RSA® NETWITNESS®
Logs
Implementation Guide

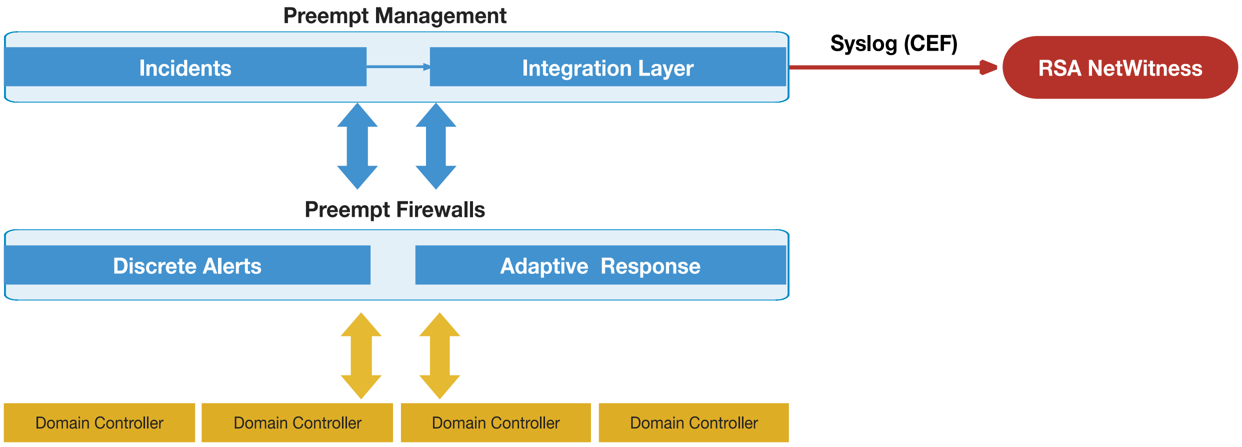
Preempt Security
Preempt Behavioral Firewall 2.2

Daniel R. Pintal, RSA Partner Engineering
Last Modified: October 31, 2017

Solution Summary

Preempt Security and RSA work together to identify and track threats within your network infrastructure.

RSA NetWitness Features Preempt Behavioral Firewall 2.2	
Integration package name	Common Event Format
Device display name within Security Analytics	preemptsecurity_pbf
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
10/31/2017	Initial support for Preempt Security Behavioral Firewall 2.0.

! 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 Preempt Behavioral Firewall 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.

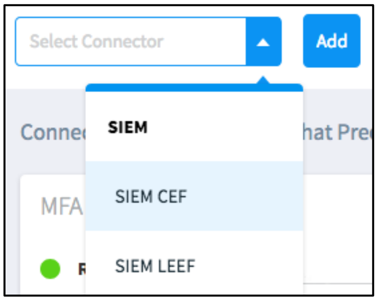
All Preempt Behavioral Firewall components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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 Preempt Behavioral Firewall is properly configured and secured before deploying to a production environment. For more information, please refer to Preempt Behavior Firewall SIEM Integration Guide.

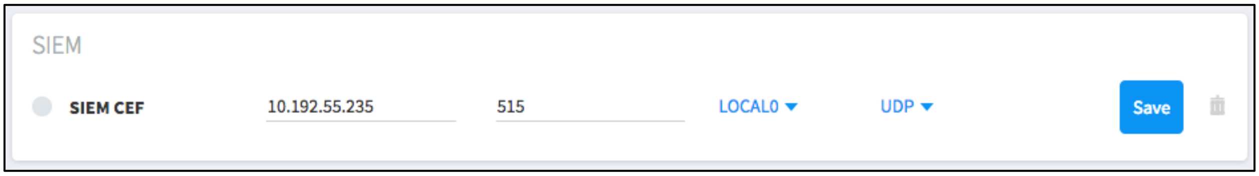
Preempt Behavioral Firewall Configuration

In order to report threats, a SIEM CEF connector should be configured on PBF. To do so, log in to PBF Dashboard and perform the following actions:

1. From the menu, select **Administration > Connectors**.
2. From the connectors menu, select **SIEM CEF.**



3. Click **Add**. A new SIEM CEF connector will now show up in the SIEM category panel
4. Fill in the Syslog Server IP address, port and protocol (TCP/UDP) to match the Event Source configured in NetWitness.
5. Choose **LOCAL0** as the syslog facility.


SIEM

SIEM CEF 10.192.55.235 515 LOCAL0 UDP

6. Click **Save**.

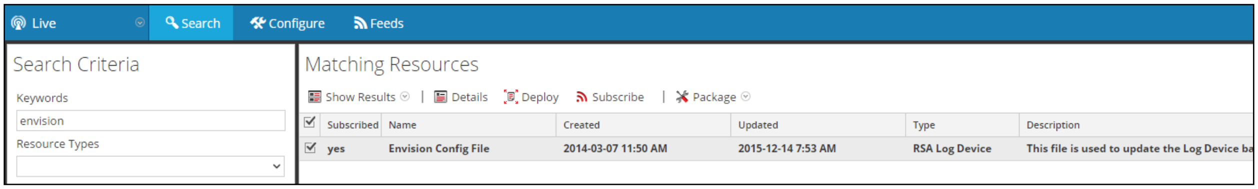
RSA NetWitness Configuration

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**.

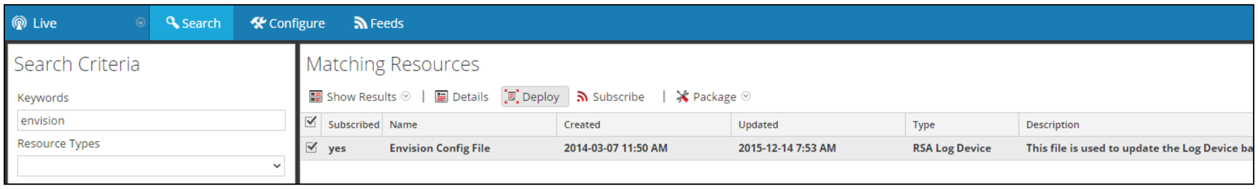


Keywords: envision

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.

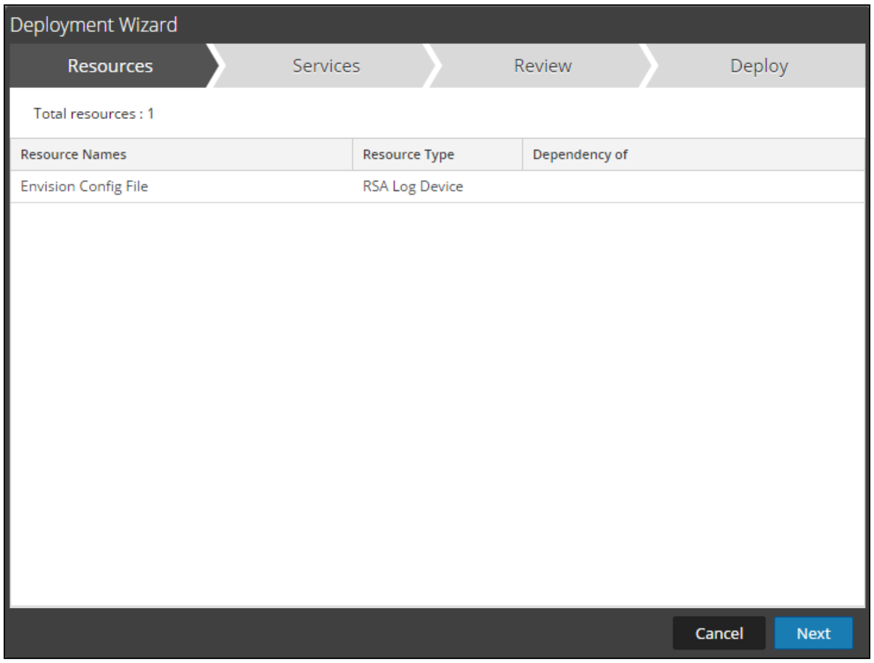


Keywords: envision

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

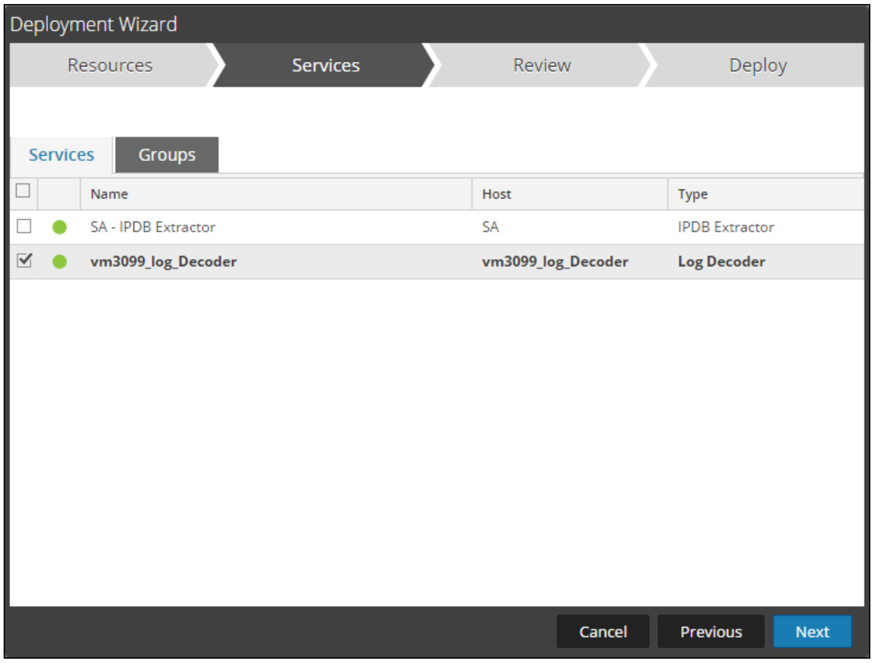
6. Select **Next**.



Total resources : 1

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

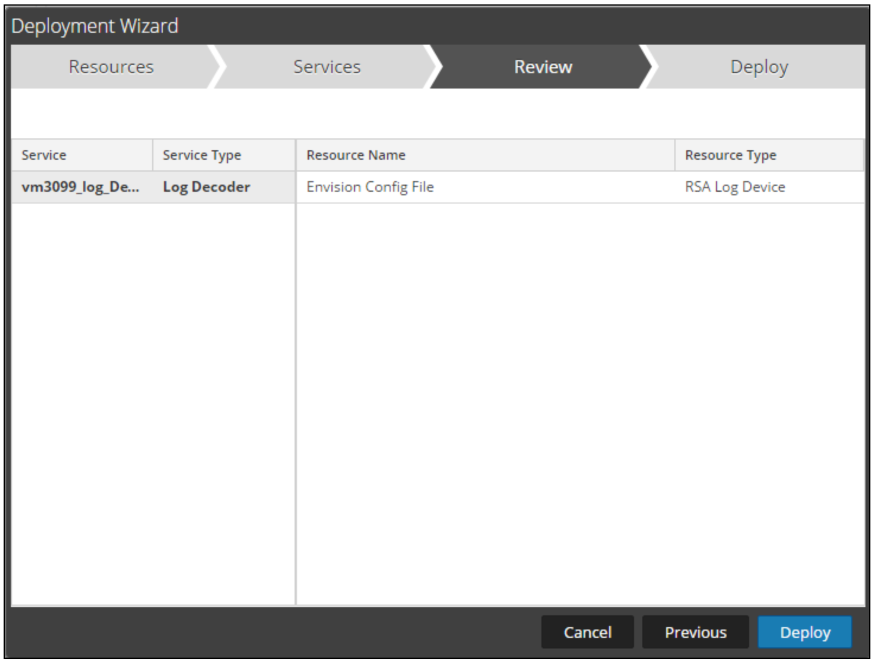
7. Select the **Log Decoder** and select **Next.**



□		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.

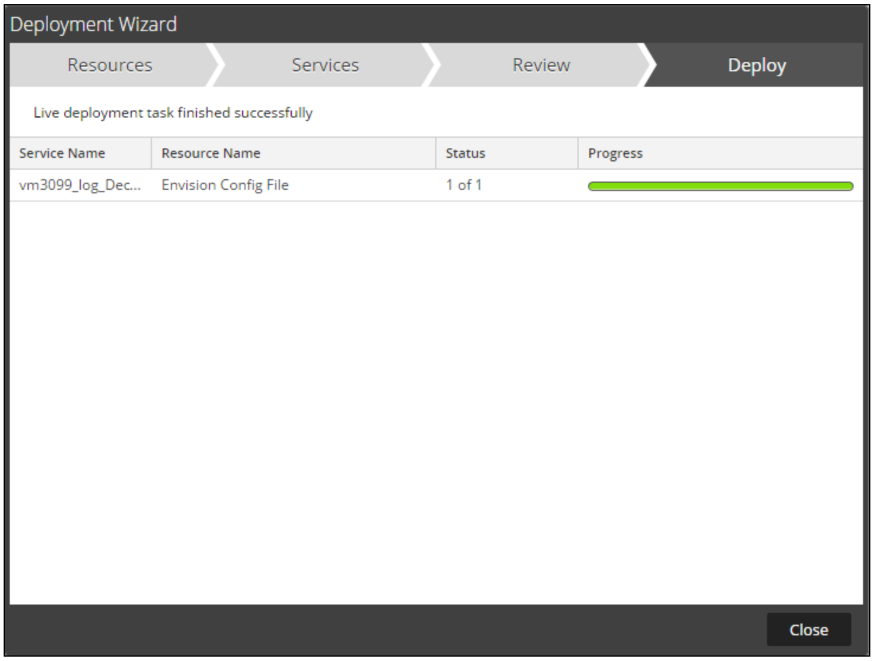
8. Select **Deploy**.



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	🟩

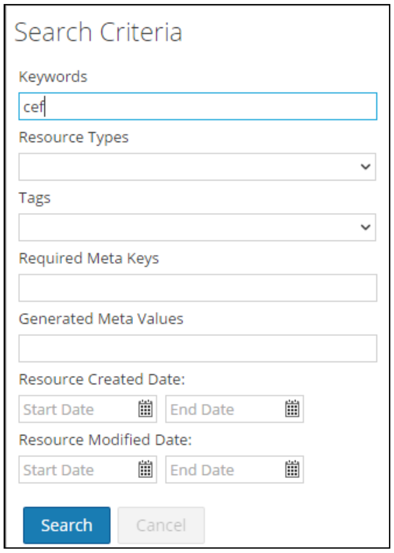
Deploy the Common Event Format

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

! Important: Using this procedure will overwrite an existing cef.xml.

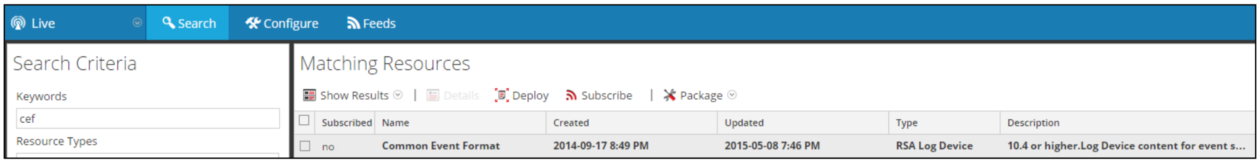
In addition it is recommended that NetWitness Live updates be disabled for cef.xml to prevent overwriting the customizations detailed in this guide.

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



Keywords: cef

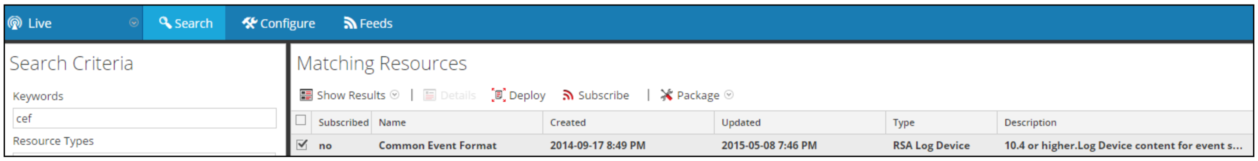
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



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...

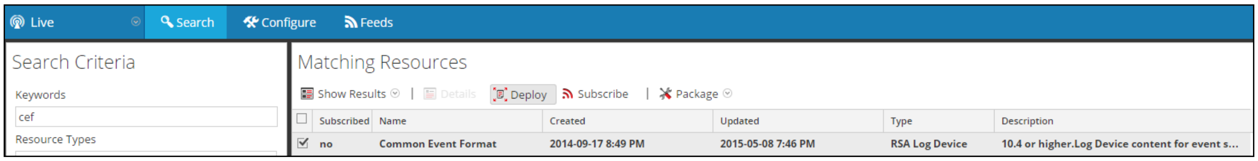
4. Select the checkbox next to **Common Event Format**.



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...

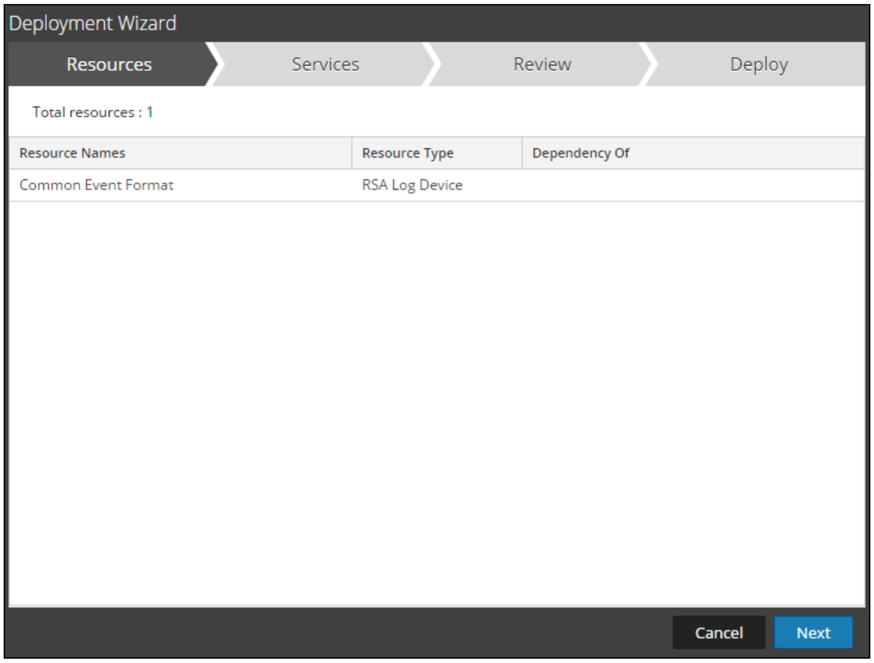
5. Click **Deploy** in the menu bar.



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...

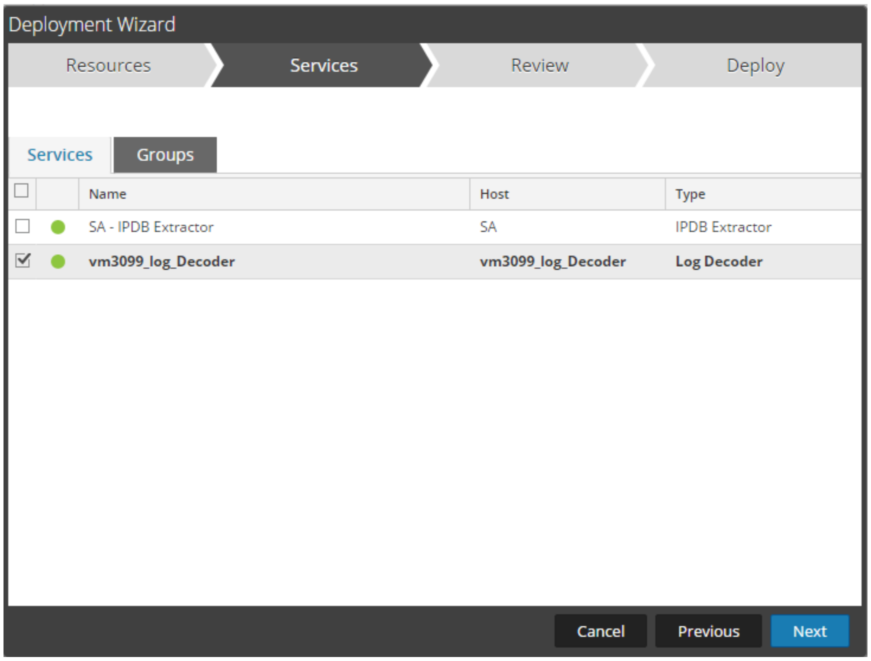
6. Select **Next**.



Total resources : 1

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

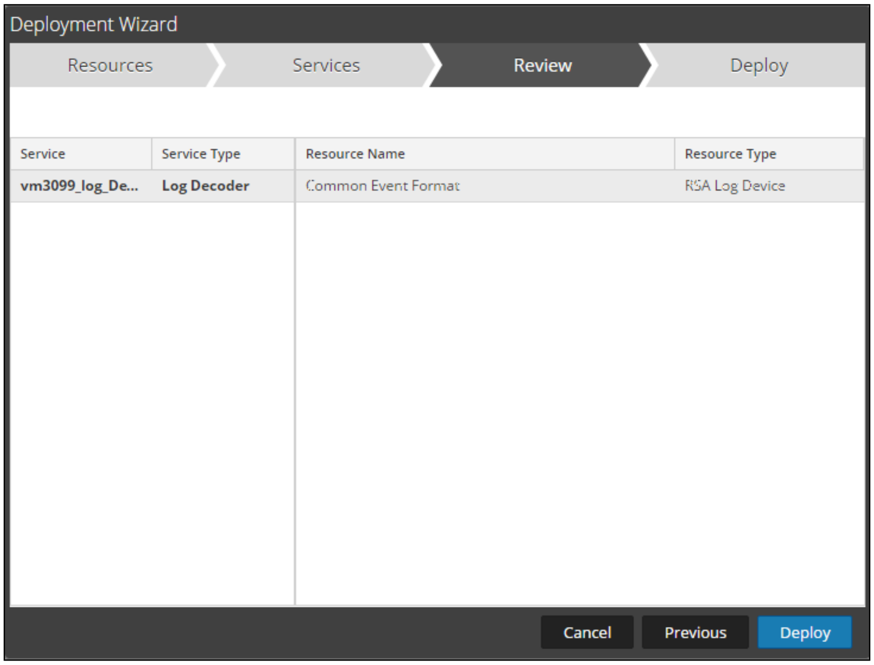
7. Select the **Log Decoder** and Select **Next**.



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

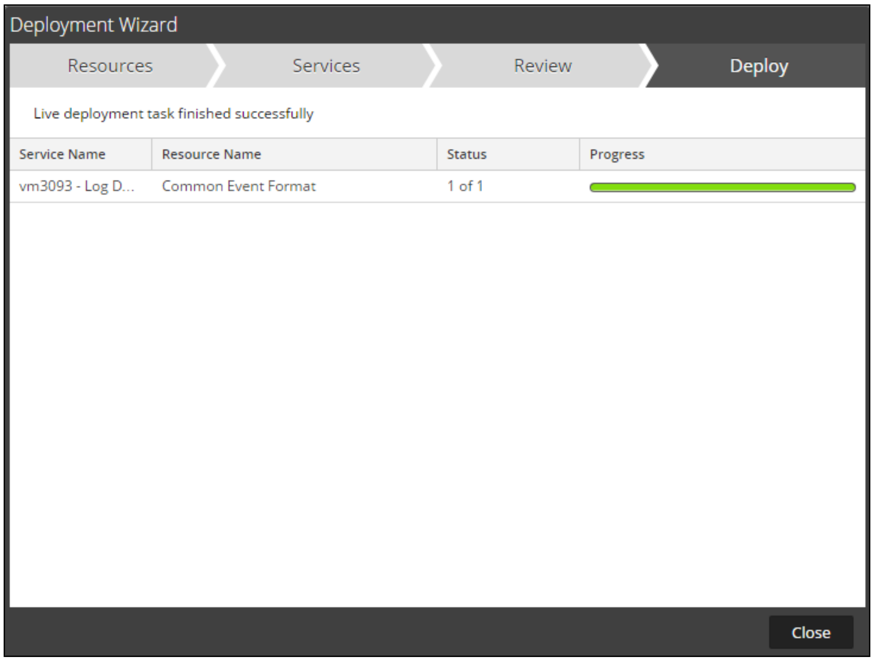
! > Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



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

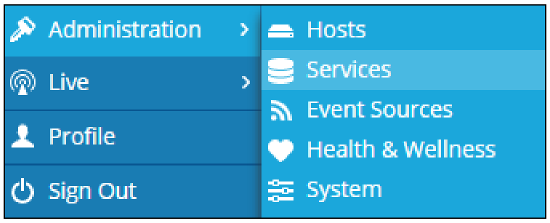
9. Select **Close**, to complete the deployment of the Common Event Format.



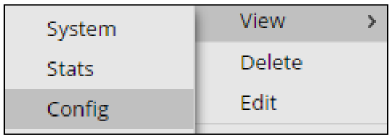
Live deployment task finished successfully

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

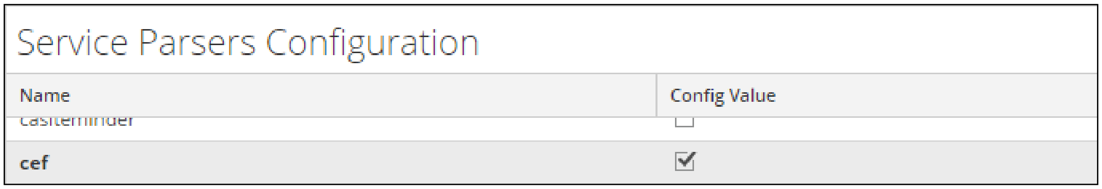
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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 collect Preempt 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;

Example.

```
<MESSAGE
                level="4"
                parse="1"
                parsedefvalue="1"
                tableid="74"
                id1="preemptsecurity_pbf"
                id2="preemptsecurity_pbf"
                eventcategory="1612000000"

        content="&lt;@event_name:*HDR(event_description)&gt;&lt;@msg:*PARMVAL($MS
G)&gt;&lt;@starttime:*EVNTTIME($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&g
t;" />
```

3. Locate the beginning of the <VendorProducts section and copy/paste the following line below into the file after before the </VendorProducts>;

Example.

```
<VendorProducts>
        <Vendor2Device vendor="Preempt" product="Preempt Security"
device="preemptsecurity_pbf" group="Analysis"/>
</VendorProducts>
```

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.

Example.

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

<MESSAGE
              level="4"
              parse="1"
              parsedefvalue="1"
              tableid="74"
              id1="preemptsecurity_pbf"
              id2="preemptsecurity_pbf"
              eventcategory="1612000000"

       content="&lt;@event_name:*HDR(event_description)&gt;&lt;@msg:*PARMVAL($MS
G)&gt;&lt;@starttime:*EVNTTIME($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&g
t;" />

<VendorProducts>
       <Vendor2Device vendor="Preempt" product="Preempt Security"
device="preemptsecurity_pbf" group="Analysis"/>
</VendorProducts>

-->

           <ExtensionKeys>
              <ExtensionKey cefName="externalID" metaName="hardware_id"/>

              <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="preemptsecurity_pbf"
metaName="incidentLink" label="incidentLink"/>
              </ExtensionKey>
              <ExtensionKey cefName="cs1Label" metaName="cs_fld" />

              <ExtensionKey cefName="cs2" metaName="cs_fld">
                     <device2meta device="bit9" metaName="v_instafname"
label="installerFilename"/>
```

```
                    <device2meta device="preemptsecurity_pbf" metaName="status"
label="status"/>
                    </ExtensionKey>
             <ExtensionKey cefName="cs2Label" metaName="cs_fld"/>

             <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="preemptsecurity_pbf"
metaName="numberOfAlerts" label="numberOfAlerts"/>
             </ExtensionKey>
             <ExtensionKey cefName="cn1Label" metaName="cs_fld"/>

             <ExtensionKey cefName="cn2" metaName="cn_fld">
                    <device2meta device="preemptsecurity_pbf"
metaName="numberOfCompromisedEntities" label="numberOfCompromisedEntities"/>
             </ExtensionKey>
             <ExtensionKey cefName="cn2Label" metaName="cs_fld"/>

             </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;

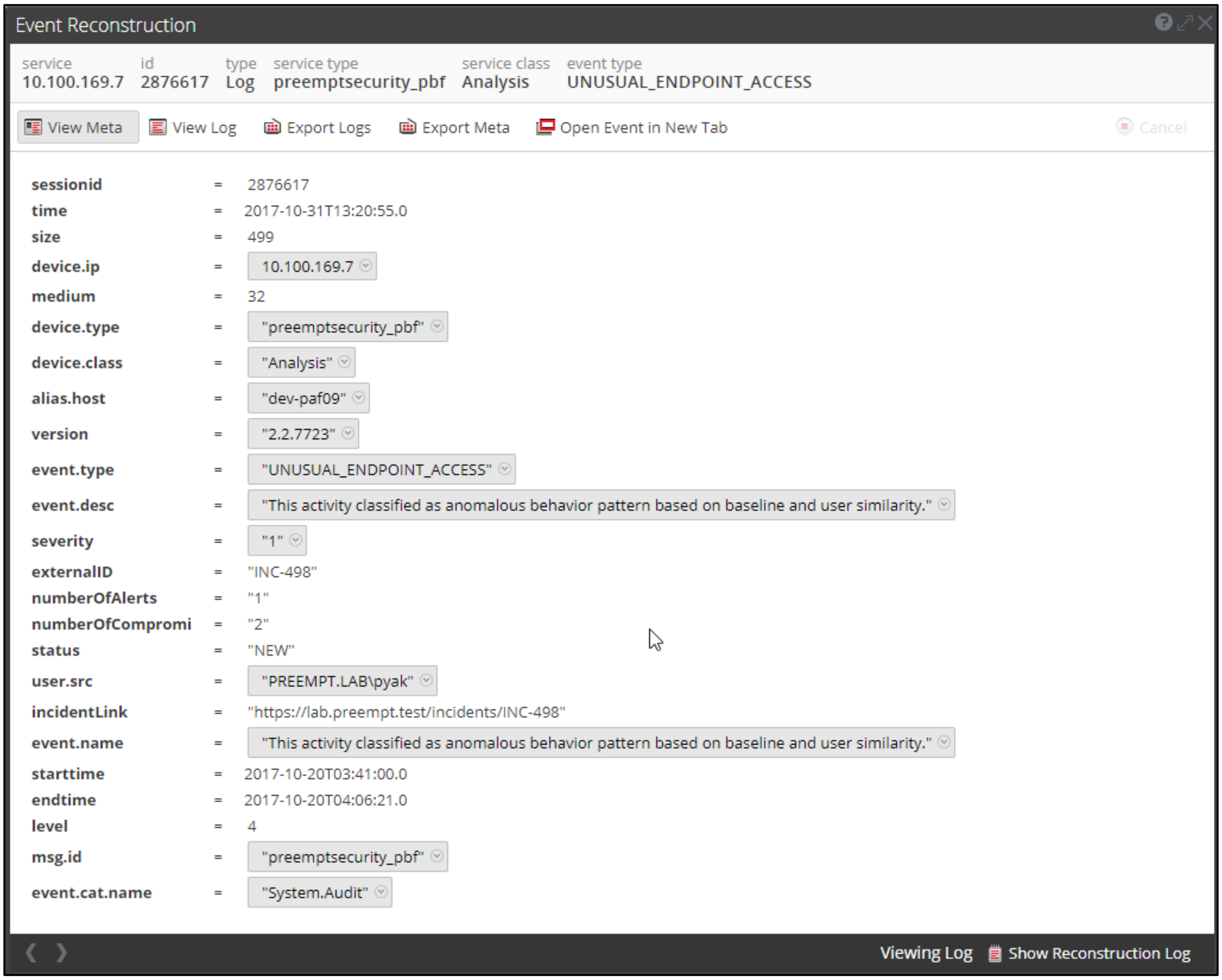
```
Example.
      <?xml version="1.0" encoding="utf-8"?>
      <!--
      # attributes:
      #      envisionName: The name of the column in the universal table
      #      nwName:                    The name of the NetWitness meta field
      #      format:                    Optional. The language 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.
      -->
      <mappings>

             <mapping envisionName="starttime" nwName="starttime" 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="hardware_id" nwName="externalID" flags="None"/>
             <mapping envisionName="incidentLink" nwName="incidentLink" flags="None"
      format="Text"/>
             <mapping envisionName="numberOfAlerts" nwName="numberOfAlerts"
      flags="None" format="Text"/>
             <mapping envisionName="numberOfCompromisedEntities"
      nwName="numberOfCompromisedEntities" flags="None" format="Text"/>
             <mapping envisionName="status" nwName="status" flags="None"/>

      </mappings>
```

NetWitness Collection Example:



service	id	type	service type	service class	event type
10.100.169.7	2876617	Log	preemptsecurity_pbf	Analysis	UNUSUAL_ENDPOINT_ACCESS

```
sessionid          =  2876617
time               =  2017-10-31T13:20:55.0
size               =  499
device.ip          =  10.100.169.7
medium             =  32
device.type        =  "preemptsecurity_pbf"
device.class       =  "Analysis"
alias.host         =  "dev-paf09"
version            =  "2.2.7723"
event.type         =  "UNUSUAL_ENDPOINT_ACCESS"
event.desc         =  "This activity classified as anomalous behavior pattern based on baseline and user similarity."
severity           =  "1"
externalID         =  "INC-498"
numberOfAlerts     =  "1"
numberOfCompromi   =  "2"
status             =  "NEW"
user.src           =  "PREEMPT.LAB\pyak"
incidentLink       =  "https://lab.preempt.test/incidents/INC-498"
event.name         =  "This activity classified as anomalous behavior pattern based on baseline and user similarity."
starttime          =  2017-10-20T03:41:00.0
endtime            =  2017-10-20T04:06:21.0
level              =  4
msg.id             =  "preemptsecurity_pbf"
event.cat.name     =  "System.Audit"
```

Certification Checklist for RSA NetWitness

Date Tested: October 31, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4	Virtual Appliance
Preempt Behavioral Firewall	2.2	Virtual Appliance

Security Analytics Test Case	Result
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

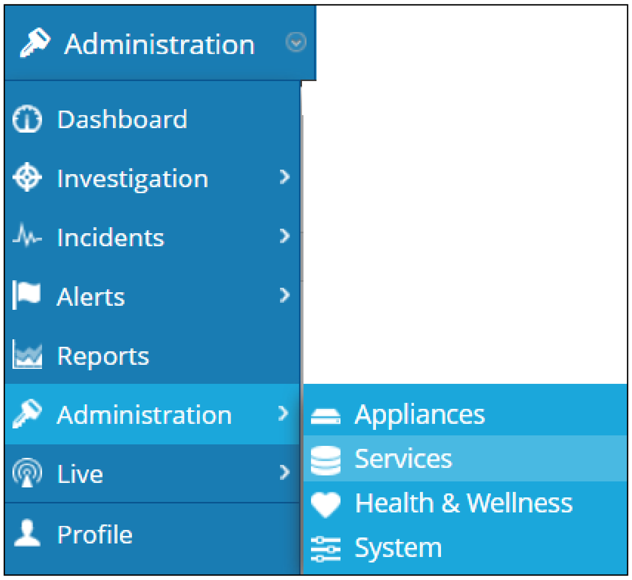
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

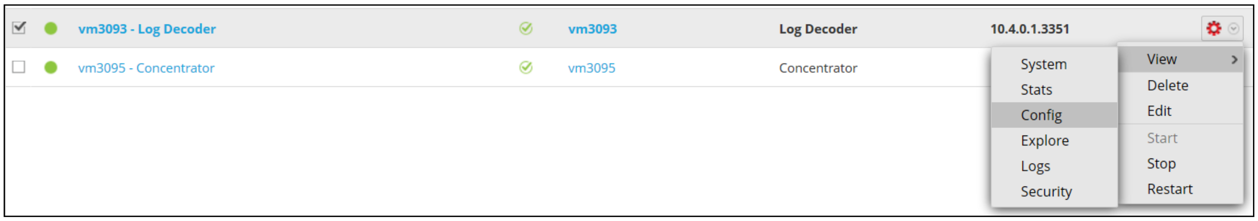
NetWitness Disable the Common Event Format Parser

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

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

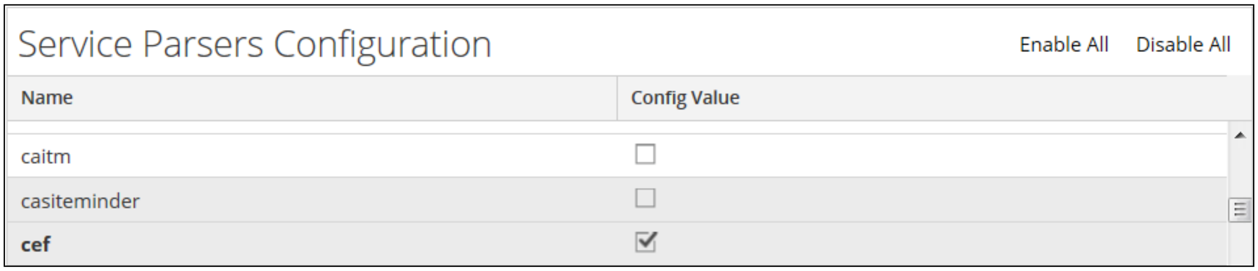


2. Select the Log Decoder, then select **View > Config.**



☑	●	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

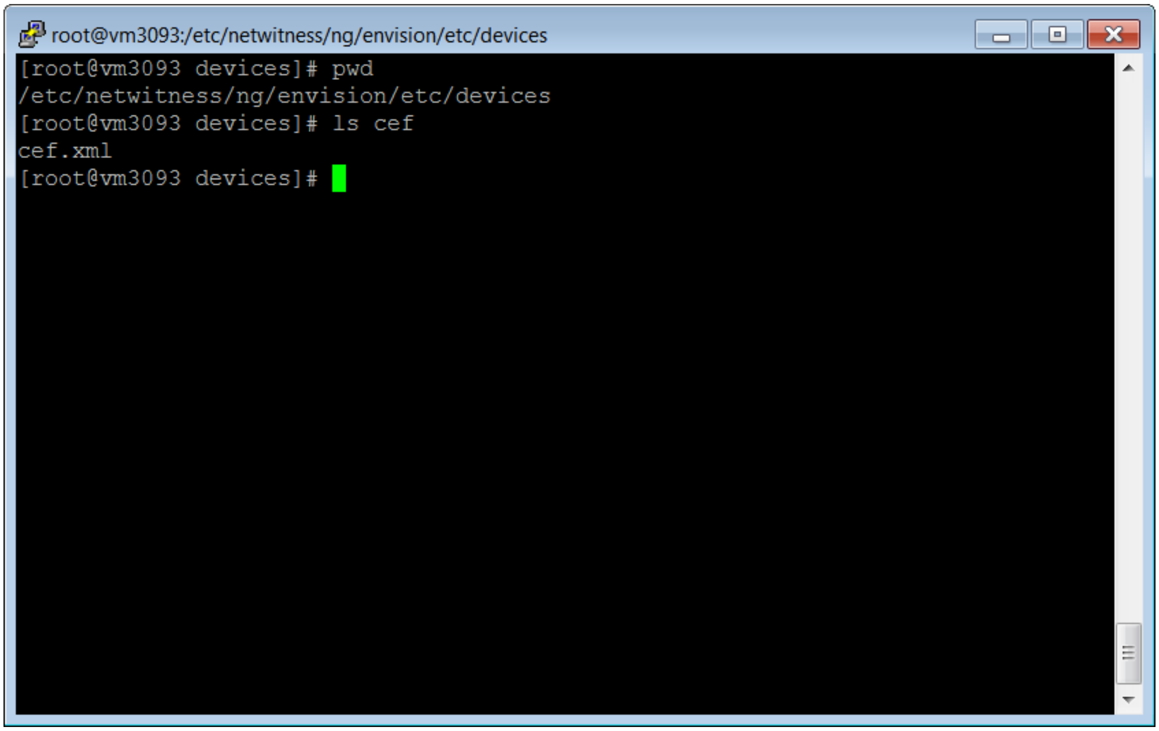
Name	Config Value
caitm	☐
casiteminder	☐
cef	☑

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

NetWitness Remove Device Parser

To remove the NetWitness 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.