

RSA® NETWITNESS®

Logs Implementation Guide

**Skyhigh Networks
Skyhigh 3.3.3**

Daniel R. Pintal, RSA Partner Engineering
Last Modified: September 26, 2017

RSA
READY

Solution Summary

Skyhigh Networks integrates with RSA NetWitness to provide customers the means to identify and investigate various anomalies and incidents detected by Skyhigh's Machine Learning Algorithms. Skyhigh Enterprise Connector is an on-premise component that leverages various types of incidents generated through Skyhigh analytics and machine learning, and can integrate with customer's SIEM solutions such as RSA NetWitness. This provides users with single pane of glass for reviewing incidents generated from Skyhigh and other sources in a single console for remediation or action.

RSA NetWitness Features	
Skyhigh Networks Skyhigh 3.3.3	
Integration package name	Common Event Format
Device display name within NetWitness	skyhigh_anomalies
Event source class	Analysis
Collection method	syslog cef



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
8/30/2017	Initial support for Skyhigh 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 Skyhigh Networks 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 Skyhigh Networks 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 Skyhigh Networks is properly configured and secured before deploying to a production environment. For more information, please refer to the Skyhigh Networks documentation or website.

Skyhigh Networks Configuration

Incidents can be exported from Skyhigh Networks to your SIEM systems using syslog export. This export is handled through the Enterprise Connector.

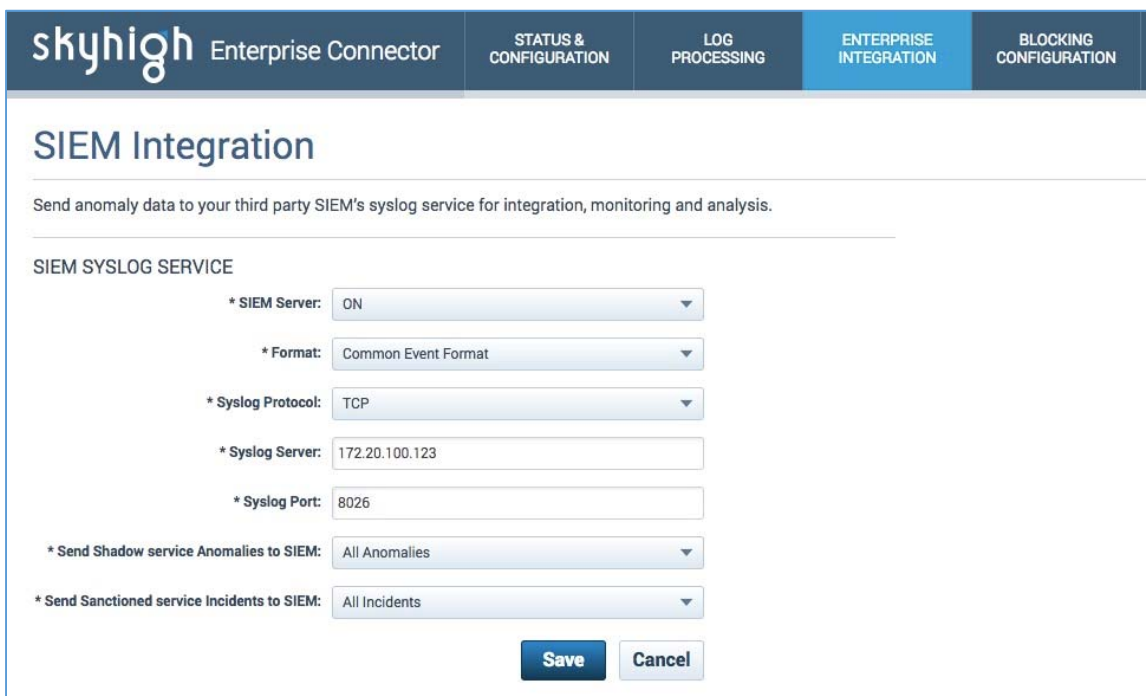
To Configure a SIEM Syslog Service

1. Navigate to the Enterprise Connector UI by entering the IP Address and port number configured during EC installation into your web browser's address bar.
2. Sign in using an email address and password with Enterprise Connector privileges.
3. Go to **Enterprise Integration > SIEM Integration**.
4. For **SIEM Server**, select **ON**.
5. In the **Format** field, choose the format for the anomaly event export, based on the requirements of your SIEM
 - Key Value Pairs
 - Log Event Extended Format (LEEF)
 - Common Event Format
6. In the **Syslog Protocol** field, Select **UDP** or **TCP** for the protocol for your Syslog server exports, based on the requirements for your SIEM.
7. In the **Syslog Server** field, enter the Host Name or IP Address of the SIEM that will receive the anomaly exports. This information should be available from your SIEM's user interface.
8. In the **Syslog Port** field, set the port that your SIEM is listening on for traffic. This information should be available from your SIEM's user interface.
9. **Send Shadow service Anomalies to SIEM**. Select the option against which you want to send Shadow IT anomalies to the SIEM:
 - All: Send every Shadow IT anomaly to your SIEM with each export.
 - New Anomalies Only: Only send Shadow IT anomalies that have been created since your last export.

10. **Send Sanctioned service Incidents to SIEM.** Select the frequency at which you want to send Sanctioned IT anomalies to the SIEM:

- All Anomalies: Send every Sanctioned IT anomaly to your SIEM with each export.
- **New Anomalies Only:** Only send Sanctioned IT anomalies that have been created since your last export.

11. Click **Save**.



The screenshot shows the 'SIEM Integration' configuration page within the Skyhigh Enterprise Connector. The page has a dark blue header with the 'skyhigh Enterprise Connector' logo and five navigation tabs: 'STATUS & CONFIGURATION', 'LOG PROCESSING', 'ENTERPRISE INTEGRATION' (which is highlighted in blue), and 'BLOCKING CONFIGURATION'. Below the header, the page title 'SIEM Integration' is displayed. A descriptive text states: 'Send anomaly data to your third party SIEM's syslog service for integration, monitoring and analysis.' The main configuration area is titled 'SIEM SYSLOG SERVICE' and contains several settings:

- * SIEM Server: A dropdown menu set to 'ON'.
- * Format: A dropdown menu set to 'Common Event Format'.
- * Syslog Protocol: A dropdown menu set to 'TCP'.
- * Syslog Server: A text input field containing '172.20.100.123'.
- * Syslog Port: A text input field containing '8026'.
- * Send Shadow service Anomalies to SIEM: A dropdown menu set to 'All Anomalies'.
- * Send Sanctioned service Incidents to SIEM: A dropdown menu set to 'All Incidents'.

At the bottom right of the configuration area, there are two buttons: a blue 'Save' button and a light blue 'Cancel' button.

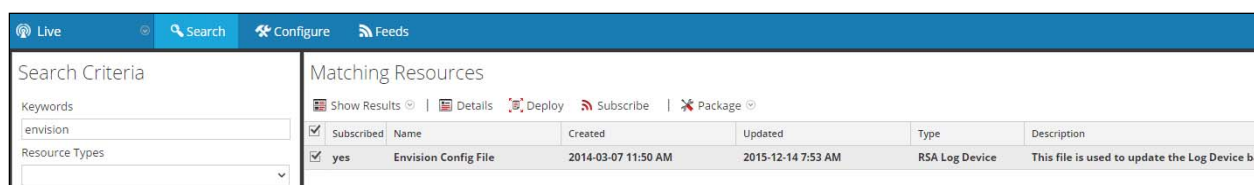
RSA NetWitness Configuration

Deploy the enVision Config File

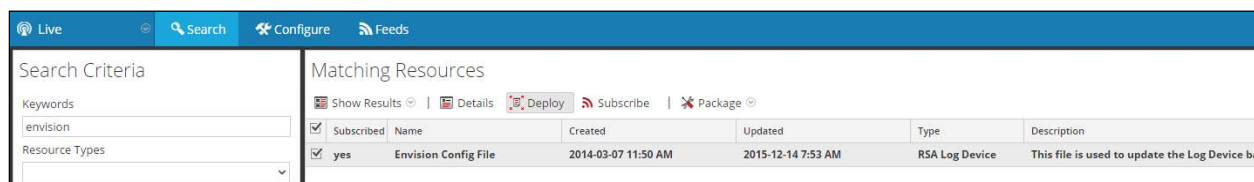
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

! > 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**.



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



6. Select **Next**.

Deployment Wizard

Resources Services Review Deploy

Total resources : 1

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

Cancel Next

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

Deployment Wizard

Resources Services Review Deploy

Services Groups

<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

Cancel Previous Next

! > 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

Resources > Services > **Review** > Deploy

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

Cancel Previous **Deploy**

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

Deployment Wizard

Resources > Services > Review > **Deploy**

Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3099_log_Dec...	Envision Config File	1 of 1	<div></div>

Close



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**

Search Criteria

Keywords

cef

Resource Types

Tags

Required Meta Keys

Generated Meta Values

Resource Created Date:

Start Date

End Date

Resource Modified Date:

Start Date

End Date

Search

Cancel

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef		<div>Show Results Details Deploy Subscribe Package</div>				
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...

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef		<div>Show Results Details Deploy Subscribe Package</div>				
Resource Types						
		<input checked="" type="checkbox"/> Subscribed	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...

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

Live Search Configure Feeds						
Search Criteria		Matching Resources				
Keywords cef		<div>Show Results Details Deploy Subscribe Package</div>				
Resource Types						
		<input checked="" type="checkbox"/> Subscribed	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...

6. Select **Next**.

Deployment Wizard

Resources Services Review Deploy

Total resources : 1

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

Cancel Next

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

Deployment Wizard

Resources Services Review Deploy

Services Groups

<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

Cancel Previous Next

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

8. Select **Deploy**.

Deployment Wizard

Resources Services Review Deploy

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

Cancel Previous Deploy

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

Deployment Wizard

Resources Services Review Deploy

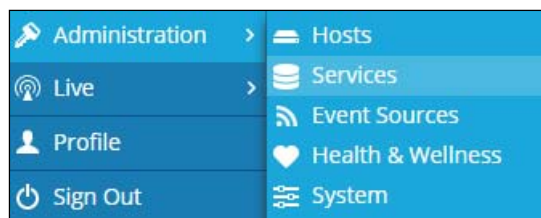
Live deployment task finished successfully


Service Name	Resource Name	Status	Progress
vm3093 - Log D...	Common Event Format	1 of 1	<div></div>

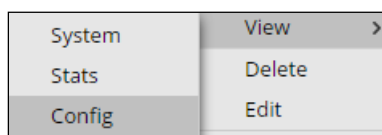
Close



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 within the Service Parsers Configuration and select **Apply**.

Service Parsers Configuration	
Name	Config Value
casiteminder	<input type="checkbox"/>
cef	<input checked="" type="checkbox"/>

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

Edit the Common Event Format to collect Skyhigh event times

! » 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 <MESSAGE section and copy/paste the following lines below into the file after the /> of the preceding <MESSAGE and contents;

```
<MESSAGE
    level="4"
    parse="1"
    parsedefault="1"
    tableid="74"
    id1="skyhigh_anomalies"
    id2="skyhigh_anomalies"
    eventcategory="1612000000"

    content="&lt; @event_name: *HDR(event_description)&gt; &lt; @msg: *PARMVAL($MSG)&gt; &lt; @starttime: *EVNTTIME($MSG, '%B %D %W %Z', param_starttime)&gt; &lt; @endtime: *EVNTTIME($MSG, '%B %D %W %Z', param_endtime)&gt; &lt; param_starttime&gt; &lt; param_endtime&gt; &lt; msghold&gt;";" />
```

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

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

    <VendorProducts>
        <!--Example <Vendor2Device
        <Vendor2Device vendor="RSA" product=" NetWitness NetFlow Collector"
device="My Own Device" group="switch"/>
        -->
        <Vendor2Device vendor="Skyhigh" product="Skyhigh"
device="skyhigh_anomalies" group="Analysiss"/>
    </VendorProducts>

    <ExtensionKeys>
        <!--Example <ExtensionKey

                <ExtensionKey cefName="proto" metaName="protocol">
                <device2meta device="rsaflow" metaName="proto1"/>
                </ExtensionKey>

        -->
        <ExtensionKey cefName="updatedOn"
metaName="param_endtime"/>
        <ExtensionKey cefName="userAction" metaName="userAction"/>
        <ExtensionKey cefName="thresholdValue"
metaName="alert_id"/>
        <ExtensionKey cefName="incidentGroupID" metaName="group"/>
        <ExtensionKey cefName="incidentID" metaName="incidentID"/>
        <ExtensionKey cefName="anomalyValue"
metaName="anomalyValue"/>
        <ExtensionKey cefName="activityName"
metaName="activityName"/>
        <ExtensionKey cefName="serviceName"
metaName="serviceName"/>
        <ExtensionKey cefName="response" metaName="response"/>

        <ExtensionKey cefName="riskSeverity"
metaName="riskSeverity"/>

    </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.

```
<!--
# 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="starttime" nwName="start" flags="None"
format="TimeT" envisionDisplayName="StartTime"/>
  <mapping envisionName="endtime" nwName="updatedAt" flags="None"
format="TimeT" envisionDisplayName="EndTime, rt, end"/>

  <mapping envisionName="userAction" nwName="userAction" flags="None"/>
  <mapping envisionName="alert_id" nwName="thresholdValue" flags="None"/>
  <mapping envisionName="group" nwName="incidentGroupId" flags="None"/>
  <mapping envisionName="incidentId" nwName="incidentId" flags="None"/>
  <mapping envisionName="anomalyValue" nwName="anomalyValue" flags="None"/>
  <mapping envisionName="activityName" nwName="activityName" flags="None"/>
  <mapping envisionName="serviceNames" nwName="serviceNames" flags="None"/>
  <mapping envisionName="response" nwName="response" flags="None"/>
  <mapping envisionName="riskSeverity" nwName="riskSeverity" flags="None"/>
  <mapping envisionName="severity" nwName="severity" flags="None"
envisionDisplayName="Severity|SeverityLevel"/>

</mappings>
```

Edit the NetWitness index-concentrator-custom file

!> Important: The index-custom-concentrator.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 Concentrator open a connection and locate the **/etc/netwitness/ng** folder.
2. If one exists, backup the **index-concentrator-custom.xml** and then edit the index-concentrator-custom.xml file.
3. Copy and paste the entire section below into the file between the <!-- Add your custom index keys below this line -->...<!-- Add your custom index keys above this line -->;

Example.

```
<!-- Custom Index Revision 1.0 07/31/17-->
<!-- Add your custom index keys below this line -->

    <key description="userAction" level="IndexValues" name="userAction"
format="Text" valueMax="100000"/>
    <key description="thresholdValue" level="IndexValues"
name="thresholdValue" format="Text" valueMax="100000"/>
    <key description="incidentGroupId" level="IndexValues"
name="incidentGroupId" format="Text" valueMax="100000"/>
    <key description="incidentId" level="IndexValues" name="incidentId"
format="Text" valueMax="100000"/>
    <key description="anomalyValue" level="IndexValues" name="anomalyValue"
format="Text" valueMax="100000"/>
    <key description="activityName" level="IndexValues" name="activityName"
format="Text" valueMax="100000"/>
    <key description="serviceName" level="IndexValues" name="serviceName"
format="Text" valueMax="100000"/>
    <key description="response" level="IndexValues" name="response"
format="Text" valueMax="100000"/>
    <key description="riskSeverity" level="IndexValues" name="riskSeverity"
format="Text" valueMax="100000"/>
    <key description="event.name" level="IndexValues" name="event.name"
format="Text" valueMax="100000"/>
    <key description="severity" level="IndexValues" name="severity"
format="Text" valueMax="100000"/>

<!-- Add your custom index keys above this line -->
```


Skyhigh Collection Example within NetWitness Investigator:

Event Reconstruction

service

10.100.169.3

id

1258788

type

Log

service type

skyhigh_anomalies

service class

Analysis

event type

DataTransfer

View Meta

View Log

Export Logs

Export Meta

Open Event in New Tab

Cancel

sessionid

=

1258788

time

=

2017-08-04T15:39:36.0

size

=

527

device.ip

=

10.100.169.3

medium

=

32

device.type

=

skyhigh_anomalies

device.class

=

Analysis

alias.host

=

lpvm02.app.qa.sjc.shn

event.type

=

DataTransfer

event.desc

=

Alert.Data

severity

=

3

user.src

=

d06eb75aab45ebfc2378386ed9733246060d2534c37bde059cc0198646533db1

host.dst

=

ccsn.service-now.com

activityName

=

Upload

anomalyValue

=

1811130

incidentGroupld

=

10029

incidentld

=

4821634

response

=

Allowed

riskSeverity

=

Medium

serviceNames

=

[ServiceNow - Platform]

thresholdValue

=

344500

userAction

=

Upload

event.name

=

Alert.Data

starttime

=

2017-01-20T17:16:59.0

endtime

=

2017-01-30T17:03:18.0

level

=

4

msg.id

=

skyhigh_anomalies

event.cat.name

=

System.Audit

<

>

Viewing Log

Show Reconstruction Log

Certification Checklist for RSA NetWitness

Date Tested: September 26, 2017

Certification Environment		
Product Name	Version Information	Operating System
RSA NetWitness	10.6.4	Virtual Appliance
Skyhigh Networks	3.3.3	

NetWitness Test Case	Result
Device Administration	
Partner's device name appears in Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be enabled from Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be disabled from Device Parsers Configuration	<input checked="" type="checkbox"/>
Device can be removed from Device Parsers Configuration	<input checked="" type="checkbox"/>
Investigation	
Device name displays properly from Device Type	<input checked="" type="checkbox"/>
Displays Meta Data properly within Investigator	<input checked="" type="checkbox"/>

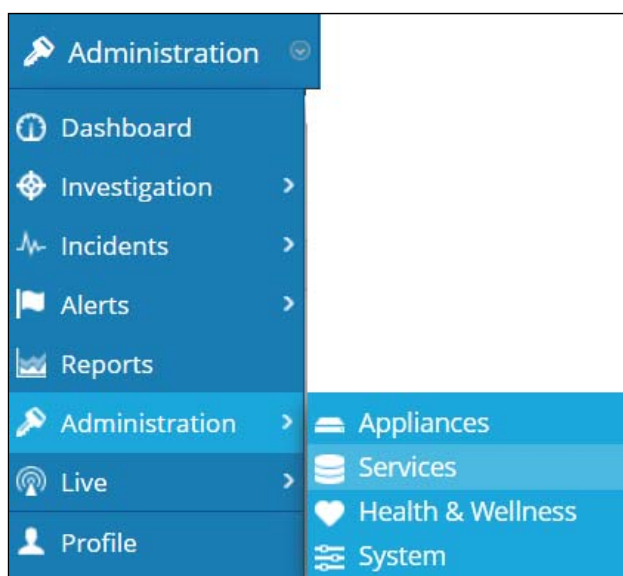
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

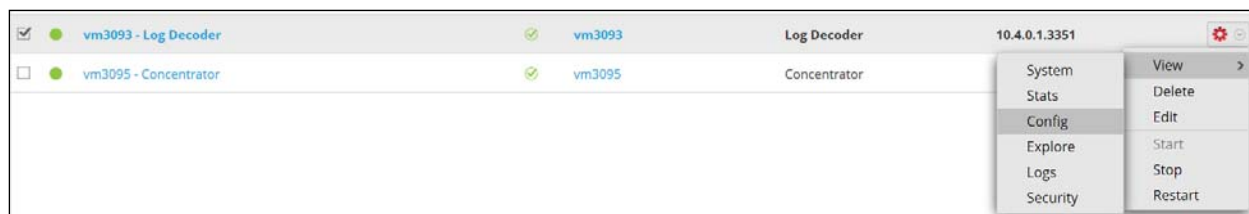
NetWitness Disable the Common Event Format Parser

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**.



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

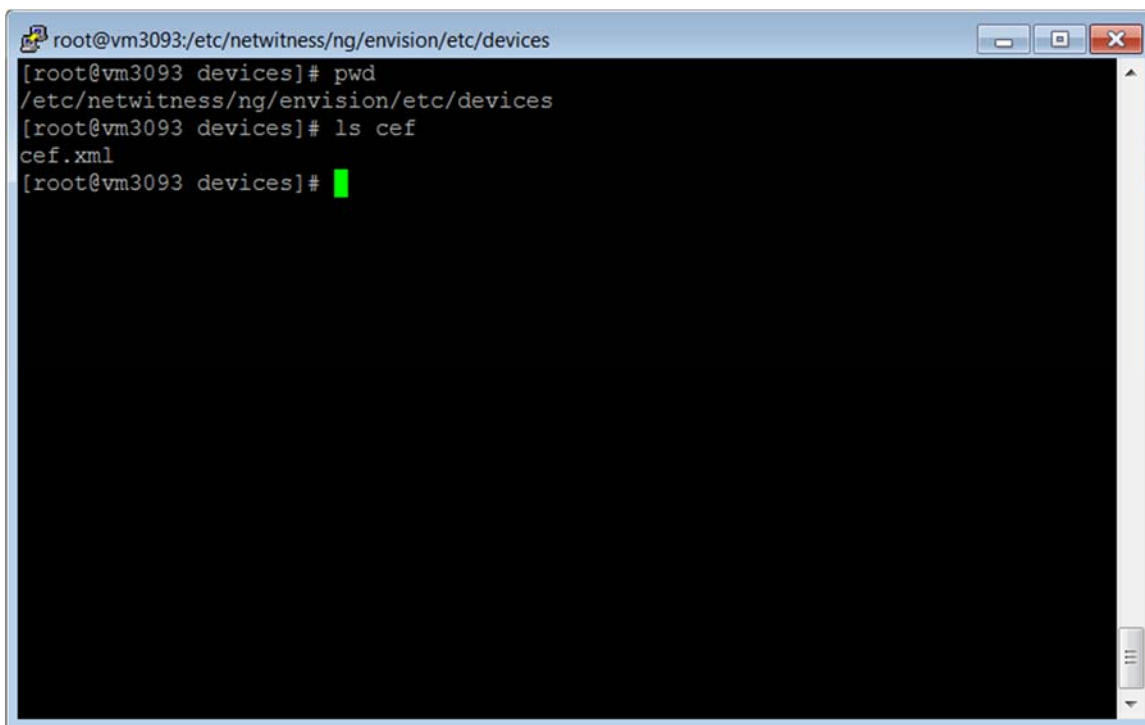
Service Parsers Configuration		Enable All	Disable All
Name	Config Value		
caitm	<input type="checkbox"/>		
casiteminder	<input type="checkbox"/>		
cef	<input checked="" type="checkbox"/>		

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.

A terminal window titled 'root@vm3093:/etc/netwitness/ng/envision/etc/devices' with standard window controls. The terminal shows the following commands and output:

```
[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.