RSA® NETWITNESS®

Logs

Implementation Guide

SkyFormation, SkyFormation 2.2.4

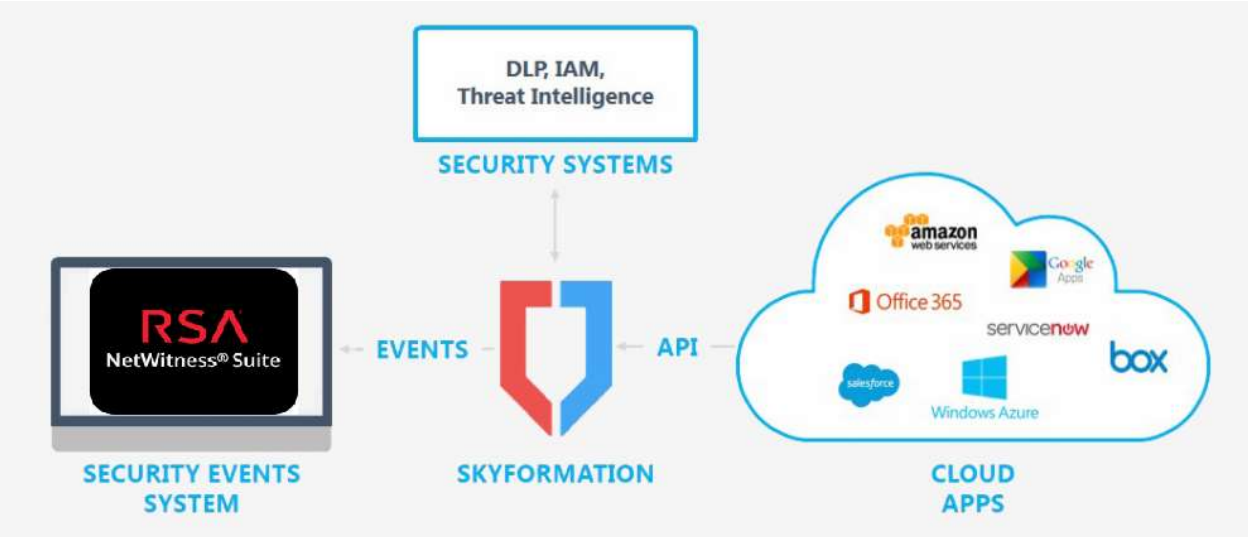
Daniel R. Pintal, RSA Partner Engineering
Last Modified: January 24, 2018

Solution Summary

SkyFormation cloud apps connector’s integration with RSA NetWitness extends NetWitness with unified visibility of audit and security activities across the organization's SaaS, PaaS and IaaS services.

SkyFormation integration with NetWitness provides the security operations center with a single pane of glass to monitor, hunt and remediate security events and threats within cloud applications and network infrastructure using their existing NetWitness. A list of the supported cloud apps and services could be found at: **SkyFormation supported cloud apps connectors**

RSA NetWitness Features	
SkyFormation 2.2.4	
Integration package name	Common Event Format
Device display name within NetWitness	skyformation_skyformation_cloud_apps_security
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
1/24/2018	Initial support for SkyFormation 2.2.4

! 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.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the SkyFormation 2.2.4 with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

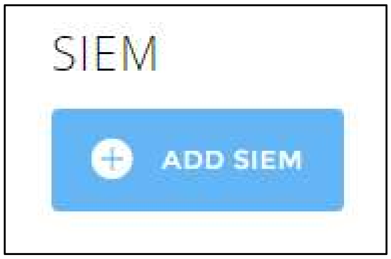
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

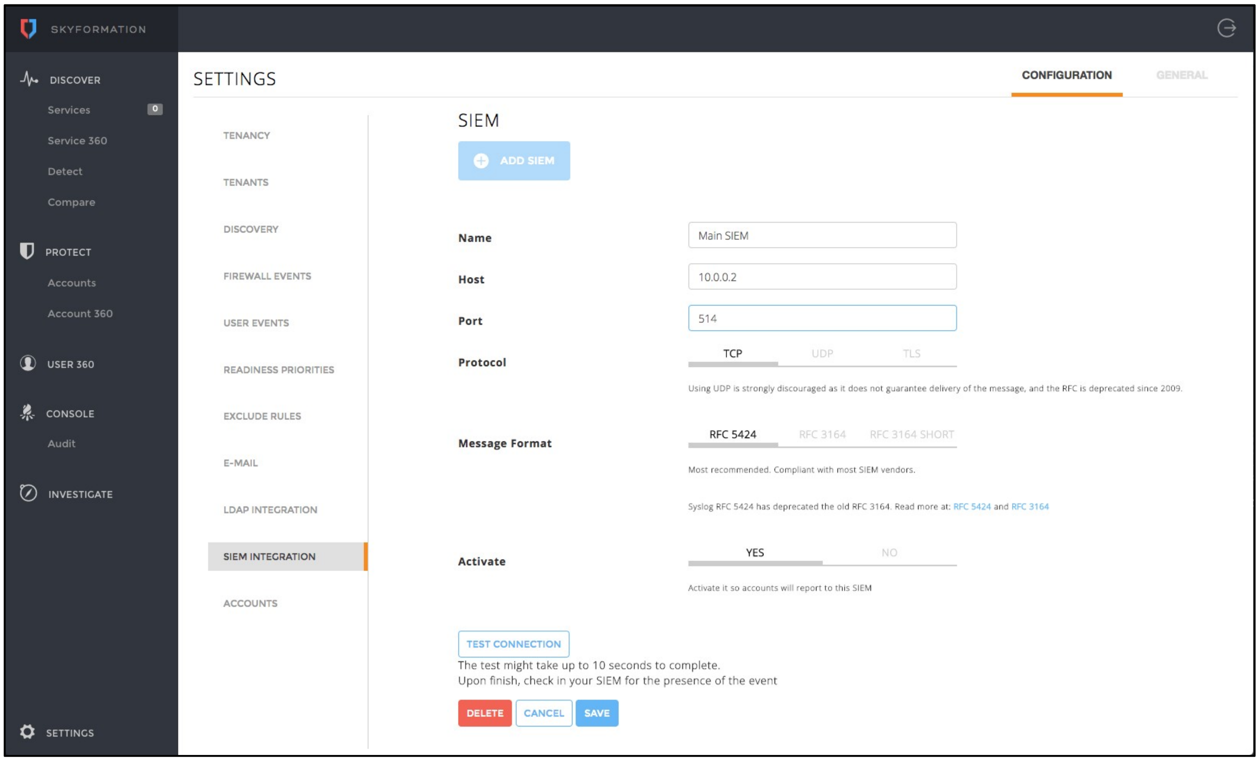
! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure SkyFormation 2.2.4 is properly configured and secured before deploying to a production environment. For more information, please refer to the SkyFormation 2.2.4 documentation or website.

SkyFormation 2.2.4 Configuration

1. Go to SETTINGS -> SIEM INTEGRATION and select "ADD SIEM"



2. Fill in the SIEM parameters as followed



SETTINGS

SIEM

Name: Main SIEM

Host: 10.0.0.2

Port: 514

Protocol: TCP | UDP | TLS

Using UDP is strongly discouraged as it does not guarantee delivery of the message, and the RFC is deprecated since 2009.

Message Format: RFC 5424 | RFC 3164 | RFC 3164 SHORT

Most recommended. Compliant with most SIEM vendors.

Syslog RFC 5424 has deprecated the old RFC 3164. Read more at: RFC 5424 and RFC 3164

Activate: YES | NO

Activate it so accounts will report to this SIEM

The test might take up to 10 seconds to complete.
Upon finish, check in your SIEM for the presence of the event

- **Name**

  Give this SIEM a friendly name for you to later use and refer to.

  Example: Main SIEM

- **Host**

  The SIEM IPv4 address or DNS name

  Examples: 10.0.0.2 or mysiem.corp.net

- **Port**

  The port in use by the SIEM to get the SkyFormation syslog events at

  Examples: 514

- **Protocol**

  Choose the protocol to be used (TCP/UDP/TLS) for the syslog channel with the SIEM.

  Examples: TCP

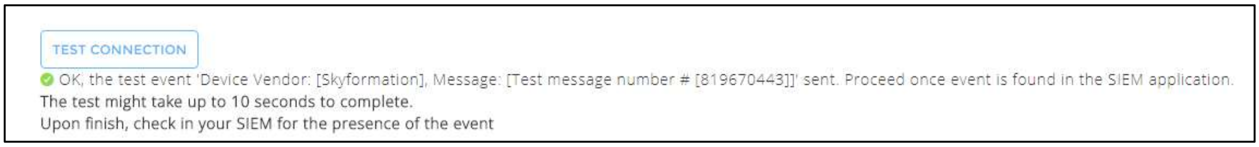
- **Message Format**

  According to your SIEM requirements choose the syslog spec to be used. Default RFC 5424 should be used unless the deprecated RFC 3164 is must. RSA NetWitness requires the use of the "***RFC 3164 SHORT***" option.

- **Activate** (Only for single-tenant mode)

  When SkyFormation single-tenant mode is used, SkyFormation will offer you to automatically activate the new SIEM just added by attach it to the default-tenant. In case you do not want to use the SIEM just added change to **NO**.

3. Select "TEST CONNECTION" to send a test syslog event to the configured SIEM, you should get the below indication in case the SIEM configuration is correct and the target SIEM have accepted the test event (only relevant in TCP/TLS case).



✓ OK, the test event 'Device Vendor: [Skyformation], Message: [Test message number # [819670443]]' sent. Proceed once event is found in the SIEM application.
The test might take up to 10 seconds to complete.
Upon finish, check in your SIEM for the presence of the event

To double check you could also search your SIEM for a syslog/CEF event where:

cef_name = "Skyformation-test SIEM settings event"

4. Select **SAVE**.

! Important: To start getting your business cloud applications events continuously into your RSA NetWitness Appliance please add any of your licensed cloud apps connectors to SkyFormation as explained at SkyFormation Cloud Connectors Modules guides.

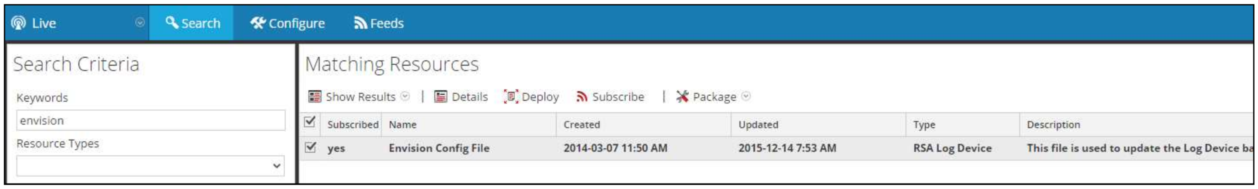
RSA NetWitness Configuration

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

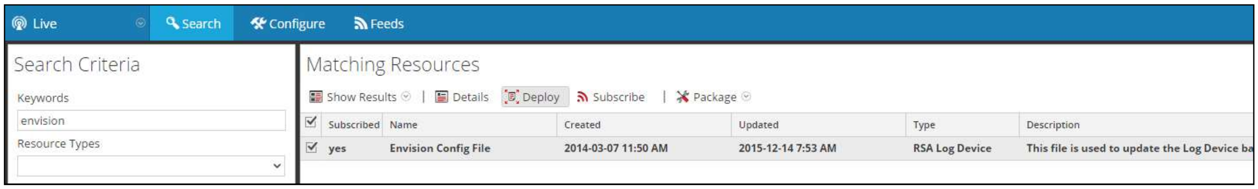


Keywords: envision

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.

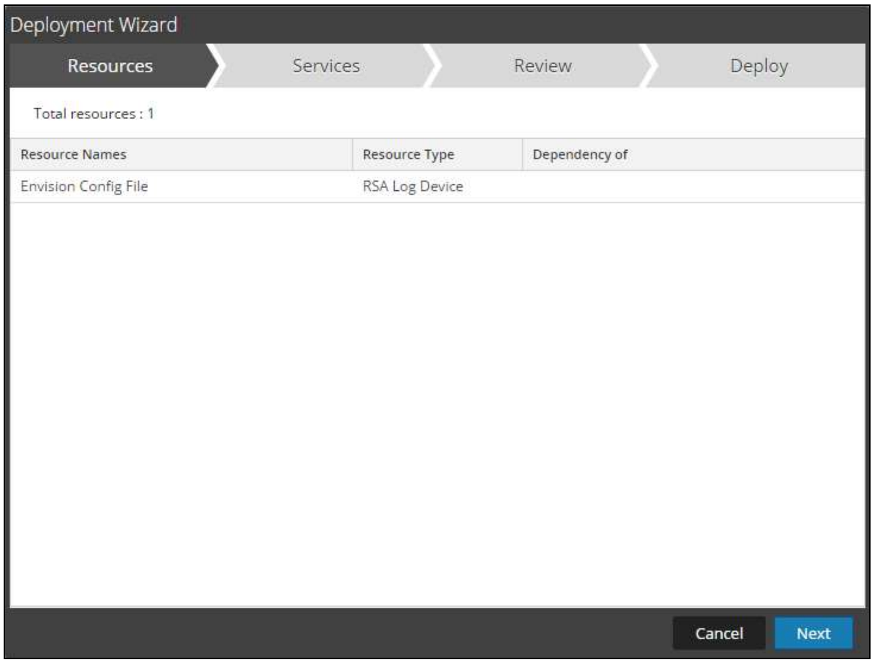


Keywords: envision

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

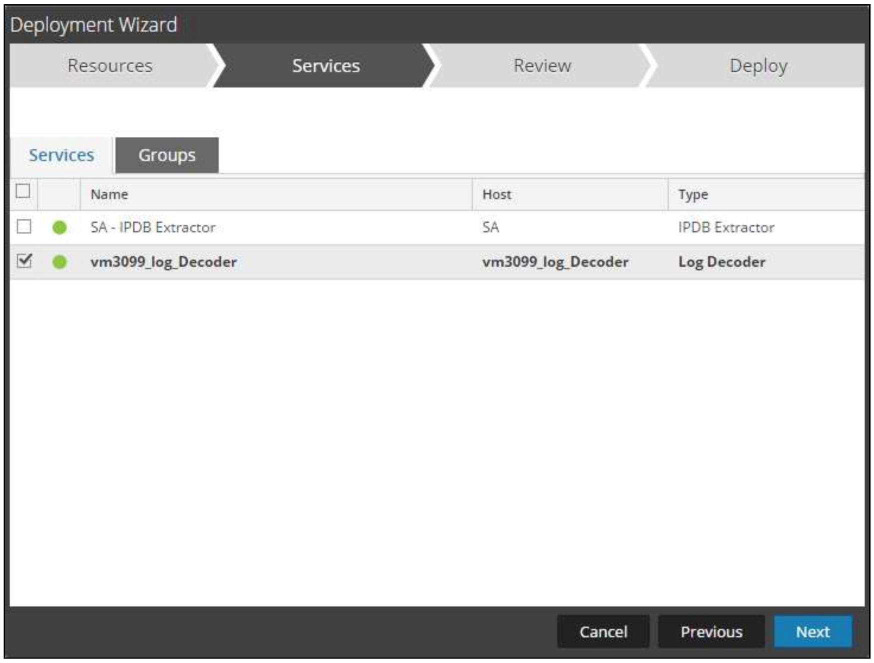
6. Select **Next**.



Total resources : 1

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

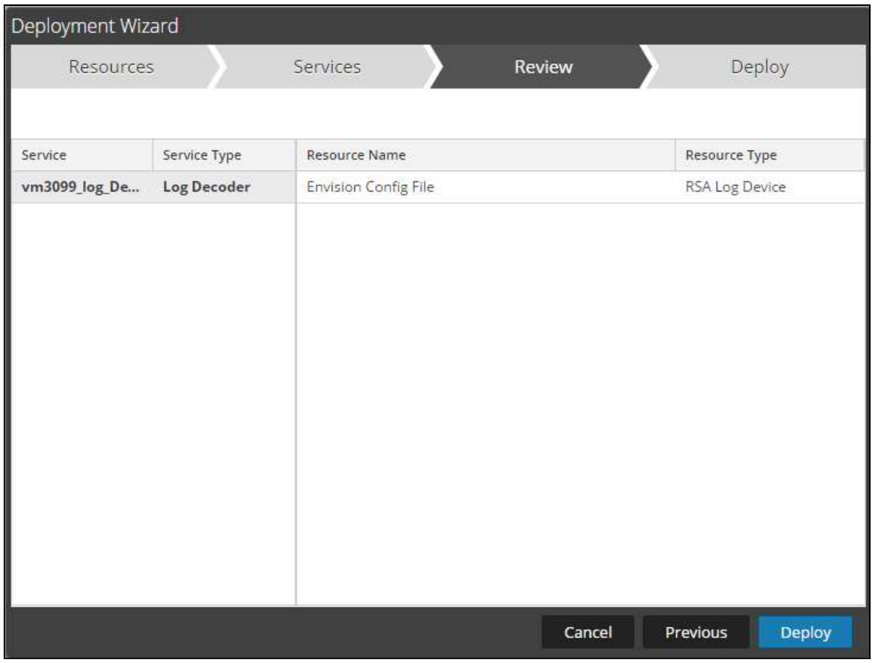
7. Select the **Log Decoder** and select **Next**.



☐		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.

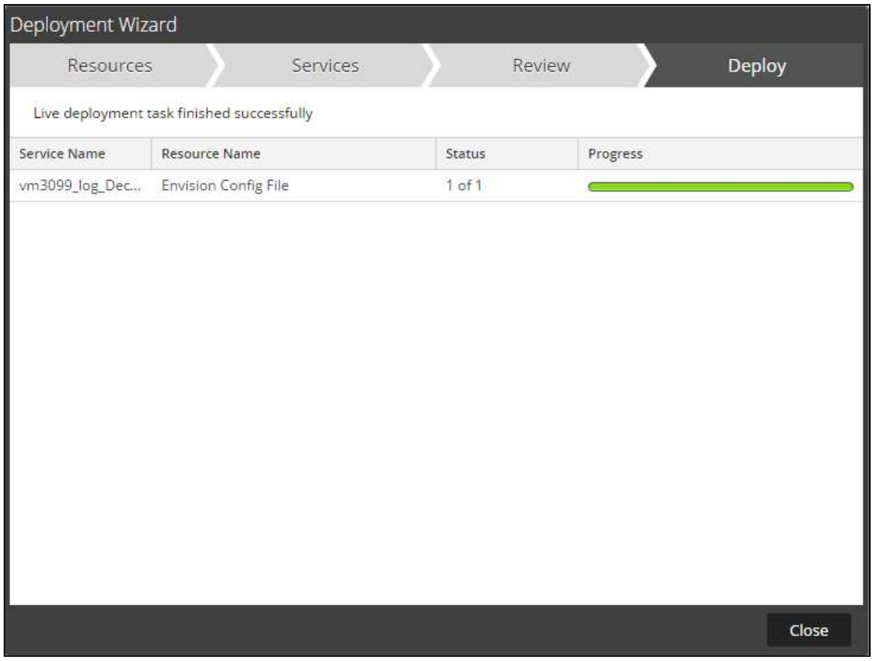
8. Select **Deploy**.



Deployment Wizard

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.



Deployment Wizard

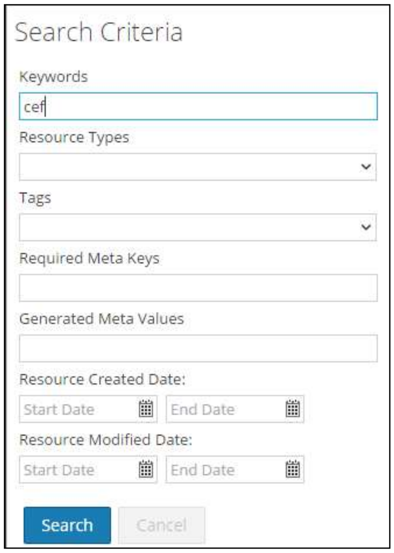
Live deployment task finished successfully

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:

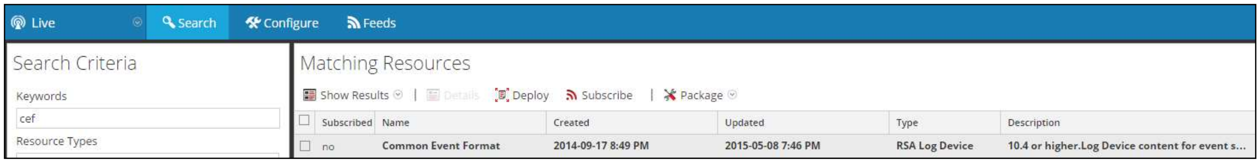
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **CEF**



Keywords: cef

.

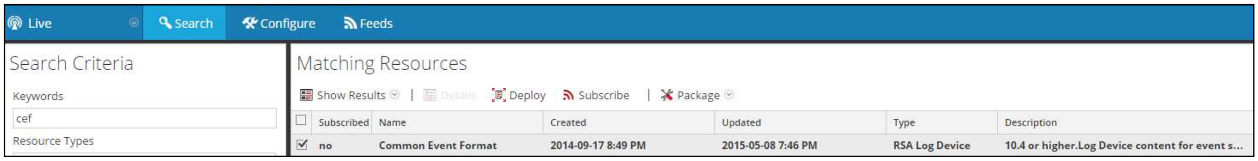
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



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...

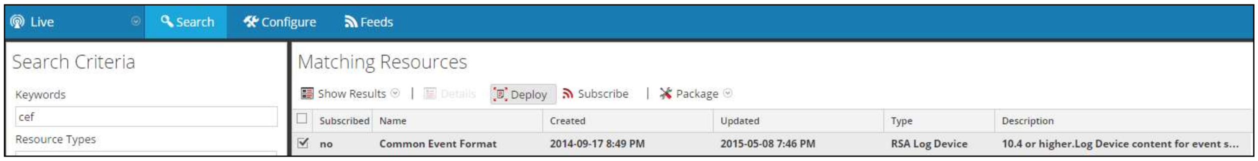
4. Select the checkbox next to **Common Event Format**.



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...

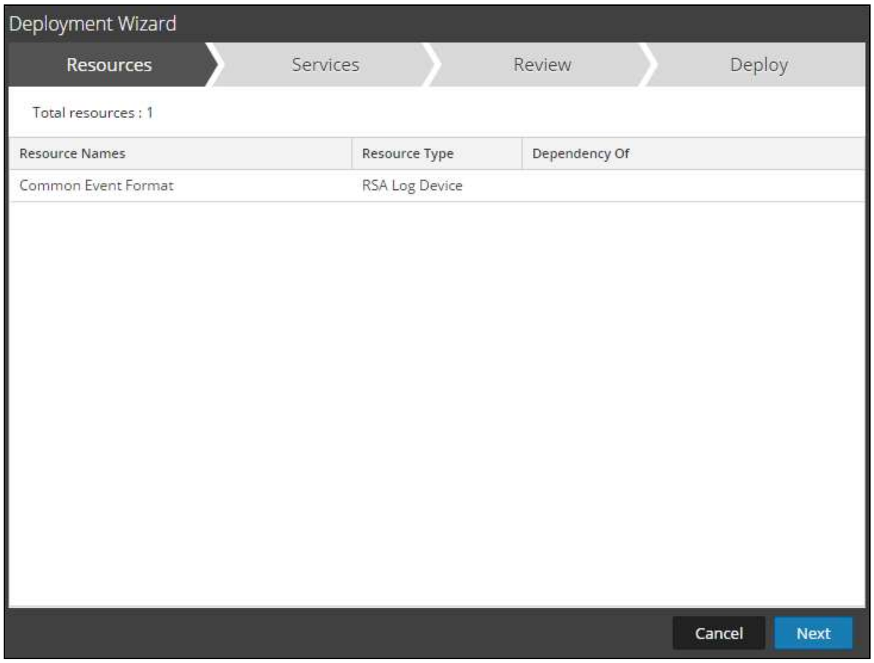
5. Click **Deploy** in the menu bar.



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...

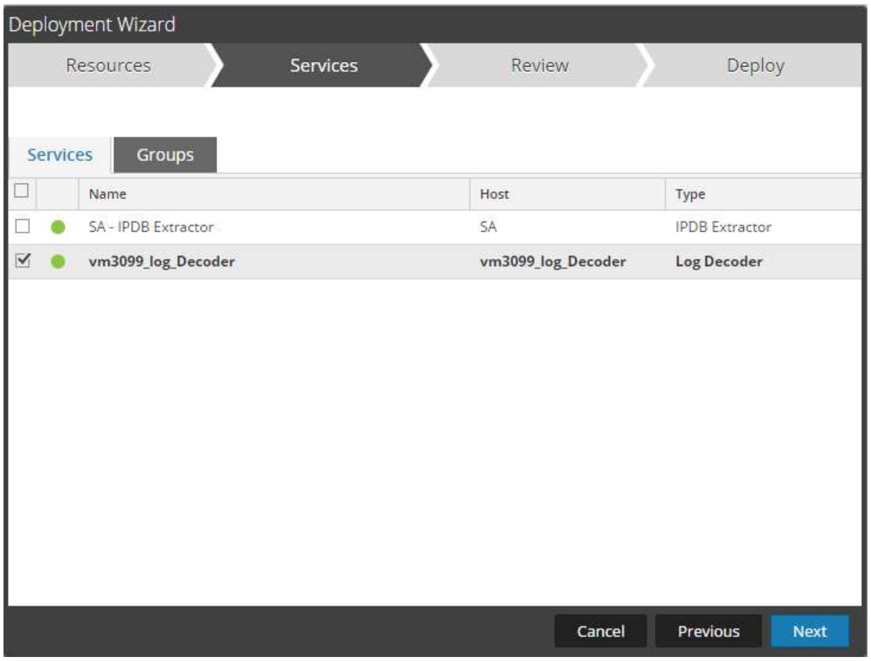
6. Select **Next**.



Total resources : 1

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

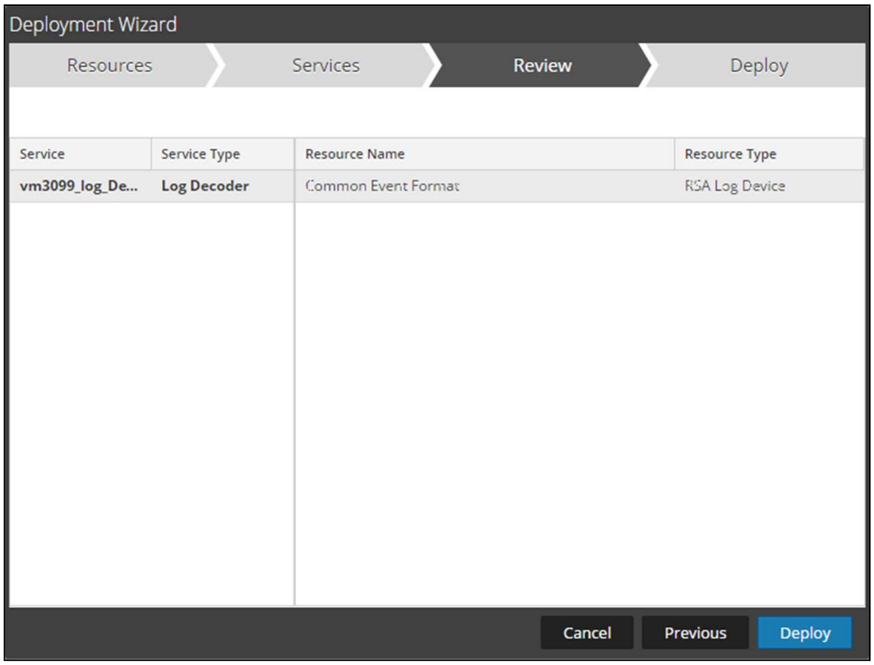
7. Select the **Log Decoder** and Select **Next**.



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

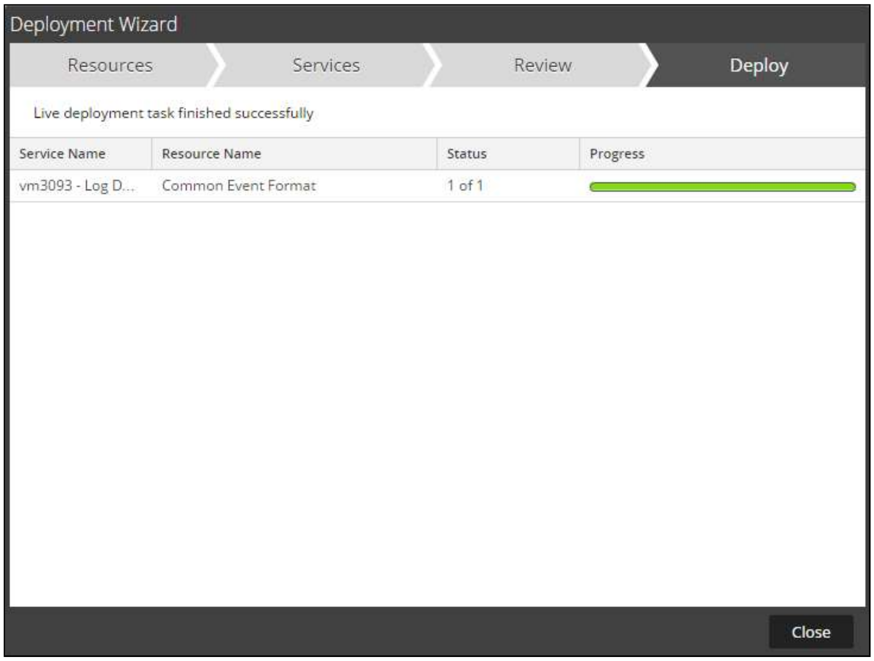
! > Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



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

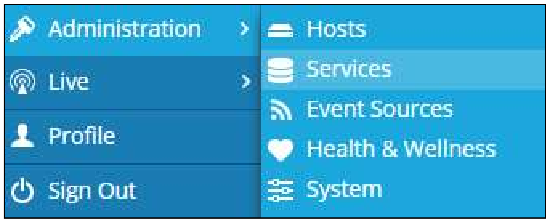
9. Select **Close**, to complete the deployment of the Common Event Format.



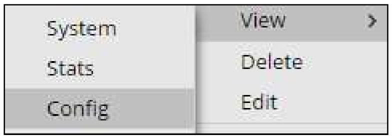
Live deployment task finished successfully

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

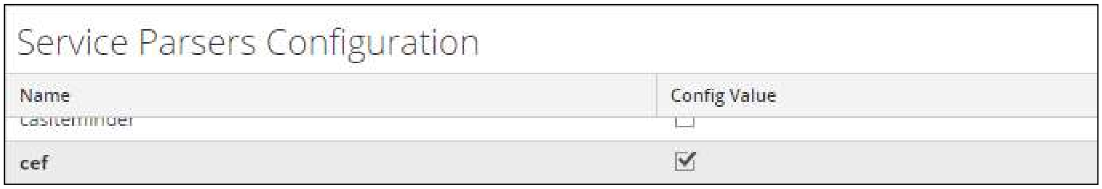
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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**.

Edit the Common Event Format to add SkyFormation

! > Important: The cef.xml file is overwritten by NetWitness Live during updates, it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/devices/cef** folder. Backup cef.xml and edit the existing CEF.XML file.
2. Locate the end of the <VendorProducts section and copy/paste the following lines below into the file before the end denoted by </VendorProducts>.

```
<Vendor2Device vendor="Skyformation" product="Skyformation_cloud_apps_security"
device="skyformation_skyformation_cloud_apps_security" group="Analysis"/>
```

Edit the Common Event Format Custom to support custom fields

! Important: The cef-custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/devices/cef** folder. If the cef-custom.xml file does not exist create one. If the file exists create a backup cef-custom.xml and edit the file.

   If this is a new **cef-custom.xml** file, copy the following into the file, otherwise copy only the required sections.

```
Example.

       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
       <DEVICEMESSAGES>
       <!--
       #
       # cef-custom.xml Reference: https://community.rsa.com/docs/DOC-79189
       #
       -->

       <VendorProducts>

       </VendorProducts>

                  <ExtensionKeys>
                    <ExtensionKey cefName="cs1" metaName="cs_fld">
                           <device2meta device="trendmicrodsa" metaName="context"/>
                           <device2meta device="bluecat" metaName="action"
       label="query"/>
                           <device2meta device="websense" metaName="policyname"
       label="Policy"/>
                           <device2meta device="mcafeewg" metaName="virusname"
       label="Virus Name"/>
                           <device2meta device="bit9" metaName="checksum" label="File
       Hash"/>
                           <device2meta device="mcafeereconnex"
       metaName="policyname"/>
                           <device2meta
       device="skyformation_skyformation_cloud_apps_security" metaName="sk4-cs1key"/>
                    </ExtensionKey>
                    <ExtensionKey cefName="cs1Label" metaName="cs_fld"/>

                    <ExtensionKey cefName="cs2" metaName="cs_fld">
                           <device2meta device="bit9" metaName="v_instafname"
       label="installerFilename"/>
                           <device2meta
       device="skyformation_skyformation_cloud_apps_security" metaName="sk4-cs2key"/>
                    </ExtensionKey>
                    <ExtensionKey cefName="cs2Label" metaName="cs_fld"/>

                    <ExtensionKey cefName="cs3" metaName="cs_fld">
                           <device2meta device="websense" metaName="content_type"
       label="ContentType"/>
                           <device2meta device="bit9" metaName="policyname"/>
                           <device2meta device="mcafeereconnex"
       metaName="content_type"/>
                           <device2meta
       device="skyformation_skyformation_cloud_apps_security" metaName="Property-
       name"/>
                    </ExtensionKey>
                    <ExtensionKey cefName="cs3Label" metaName="cs_fld"/>
```

```
             <ExtensionKey cefName="cs6" metaName="cs_fld">
                    <device2meta device="mcafeewg" metaName="risk"
label="Reputation"/>
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="raw-event"/>

             </ExtensionKey>
             <ExtensionKey cefName="cs6Label" metaName="cs_fld"/>

             <ExtensionKey cefName="cfp3" metaName="cn_fld">
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="latitude"/>
             </ExtensionKey>
             <ExtensionKey cefName="cfp3Label" metaName="cs_fld"/>

             <ExtensionKey cefName="cfp4" metaName="cn_fld">
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="longitude"/>
             </ExtensionKey>
             <ExtensionKey cefName="cfp4Label" metaName="cs_fld"/>

             <ExtensionKey cefName="msg" metaName="msg">
                    <device2meta device="trendmicrodsa" metaName="info"/>
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="info"/>
             </ExtensionKey>

             <ExtensionKey cefName="smac" metaName="smac">
                                  <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="sk4-smac"/>
             </ExtensionKey>

             <ExtensionKey cefName="request" metaName="request">
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="request"/>
             </ExtensionKey>

             <ExtensionKey cefName="cn1" metaName="cn_fld">
                    <device2meta device="trendmicrods" metaName="hostid"
label="Host ID"/>
                    <device2meta device="trendmicrodsa" metaName="hostid"
label="Host ID"/>
                    <device2meta device="mcafeewg" metaName="result"
label="Block Reason"/>
                    <device2meta
device="skyformation_skyformation_cloud_apps_security" metaName="failure-
number" label="failure-number"/>
             </ExtensionKey>
             <ExtensionKey cefName="cn1Label" metaName="cs_fld"/>

             <ExtensionKey cefName="LoginTime" metaName="LoginTime"/>
             <ExtensionKey cefName="ApiVersion" metaName="ApiVersion"/>
             <ExtensionKey cefName="LoginGeo.type" metaName="LoginGeo.type"/>
             <ExtensionKey cefName="LoginGeo.Id" metaName="LoginGeo.Id"/>
             <ExtensionKey cefName="LoginGeo.City" metaName="LoginGeo.City"/>
             <ExtensionKey cefName="LoginGeo.Country"
metaName="LoginGeo.Country"/>
             <ExtensionKey cefName="LoginGeo.Latitude"
metaName="LoginGeo.Latitude"/>
             <ExtensionKey cefName="LoginGeo.PostalCode"
metaName="LoginGeo.PostalCode"/>
             <ExtensionKey cefName="LoginGeo.Longitude"
metaName="LoginGeo.Longitude"/>
             <ExtensionKey cefName="CountryIso" metaName="CountryIso"/>
             <ExtensionKey cefName="Platform" metaName="Platform"/>
             <ExtensionKey cefName="CipherSuite" metaName="CipherSuite"/>
             <ExtensionKey cefName="NetworkId" metaName="NetworkId"/>
             <ExtensionKey cefName="ClientVersion" metaName="ClientVersion"/>
             <ExtensionKey cefName="LoginUrl" metaName="LoginUrl"/>
             <ExtensionKey cefName="SourceIp" metaName="SourceIp"/>
             <ExtensionKey cefName="UserId" metaName="UserId"/>
             <ExtensionKey cefName="AuthenticationServiceId"
metaName="AuthenticationServiceId"/>
             <ExtensionKey cefName="ApiType" metaName="ApiType"/>
             <ExtensionKey cefName="TlsProtocol" metaName="TlsProtocol"/>
             <ExtensionKey cefName="Id" metaName="Id"/>
             <ExtensionKey cefName="LoginType" metaName="LoginType"/>
             <ExtensionKey cefName="Application" metaName="Application"/>
             <ExtensionKey cefName="Browser" metaName="Browser"/>
             <ExtensionKey cefName="app" metaName="application"/>
             <ExtensionKey cefName="sourceDnsDomain" metaName="sdomain"/>
             <ExtensionKey cefName="sntdom" metaName="sntdomain"/>
             <ExtensionKey cefName="dtz" metaName="dtz"/>
             <ExtensionKey cefName="dntdom" metaName="dntdom"/>
             <ExtensionKey cefName="type" metaName="type"/>
             <ExtensionKey cefName="flexString1" metaName="app-action"/>
             <ExtensionKey cefName="destinationDnsDomain"
metaName="destdomain"/>
             <ExtensionKey cefName="sourceDnsDomain" metaName="sourcedomain"/>
             <ExtensionKey cefName="flexString2" metaName="application-msg"/>

             </ExtensionKeys>

</DEVICEMESSAGES>
```

Edit the NetWitness Table-Map-Custom.xml file

! Important: The Table-Map-Custom.xml file is not overwritten by NetWitness Live during updates, however it is important to maintain backups of the file in the event of a typing error or unforeseen event.

1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/** folder.
2. If one exists, backup the **table-map-custom.xml** and then edit the existing **table-map-custom.xml** file.
3. Copy and paste the entire section below into a new file or only the lines between the <mappings>…</mappings> if the Table-Map-Custom.xml file exists;

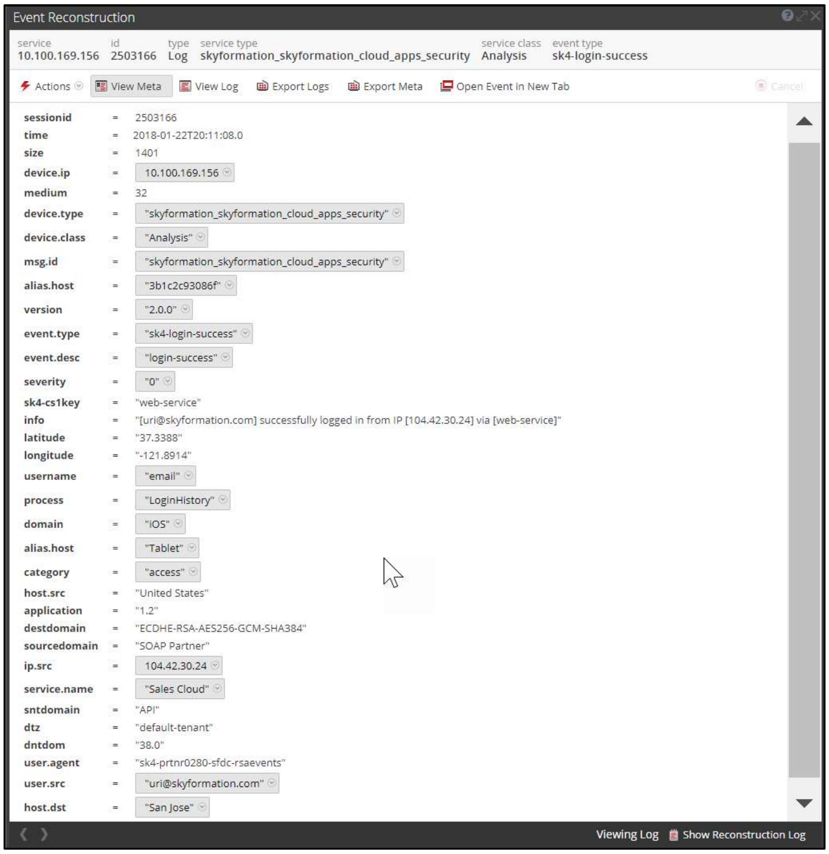
Example.

```
<?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 generated "parse.error" meta.
#      nullTokens:          Optional. The list of "null" tokens. Pipe separated.
Default is no null tokens.
<!--
Move the following mapping to the body of mappings to display raw-event key
       <mapping envisionName="raw-event" nwName="raw-event" flags="None"/>
       -->
-->
<mappings>

       <mapping envisionName="starttime" nwName="start" flags="None"
format="TimeT" envisionDisplayName="StartTime"/>
       <mapping envisionName="endtime" nwName="endtime" flags="None"
format="TimeT" envisionDisplayName="EndTime,rt,end"/>
       <mapping envisionName="version" nwName="version" flags="None"/>
       <mapping envisionName="severity" nwName="severity" flags="None"
envisionDisplayName="Severity|SeverityLevel"/>
       <mapping envisionName="sk4-cs1key" nwName="sk4-cs1key" flags="None"/>
       <mapping envisionName="event_state" nwName="event.state" flags="None"/>
       <mapping envisionName="LoginTime" nwName="LoginTime" flags="None"/>
       <mapping envisionName="ApiVersion" nwName="ApiVersion" flags="None"/>
       <mapping envisionName="LoginGeo.type" nwName="LoginGeo.type"
flags="None"/>
       <mapping envisionName="LoginGeo.Id" nwName="LoginGeo.Id" flags="None"/>
       <mapping envisionName="LoginGeo.City" nwName="LoginGeo.City"
flags="None"/>
       <mapping envisionName="LoginGeo.Country" nwName="LoginGeo.Country"
flags="None"/>
       <mapping envisionName="LoginGeo.Latitude" nwName="LoginGeo.Latitude"
flags="None"/>
       <mapping envisionName="LoginGeo.PostalCode" nwName="LoginGeo.PostalCode"
flags="None"/>
       <mapping envisionName="LoginGeo.Longitude" nwName="LoginGeo.Longitude"
flags="None"/>
       <mapping envisionName="CountryIso" nwName="CountryIso" flags="None"/>
       <mapping envisionName="Platform" nwName="Platform" flags="None"/>
       <mapping envisionName="dtz" nwName="dtz" flags="None"/>
       <mapping envisionName="process" nwName="process" flags="None"
envisionDisplayName="Process"/>
       <mapping envisionName="info" nwName="info" flags="None"/>
       <mapping envisionName="app-action" nwName="app-action" flags="None"/>
       <mapping envisionName="filetype" nwName="filetype" flags="None" />
       <mapping envisionName="sk4-smac" nwName="sk4-smac" flags="None" />
       <mapping envisionName="cs_fileid" nwName="cs_fileid" flags="None" />
       <mapping envisionName="request" nwName="request" flags="None" />
       <mapping envisionName="failure-number" nwName="failure-number"
flags="None" />
       <mapping envisionName="cs_reqcookies" nwName="cs_reqcookies" flags="None"
/>
       <mapping envisionName="sdomain" nwName="sdomain" flags="None" />
       <mapping envisionName="ddomain" nwName="ddomain" flags="None" />
       <mapping envisionName="application" nwName="application" flags="None" />
       <mapping envisionName="destdomain" nwName="destdomain" flags="None" />
       <mapping envisionName="sourcedomain" nwName="sourcedomain" flags="None"
/>
       <mapping envisionName="longitude" nwName="longitude" flags="None" />
       <mapping envisionName="latitude" nwName="latitude" flags="None" />
       <mapping envisionName="sntdomain" nwName="sntdomain" flags="None" />
       <mapping envisionName="dntdom" nwName="dntdom" flags="None" />
       <mapping envisionName="privilege" nwName="privilege" flags="None"
envisionDisplayName="Privilege|Privileges"/>
       <mapping envisionName="process_src" nwName="process.src" flags="None"
envisionDisplayName="SourceProcess"/>
       <mapping envisionName="application-msg" nwName="application-msg"
flags="None"/>
       <mapping envisionName="sk4-cs2key" nwName="sk4-cs2key" flags="None"/>
       <mapping envisionName="cs_fileperm" nwName="cs_fileperm" flags="None"/>
       <mapping envisionName="Property-name" nwName="Property-name"
flags="None"/>

</mappings>
```

NetWitness Collection Example:



```
service         id       type  service type                                      service class  event type
10.100.169.156  2503166  Log   skyformation_skyformation_cloud_apps_security     Analysis       sk4-login-success
```

```
sessionid     =  2503166
time          =  2018-01-22T20:11:08.0
size          =  1401
device.ip     =  10.100.169.156
medium        =  32
device.type   =  "skyformation_skyformation_cloud_apps_security"
device.class  =  "Analysis"
msg.id        =  "skyformation_skyformation_cloud_apps_security"
alias.host    =  "3b1c2c93086f"
version       =  "2.0.0"
event.type    =  "sk4-login-success"
event.desc    =  "login-success"
severity      =  "0"
sk4-cs1key    =  "web-service"
info          =  "[uri@skyformation.com] successfully logged in from IP [104.42.30.24] via [web-service]"
latitude      =  "37.3388"
longitude     =  "-121.8914"
username      =  "email"
process       =  "LoginHistory"
domain        =  "iOS"
alias.host    =  "Tablet"
category      =  "access"
host.src      =  "United States"
application   =  "1.2"
destdomain    =  "ECDHE-RSA-AES256-GCM-SHA384"
sourcedomain  =  "SOAP Partner"
ip.src        =  104.42.30.24
service.name  =  "Sales Cloud"
sntdomain     =  "API"
dtz           =  "default-tenant"
dntdom        =  "38.0"
user.agent    =  "sk4-prtnr0280-sfdc-rsaevents"
user.src      =  "uri@skyformation.com"
host.dst      =  "San Jose"
```

Certification Checklist for RSA NetWitness

Date Tested: January 24, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.0 & 10.6.5	Virtual Appliance
SkyFormation	2.2.4	Virtual Appliance

NetWitness Test Case	Result
Device Administration	
Partner's 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	✓

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

Known Issues

Due to a 256 character limitation on key values, NetWitness is unable to collect the entire key value for the following key name.

```
raw-event
```

RSA is unable to differentiate from three SkyFormation cs1 keys with different cs1Labels. As a result the following cs1 key names/key labels have been mapped to a common NetWitness key name sk4-cs1key.

```
login type
Reset by
Sender
```

RSA is unable to differentiate from three SkyFormation cs2 keys with different cs2Labels. As a result the following cs2 key names/key labels have been mapped to a common NetWitness key name sk4-cs2key.

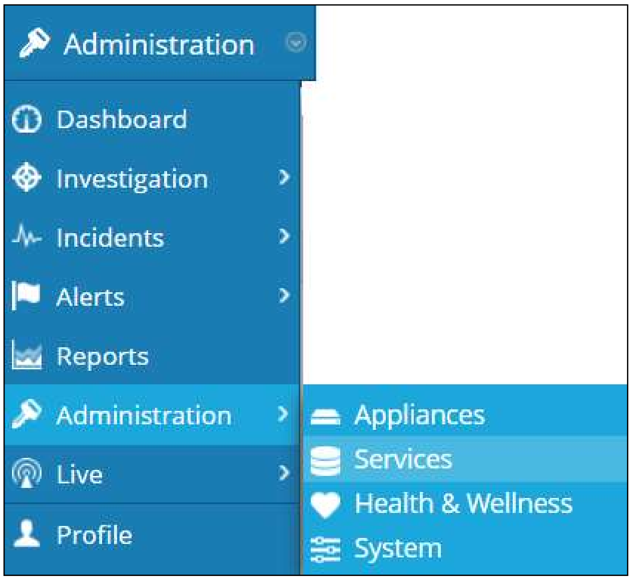
```
Effective from
Recipient
Old-value
```

Appendix

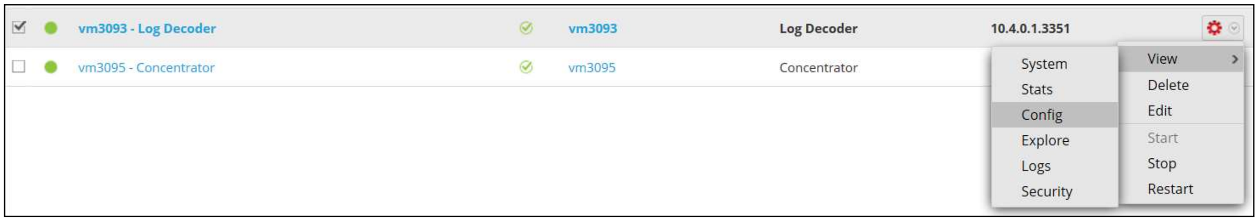
NetWitness Disable the Common Event Format Parser

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

1. Select the NetWitness **Administration > Services menu**.

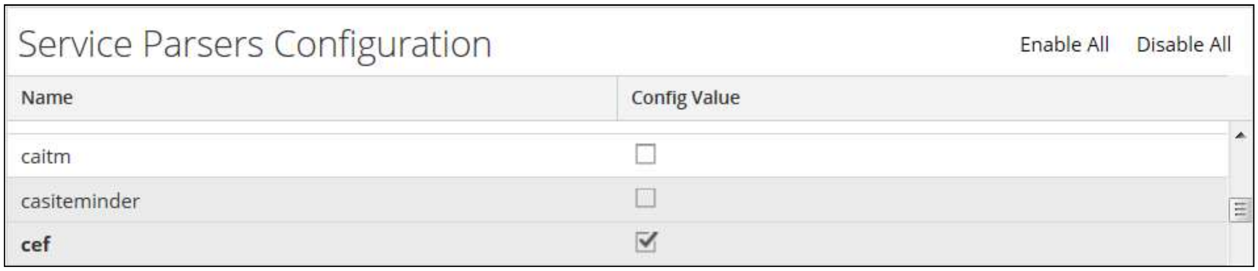


2. Select the Log Decoder, then select **View > Config.**



☑	●	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

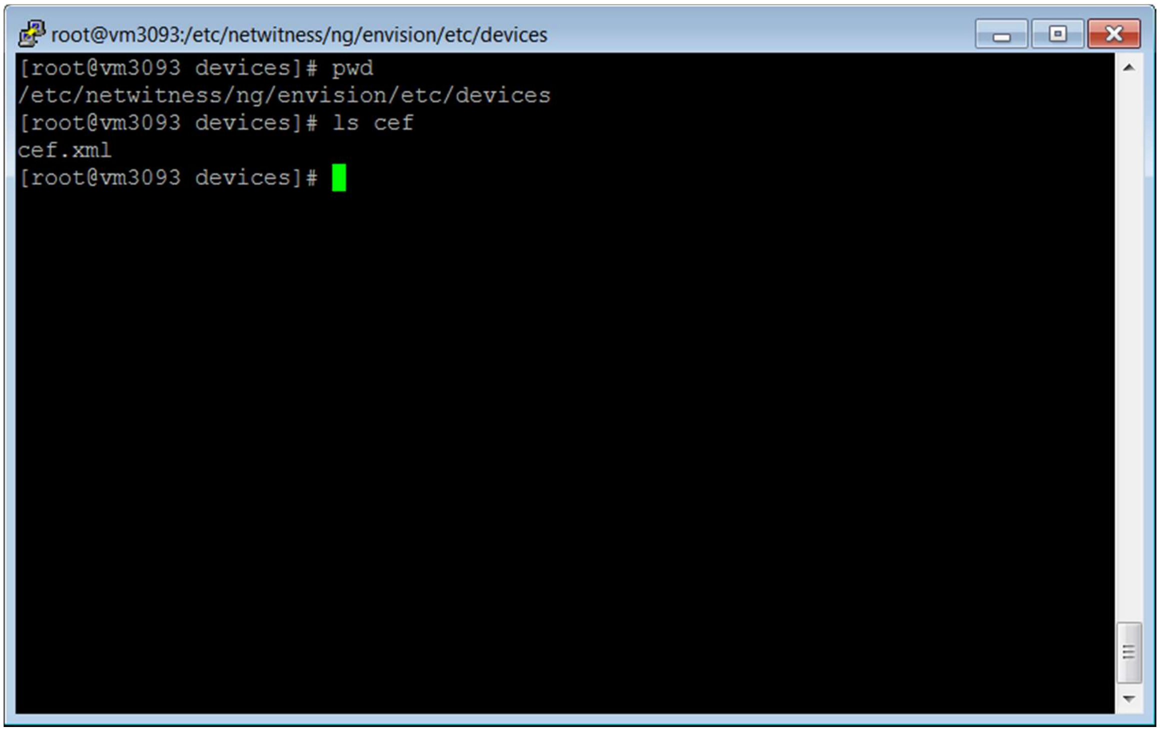
Name	Config Value
caitm	□
casiteminder	□
cef	☑

4. Click **Apply** to save settings.

NetWitness Remove Device Parser

To remove the NetWitness Integration Package files from the environment, perform the following:

1. Connect to the NetWitness 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.