

RSA® NETWITNESS®

**Logs
Implementation Guide**

Attivo Networks, ThreatDefend Platform 4.0

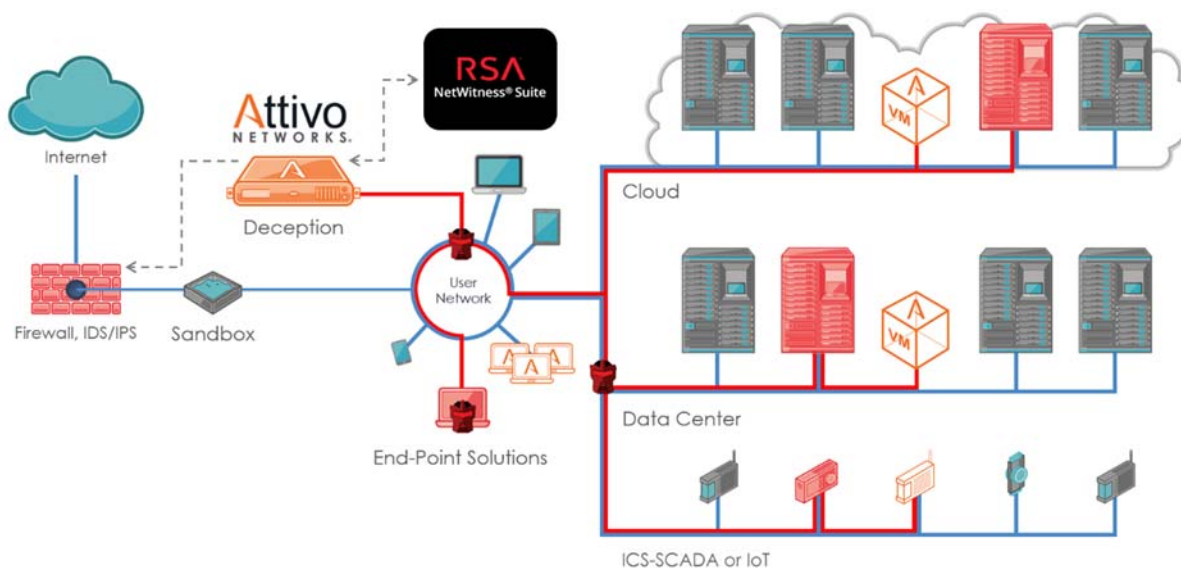
Daniel Pinal, RSA Partner Engineering
Last Modified: July 31, 2017

RSA
READY

Solution Summary

When integrated, Attivo Networks ThreatDefend and RSA NetWitness partner to provide a monitoring and threat detection solution providing our mutual customers with a robust solution to effectively detect network anomalies.

RSA NetWitness Features	
Attivo Networks, ThreatDefend Platform 4.x	
Integration package name	Common Event Format
Device display name within Security Analytics	attivo_botsink
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
07/31/2017	Initial support for Attivo Networks

! ▷ 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 Attivo Networks ThreatDefend Platform 4.0 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 Attivo Networks ThreatDefend Platform 4.0 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 Attivo Networks ThreatDefend Platform 4.0 is properly configured and secured before deploying to a production environment. For more information, please refer to the Attivo Networks ThreatDefend Platform 4.0 documentation or website.

Attivo Networks ThreatDefend Platform 4.0 Configuration

1. Configure Attivo to forward syslog CEF to RSA. Select Syslog under Administration->Management as shown below.

#	Name	Events	Faults	In Use	Audit Logs	More
1	Attivo_Default_TCP	✓	✗	✗	✗	Details
2	Attivo_Default_UDP	✓	✗	✗	✗	Details
3	Attivo_Default_TCP_CEF	✓	✗	✗	✗	Details
4	Attivo_Default_UDP_CEF	✓	✗	✗	✗	Details
5	CEF	✓	✓	✓	✓	Details

2. Create CEF Syslog profile as shown below. Select CEF as message format and select "Syslog Profile"

Details

Name : RSA_CEF

Events Forwarding Enabled

Severity : Medium

Severity Mapping : **BOTSink Standard**

Very Low
Low
Medium
High
Very High

Syslog Standard

Informational
Warning
Alert
Critical
Emergency

Message Format: Custom CEF CIM

Include Syslog Prefix:

3. Add new connection to RSA in Profiles, select the CEF Syslog Profile you have created

Edit Server Config

Enable:

Server Name: RSA

Profile Name: RSA_CEF

IP Address: 192.168.3.198

Port: 514

Protocol: UDP

Cancel Test Connection OK

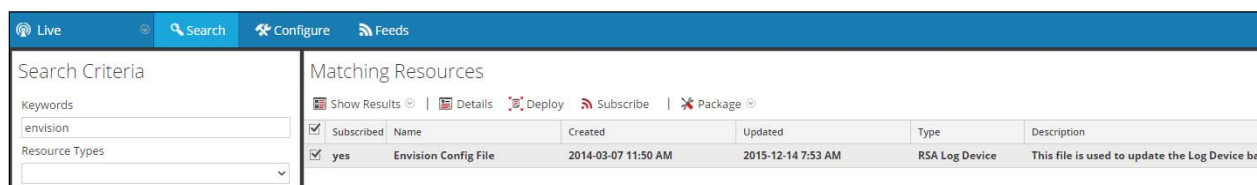
RSA NetWitness Configuration

Deploy the enVision Config File

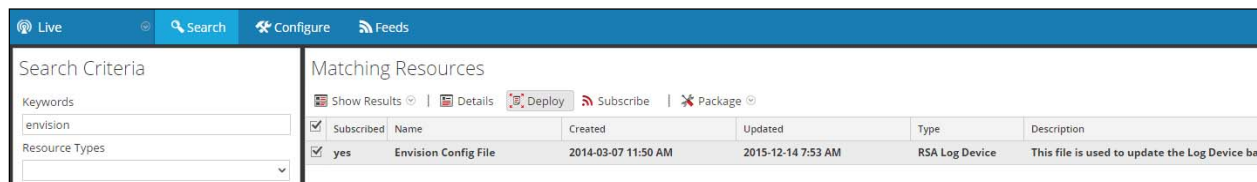
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

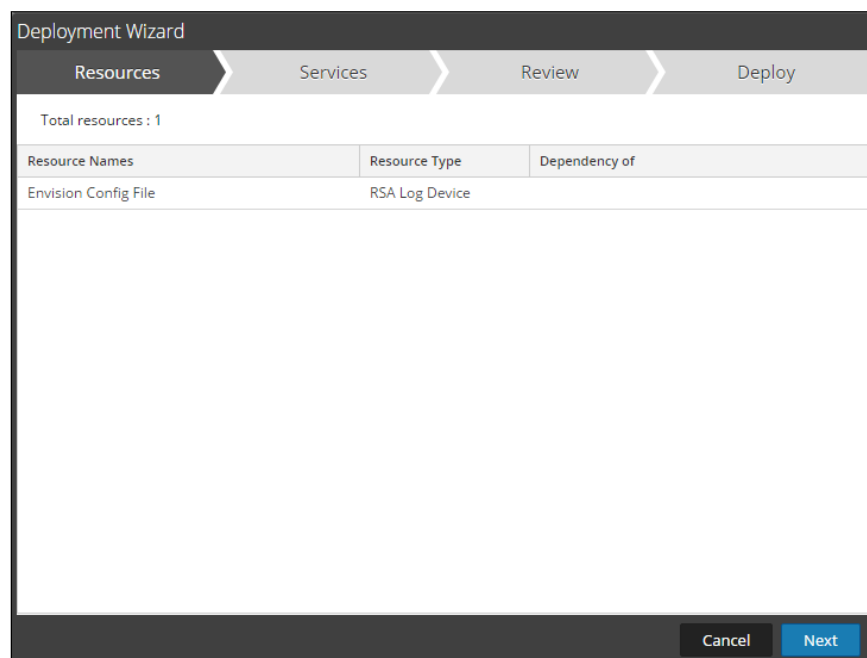
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



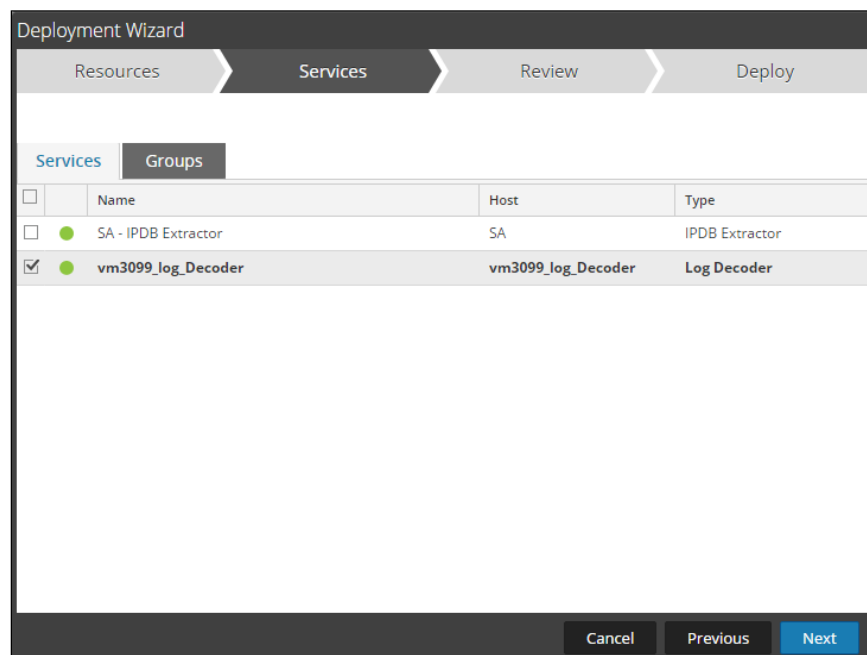
5. Click **Deploy** in the menu bar.



6. Select **Next**.

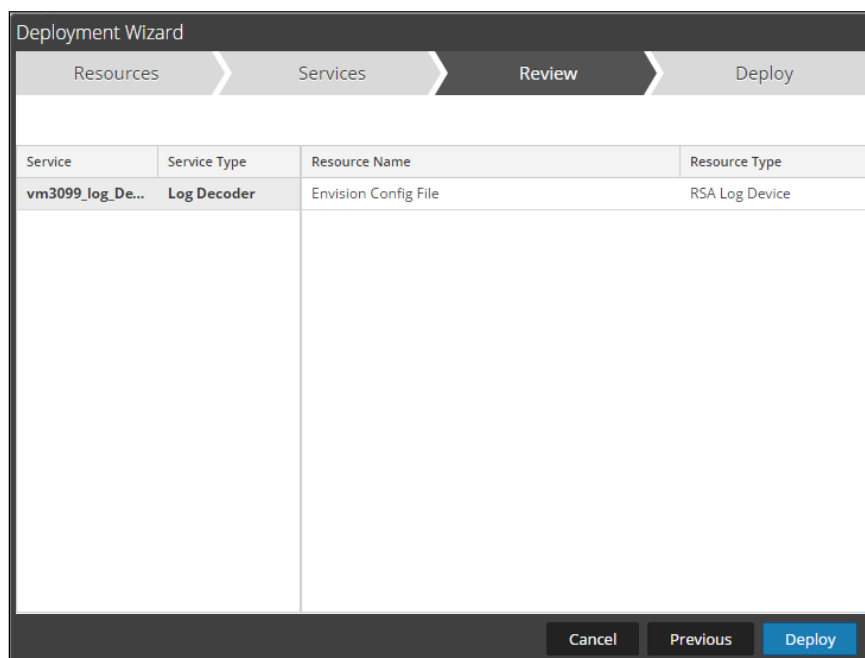


7. Select the **Log Decoder** and select **Next**.

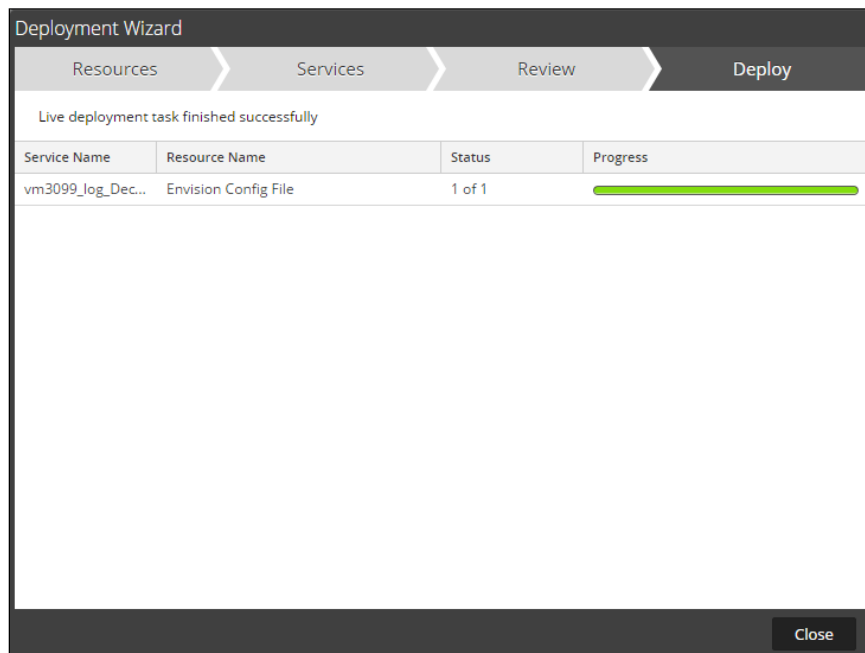


!> Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



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



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:

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

Search Criteria

Keywords

Resource Types

Tags

Required Meta Keys

Generated Meta Values

Resource Created Date:
 Start Date End Date

Resource Modified Date:
 Start Date End Date

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef	Show Results Details Deploy Subscribe Package					
Resource Types	<input type="checkbox"/> Subscribed	Name	Created	Updated	Type	Description
	<input type="checkbox"/> 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...

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef	Show Results Details Deploy Subscribe Package					
Resource Types	<input checked="" type="checkbox"/> no	Name	Created	Updated	Type	Description
	<input checked="" type="checkbox"/> 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...

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef	Show Results Details Deploy Subscribe Package					
Resource Types	<input checked="" type="checkbox"/> no	Name	Created	Updated	Type	Description
	<input checked="" type="checkbox"/> 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...

15. Select **Next**.

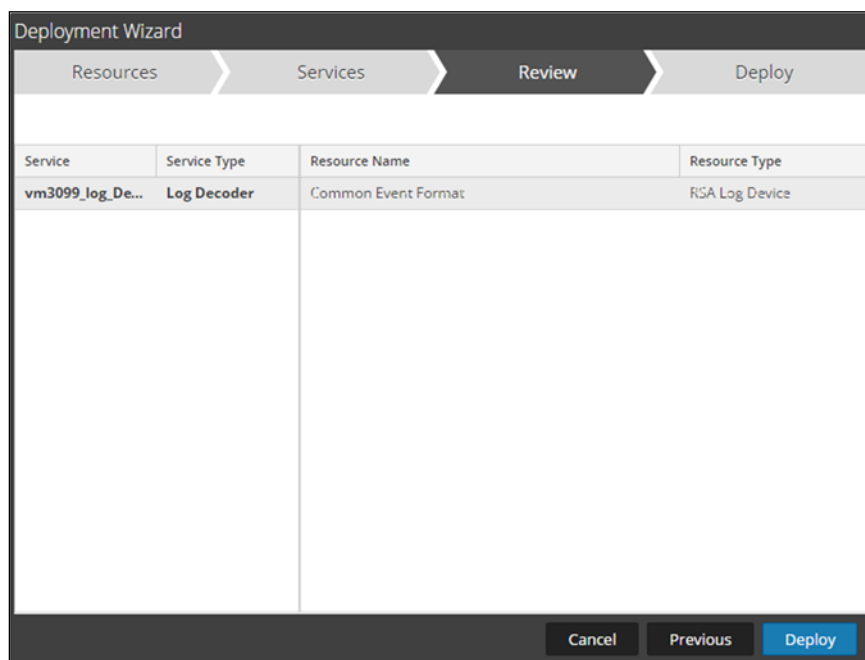
Resource Names	Resource Type	Dependency Of
Common Event Format	RSA Log Device	

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

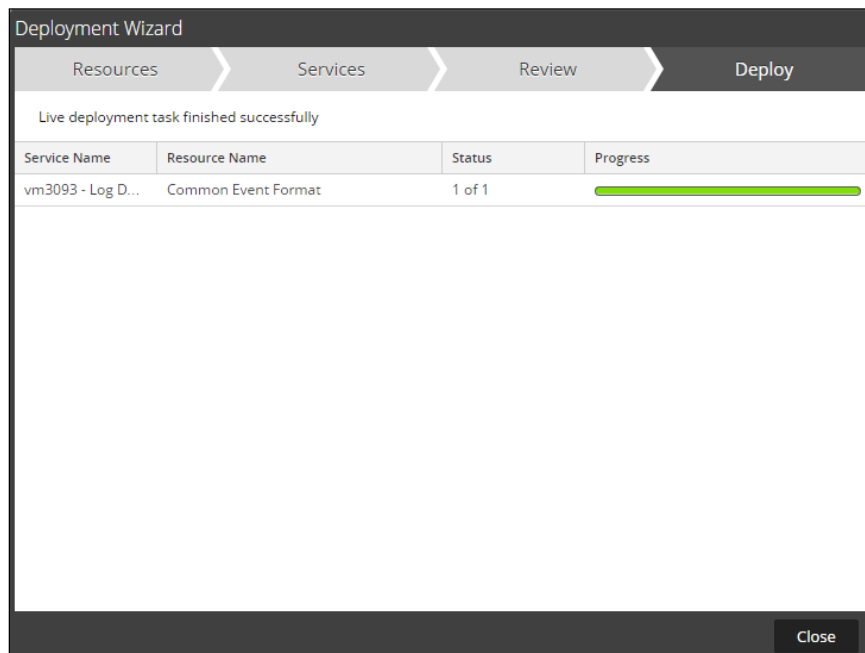
<input type="checkbox"/>	Name	Host	Type
<input type="checkbox"/>	SA - IPDB Extractor	SA	IPDB Extractor
<input checked="" type="checkbox"/>	vm3099_log_Decoder	vm3099_log_Decoder	Log Decoder

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

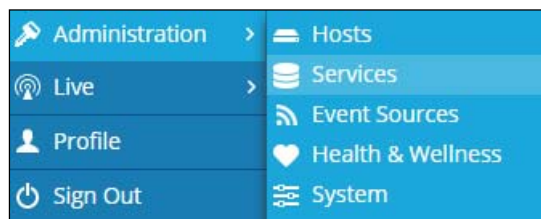
17. Select **Deploy**.




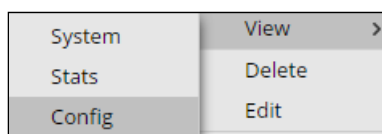
18. Select **Close**, to complete the deployment of the Common Event Format.



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



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



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



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.

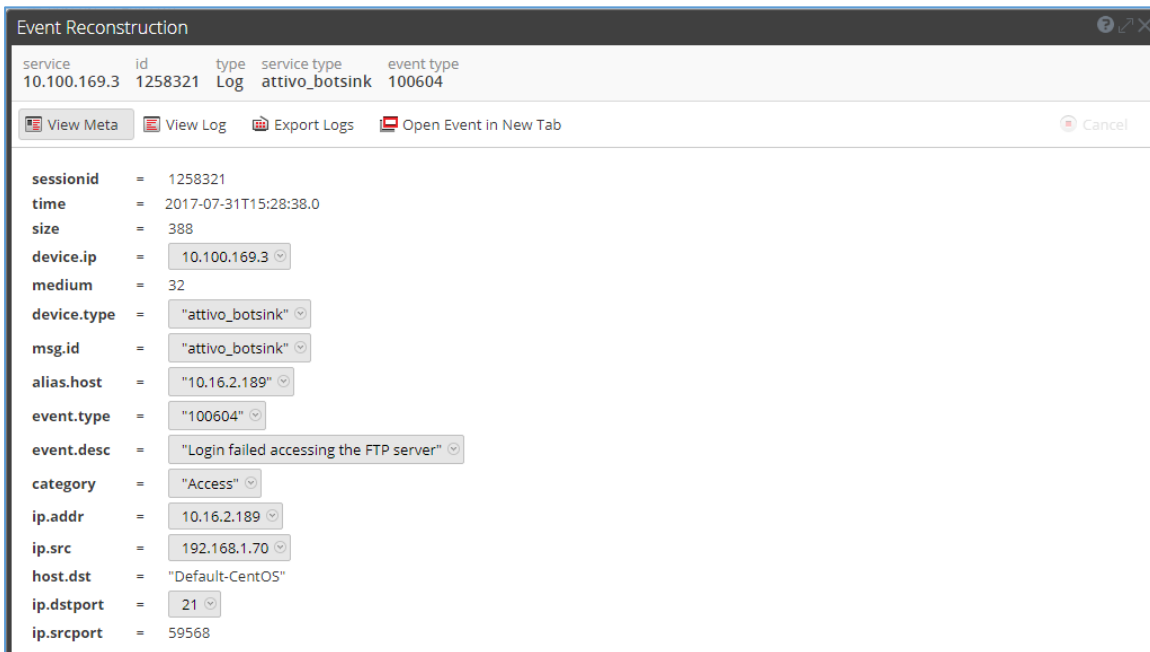
```
<?xml version="1.0" encoding="utf-8"?>
<!--
# attributes:
#   envisionName: The name of the column in the universal table
#   nwName:       The name of the NetWitness meta field
#   format:      Optional. The language key data type. See
LanguageManager. Defaults to "Text".
#   flags:       Optional. 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.
-->
<mappings>

    <mapping envisionName="sport" nwName="ip.srcport" flags="None"
format="UI nt16" envisionDisplayname="SourcePort|Local Port|ServerPort"
nullTokens="-|(null)"/>

</mappings>
```

4. Restart the **Log Decoder services**.

5. Below is an example of an event received from Attivo through the Netwitness Investigator.



service	id	type	service type	event type
10.100.169.3	1258321	Log	attivo_botsink	100604

View Meta View Log Export Logs Open Event in New Tab Cancel

sessionid = 1258321
time = 2017-07-31T15:28:38.0
size = 388
device.ip = 10.100.169.3
medium = 32
device.type = attivo_botsink
msg.id = attivo_botsink
alias.host = 10.16.2.189
event.type = 100604
event.desc = Login failed accessing the FTP server
category = Access
ip.addr = 10.16.2.189
ip.src = 192.168.1.70
host.dst = Default-CentOS
ip.dstport = 21
ip.srcport = 59568

Certification Checklist for RSA NetWitness

Date Tested: July 31, 2017

Certification Environment		
Product Name	Version Information	Operating System
RSA NetWitness	10.6.3	Virtual Appliance
Attivo Networks ThreatDefend	4.0.5.x	

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	✓

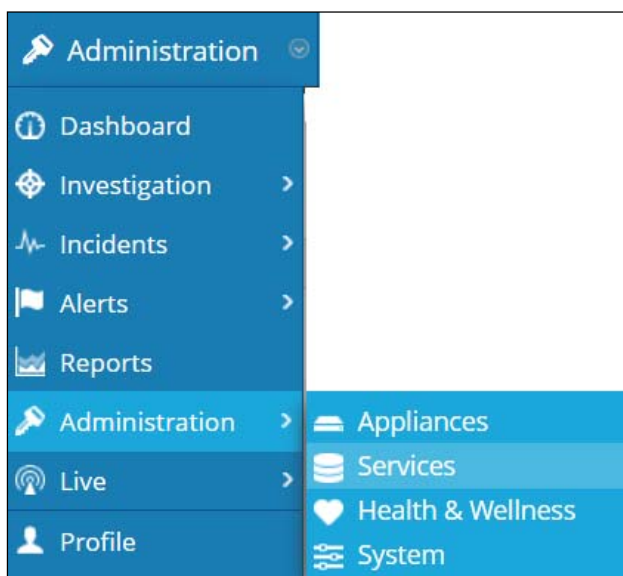
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

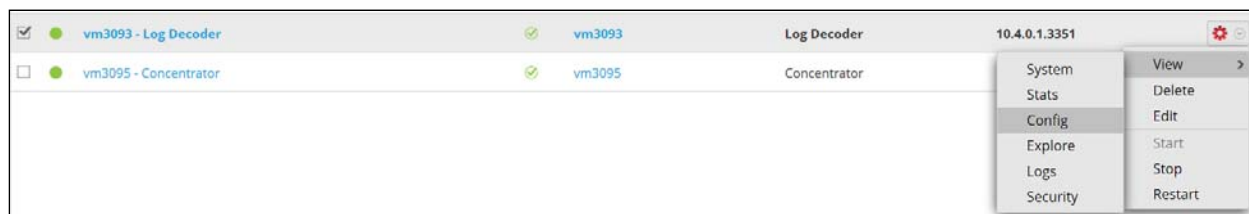
Security Analytics Disable the Common Event Format Parser

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

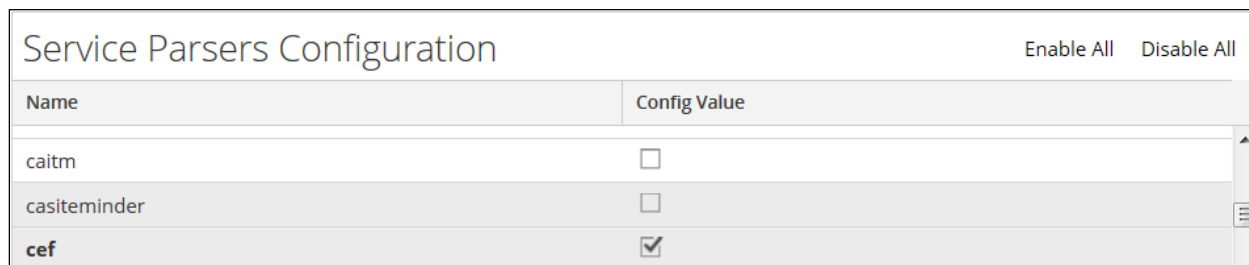
1. Select the Security Analytics **Administration > Services** menu.



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



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

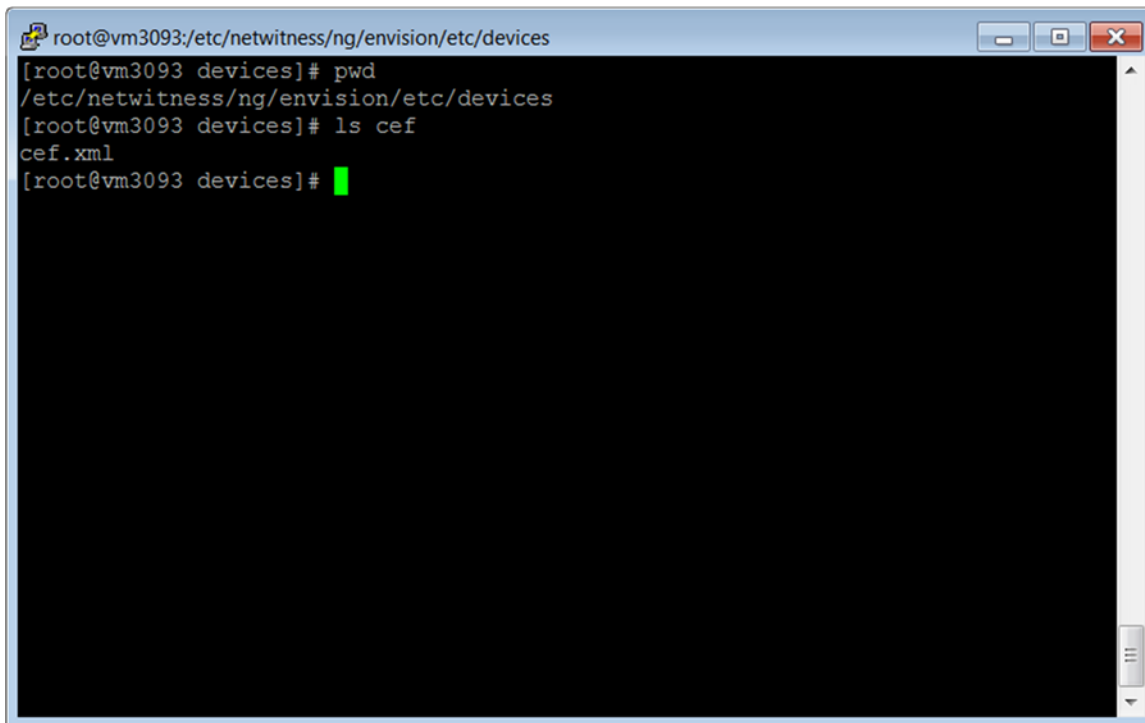


4. Click **Apply** to save settings.

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:/etc/netwitness/ng/envision/etc/devices
[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.