RSA® NETWITNESS®
Logs
Implementation Guide

Radiflow iSID – Industrial IDS

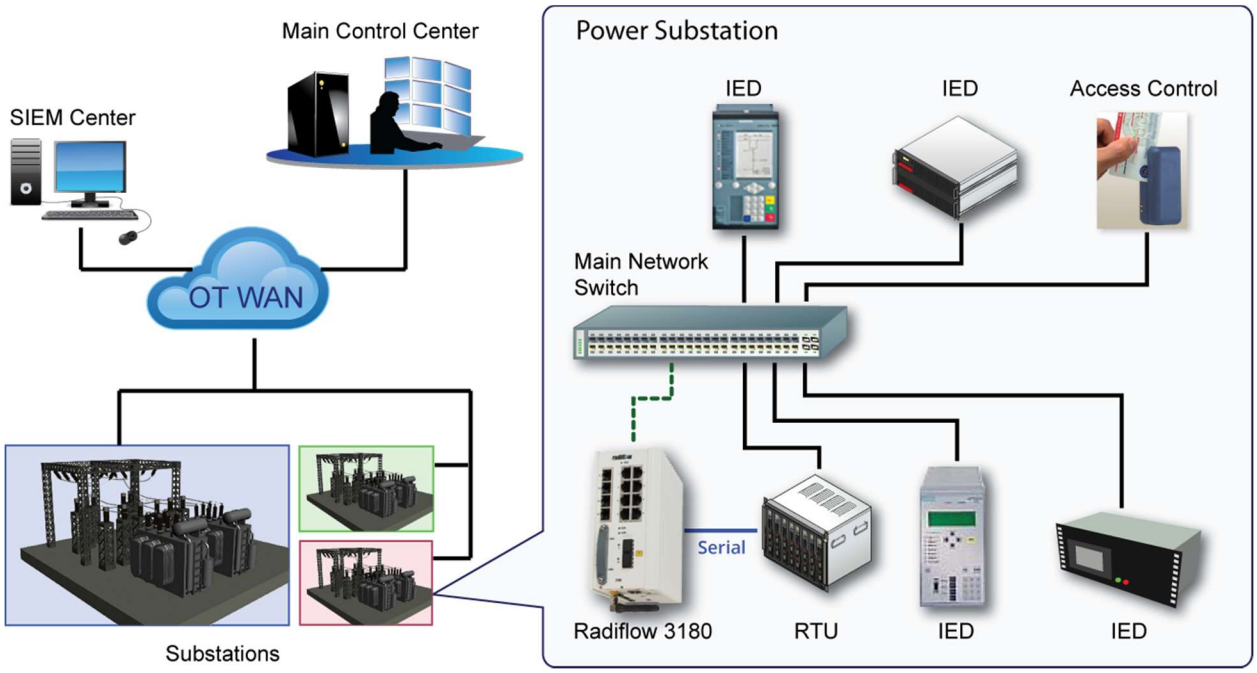
Daniel R. Pintal, RSA Partner Engineering
Last Modified: December 13, 2017

RSA READY

Solution Summary

Radiflow iDS Intrusion Detection System for SCADA networks integrates with RSA NetWitness to provide a single pane of glass for all events within your Network. The integration provides security administrators with a deep view into the security of your network landscape.

RSA NetWitness Features	
Radiflow_iSID	
Integration package name	Common Event Format
Device display name within Security Analytics	radiflow_isid
Event source class	SCADA
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
12/6/2017	Initial support for Radiflow iSID.

! > 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 Radiflow iSID 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.

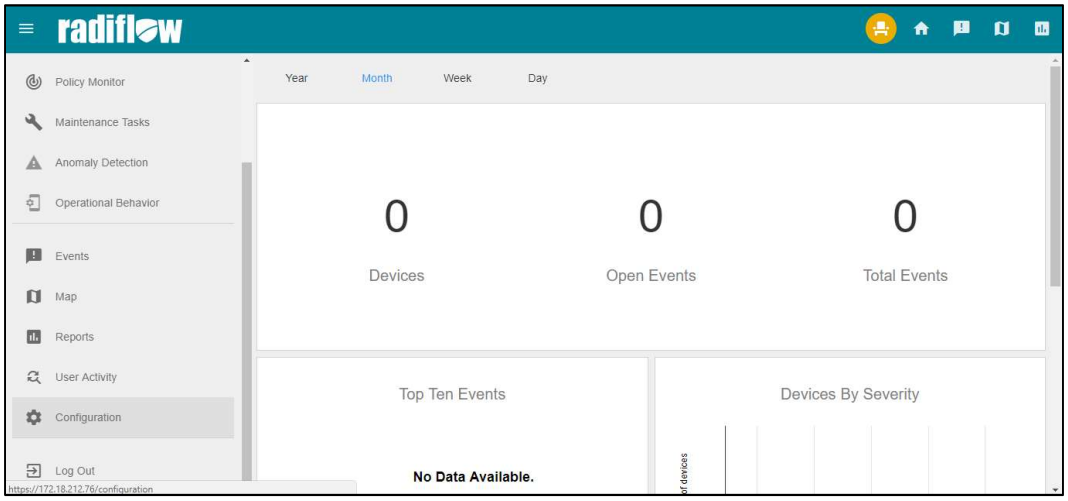
All Radiflow iSID components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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

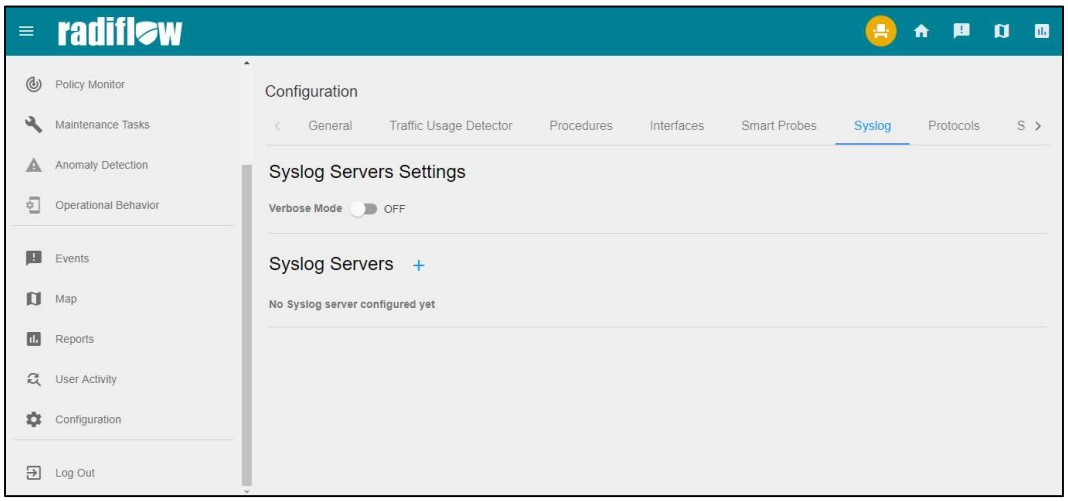
Radiflow iSID Configuration

1. Connect to iSID Web UI at: **https://<iSID_IP_Address>.**
2. Enter the user name and password at the entrance screen [Default: usr: radiflow / password: Secured1492].

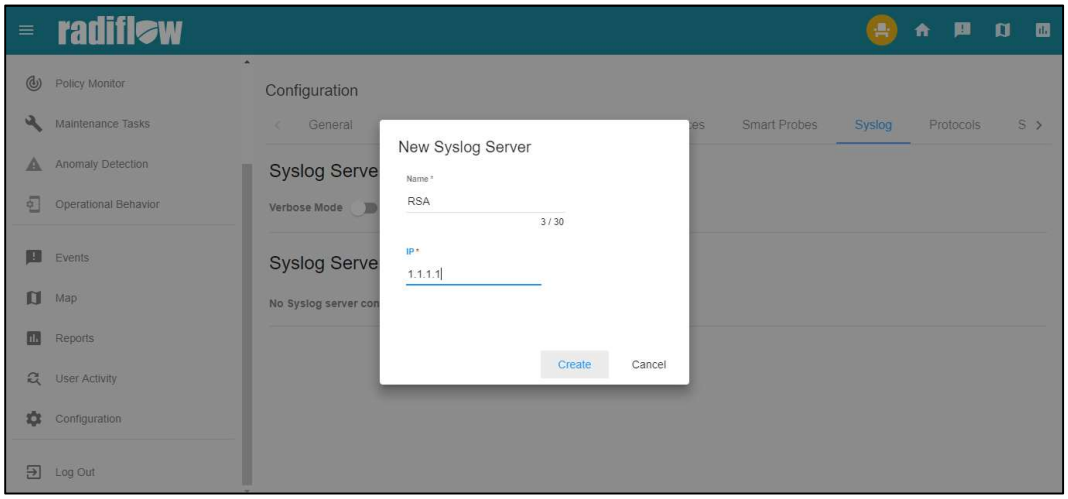
3. At the left side bar, choose the configuration screen.



4. In the configuration screen, choose the syslog tab.



5. Press "+" at the Syslog Servers, and configure the IP address of RSA NetWitness (that will act as the syslog server. iSID will send syslog messages to that configured IP). In the Name field, user can give any indicative name for the configured server.



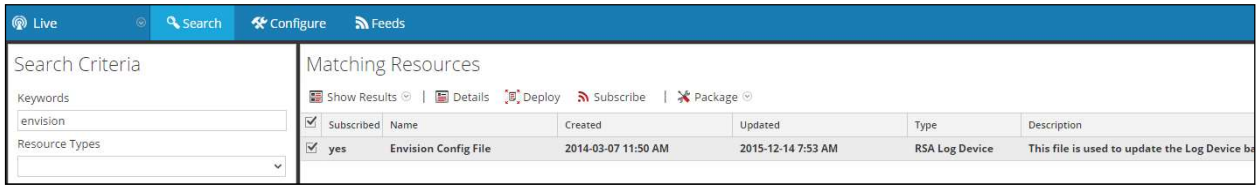
RSA NetWitness Configuration

Deploy the enVision Config File

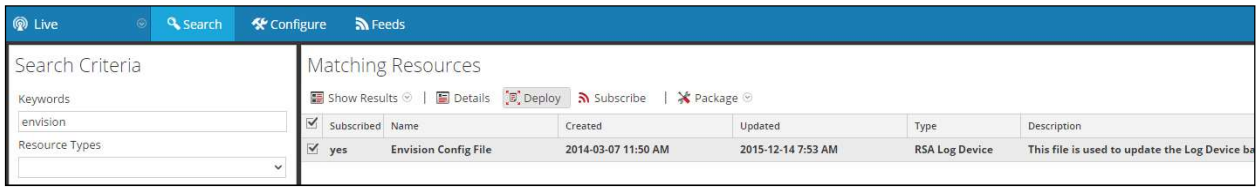
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

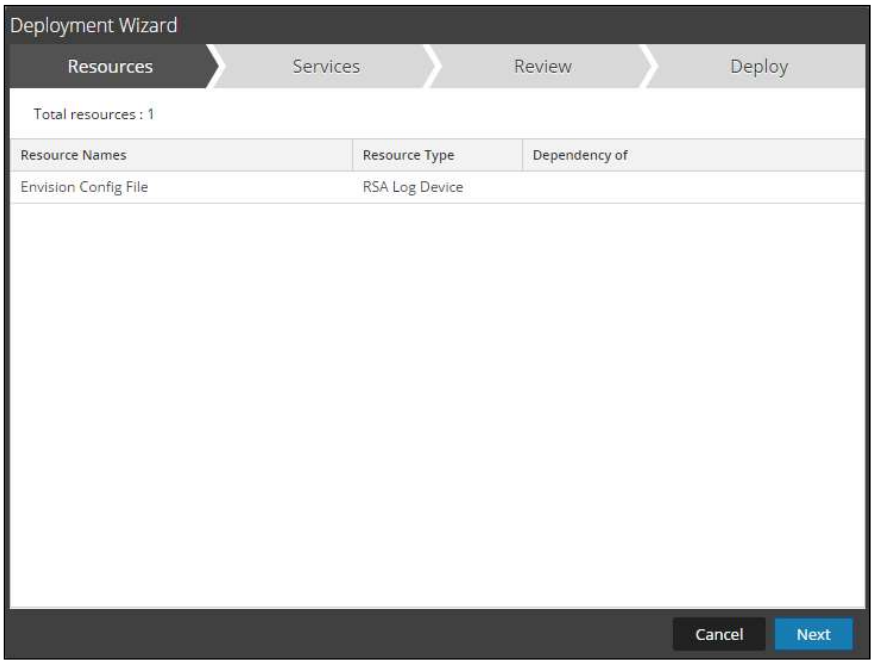
1. From the Security Analytics menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. Security Analytics will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



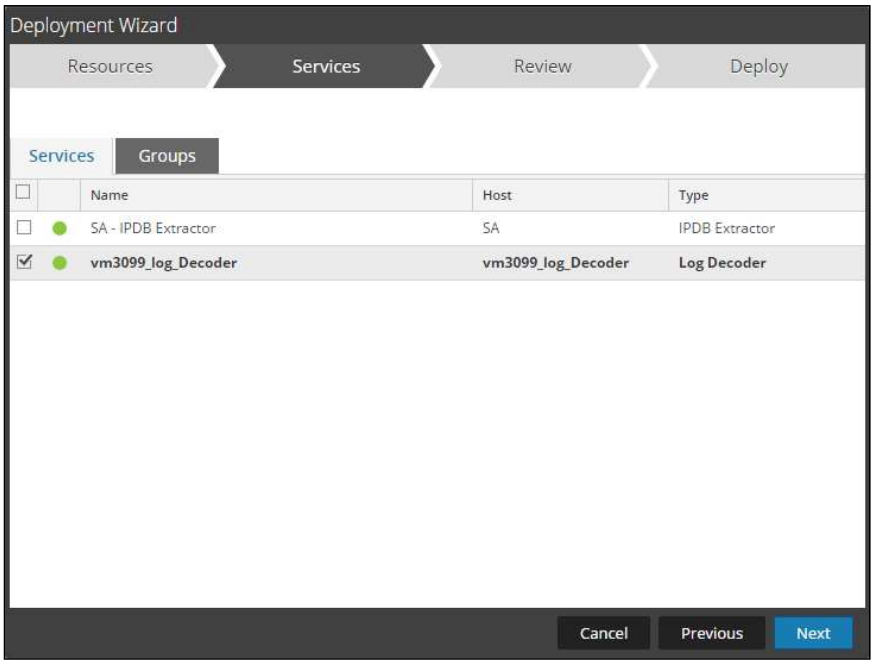
5. Click **Deploy** in the menu bar.



6. Select **Next**.

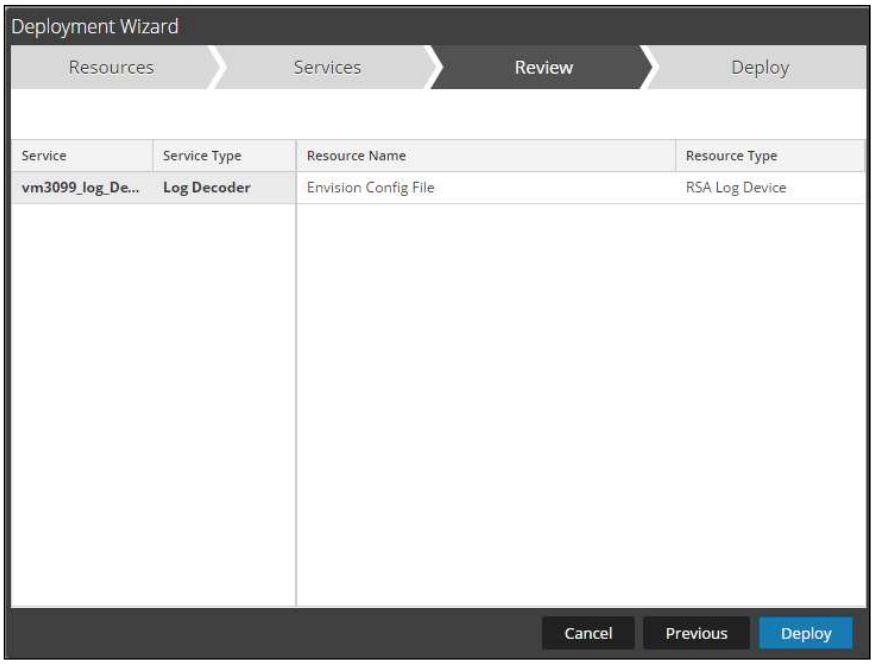


7. Select the **Log Decoder** and select **Next**.

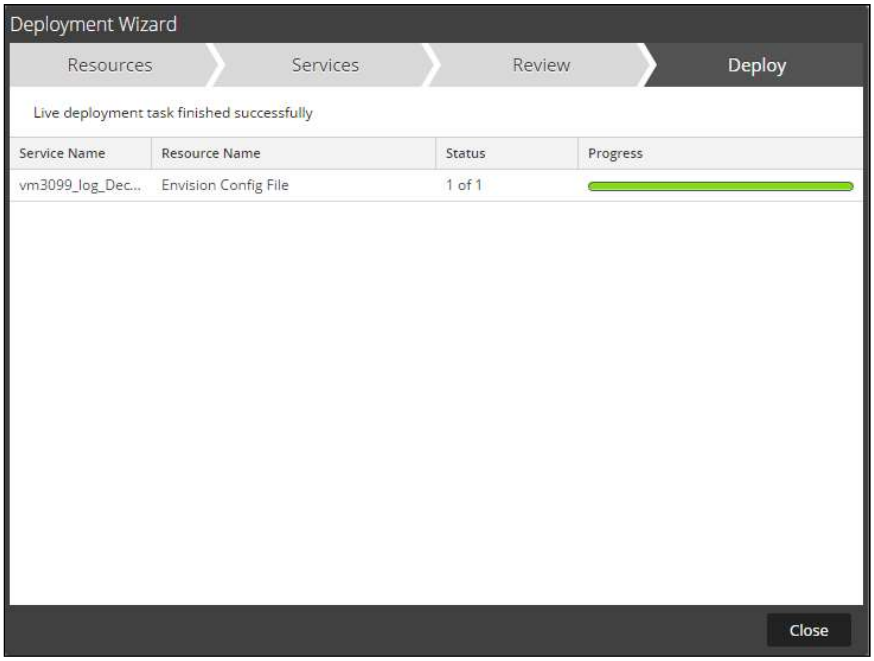


! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



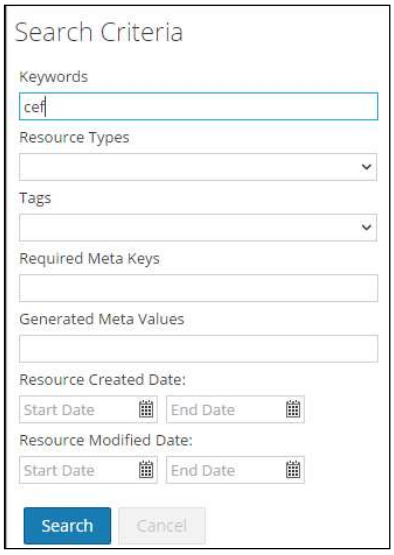
9. Select **Close**, to complete the deployment of the Envision Config file.



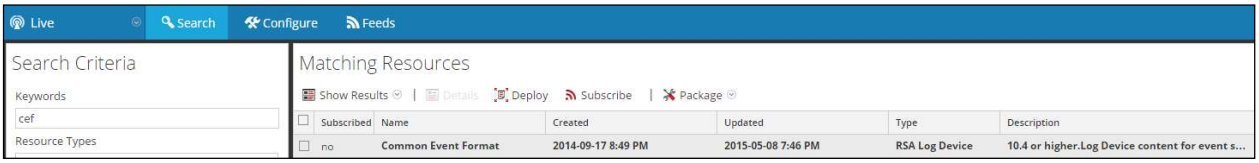
Deploy the Common Event Format

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

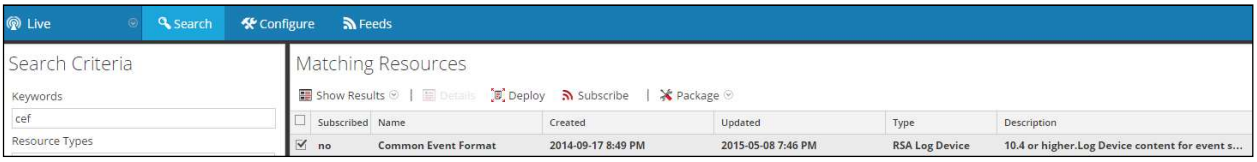
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **CEF**



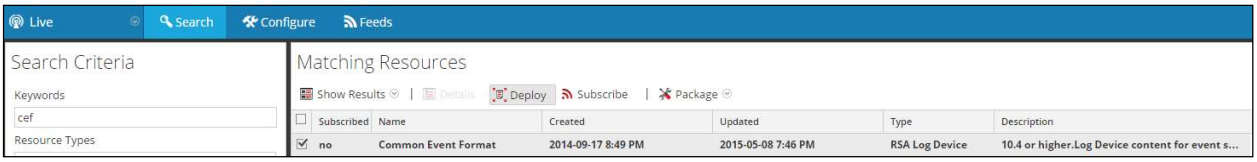
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



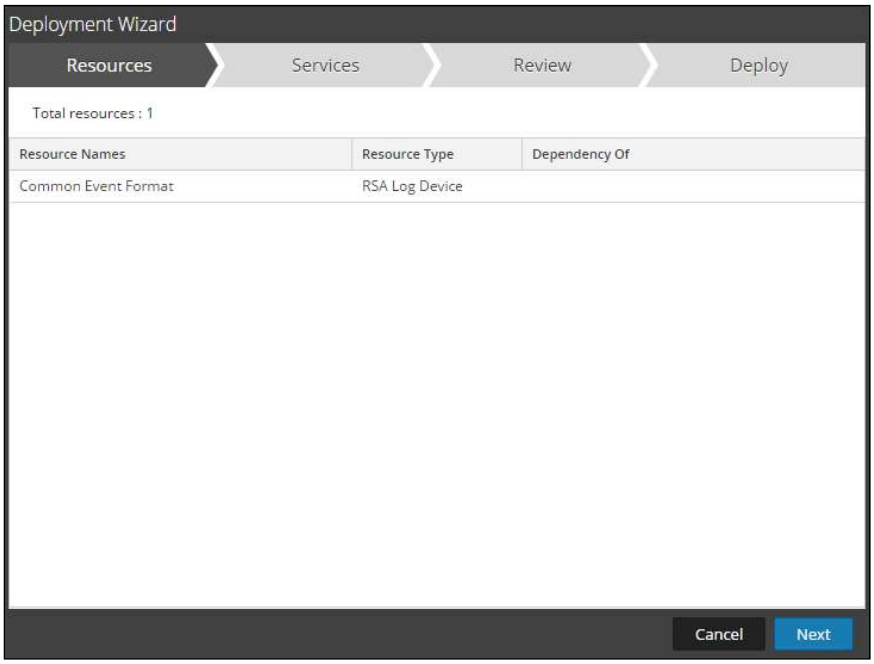
4. Select the checkbox next to **Common Event Format**.



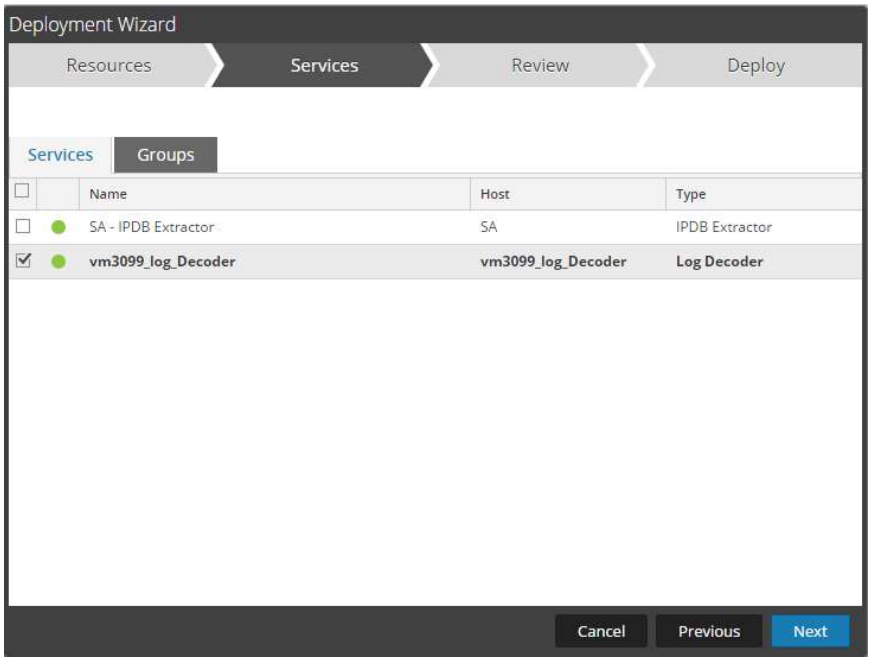
5. Click **Deploy** in the menu bar.



6. Select **Next**.

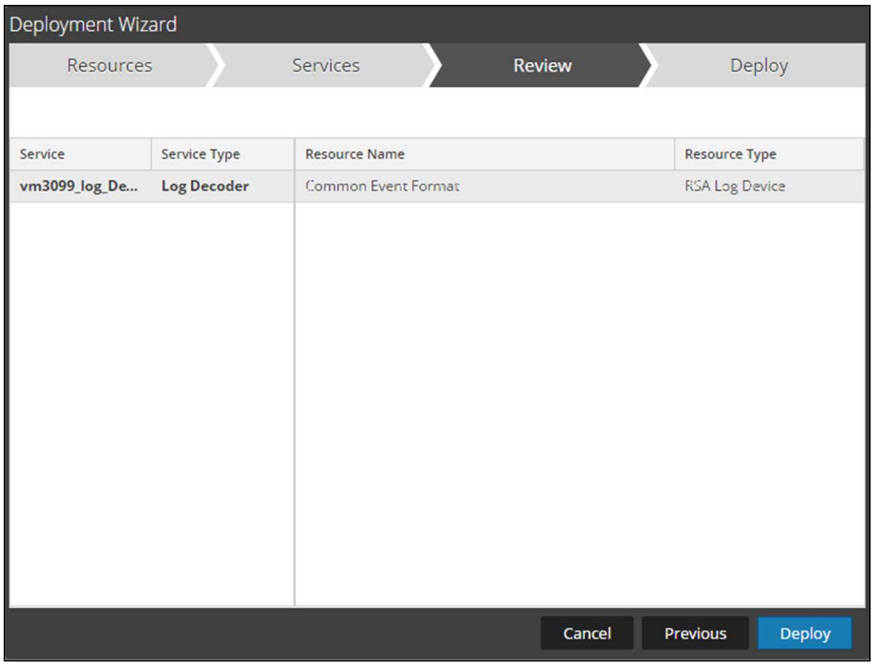


7. Select the **Log Decoder** and Select **Next**.

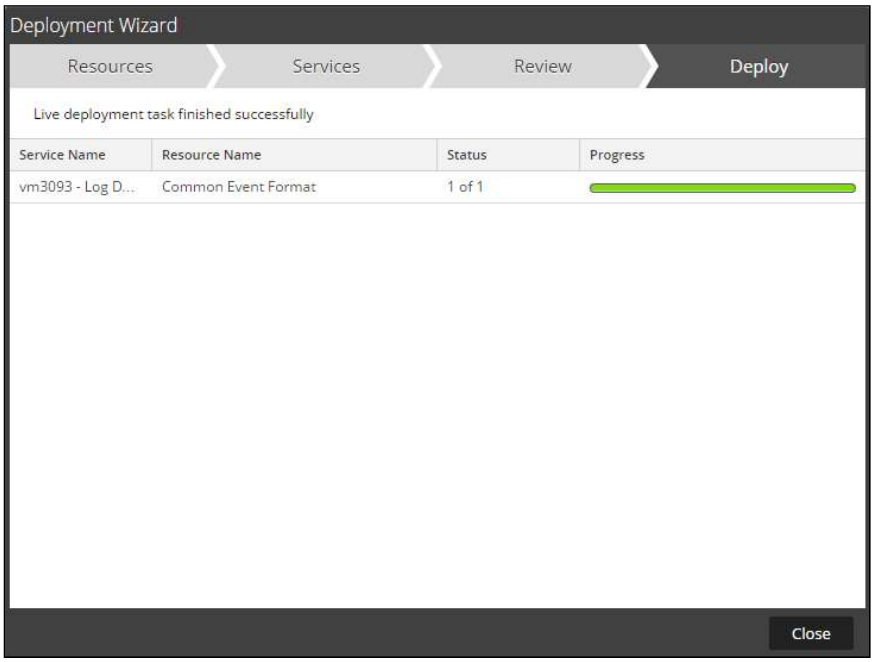


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

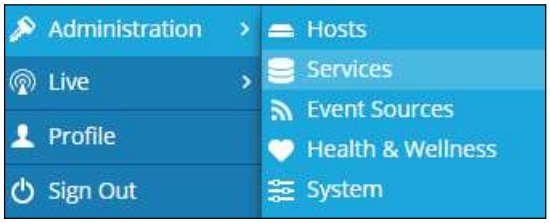
8. Select **Deploy**.



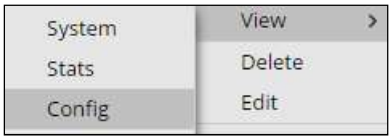
9. Select **Close**, to complete the deployment of the Common Event Format.



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 Radiflow 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 line below into the file before the start of the <VendorProducts> section.

Example:

```
<MESSAGE
                level="4"
                parse="1"
                parsedefvalue="1"
                tableid="74"
                id1="radiflow_isid"
                id2="radiflow_isid"
                eventcategory="1901000000"

        content="&lt;@event_name:*HDR(event_description)&gt;&lt;@event_time:*EVNTTIME($
HDR,'%B %F %Z',event_time_string)&gt;&lt;event_time_string&gt;&lt;msghold&gt;" />
```

Edit the Common Event Format Custom file 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="radiflow_isid"
              id2="radiflow_isid"
              eventcategory="1901000000"

       content="&lt;@event_name:*HDR(event_description)&gt;&lt;@event_time:*EVNT
TIME($HDR,'%B %F
%Z',event_time_string)&gt;&lt;event_time_string&gt;&lt;msghold&gt;" />

              -->

<VendorProducts>
       <Vendor2Device vendor="radiflow" product="Insight" device="radiflow_isid"
group="SCADA"/>
</VendorProducts>

       <ExtensionKeys>
              <ExtensionKey cefName="Version" metaName="version"/>
              <ExtensionKey cefName="level" metaName="severity"/>
              <ExtensionKey cefName="pt" metaName="pt"/>
       </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;

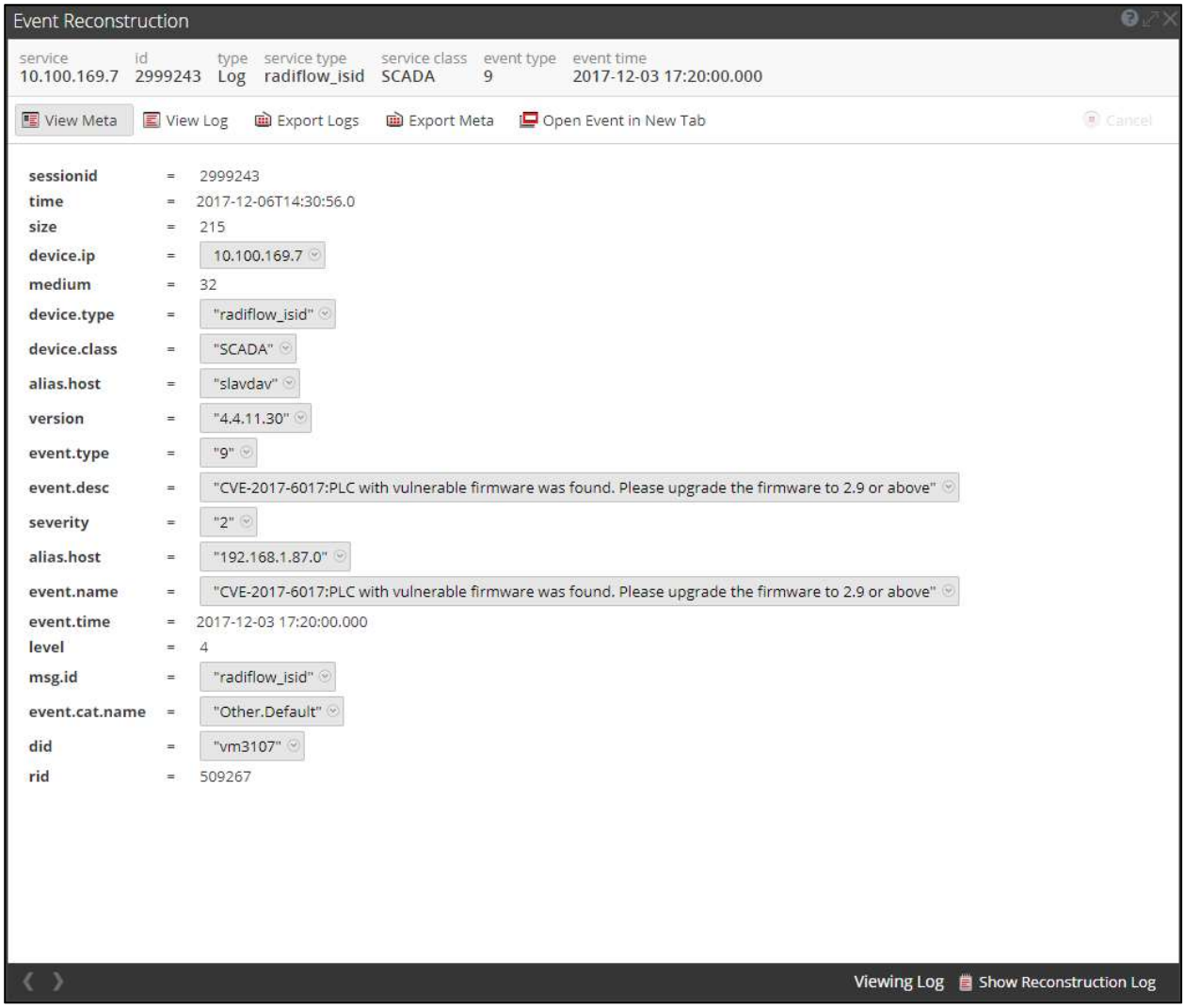
Example.

```
<?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="severity" nwName="severity" flags="None"
envisionDisplayName="Severity|SeverityLevel"/>
       <mapping envisionName="version" nwName="version" flags="None"/>
       <mapping envisionName="pt" nwName="pt" flags="None"/>

</mappings>
```

Radiflow iSID log collection as viewed from NetWitness Investigator Event Reconstruction:



Certification Checklist for RSA NetWitness

Date Tested: December 13, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.4	Virtual Appliance
Radiflow iSID	4.4.12	Virtual Appliance (Based on CentOS 7 Minimal)

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	✓

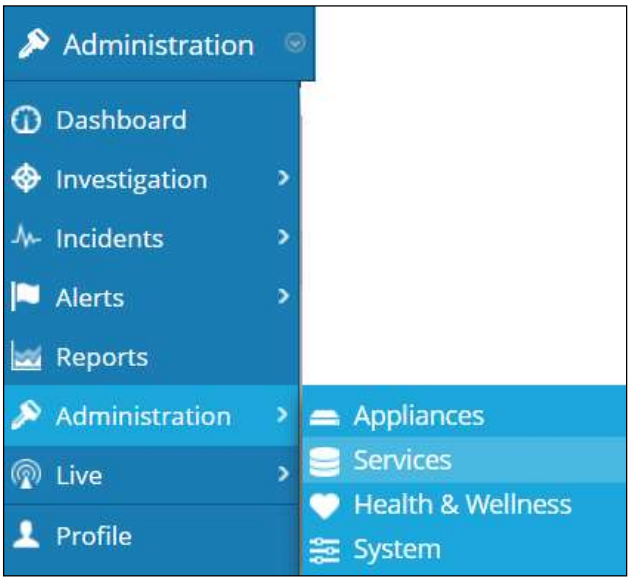
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Security Analytics Disable the Common Event Format Parser

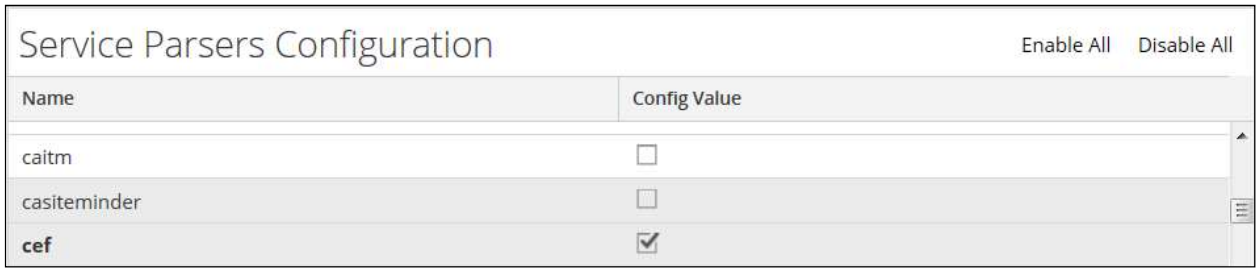
To disable the Security Analytics Common Event Format Parser and not delete it perform the following:

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.

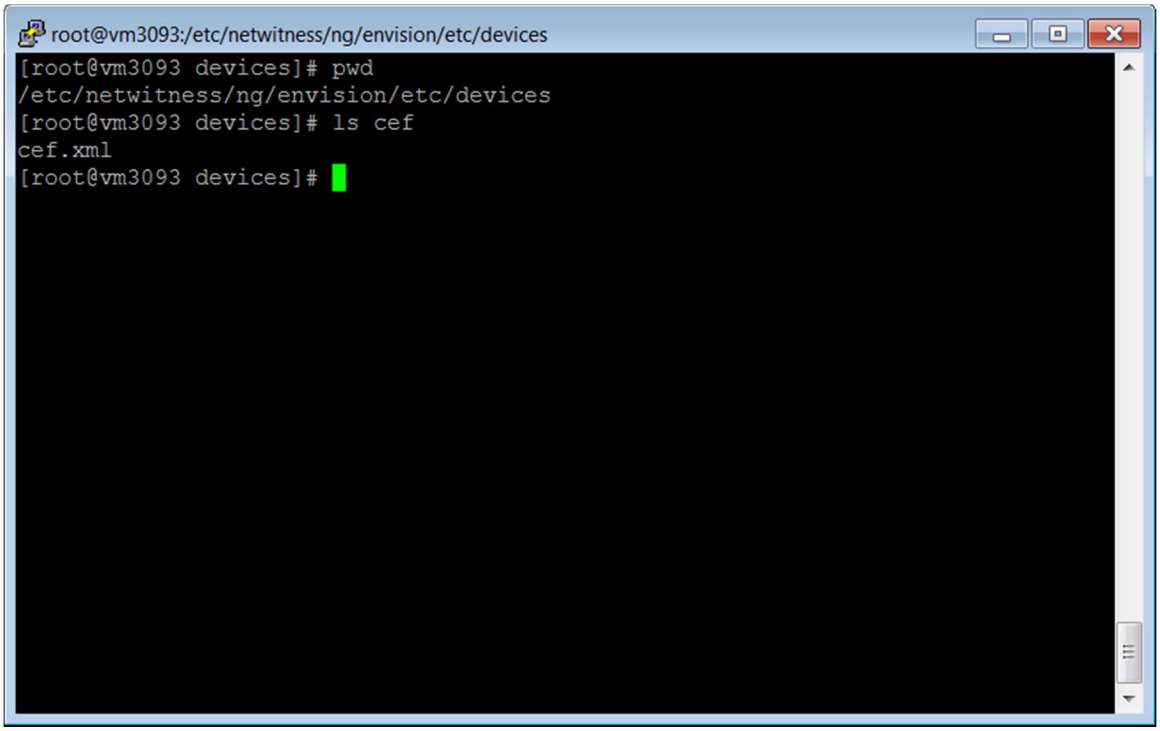


4. Click **Apply** to save settings.

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.