RSA® NETWITNESS®
Logs
Implementation Guide

Securonix Snypr 6.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: July 17th, 2017

RSA READY

Solution Summary

Securonix Snypr sends out CEF formatted violation events into the Log Decoder of RSA NetWitness. These CEF formatted events are parsed on the Log Decoder and forwarded to the RSA NetWitness Concentrator where analysts can perform enterprise-wide querying and real-time analytics while facilitating reporting and alerting.

RSA NetWitness Features	
Securonix Snypr 6.0	
Integration package name	Common Event Format
Device display name within Security Analytics	Securonix Snypr
Event source class	CEF
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
07/17/2017	Initial support for Securonix

! 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]

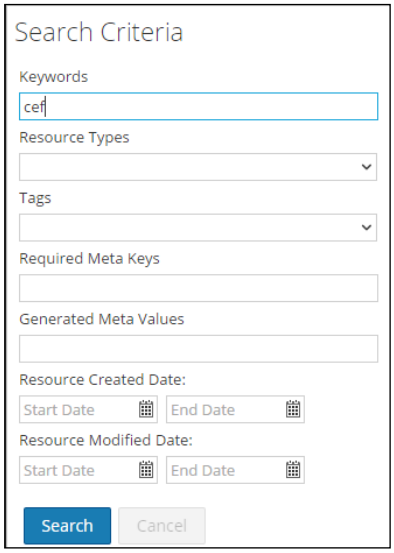
! Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.

RSA NetWitness Configuration

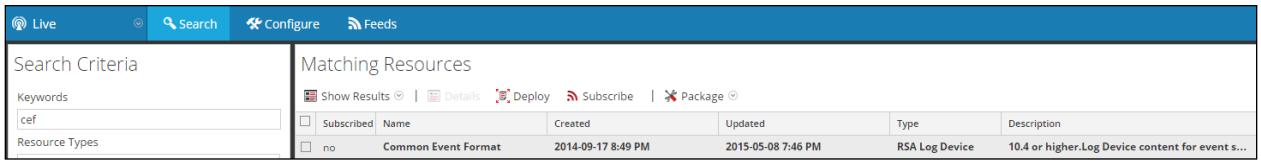
Deploy the Common Event Format (CEF) Parser

You will need to deploy the *Common Event Format parser* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

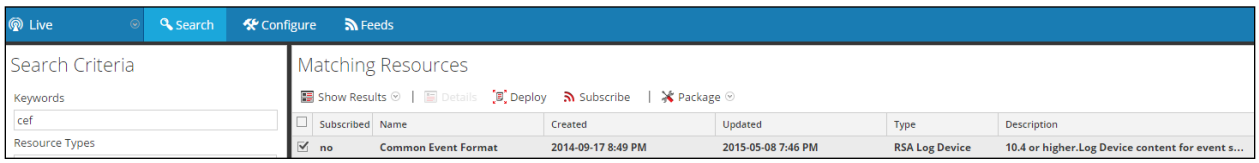
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **CEF**



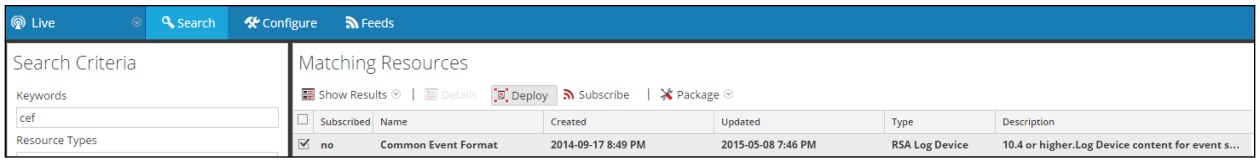
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



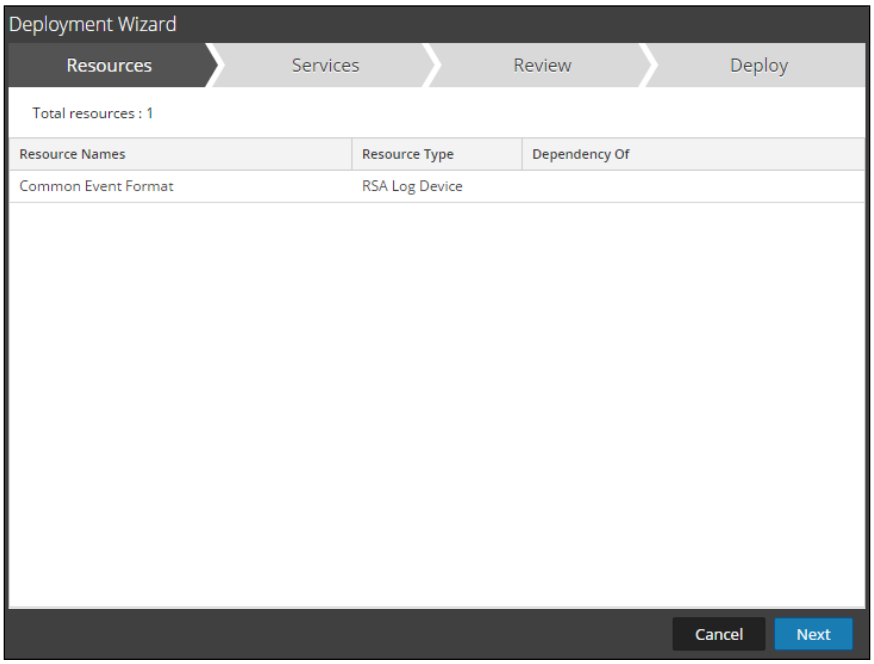
4. Select the checkbox next to **Common Event Format**.



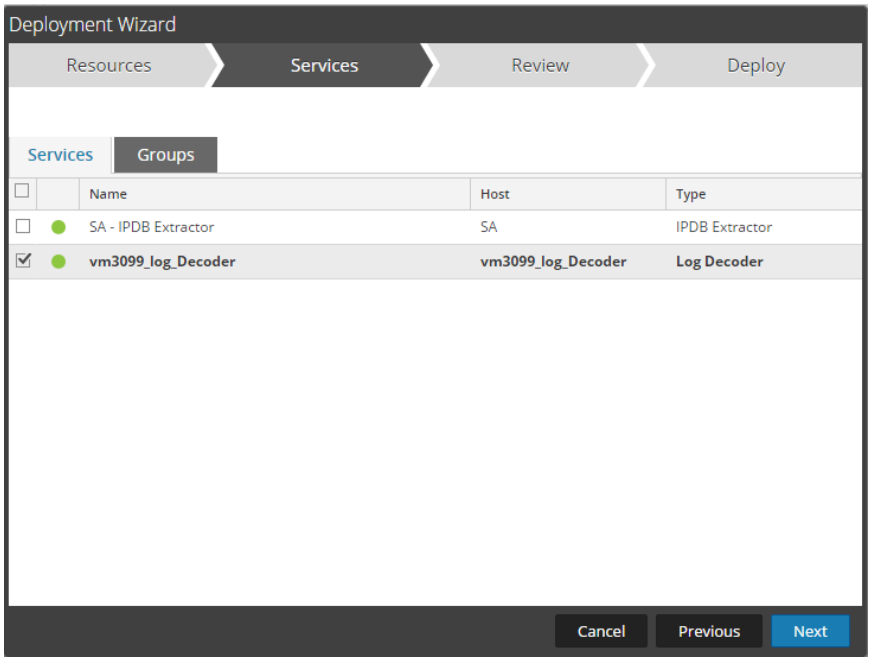
5. Click **Deploy** in the menu bar.



6. Select **Next**.

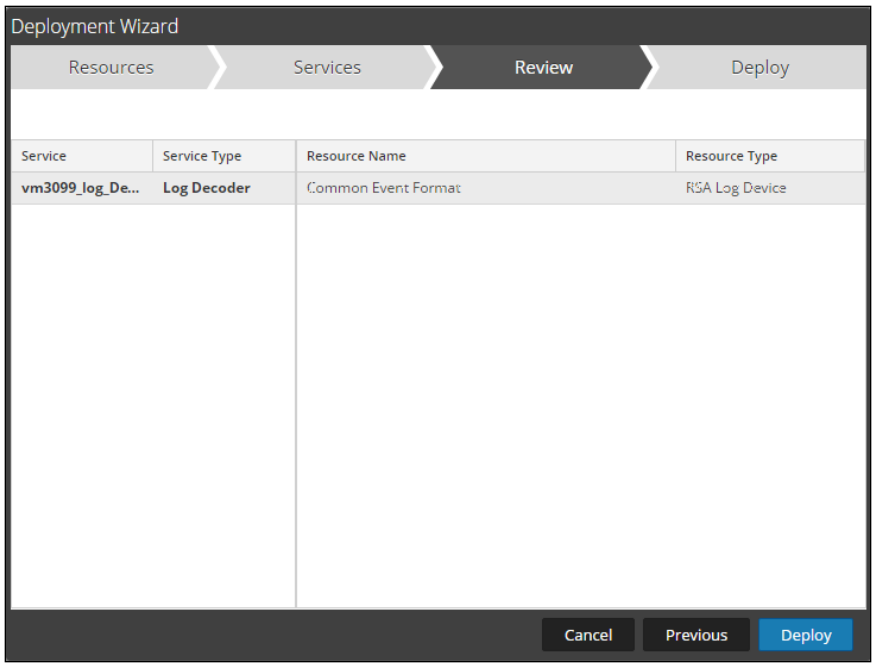


7. Select the **Log Decoder** and Select **Next**.

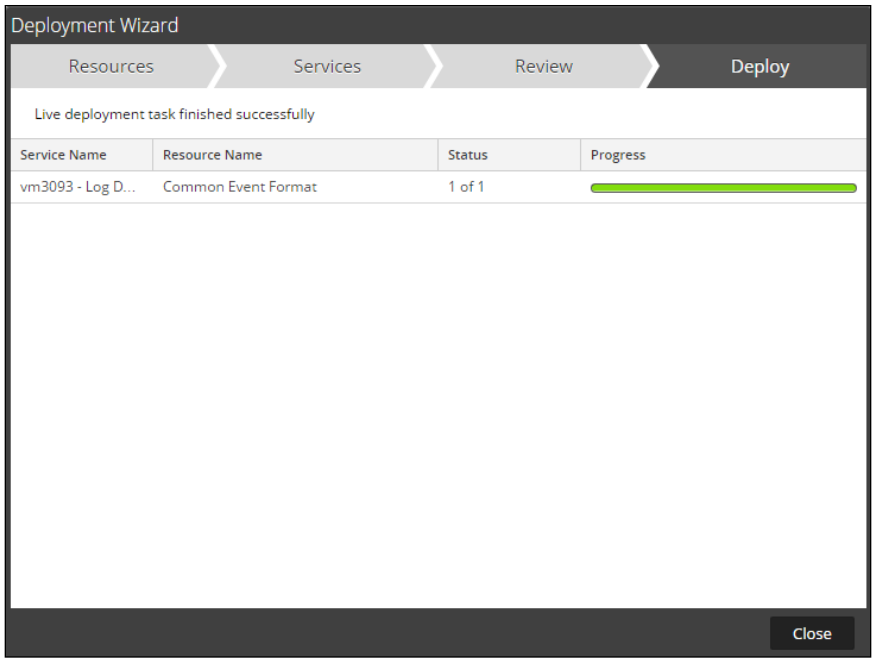


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

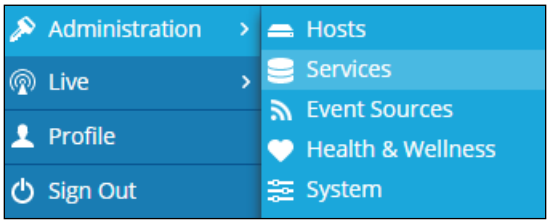
8. Select **Deploy**.



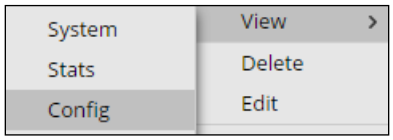
9. Select **Close**, to complete the deployment of the Common Event Format.



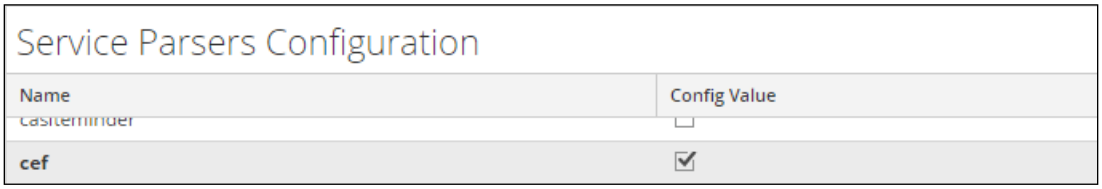
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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**.



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

Configuring Custom CEF Fields on The NetWitness Log Decoder

1. In the /etc/netwitness/ng/envision/etc/devices/cef/cef.xml file,
    a. Under the

       <VendorProducts> key, if you are using the HPE UBA Version of Securonix add,

       <Vendor2Device vendor="HPE" product="ArcSight User Behavior Analytics" device="securonix_uba" group="Analytics"/>

       Else if you are using Securonix UBA the add,

       <Vendor2Device vendor="Securonix" product="Risk and Threat Intelligence" device="securonix_uba" group="Analytics"/>

       The vendor and product values are obtained from the CEF logs.
    b. Under the <ExtensionKey> cefName=”cs1”, add

       <device2meta device="securonix_uba" metaName="firstname" label="First Name"/>
    c. Under the <ExtensionKey> cefName=”cs2”, add

       <device2meta device="securonix_uba" metaName="lastname" label="Last Name"/>
    d. Under the <ExtensionKey> cefName=”cs3”, add

       <device2meta device="securonix_uba" metaName="title" label="Title"/>
    e. Under the <ExtensionKey> cefName=”cs4”, add

       <device2meta device="securonix_uba" metaName="employeeid" label="Employee ID"/>
    f. Under the <ExtensionKey> cefName=”cs5”, add

       <device2meta device="securonix_uba" metaName="department" label="Department"/>
    g. Under the <ExtensionKey> cefName=”cs6”, add

       <device2meta device="securonix_uba" metaName="manageremployeeid" label="Manager Employee ID"/>
    h. Under the <ExtensionKey> cefName=”cfp1”, add

       <device2meta device="securonix_uba" metaName="violationriskscore" label="Violation Risk Score"/>
2. In the **/etc/netwitness/ng/envision/etc** folder, look for the **table-map-custom.xml** file. If it is not present, create one which is a copy of the **table-map-custom.xml** file that is already present in the same folder. If you have created a copy, then remove all the <mapping> keys from table-map-custom.xml since they are already present in table-map.xml.

   Add new <mapping> for each of the metaNames that you just added to the **cef.xml** file in step 1 above.

a. <mapping envisionName="firstname" nwName="firstname" flags="None" format="Text"/>

b. <mapping envisionName="lastname" nwName="lastname" flags="None" format="Text"/>

c. <mapping envisionName="title" nwName="title" flags="None" format="Text"/>

d. <mapping envisionName="employeeid" nwName="employeeid" flags="None" format="Text"/>

e. <mapping envisionName="department" nwName="department" flags="None" format="Text"/>

f. <mapping envisionName="manageremployeeid" nwName="manageremployeeid" flags="None" format="Text"/>

g. <mapping envisionName="violationriskscore" nwName="violationriskscore" flags="None" format="Text"/>

3. Restart the Log Decoder services in the NetWitness UI. When new CEF events are sent, the Securonix meta keys should now be present in the Log Decoder and Concentrator.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Securonix Snypr 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.

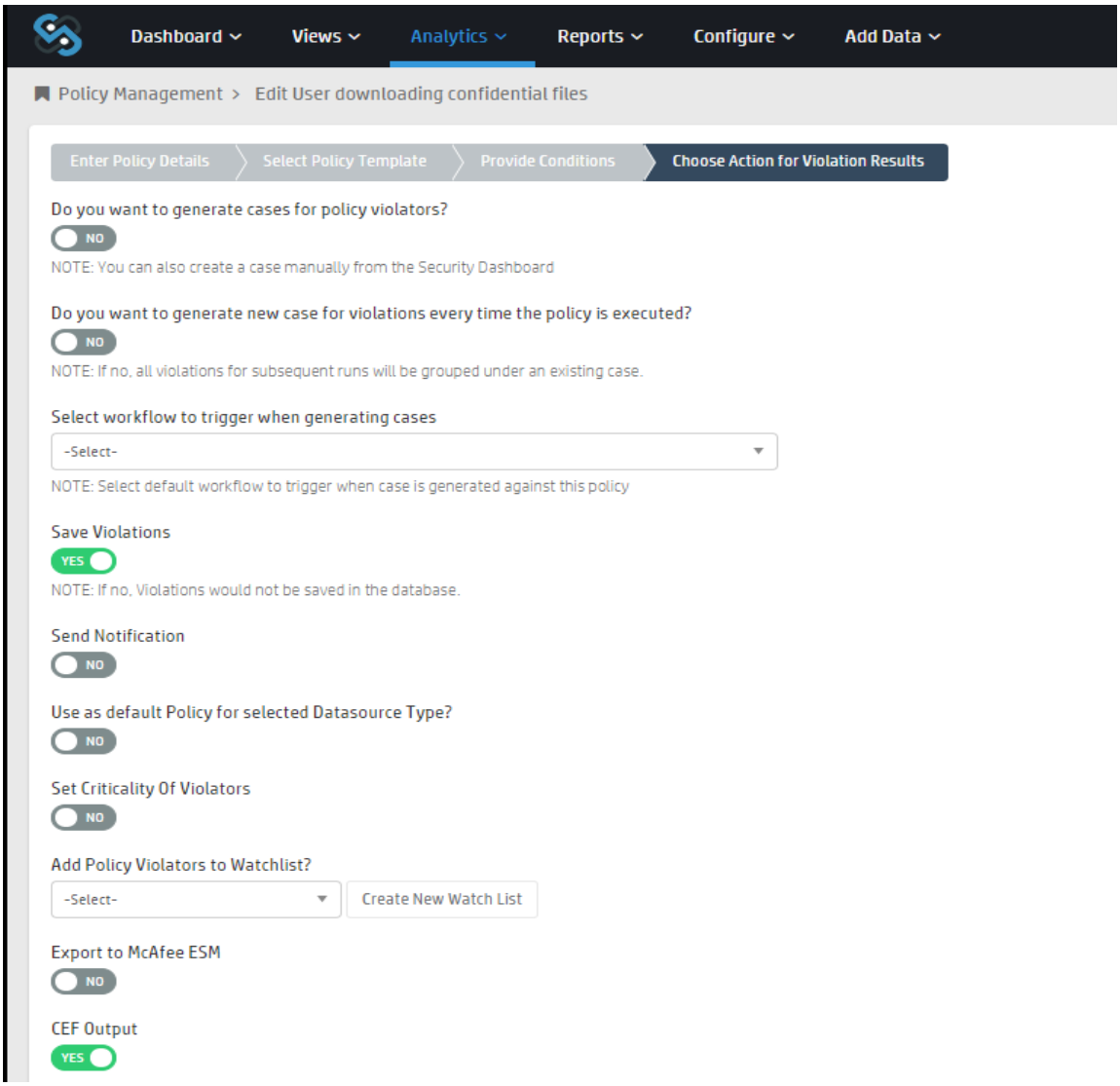
All Snypr components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! 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 Securonix Snypr is properly configured and secured before deploying to a production environment. For more information, please refer to the Securonix Snypr documentation or website.

Securonix Snypr Configuration

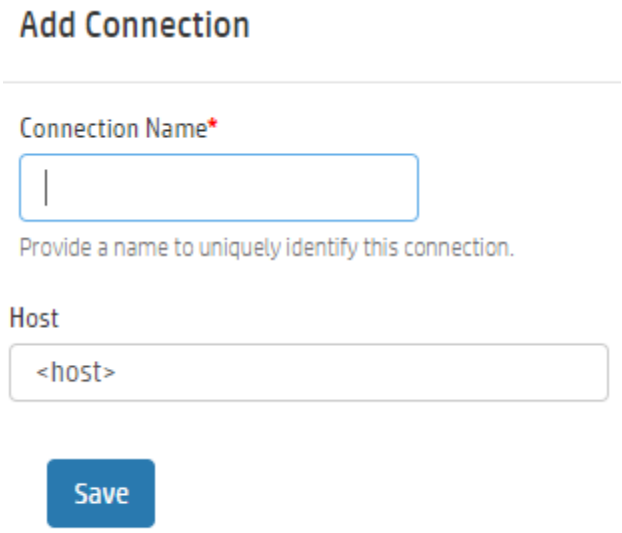
To begin process of configuring Securonix Snypr, select the policy in Snypr for which you want to edit and send CEF formatted alerts to NetWitness.

1. In the 4th step of the policy configuration, **Choose Action For Violation Results**, enable the **CEF Ouput** button:



2. This opens up a new box below,

3. In the drop down, select **Create New Connection** option. This will open a new screen called **Add Connection**:



4. Enter a new **Connection Name**, Enter the IP Address of the Log Decoder under **Host**, and hit **Save**.
5. Now when the policy for which CEF violations are to be sent to NetWitness is run, the violations are sent directly to NetWitness as CEF data.

Certification Checklist for RSA NetWitness

Date Tested: July 14th, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
Securonix Snypr	6.0	

RSA 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	✓

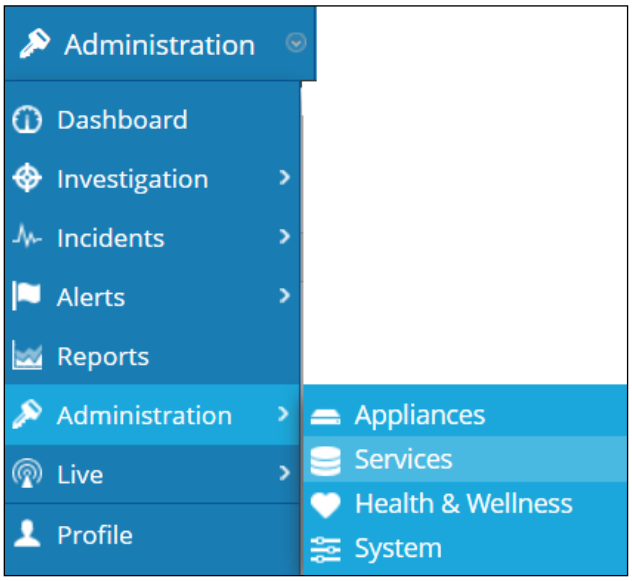
✓ = Pass ✗ Fail N/A = Non-Available Function

Appendix

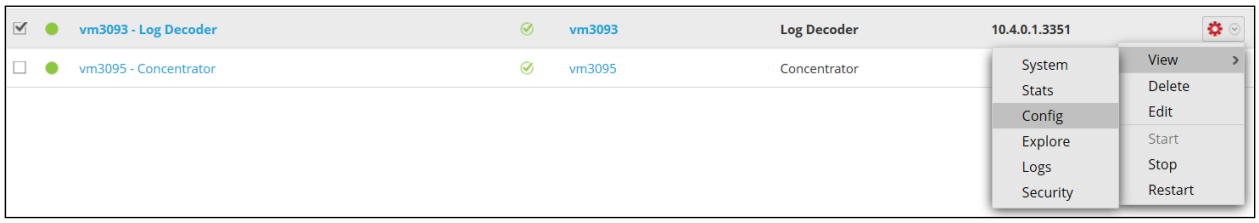
RSA NetWitness Disable the Common Event Format Parser

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

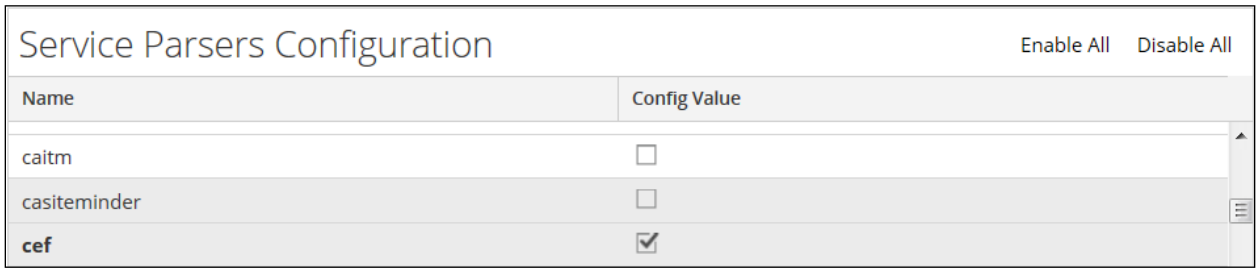
1. Select the Security Analytics **Administration > Services menu**.



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



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

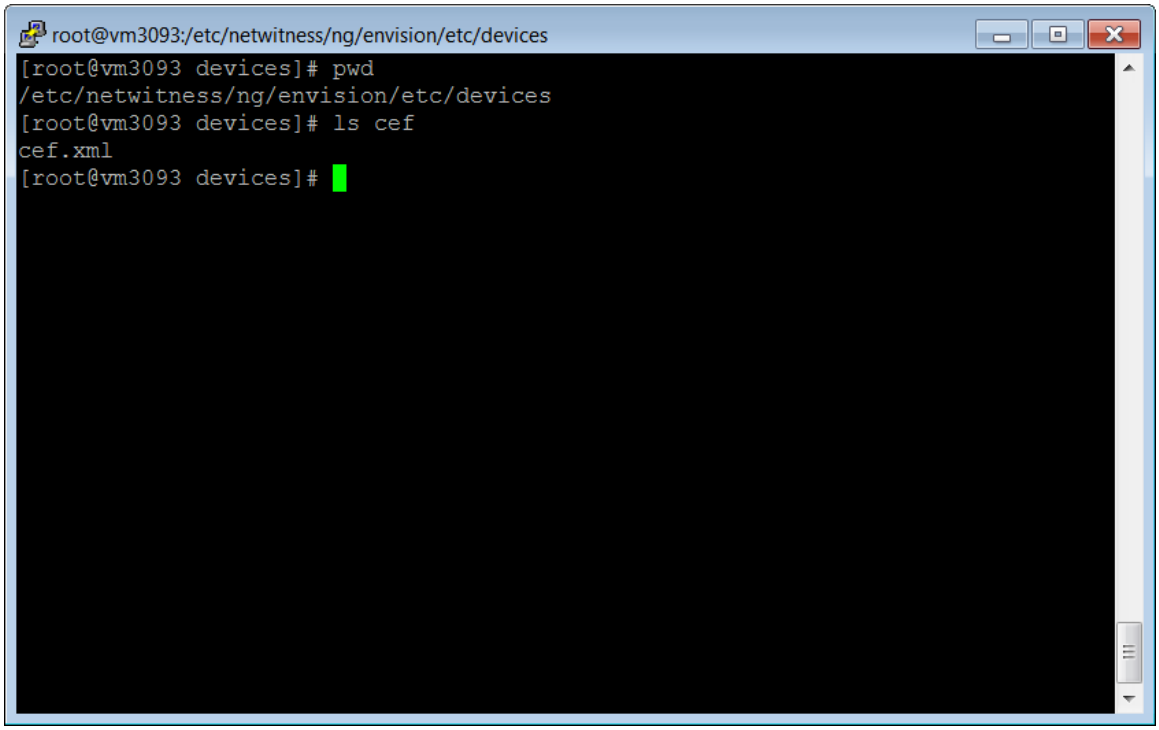


4. Click **Apply** to save settings.

RSA NetWitness Remove the Common Event Format 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 and delete the CEF folder and its contents.