NETWITNESS®

Logs
Implementation Guide

Imperva Counter Breach 11.5

Daniel Pintal, RSA Partner Engineering
Last Modified: December 2, 2016

RSA READY

Solution Summary

Imperva integrates with RSA Netwitness as a repository for CEF event logs.

RSA NetWitness Features	
Imperva Counter Breach 11.5	
Integration package name	Common Event Format
Device display name within Netwitness	imperva_inc._counterbreach
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
9/6/2016	Initial support for Imperva Counter Breach.

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.

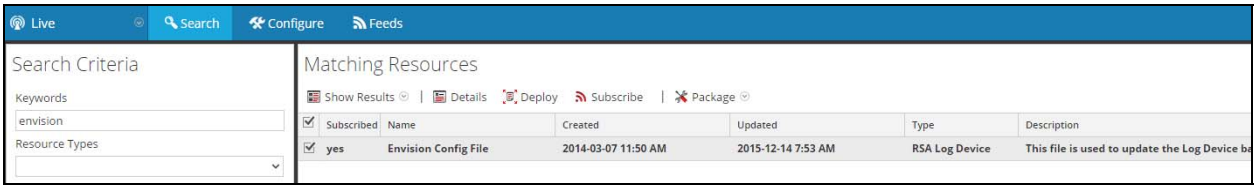
RSA NetWitness Configuration

Deploy the enVision Config File

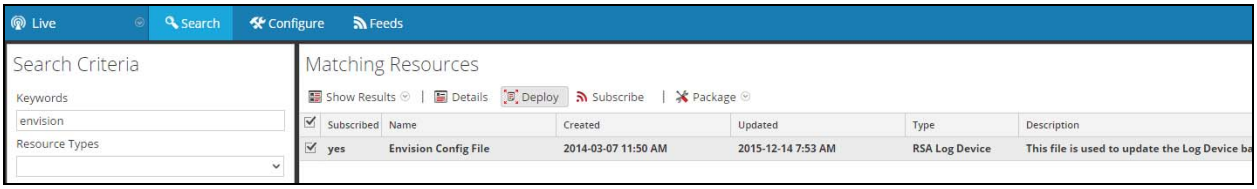
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

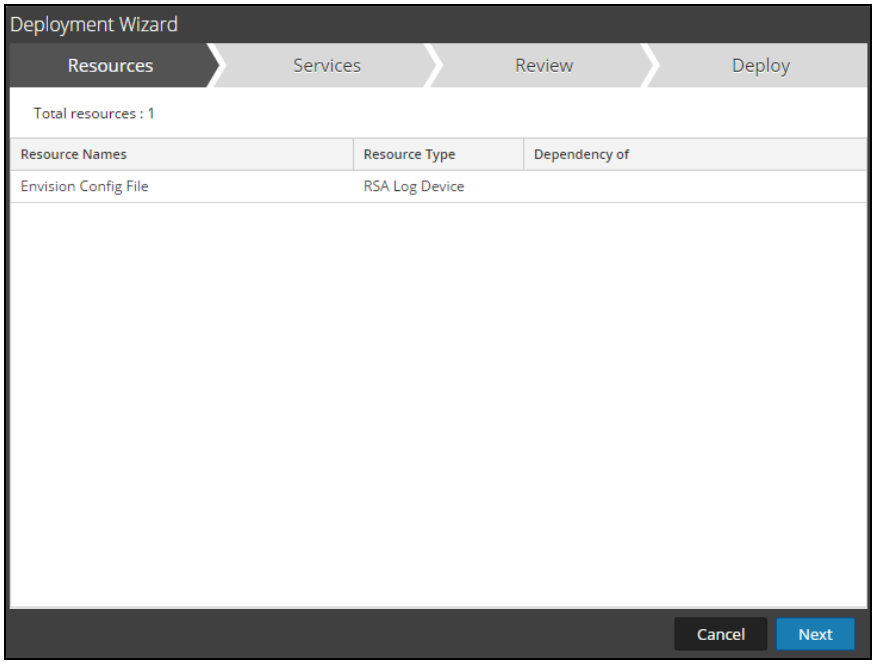
1. From the Netwitness menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Netwitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



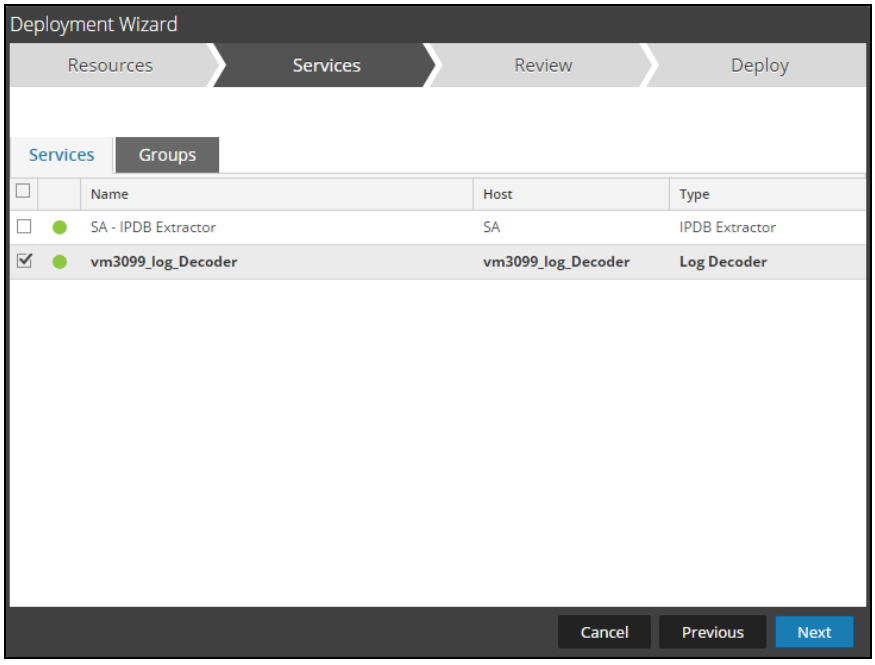
5. Click **Deploy** in the menu bar.



6. Select **Next**.

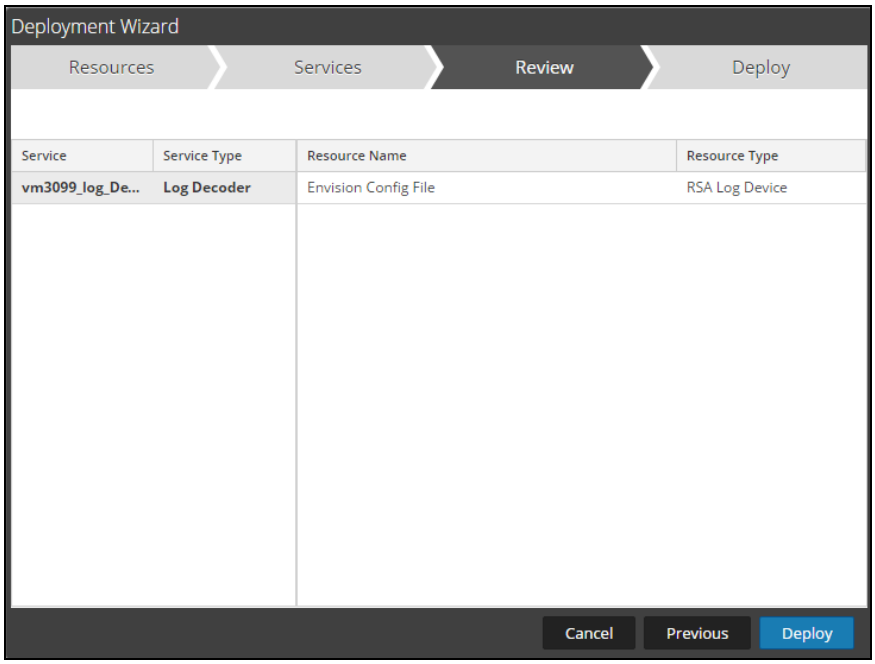


7. Select the **Log Decoder** and select **Next**.

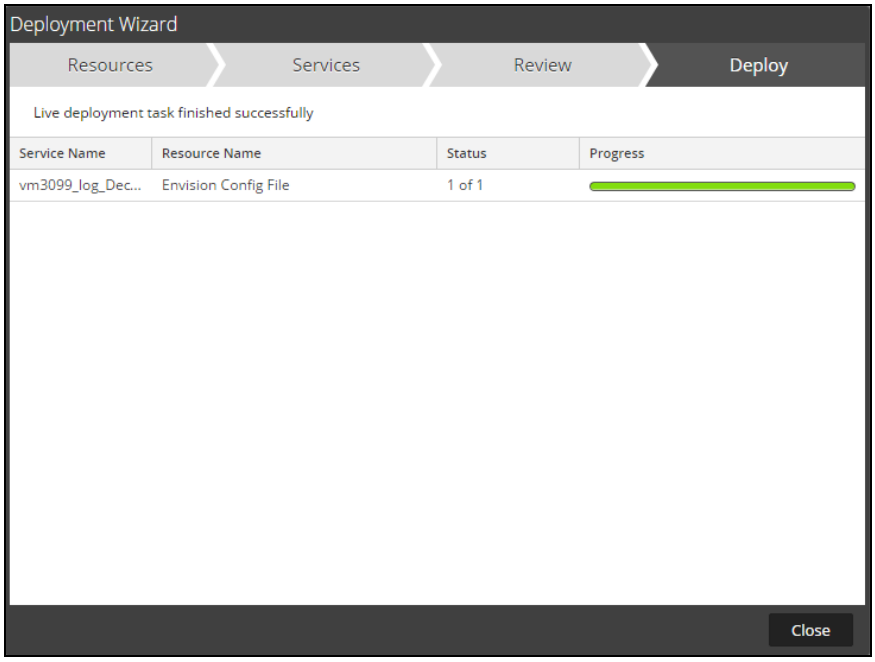


Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



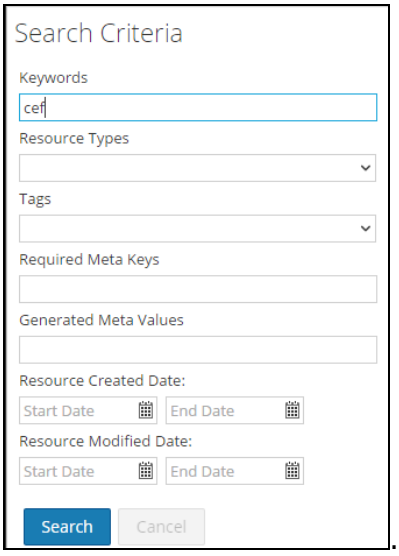
9. Select **Close**, to complete the deployment of the Envision Config file.



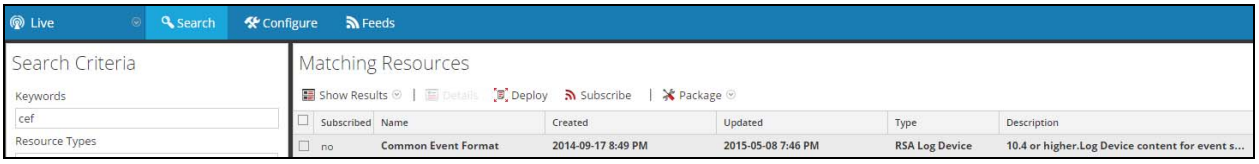
Deploy the Common Event Format

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

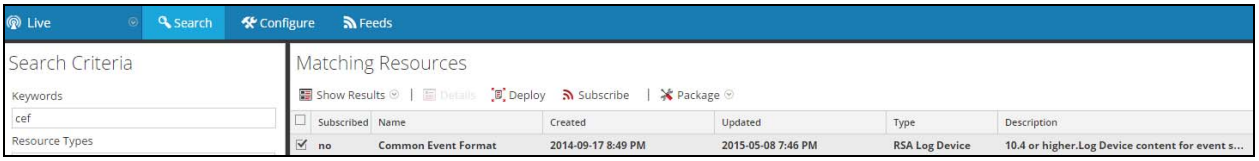
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **CEF**



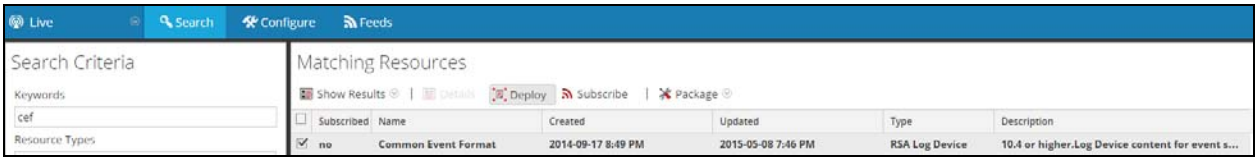
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



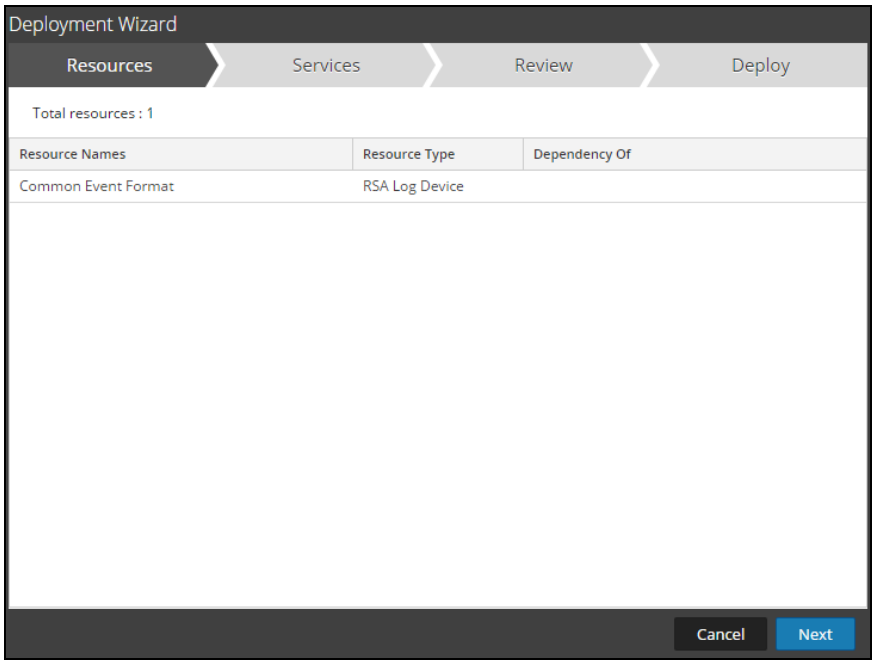
4. Select the checkbox next to **Common Event Format**.



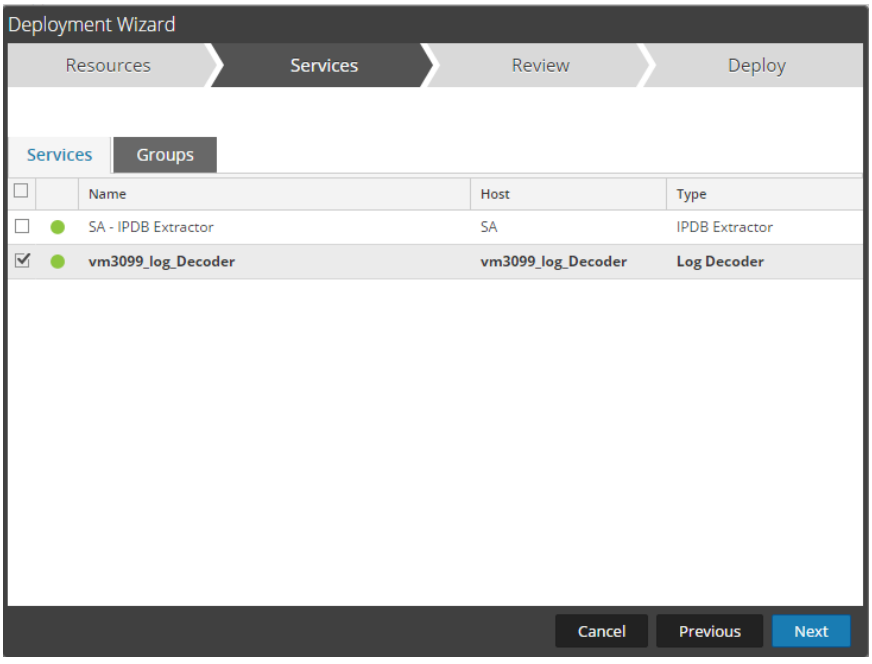
5. Click **Deploy** in the menu bar.



6. Select **Next**.

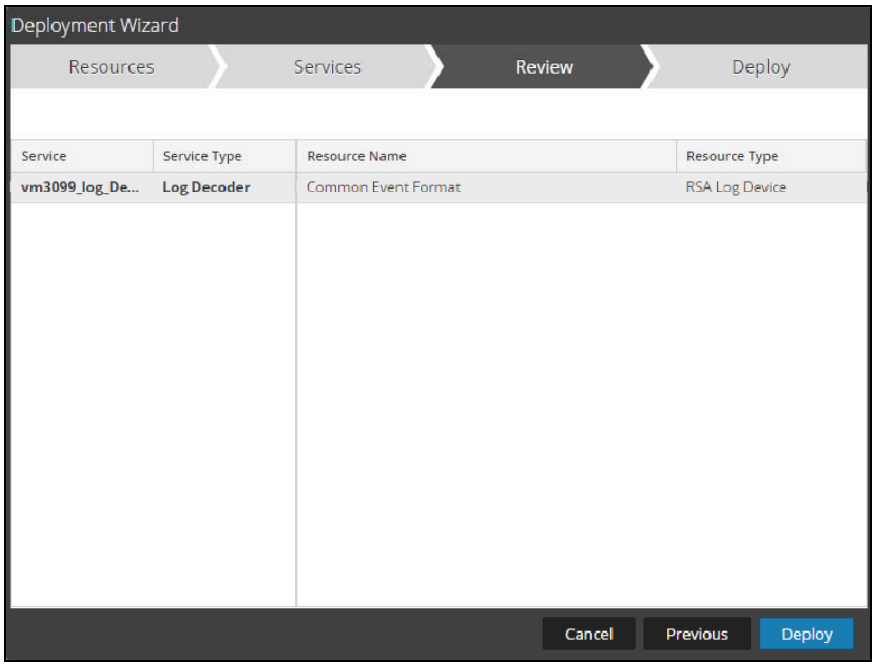


7. Select the **Log Decoder** and Select **Next**.

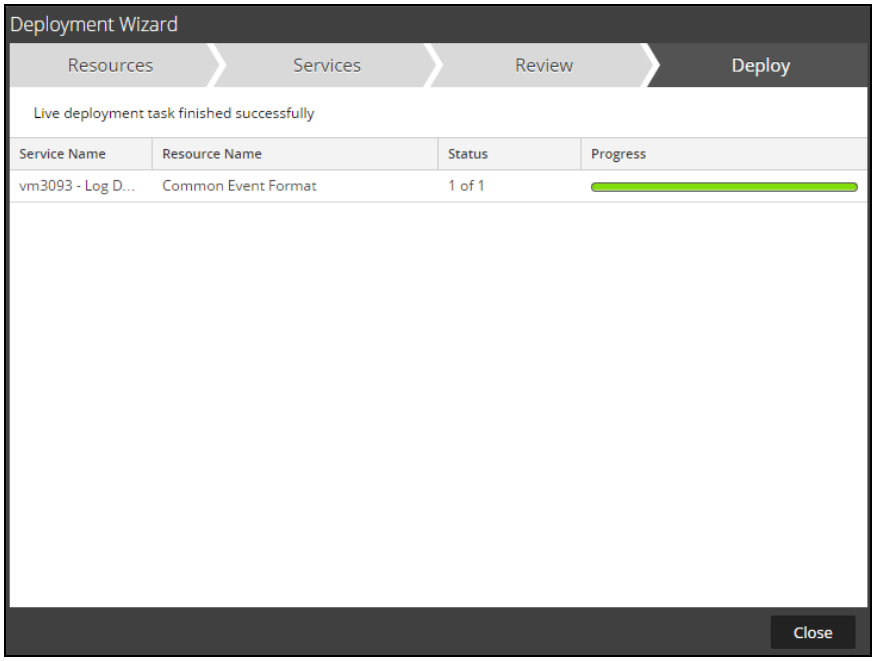


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

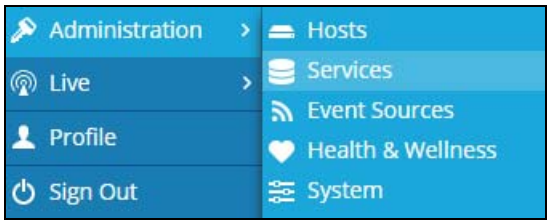
8. Select **Deploy**.



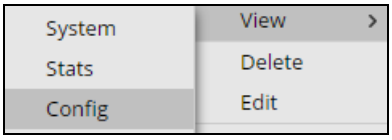
9. Select **Close**, to complete the deployment of the Common Event Format.



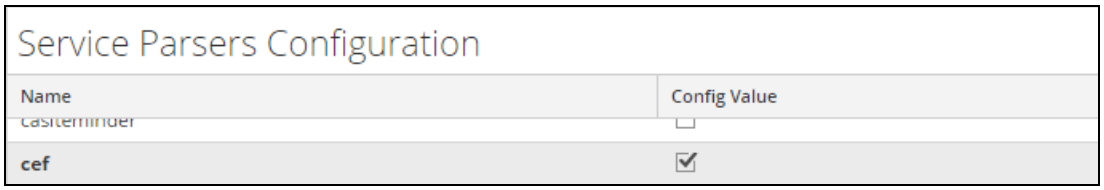
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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**.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Imperva Counter Breach 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 Imperva Counter Breach 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 Imperva Counter Breach is properly configured and secured before deploying to a production environment. For more information, please refer to the Imperva Counter Breach documentation or website.

RSA Netwitness Customization

After completing the previous section, *Deploy enVision Config File and Deploy Common Event Format*, you can now collect events from most sources supporting the Common Event Format (CEF).

To capture the Imperva Counter Breach custom messages not displayed by default in the RSA Netwitness, modification to the RSA Netwitness standard **CEF.xml** and **table-map-custom.xml** is required.

CEF.xml file Modifications

Important: Insure you have a good backup of both the CEF.xml and table-map-custom.xml files before starting.

Live updates to the RSA Netwitness servers may overwrite the CEF.xml parser if registered for updates.

Important: In an environment with multiple Log Decoders, modify the CEF File on each Log Decoder in your network.

Insure you have backed up the original CEF.xml to a safe location.

The CEF.xml file is updated when you perform a Live system update and if Live Subscription is enabled.

Prior to upgrading your Netwitness servers backup any files containing customizations to insure your work is preserved.

1. Modify the **CEF.xml** on the Log Decoder (CEF keys to modify are cs1, cs2, cs3, cs4, cs5, cs6). The **CEF.xml** file can be found in /etc/netwitness/ng/envision/etc/devices/cef/.
2. Add the entire portion of code below including the <MESSAGE…/>, place this entry below the last <MESSAGE…/> entry.

```
<MESSAGE
        level="4"
        parse="1"
        parsedefvalue="1"
        tableid="74"
        id1="imperva_inc._counterbreach"
        id2="imperva_inc._counterbreach"
        eventcategory="1303000000"
        content="&lt;@msg:*PARMVAL($MSG)&gt;@starttime:*EVNTTIME($MSG,'%W-%M-%D %H:%T:%S',param_starttime)&gt;&lt;param_starttime&gt;.&lt;fld5&gt; &lt;msghold&gt;" />
```

3. Modify the cef ExtensionKey cefName cs1, adding only the highlighted text below.

```
<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="imperva_inc._counterbreach" metaName="cs.linktoalert" label="LinkToAlert"/>
</ExtensionKey>
<ExtensionKey cefName="cs1Label" metaName="cs_fld" />
```

4. Modify the cef ExtnesionKey cefName cs2, adding only the highlighted text below.

```
<ExtensionKey cefName="cs2" metaName="cs_fld">
        <device2meta device="bit9" metaName="v_instafname" label="installerFilename"/>
        <device2meta device="imperva_inc._counterbreach" metaName="cs.account.dst" label="destinationAccount"/>
</ExtensionKey>
<ExtensionKey cefName="cs2Label" metaName="cs_fld"/>
```

5. Modify the cef ExtnesionKey cefName cs3, adding only the highlighted text below.

```
<ExtensionKey cefName="cs3" metaName="cs_fld">
        <device2meta device="websense" metaName="content_type" label="ContentType"/>
        <device2meta device="bit9" metaName="policyname"/>
        <device2meta device="imperva_inc._counterbreach" metaName="cs.dst" label="Destination"/>
</ExtensionKey>
<ExtensionKey cefName="cs3Label" metaName="cs_fld"/>
```

6. Modify the cef ExtnesionKey cefName cs4, adding only the highlighted text below.

```
<ExtensionKey cefName="cs4" metaName="cs_fld">
        <device2meta device="mcafeewg" metaName="info" label="URL Categories"/>
        <device2meta device="imperva_inc._counterbreach" metaName="cs.accessed.tables" label="AccessedTables"/>
</ExtensionKey>
<ExtensionKey cefName="cs4Label" metaName="cs_fld"/>
```

7. Modify the cef ExtnesionKey cefName cs5, adding only the highlighted text below.

```
<ExtensionKey cefName="cs5" metaName="cs_fld">
        <device2meta device="mcafeewg" metaName="policyname" label="Policy"/>
        <device2meta device="bit9" metaName="rulename" label="ruleName"/>
        <device2meta device="imperva_inc._counterbreach" metaName="cs.numofobjects" label="NumOfAccessedObjects"/>
</ExtensionKey>
<ExtensionKey cefName="cs5Label" metaName="cs_fld"/>
```

8. Modify the cef ExtnesionKey cefName cs6, adding only the highlighted text below.

```
<ExtensionKey cefName="cs6" metaName="cs_fld">
        <device2meta device="mcafeewg" metaName="risk" label="Reputation"/>
        <device2meta device="imperva_inc._counterbreach" metaName="cs.action" label="UserAction"/>
</ExtensionKey>
<ExtensionKey cefName="cs6Label" metaName="cs_fld"/>
```

Table-map-custom.xml file Modifications

Important: Insure you have a good backup of both the CEF.xml and table-map-custom.xml files before starting.

Live updates to the RSA Netwitness servers may overwrite the CEF.xml parser if registered for updates.

Important: In an environment with multiple Log Decoders, modify the CEF File on each Log Decoder in your network.

Insure you have backed up the original CEF.xml to a safe location.

The CEF.xml file is updated when you perform a Live system update and if Live Subscription is enabled.

Prior to upgrading your Netwitness servers backup any files containing customizations to insure your work is preserved.

Important: If the table-map-custom.xml does not exist, create one and set the file permissions appropriately.

If appending to an existing table-map-custom.xml file only add the individual <mapping envisionName=…> and do no repeat the <mappings> or </mappings> entries.

1. Modify the **table-map-custom.xml** on the Log Decoder.
2. If the table-map-custom file was previously created it can be found in /etc/netwitness/ng/envision/etc/ otherwise you will need to create the xml file using the following text.

```
<mappings>

        <mapping envisionName="cs.linktoalert" nwName="cs.linktoalert" flags="None" format="Text"/>
        <mapping envisionName="cs.account.dst" nwName="cs.account.dst" flags="None" format="Text"/>
        <mapping envisionName="cs.dst" nwName="cs.dst" flags="None" format="Text"/>
        <mapping envisionName="msg" nwName="msg" flags="None" format="Text" envisionDisplayName="Message"/>
        <mapping envisionName="cs.accessed.tables" nwName="cs.accessed.tables" flags="None" format="Text"/>
        <mapping envisionName="cs.numofobjects" nwName="cs.numofobjects" flags="None" format="Text"/>
        <mapping envisionName="cs.action" nwName="cs.action" flags="None" format="Text"/>

</mappings>
```

Imperva Counter Breach Configuration

Please review the Imperva Counter Breach documentation or contact Imperva customer service for instructions.

Certification Checklist for RSA NetWitness

Date Tested: December 2, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.1	Virtual Appliance
Imperva Counter Breach	11.5	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

The CEF parser within RSA Netwitness version 10.6 and 10.6.1 by default is configured to identify a MessageID within each event. If a MessageID is not found Netwitness does not display all meta collected from the source within Netwitness Investigator.

As a workaround to display all meta consumed from a CEF formatted log perform the following;

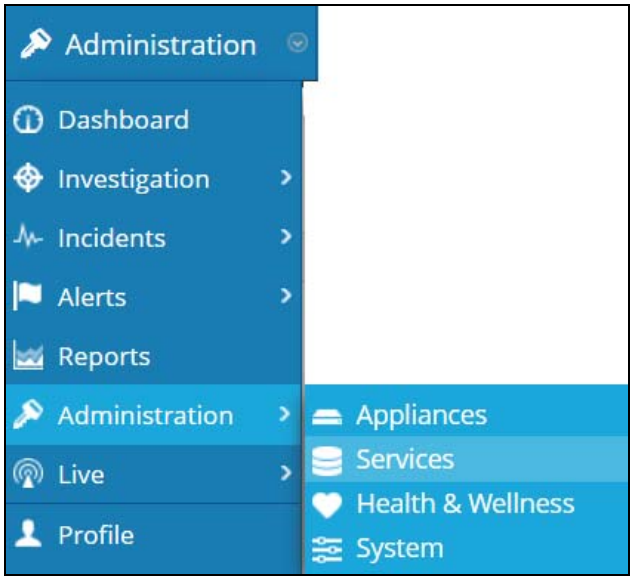
1. Select **Administration**> **Services**>.
2. Select **LogDecoder**> **View**> **Explore**> **decoder**> **parsers**> **config**> **token.device.types.**
3. Modify the **token.device.types** by changing the default setting of unknown and leaving the value blank.

Appendix

Netwitness Disable the Common Event Format Parser

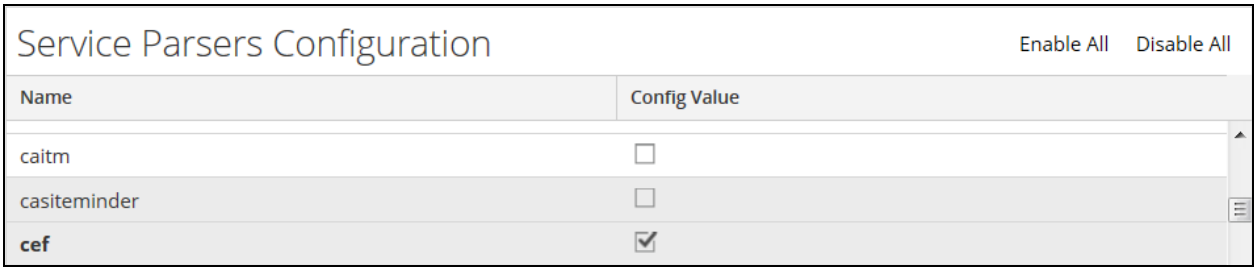
To disable the Netwitness Common Event Format Parser and not delete it perform the following:

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.

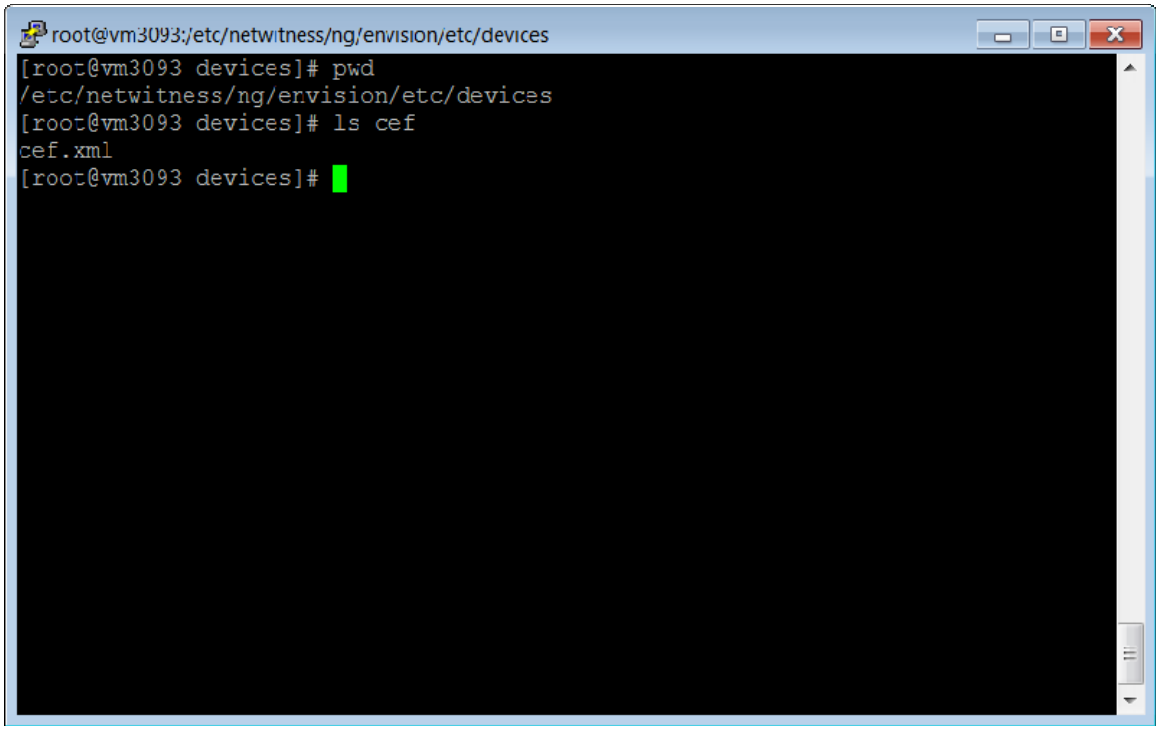


4. Click **Apply** to save settings.

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.



2. Search for and delete the CEF folder and its contents.