RSA® NETWITNESS®
Logs
Implementation Guide

Senrio Insight 1.0

Daniel R. Pintal, RSA Partner Engineering
Last Modified: January 10, 2018

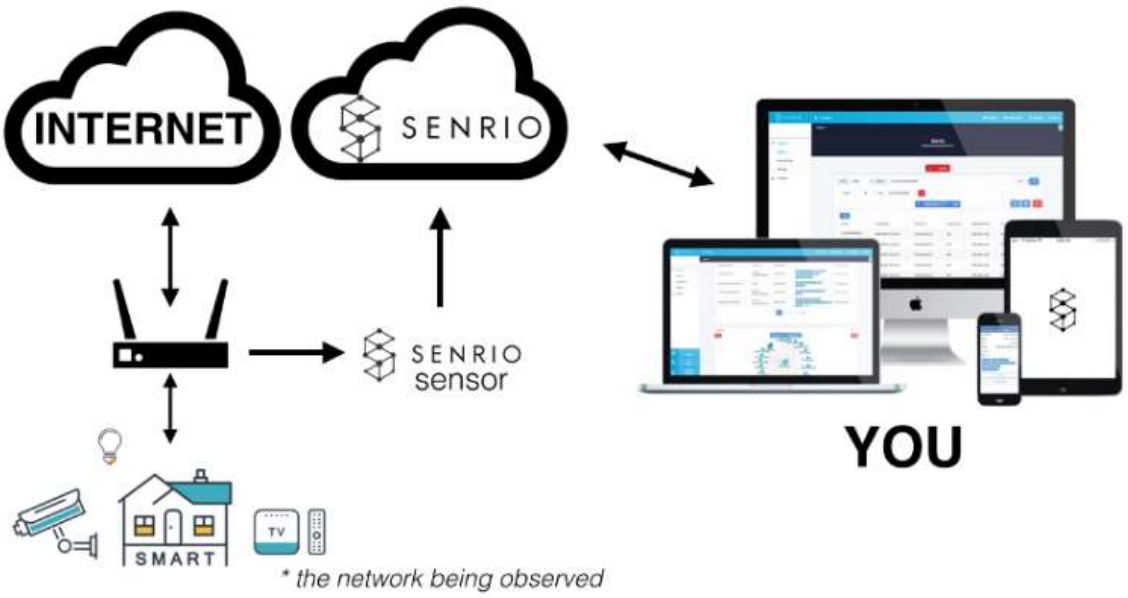
RSA READY

Solution Summary

Senrio Insight enumerates and categorizes devices on the network and provides context-rich analytics based on device-specific behavior and adaptive learning. All this is done passively and without deep-packet inspection, making Senrio incredibly scalable and easy to deploy in healthcare, industrial control, retail, and corporate environments alike.

The integration of Senrio Insight and RSA NetWitness provides Security Administrators with a single pane of glass to monitor network activity and respond quickly to anomalies in your network.

RSA NetWitness Features	
Senrio Insight 1.0	
Integration package name	Common Event Format
Device display name within Security Analytics	Senrio_Insight
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
1/10/2018	Initial support for Senrio Insight.

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

Prerequisites

Senrio Insight can be configured to forward events to NetWitness using the Senrio Insight event forwarder. This will run inside a Docker container and pull notifications from Senrio Insight and forward them on to NetWitness. The Senrio Insight event forwarder can be request from the Senrio Insight support team. It is distributed on an on-demand basis.

The installation and run script assumes a typical Unix type environment (Linux/Mac) with native Docker installed. Additionally the user most provide a valid set of authentication certs for the Senrio API. A user can re-use certs generated for them by the Senrio team or they can request specific certs be generated for this specific use case.

In order to leverage the certificates with the forwarder service, a script must be run to remove the password protections from the certificates. This can be accomplished with the following commands:

```
openssl pkcs12 -in USER_CERT.p12 -nokeys -out certificate.pem
openssl pkcs12 -in USER_CERT.p12 -nocerts -out privkey.pem
```

Where USER_CERT.p12 is the certificate provided by the Senrio team. The output from these commands are required in further configuration steps.

The system running the Senrio Insight forwarder needs to have access to the NetWitness event log decoder, which may require editing firewall rules to ensure it has access.

Senrio Insight Configuration

1. Once you've acquired the Senrio Insight forwarder packet, create a new directory where the package will be run:

```
mkdir senrio_forwarder
cd senrio_forwarder
```

2. Create a directory for the certificates and place them in the directory.

```
mkdir certs
cp ~/SOME_DIR/certificate.pem certs/certificate.pm
cp ~/SOME_DIR/privkey.pem certs/privkey.pem
```

3. Place the **senrio_forwarder.sh** script in the directory.

```
cp ~/SOME_DIR/senrio_forwarder.sh .
chmod +x ./senrio_forwarder.sh
```

4. Edit the **senrio_forwarder.sh** script and set the following configuration variables:

   - **SYSLOG_SERVER** - Set this to the IP address of the NetWitness event log decoder
   - **SYSLOG_PORT** - Set this to the port of the NetWitness event log decoder. The default value is likely sufficient.
   - **PRIVATE_KEY_FILE** - This should be the name for the private key generated in previous steps. In our example we are using the name privkey.pem.
   - **PUBLIC_CERT_FILE** - This should be the name for the certifcate generated in the previous steps. In our example we are using the name certificate.pem.
   - **API_URL** - This should point to the API URL for your specific instance.

5. Execute the script.

```
./senrio_forwarder
```

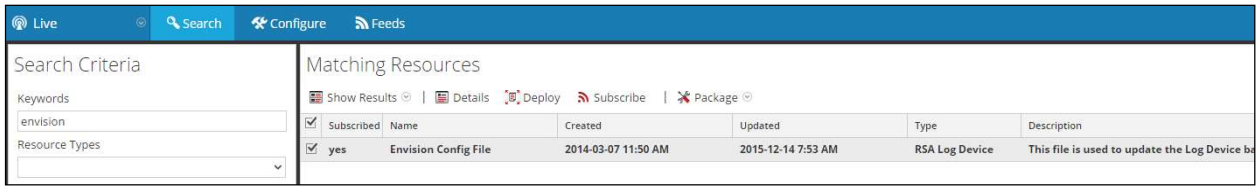
RSA NetWitness Configuration

Deploy the enVision Config File

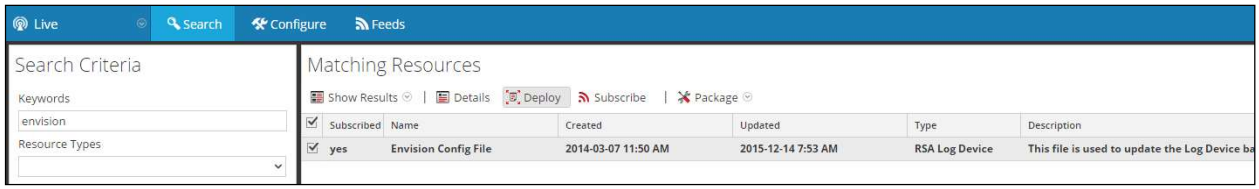
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

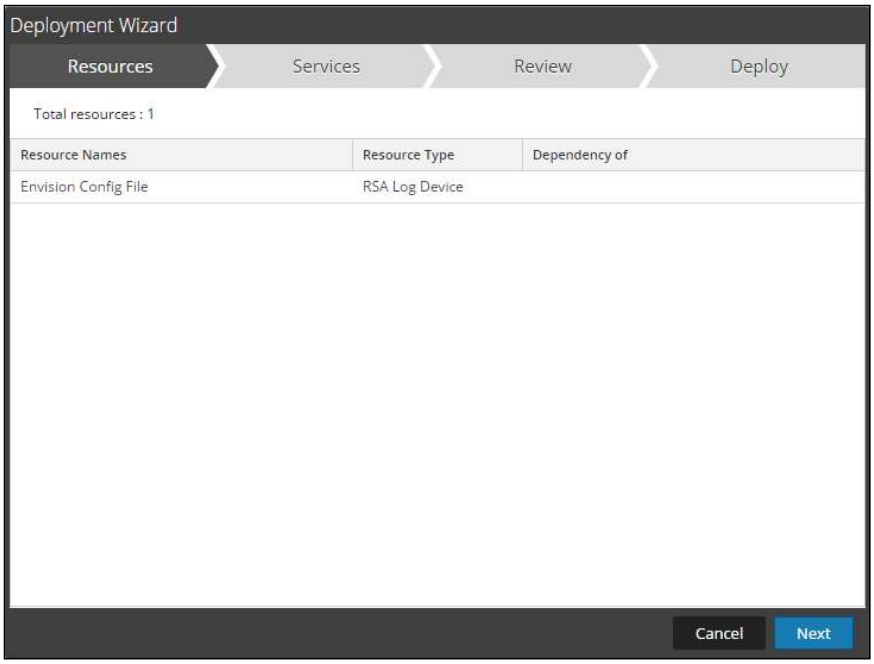
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



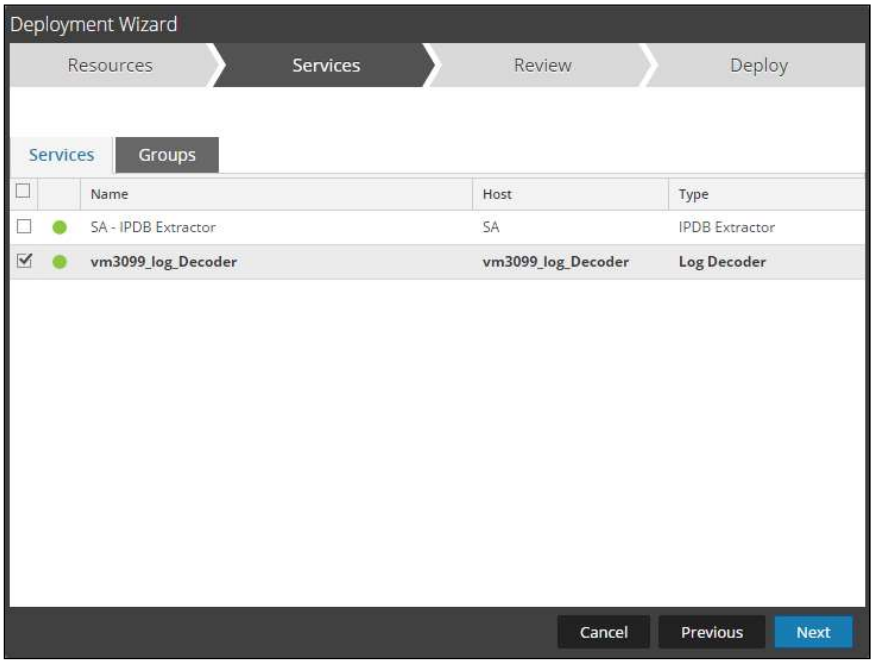
5. Click **Deploy** in the menu bar.



6. Select **Next**.

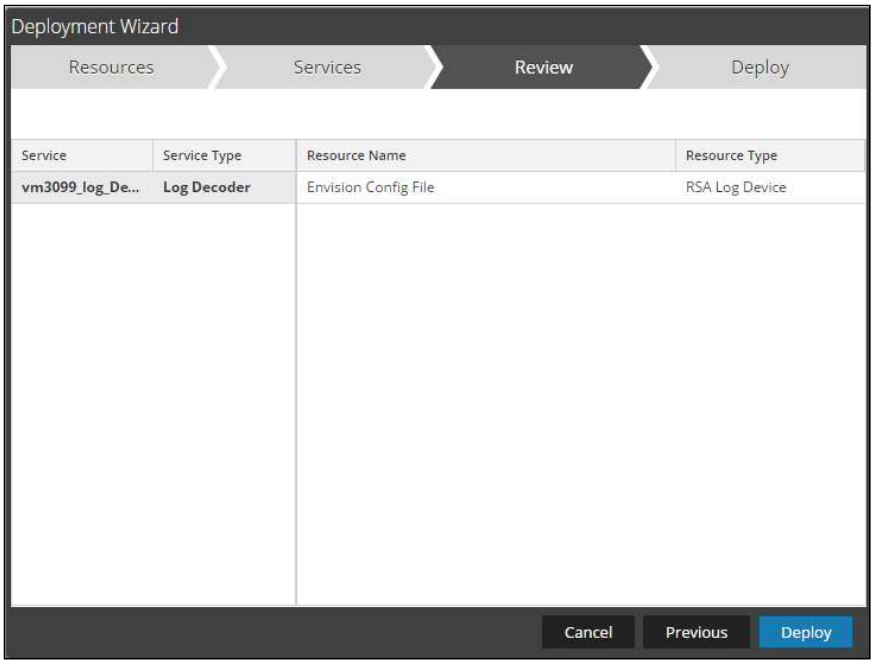


7. Select the **Log Decoder** and select **Next**.

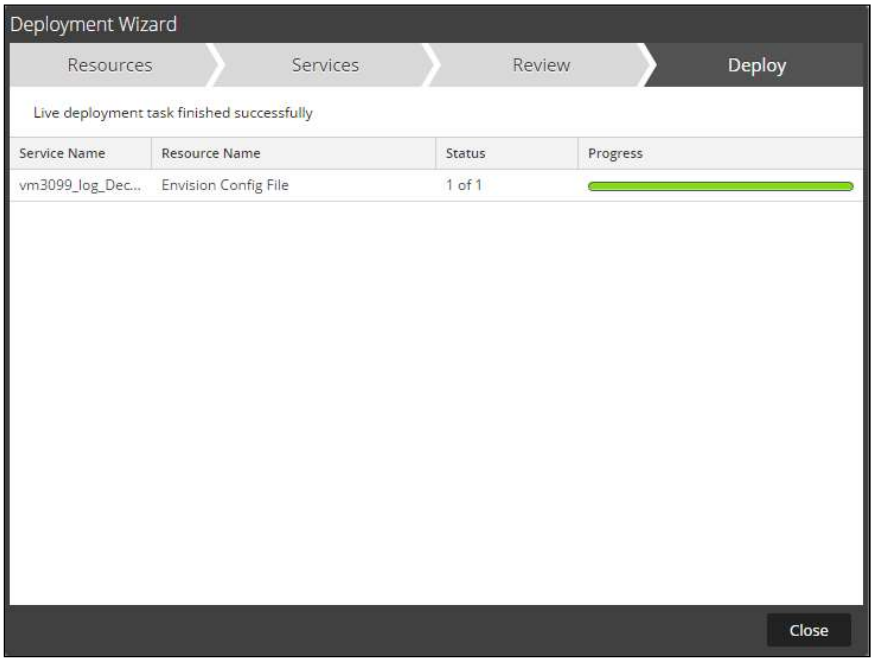


! > Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



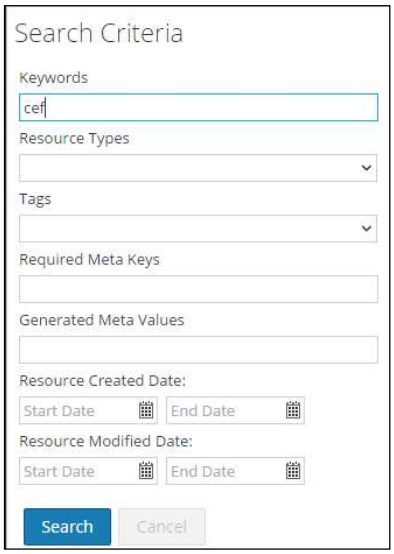
9. Select **Close**, to complete the deployment of the Envision Config file.



Deploy the Common Event Format

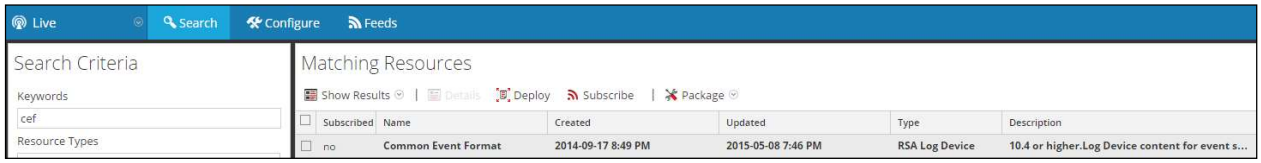
Next, you will need to deploy the *Common Event Format file* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

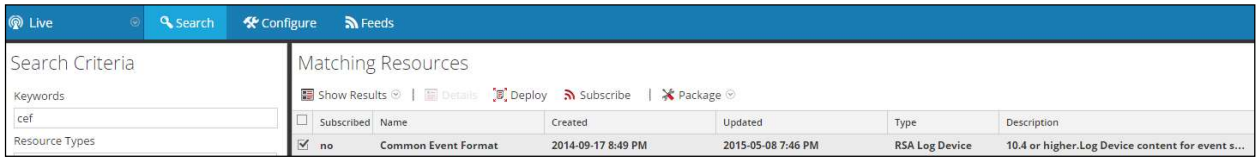


.

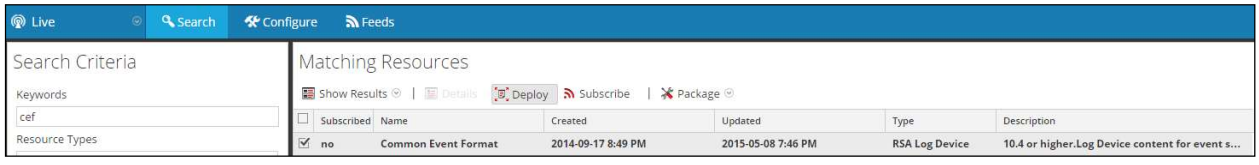
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



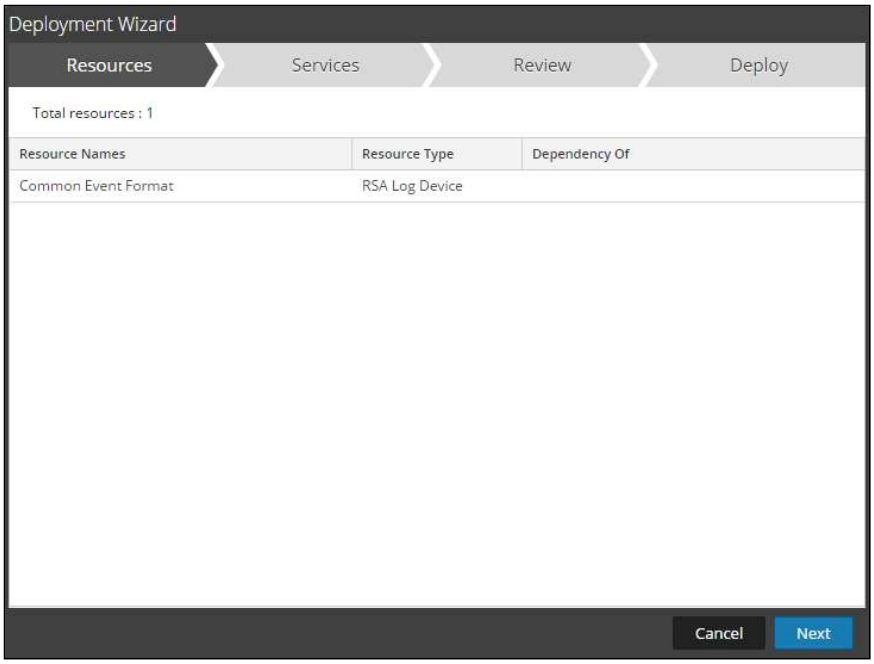
4. Select the checkbox next to **Common Event Format**.



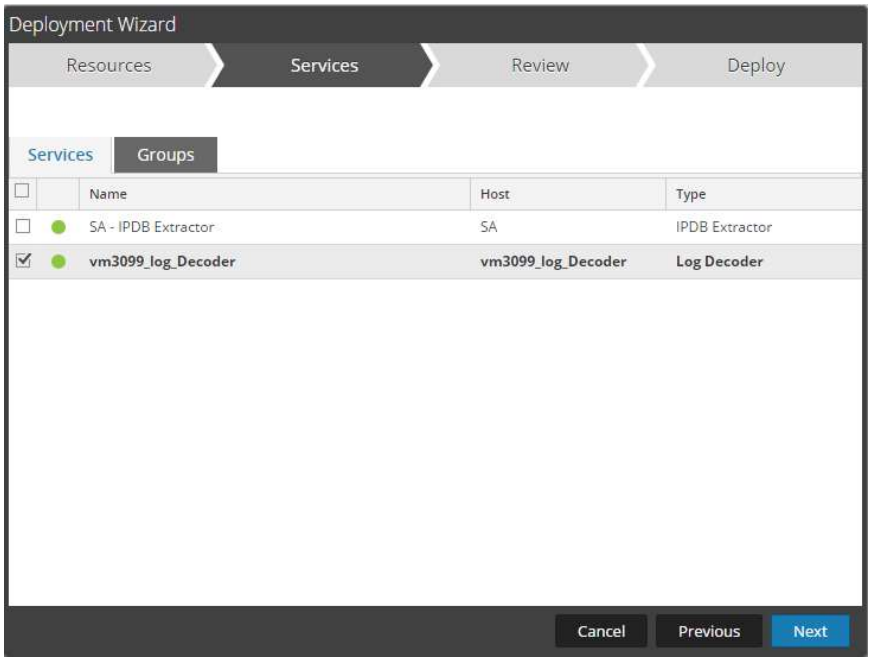
5. Click **Deploy** in the menu bar.



6. Select **Next**.

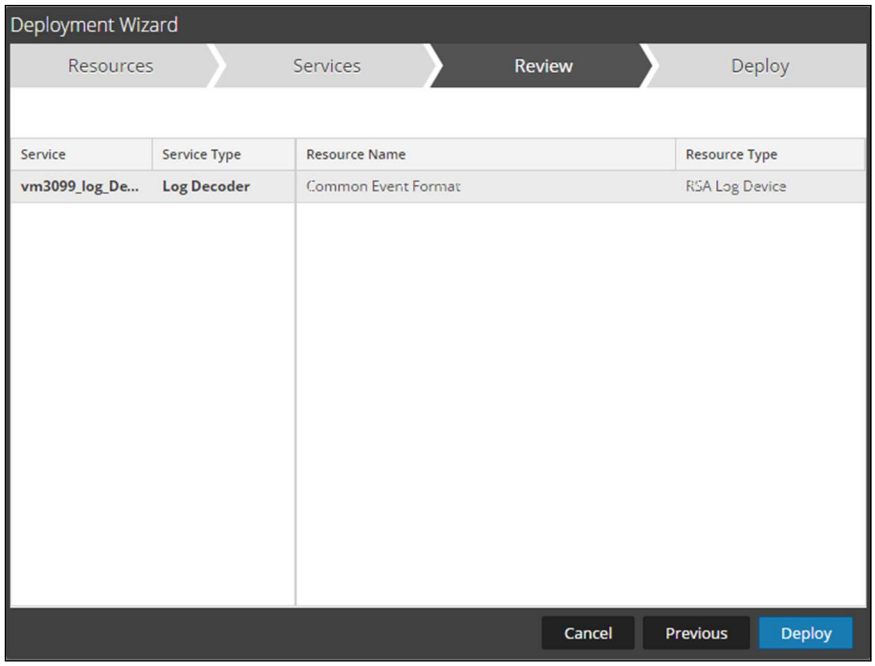


7. Select the **Log Decoder** and Select **Next**.

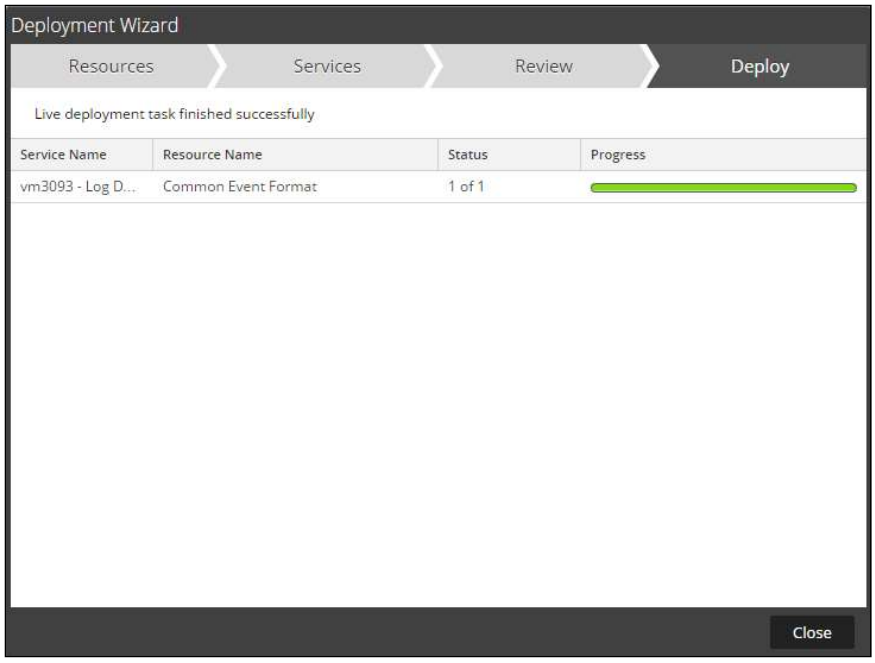


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

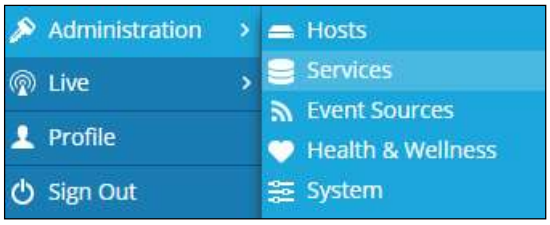
8. Select **Deploy**.



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**.

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;

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

        content="&lt;@event_name:*HDR(event_description)&gt;&lt;@msg:*PARMVAL($MS
G)&gt;&lt;@starttime:*EVNTTIME($MSG,'%X',param_event_time)&gt;&lt;param_event_t
ime&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.

   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
#
-->

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

        content="&lt;@event_name:*HDR(event_description)&gt;&lt;@msg:*PARMVAL($MS
G)&gt;&lt;@starttime:*EVNTTIME($MSG,'%X',param_event_time)&gt;&lt;param_event_t
ime&gt;&lt;msghold&gt;" />

<VendorProducts>
        <Vendor2Device vendor="Senrio" product="Senrio Insight"
device="Senrio_Insight" group="Analysis"/>
</VendorProducts>

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

                <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="Senrio_Insight" metaName="message"/>
                </ExtensionKey>
                <ExtensionKey cefName="cs1Label" metaName="cs_fld" />

                </ExtensionKeys>

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

```
                </ExtensionKey>
                <ExtensionKey cefName="cs2Label" metaName="cs_fld"/>

                <ExtensionKey cefName="start" metaName="param_starttime"/>
                <ExtensionKey cefName="end" metaName="param_endtime"/>
                <ExtensionKey cefName="rt" metaName="param_event_time"/>

</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.

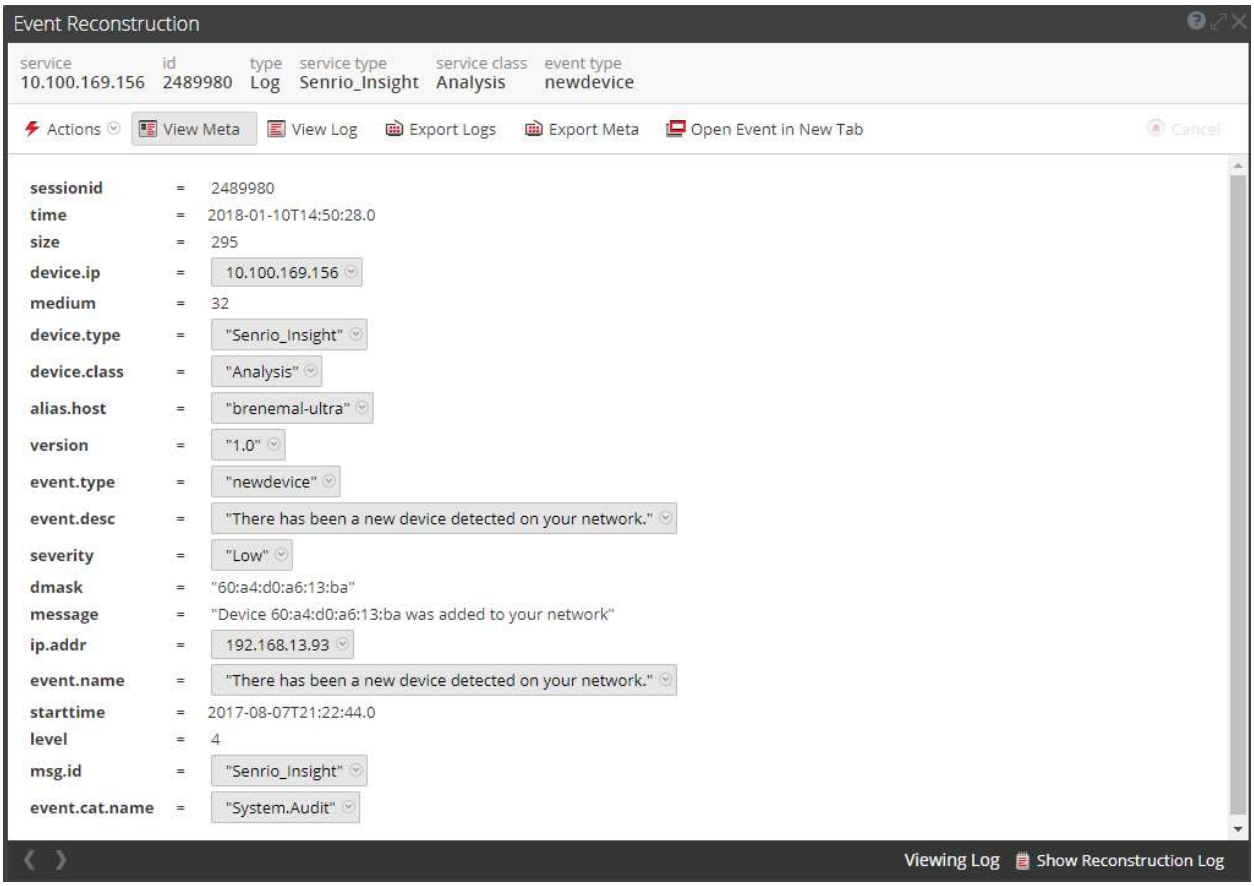
1. Using WinSCP or other application to access the RSA NetWitness Log Decoder open a connection and locate the **/etc/netwitness/ng/envision/etc/** folder.
2. If one exists, backup the **table-map-custom.xml** and then edit the existing **table-map-custom.xml** file.
3. Copy and paste the entire section 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="hardware_id" nwName="hardware.id" flags="None"/>
              <mapping envisionName="tags" nwName="tags" flags="None"/>
              <mapping envisionName="dmask" nwName="dmask" flags="None"/>
              <mapping envisionName="message" nwName="message" flags="None"/>
              <mapping envisionName="version" nwName="version" flags="None"/>
              <mapping envisionName="severity" nwName="severity" flags="None"
       envisionDisplayName="Severity|SeverityLevel"/>
              <mapping envisionName="starttime" nwName="starttime" flags="None"
       format="TimeT" envisionDisplayName="StartTime"/>
              <mapping envisionName="param_starttime" nwName="param_starttime"
       flags="None"/>
              <mapping envisionName="param_event_time" nwName="endtime" flags="None"/>

       </mappings>
```

NetWitness Collection Example:



Certification Checklist for RSA NetWitness

Date Tested: January 10, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4	Virtual Appliance
Senrio Insight	1.0	Cloud

Security Analytics 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	✓

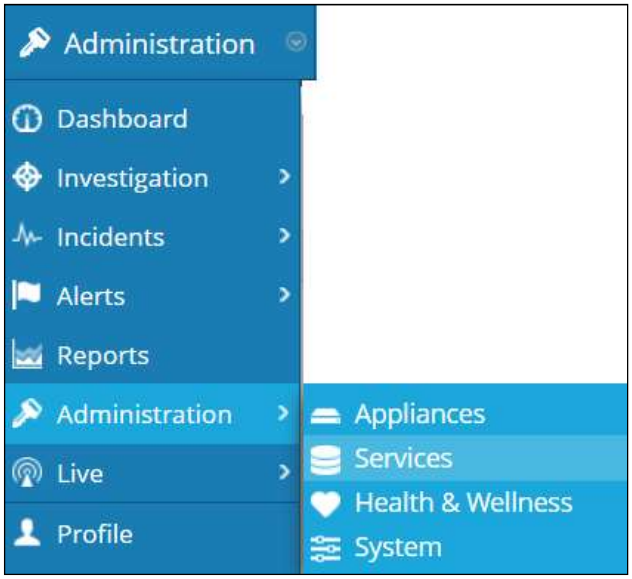
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Security Analytics Disable the Common Event Format Parser

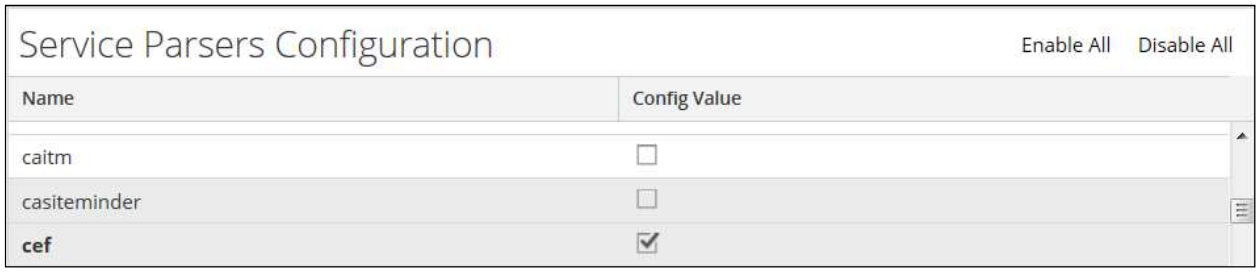
To disable the Security Analytics Common Event Format Parser and not delete it perform the following:

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



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

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

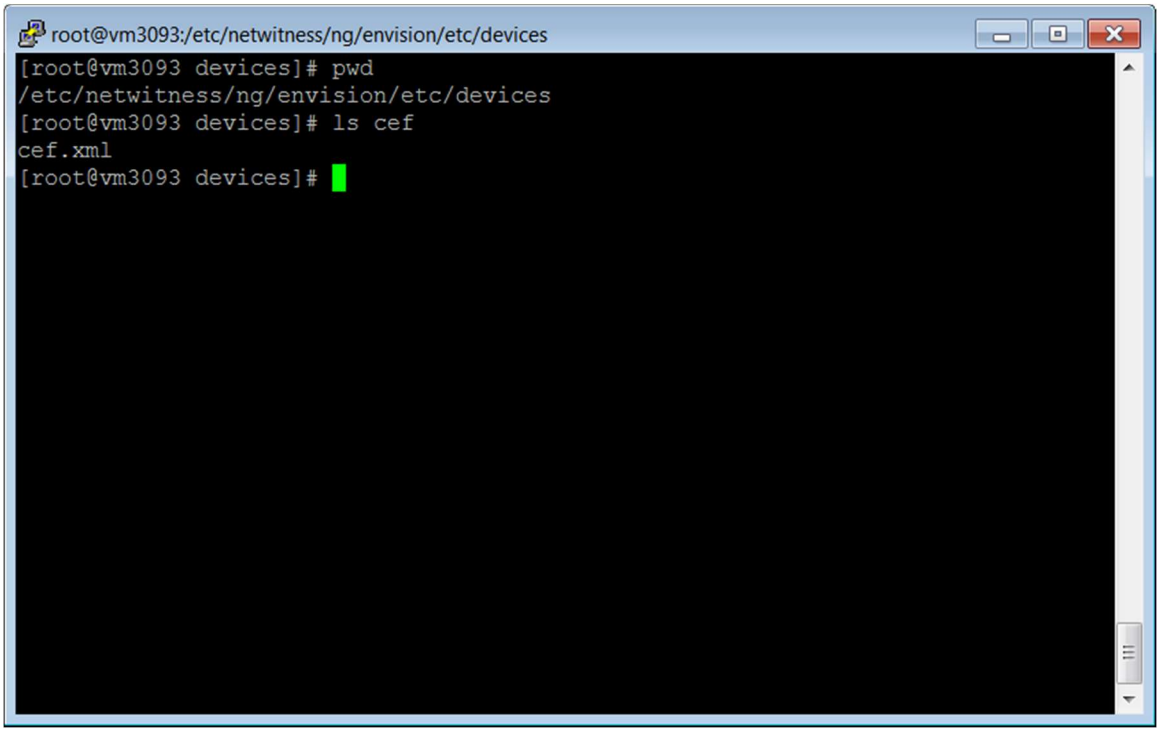


4. Click **Apply** to save settings.

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.



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