RSA® NETWITNESS®

Logs

Implementation Guide

DataSunrise 3.7

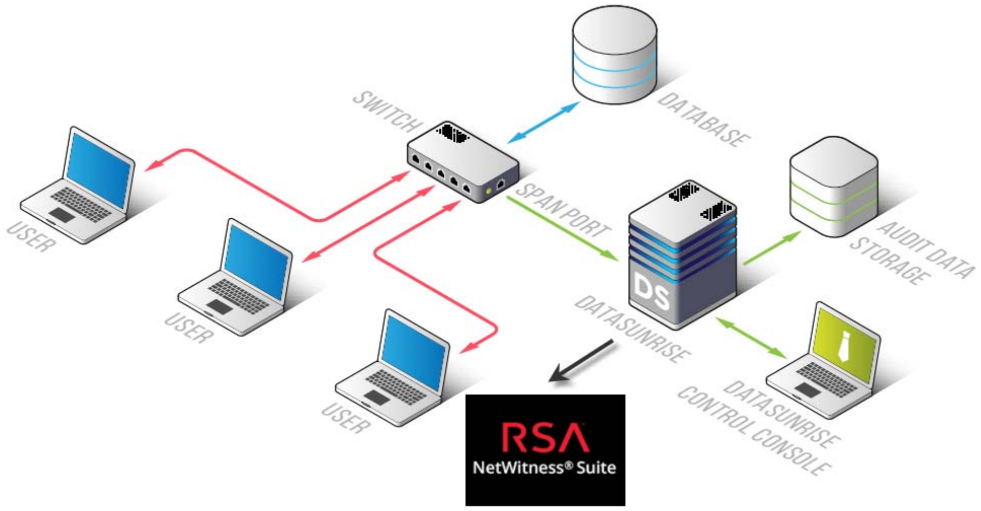
Daniel R. Pintal, RSA Partner Engineering

Last Modified: May 15, 2017

Solution Summary

DataSunrise and RSA Netwitnes

RSA NetWitness Features	
DataSunrise 3.7	
Integration package name	Common Event Format
Device display name within Security Analytics	datasunrise_datasunrise_database_security_suite
Event source class	Analysis
Collection method	Syslog



RSA NetWitness Community

The RSA NetWitness Community is an online forum for customers and partners to exchange technical information and best practices with each other. All NetWitness customers and partners are invited to register and participate in the **RSA NetWitness Community**.

Release Notes

Release Date	What's New In This Release
MM/DD/YYYY	Initial support for DataSunrise 3.7

! Important: The RSA NetWitness CEF parser is dependent on the partner adhering to the CEF Rules outlined in the *ArcSight Common Event Format (CEF) Guide*. 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.

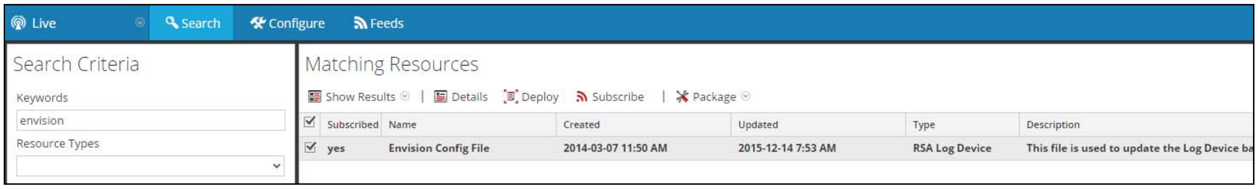
RSA NetWitness Configuration

Deploy the enVision Config File

In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

! > Important: Using this procedure will overwrite the existing table_map.xml.

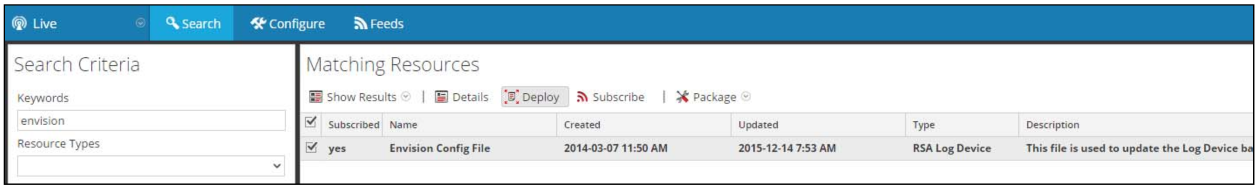
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



Keywords: envision

☑	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

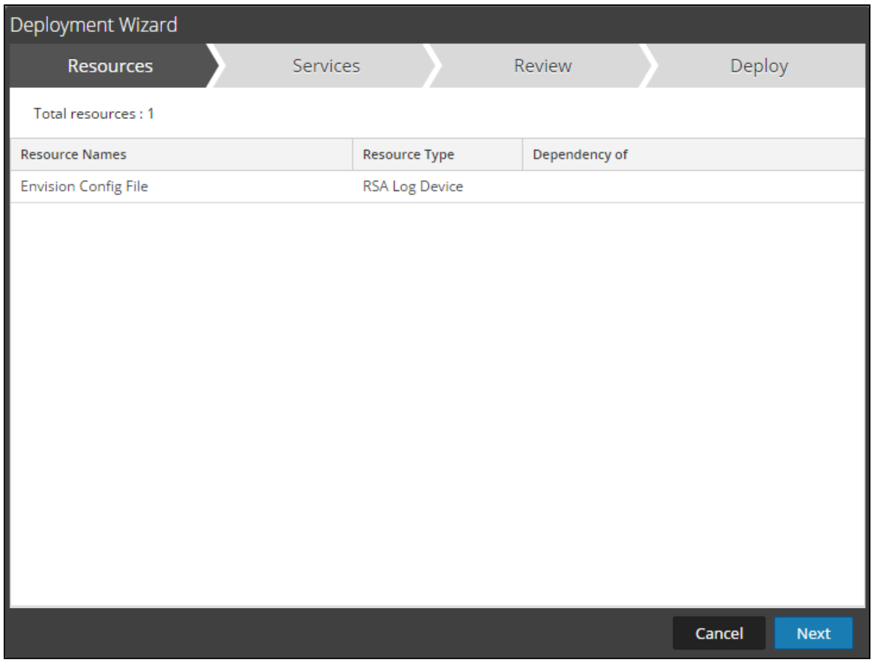
5. Click **Deploy** in the menu bar.



Keywords: envision

☑	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

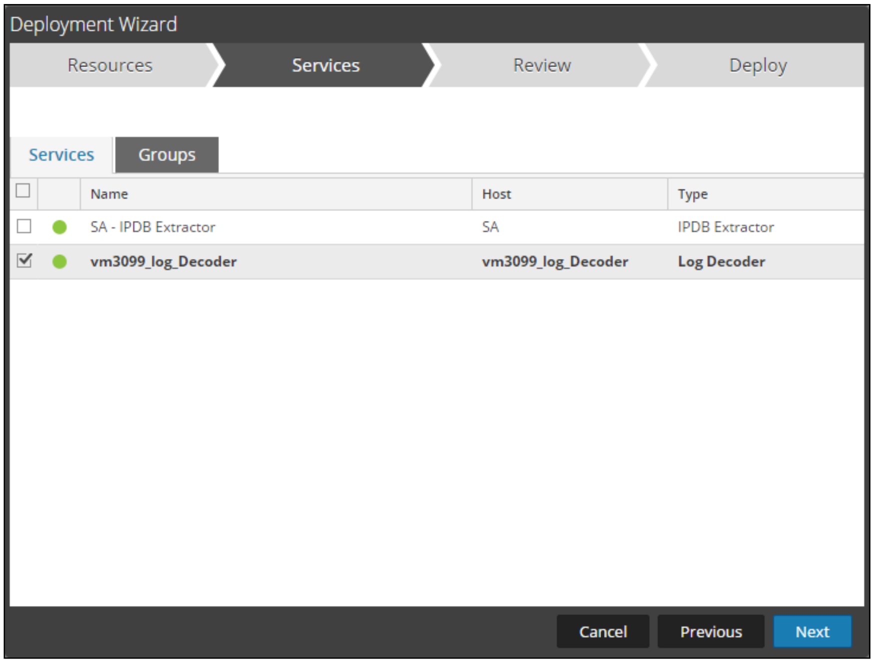
6. Select **Next**.



Total resources : 1

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

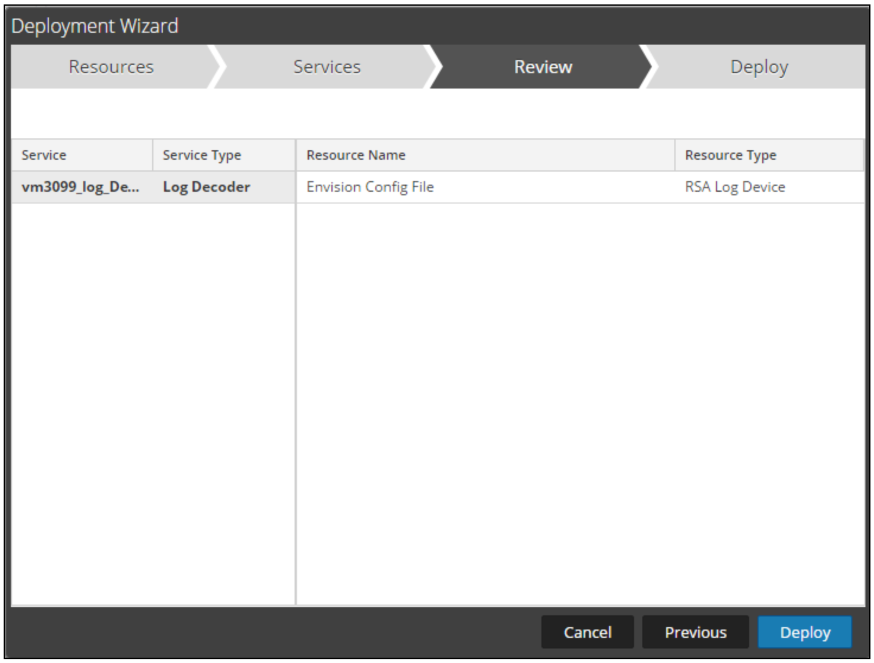
7. Select the **Log Decoder** and select **Next**.



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

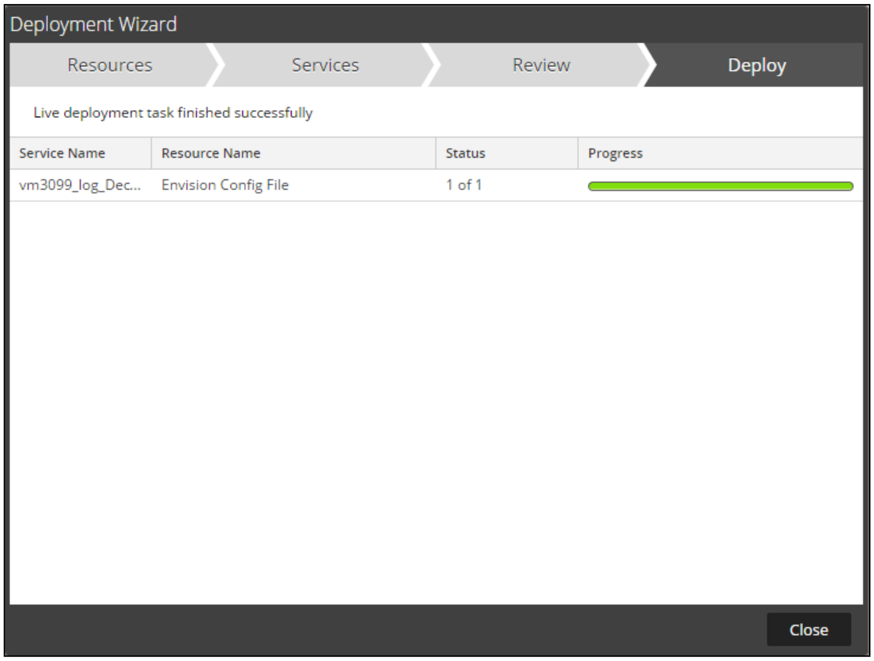
! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

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.



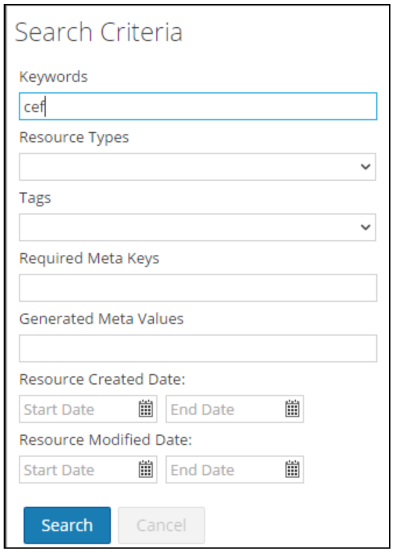
Live deployment task finished successfully

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

Deploy the Common Event Format

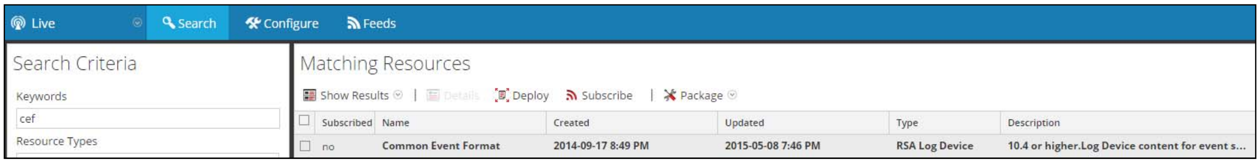
Next, you will need to deploy the *Common Event Format file* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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



Keywords: cef

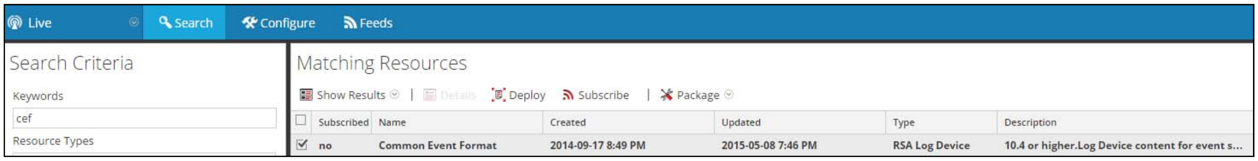
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



Keywords: cef

☐	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...

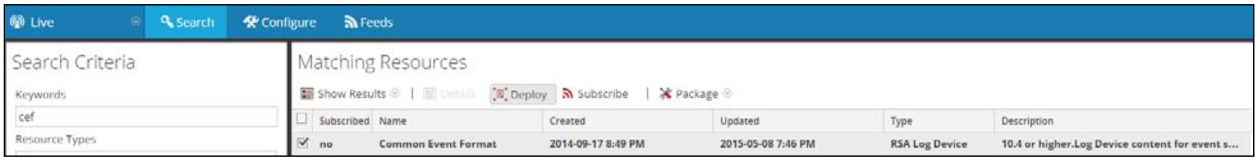
4. Select the checkbox next to **Common Event Format**.



Keywords: cef

☐	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...

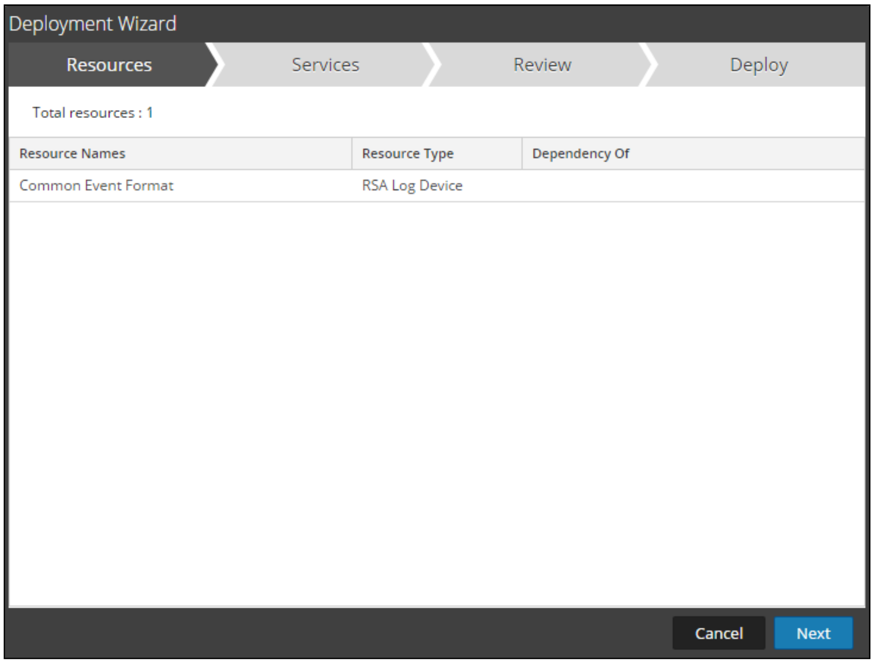
5. Click **Deploy** in the menu bar.



Keywords: cef

☐	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...

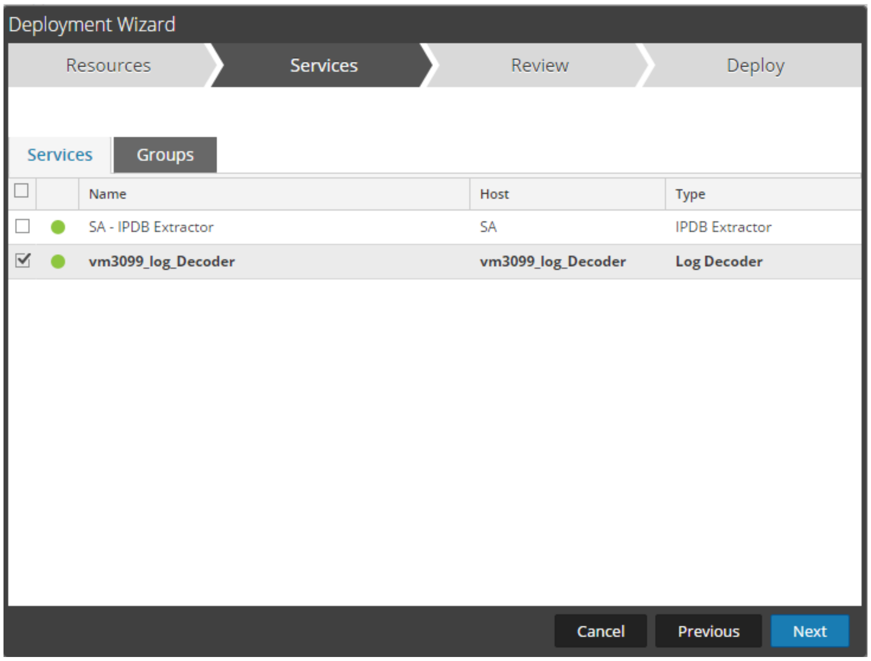
6. Select **Next**.



Total resources : 1

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

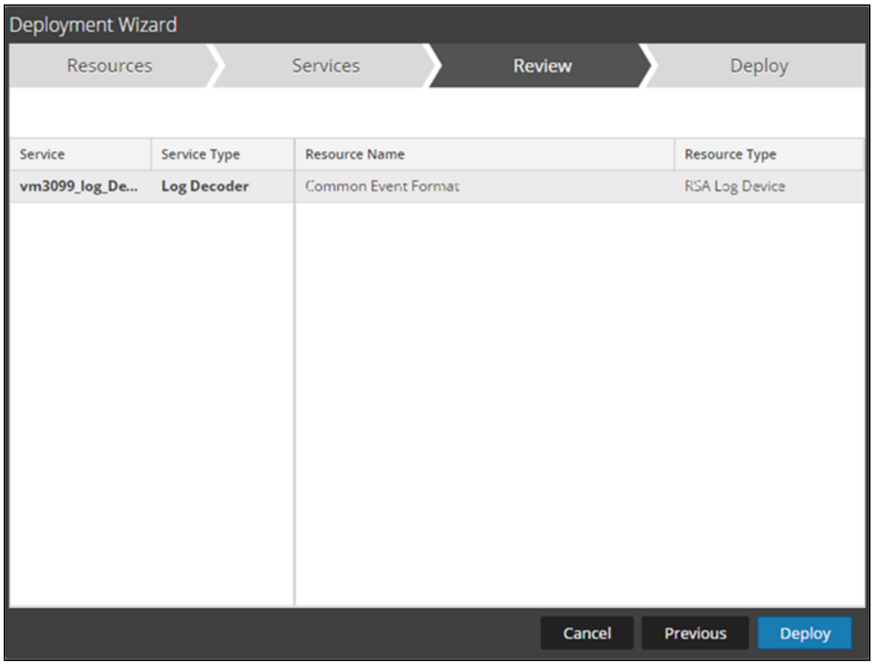
7. Select the **Log Decoder** and Select **Next**.



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

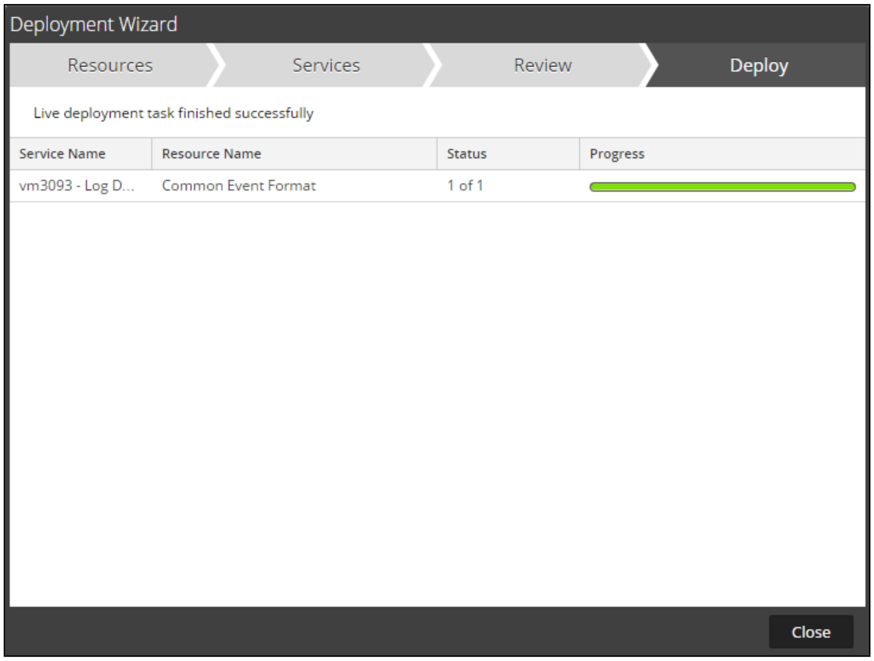
! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



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

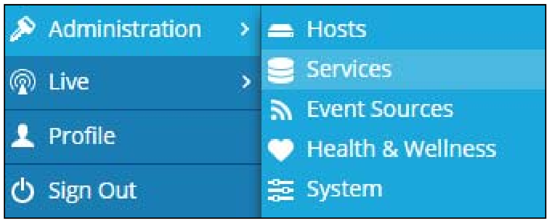
9. Select **Close**, to complete the deployment of the Common Event Format.



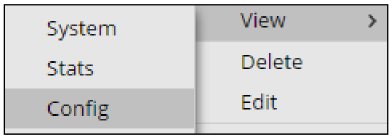
Live deployment task finished successfully

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

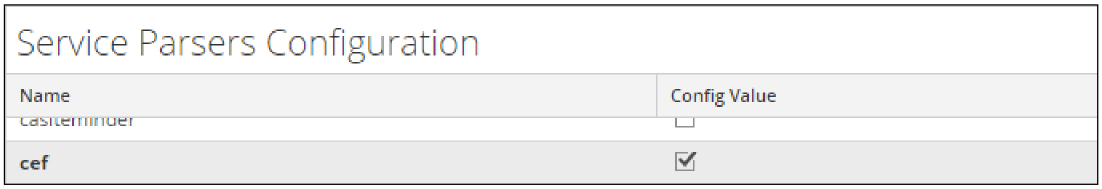
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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



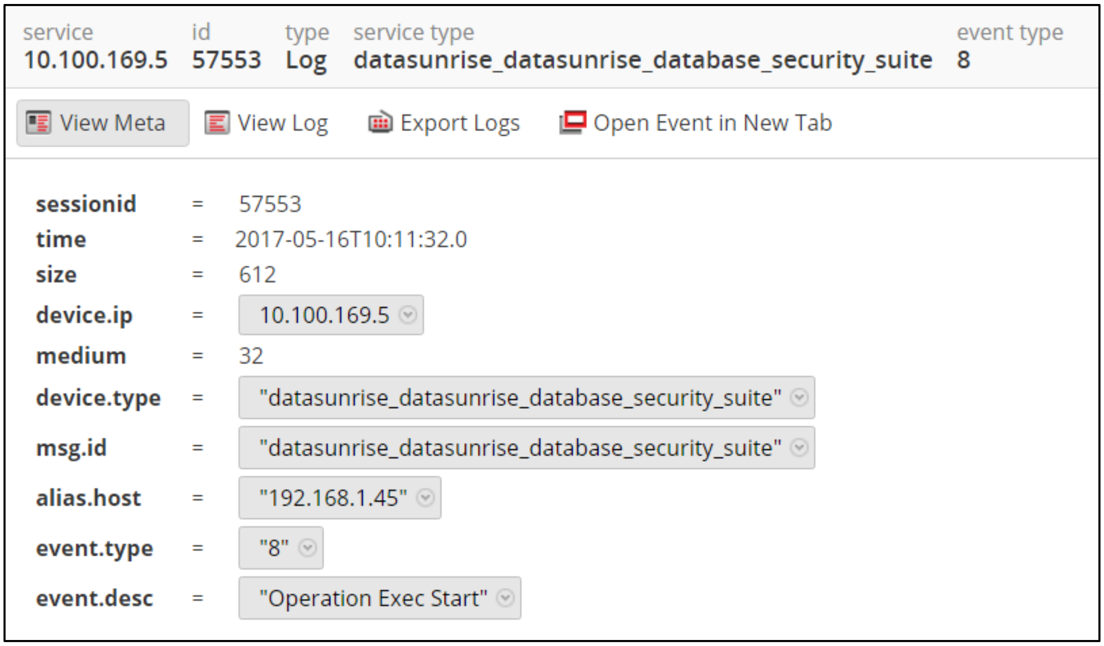
12. **Check** the box next to the cef Parser within the Service Parsers Configuration and select **Apply**.



Service Parsers Configuration

Name	Config Value
casiteminder	☐
cef	☑

13. Restart the **Log Decoder services**.
14. Below is an example of an event received from Attivo through the Netwitness Investigator.



service	id	type	service type	event type
10.100.169.5	57553	Log	datasunrise_datasunrise_database_security_suite	8

```
sessionid    =  57553
time         =  2017-05-16T10:11:32.0
size         =  612
device.ip    =  10.100.169.5
medium       =  32
device.type  =  "datasunrise_datasunrise_database_security_suite"
msg.id       =  "datasunrise_datasunrise_database_security_suite"
alias.host   =  "192.168.1.45"
event.type   =  "8"
event.desc   =  "Operation Exec Start"
```

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the DataSunrise 3.7 with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

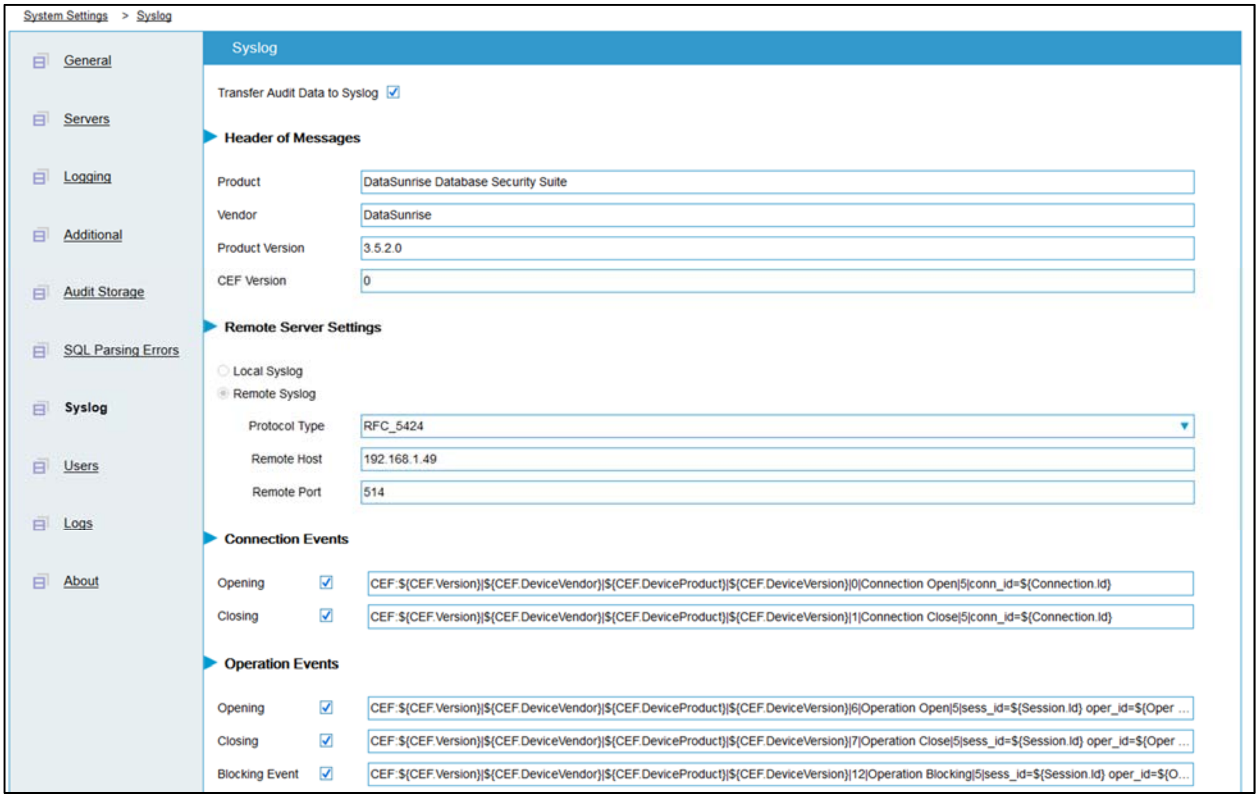
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All DataSunrise 3.7 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 DataSunrise 3.7 is properly configured and secured before deploying to a production environment. For more information, please refer to the DataSunrise 3.7 documentation or website.

DataSunrise 3.7 Configuration

1. Select **System Settings** > **Syslog** and within Remote Server Settings, set the Remote Host to the IP Address of your RSA Netwitness Log Decoder.



Transfer Audit Data to Syslog ☑

Header of Messages

Product: DataSunrise Database Security Suite
Vendor: DataSunrise
Product Version: 3.5.2.0
CEF Version: 0

Remote Server Settings

○ Local Syslog
● Remote Syslog

Protocol Type: RFC_5424
Remote Host: 192.168.1.49
Remote Port: 514

Connection Events

Opening ☑ `CEF:${CEF.Version}|${CEF.DeviceVendor}|${CEF.DeviceProduct}|${CEF.DeviceVersion}|0|Connection Open|5|conn_id=${Connection.Id}`
Closing ☑ `CEF:${CEF.Version}|${CEF.DeviceVendor}|${CEF.DeviceProduct}|${CEF.DeviceVersion}|1|Connection Close|5|conn_id=${Connection.Id}`

Operation Events

Opening ☑ `CEF:${CEF.Version}|${CEF.DeviceVendor}|${CEF.DeviceProduct}|${CEF.DeviceVersion}|6|Operation Open|5|sess_id=${Session.Id} oper_id=${Oper ...`
Closing ☑ `CEF:${CEF.Version}|${CEF.DeviceVendor}|${CEF.DeviceProduct}|${CEF.DeviceVersion}|7|Operation Close|5|sess_id=${Session.Id} oper_id=${Oper ...`
Blocking Event ☑ `CEF:${CEF.Version}|${CEF.DeviceVendor}|${CEF.DeviceProduct}|${CEF.DeviceVersion}|12|Operation Blocking|5|sess_id=${Session.Id} oper_id=${O...`

Certification Checklist for RSA NetWitness

Date Tested: May 15, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
DataSunrise	3.7	

Security Analytics Test Case	Result
Device Administration	
Partner’s device name appears in Device Parsers Configuration	✓
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

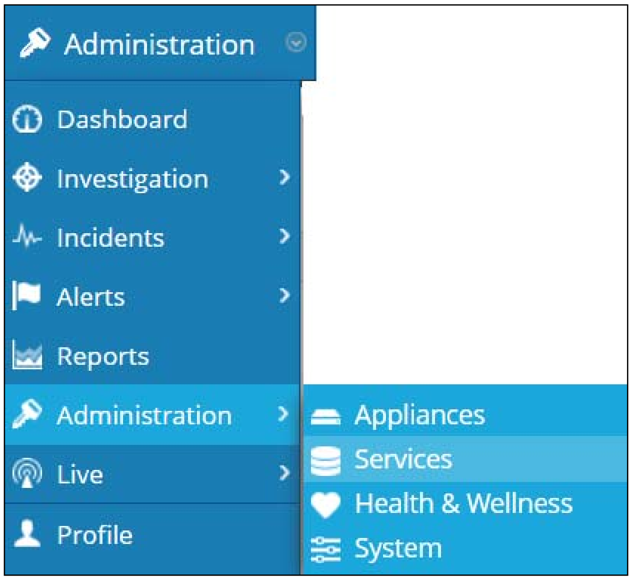
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

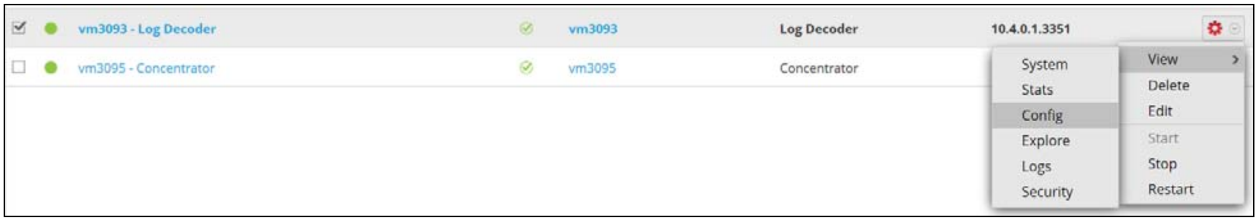
Security Analytics Disable the Common Event Format Parser

To disable the Security Analytics Common Event Format Parser and not delete it perform the following:

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

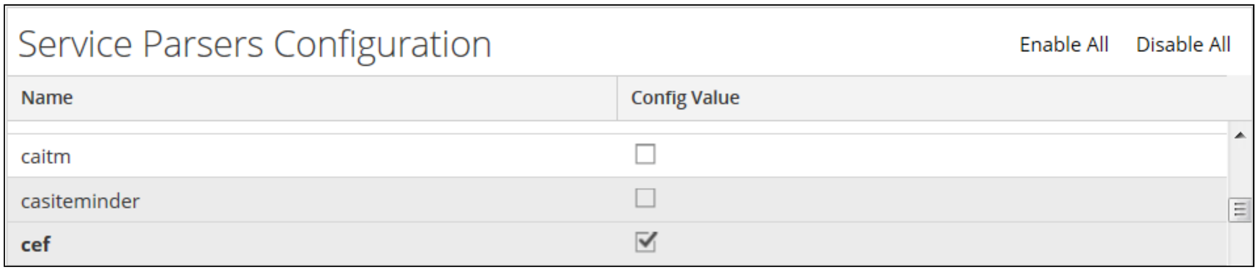


2. Select the Log Decoder, then select **View > Config.**



☑	●	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

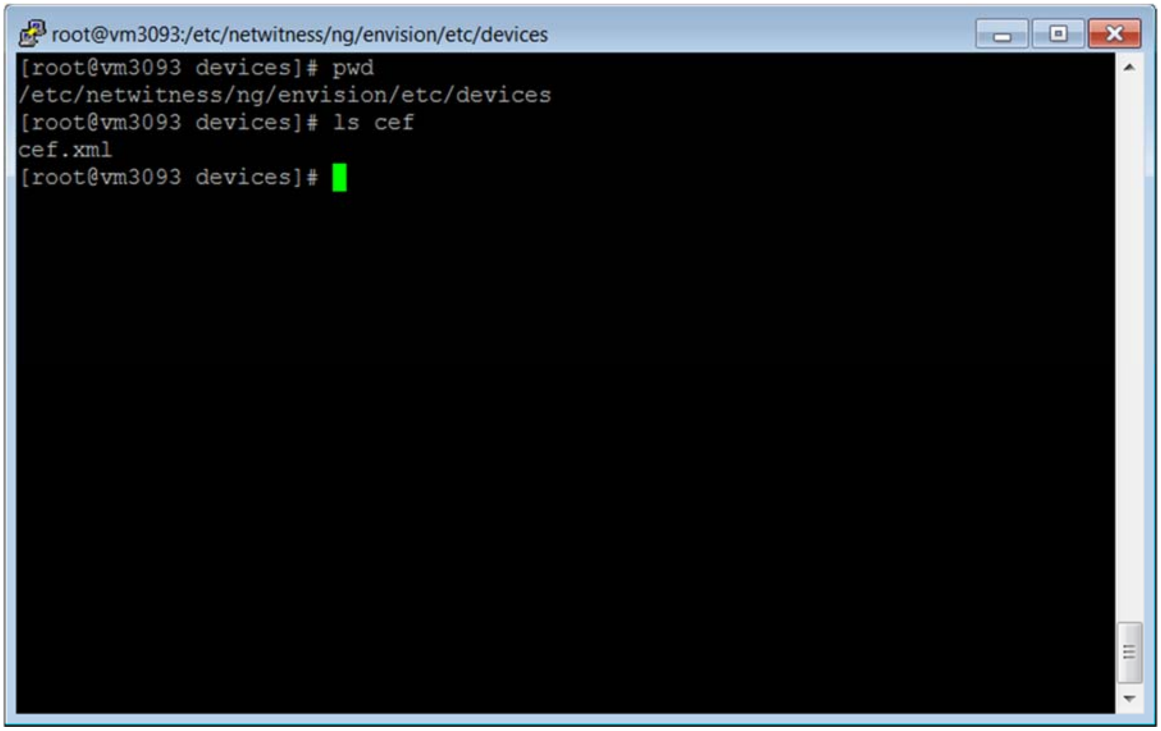
Name	Config Value
caitm	□
casiteminder	□
cef	☑

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.