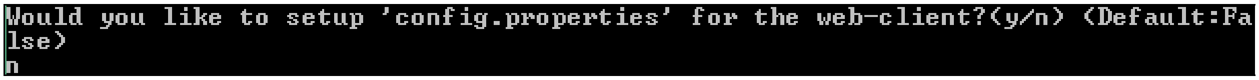
Configuration Steps

1. Stop the Tomcat on the system which Halocore Central is running.
2. Open a command line (cmd) or terminal, dependent on the System OS.
3. Change the directory to the location of halocore-tools-3.8.X.X.jar.
4. Start Halocore –tools with java –jar halocoretools-3.8.X.X.jar EN



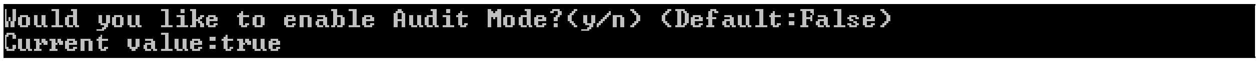
```
Do you want to update configuration properties?(y/n)(Default:False)
y
```

5. Press y and return.



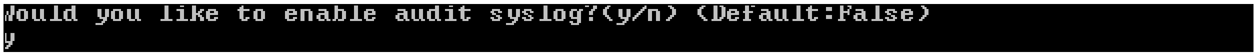
```
Would you like to setup 'config.properties' for the web-client?(y/n) (Default:Fa
lse)
n
```

6. Press n and return.



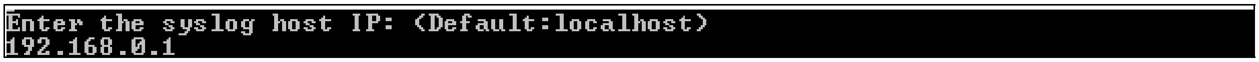
```
Would you like to enable Audit Mode?(y/n) (Default:False)
Current value:true
```

7. If not yet set to true press y and return, else simple press return.



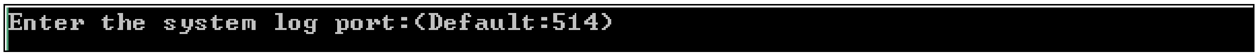
```
Would you like to enable audit syslog?(y/n) (Default:False)
y
```

8. Enable Syslog with y and pressing return.



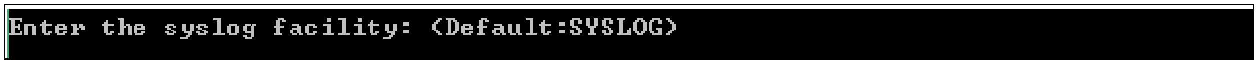
```
Enter the syslog host IP: (Default:localhost)
192.168.0.1
```

9. Enter the IP Address from the RSA Server.



```
Enter the system log port:(Default:514)
```

10. Enter the Port of Syslog from the RSA Server, (usually 514).



```
Enter the syslog facility: (Default:SYSLOG)
```

11. Use default facility by pressing return.

List of custom CEF keys and values not captured by RSA Security Analytics

```
cs2Label=DataDestination
cs2=" "
cs3Label=DataOrigin
cs3=" "
cs4Label=ClassifyProtectionData
cs4=" "
```

Certification Checklist for RSA Security Analytics

Date Tested: January 26, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.5	Virtual Appliance
Halocore	3.8	

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	✓

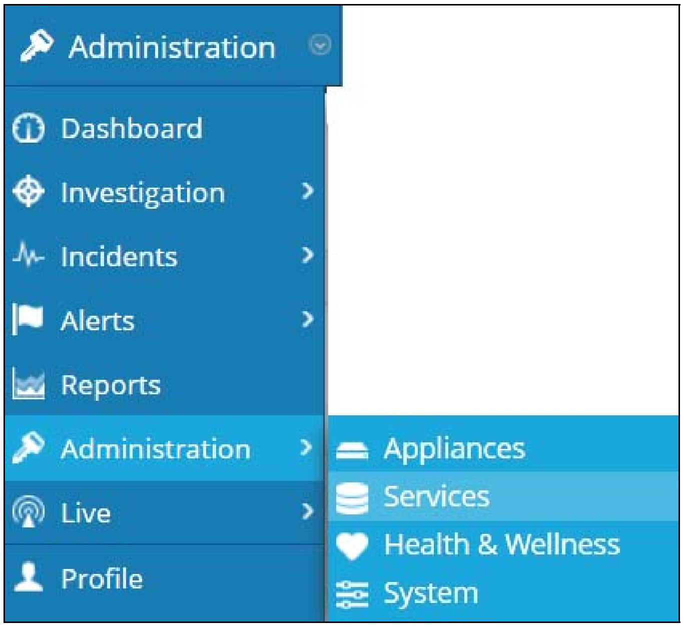
DRP / PAR ✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

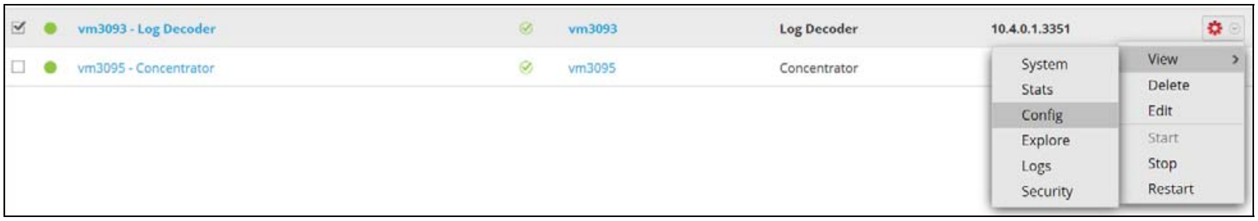
Security Analytics Disable the Common Event Format Parser

To disable the Security Analytics Common Event Format Parser without deleting it perform the following:

1. Select the Security Analytics **Administration > Services menu**.

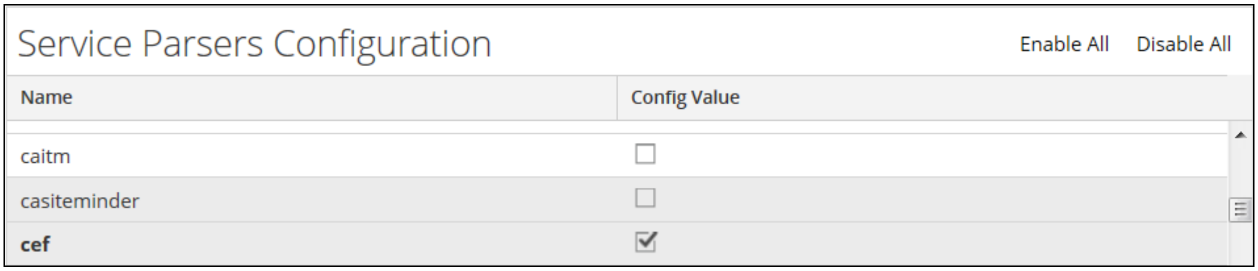


2. Select the Log Decoder, then select **View > Config.**



☑	●	vm3093 - Log Decoder	✓	vm3093	Log Decoder	10.4.0.1.3351
□	●	vm3095 - Concentrator	✓	vm3095	Concentrator	

3. From the **Service Parses Configuration** window, scroll down to the CEF parser and uncheck the Config Value checkbox.



Service Parsers Configuration

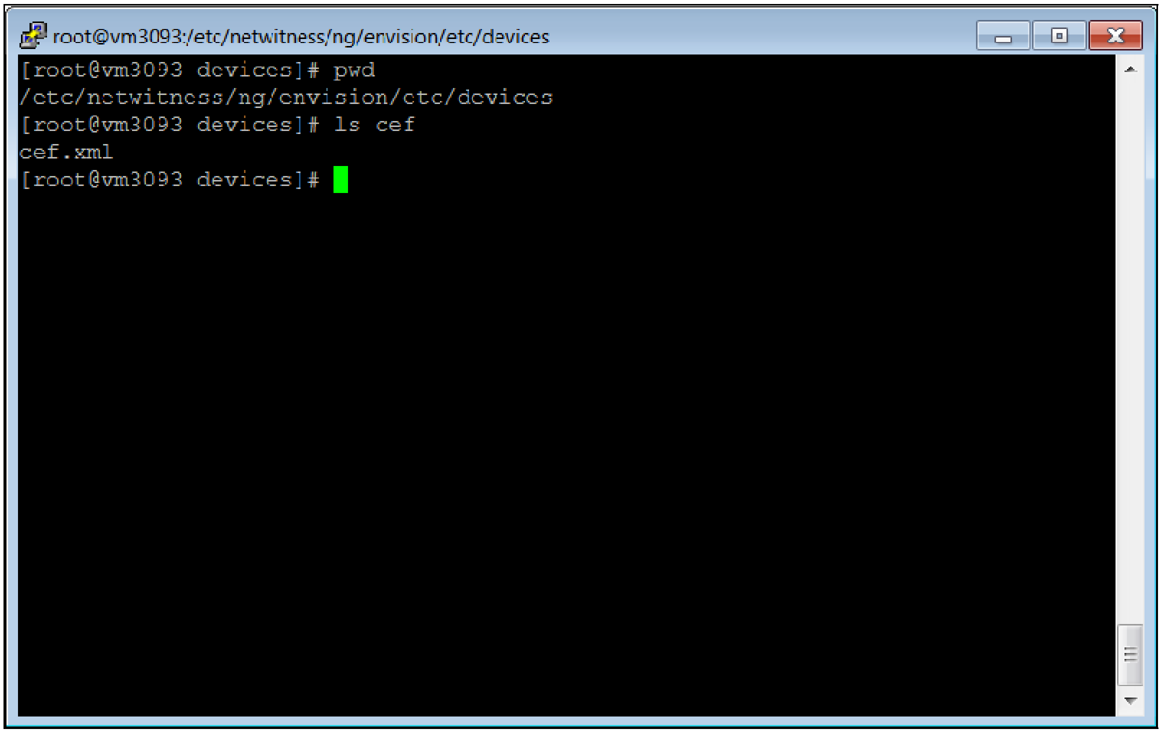
Name	Config Value
caitm	□
casiteminder	□
cef	☑

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.



```
[root@vm3093 devices]# pwd
/etc/netwitness/ng/envision/etc/devices
[root@vm3093 devices]# ls cef
cef.xml
[root@vm3093 devices]#
```

2. Search for and delete the CEF folder and its contents.