RSA® NETWITNESS®
Logs
Implementation Guide

Morphisec Endpoint Threat Prevention 2.7

Daniel R. Pintal, RSA Partner Engineering
Last Modified: July 27, 2018

RSA READY

Solution Summary

Morphisec Endpoint Threat Prevention prevents in-memory cyber-attacks on user machines. Over 40% of cyber-attacks are in-memory. 75% of breaches are caused by file less, in-memory attacks. Up to 80% of attacks happen on the endpoint. Examples of such attacks are Ransomwares, such Locky, Trojans such as Dridex, Miners such XMRigMiner, and other attacks such as CClear and NotPetya. When stopping an attack, Morphisec ETP captures valuable attack information. All information captured by Morphisec ETP is attack information, for an attack that was deterministically captured and prevented by Morphisec. The attack information is integrated into RSA NetWitness, where it can be brought together and correlated with additional information gathered by NetWitness. Having all attack information together in one place allows the user to get a full picture of every attack prevented and detected on his machines. Sec/Ops organization can be notified of the attack, and forensic analysts can further evaluate and analyze the attack.

RSA NetWitness Features	
Morphisec Endpoint Threat Prevention 2.7	
Integration package name	Common Event Format
Device display name within NetWitness	morphisec_eptp
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
7/27/2018	Initial support for Morphisec Endpoint Threat Prevention.

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 Morphisec Endpoint Threat Prevention with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

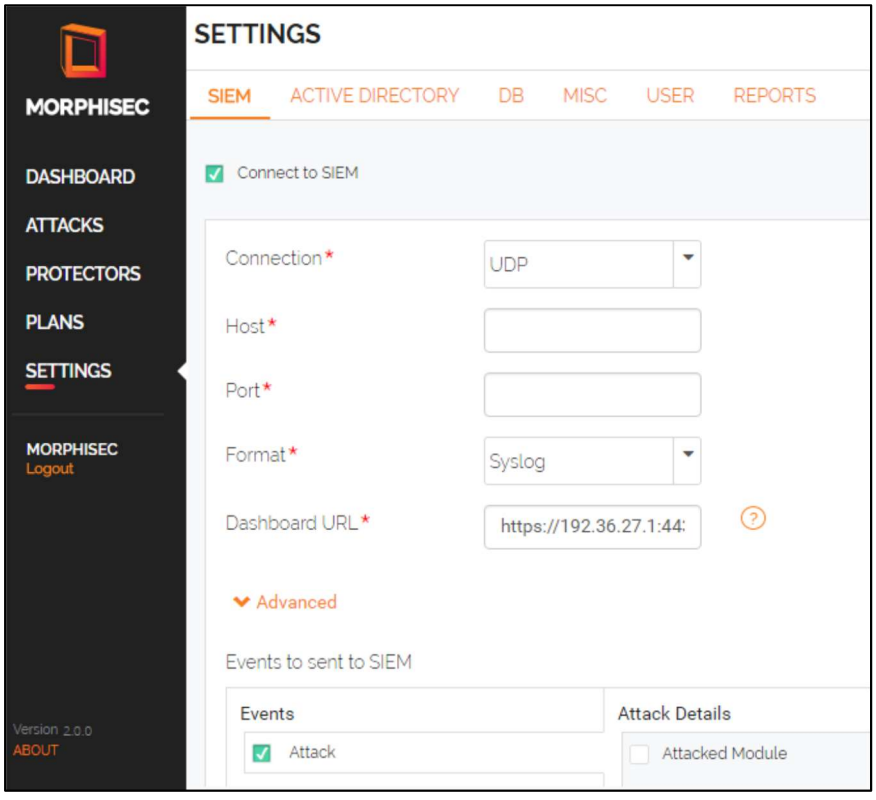
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Morphisec Endpoint Threat Prevention 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 Morphisec Endpoint Threat Prevention is properly configured and secured before deploying to a production environment. For more information, please refer to the Morphisec Endpoint Threat Prevention documentation or website.

Morphisec Endpoint Threat Prevention Configuration

To enable the Morphisec integration with RSA NetWitness, you will need to configure the related settings in the SIEM page of the Morphisec Dashboard.



To configure a connection to a SIEM server:

1. Log into the **Morphisec Dashboard**.
2. In the Settings page, click **SIEM** in the top menu.
3. Select the **Connect to SIEM** checkbox.
4. From the Connection drop-down menu, select one of these options:

   a. **TCP** – connect to RSA NetWitness via TCPIP.
   b. **UDP** – connect to RSA NetWitness via UDP.
   c. **SSL** – connect to RSA NetWitness via SSL. For this option, you'll need to enter a path to the SSL certificate in the Certificate field.

5. If you selected the TCP, UDP or SSL connection type:

   1. In the Host field, enter a **hostname or IP address** for the RSA NetWitness server.
   2. In the Port field, enter **514**.
   3. In the Format drop-down menu, select the **CEF** security log format.
   4. In the Dashboard URL field, enter the Morphisec Dashboard IP/hostname and port number in the format `<IP/hostname>:<port>`.

      Important: This value is the Morphisec Dashboard URL as seen from other machines. Therefore, it cannot be `localhost` or `127.0.0.1`.

   5. If you selected the SSL connection type, in the Certificate File field, browse to the SSL certificate file.

6. To select advanced attack details you want to send to the RSA NetWitness server, click the **Advanced** link. The Events pane is displayed.
7. Under the Events column, select the **Attacks** checkbox.
8. Under the Attack Details column, select the advanced attack details you want to send to the RSA NetWitness server:

   Important: Not all details are relevant to all attacks.

   a. **Attacked Module** – the library or executable that was attacked.
   b. **Last Stack Function Call** – the last function called before the attack.
   c. **Last Module Loaded** – the last module loaded before the attack was identified.
   d. **Command Line** – the text of the command line that launched the protected executable.
   e. **Parent Process Command Line** – the text of the command line that launched the parent of the protected executable.
   f. **Attack Signature** – the unique signature of the attack.
   g. **Process Signature** – the unique signature of the attacked executable.
   h. **Parent Signature** – the unique signature of the parent of the attacked executable.
   i. **Morphisec Ver** – the Morphisec Server version currently running.

9. Click the **Save** button.

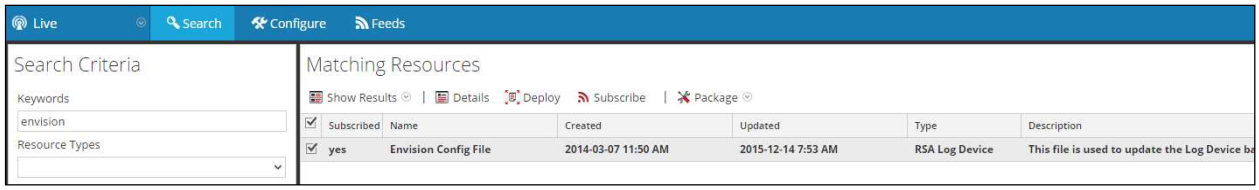
RSA NetWitness Configuration

Deploy the enVision Config File

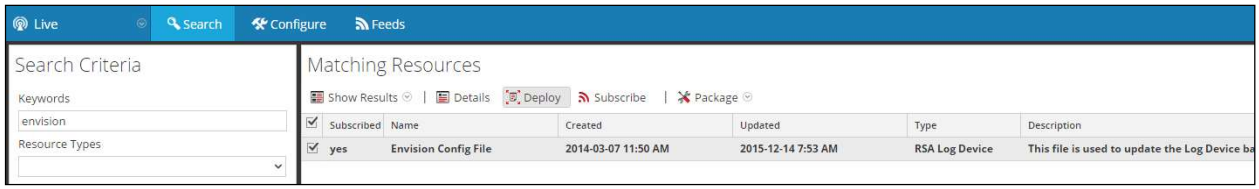
In order to use the RSA Common Event Format, you must first deploy the *enVision Config File* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

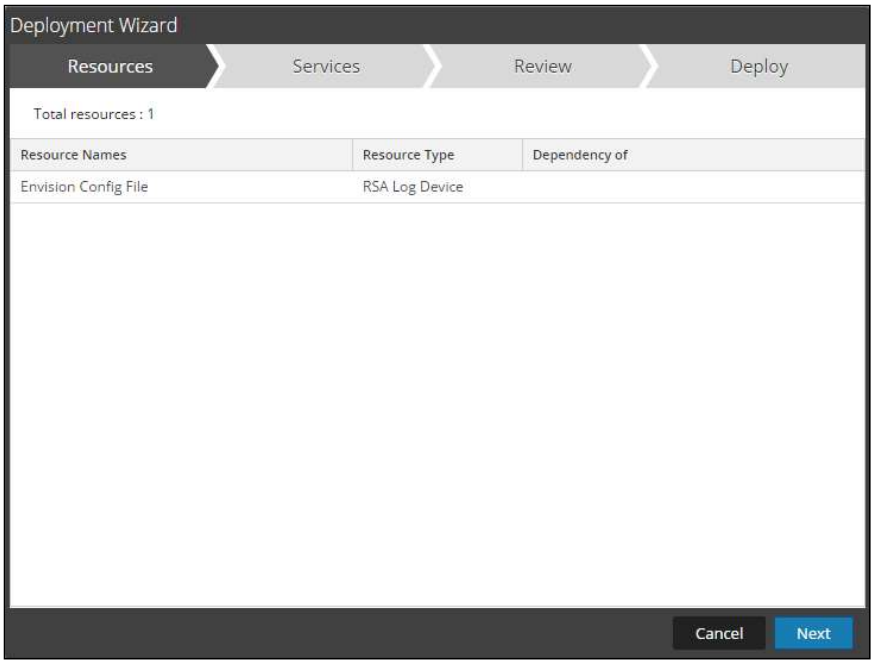
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **enVision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



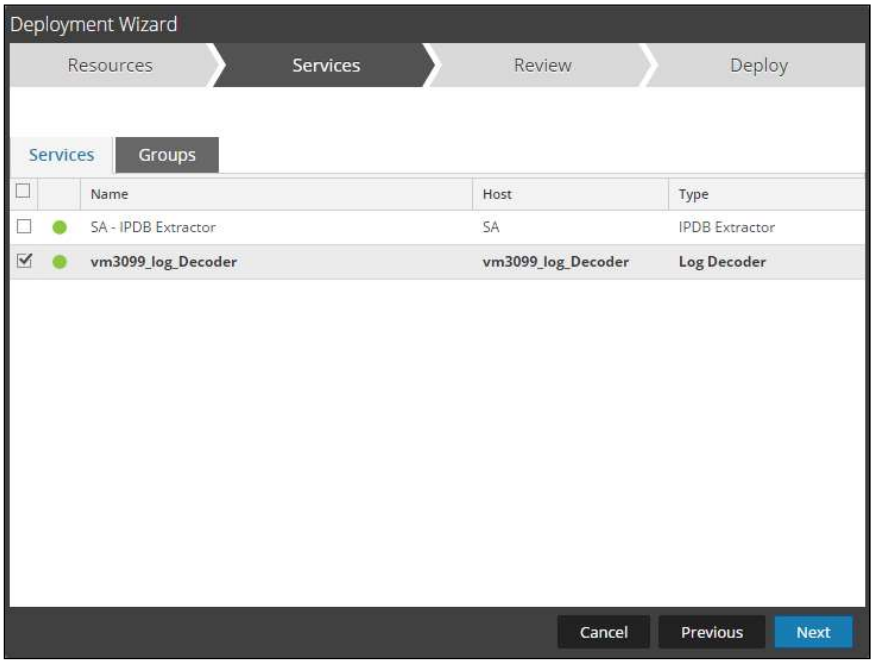
5. Click **Deploy** in the menu bar.



6. Select **Next**.

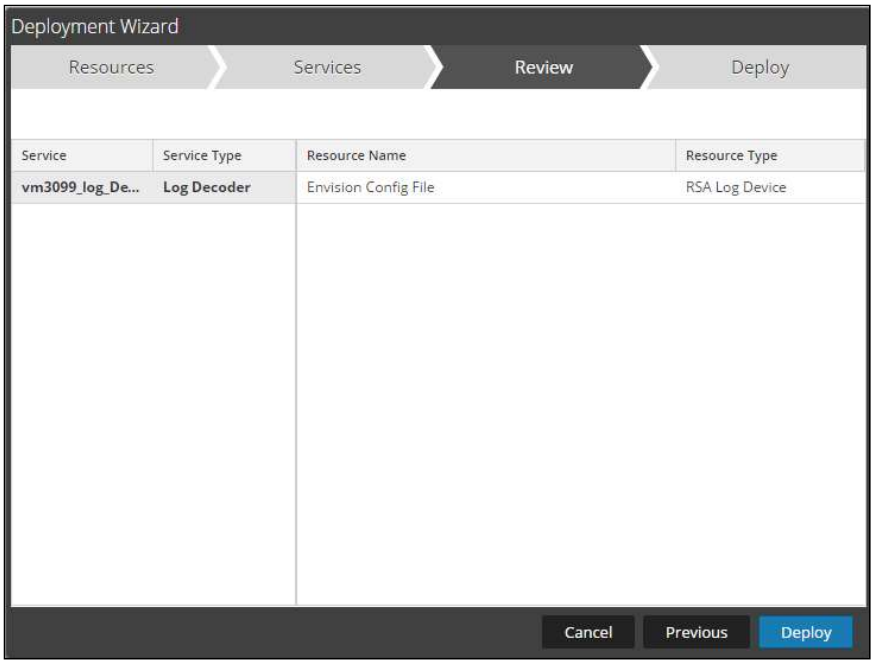


7. Select the **Log Decoder** and select **Next**.

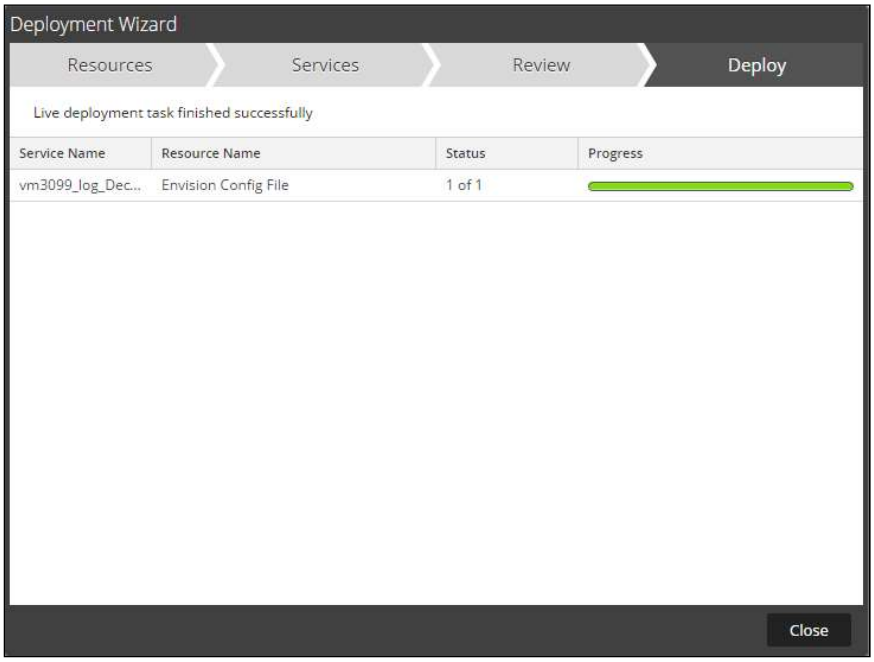


! > Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



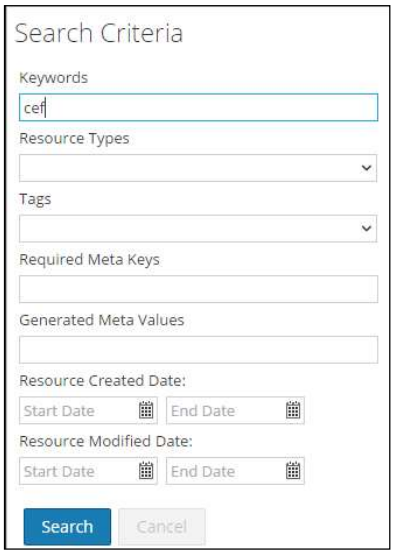
9. Select **Close**, to complete the deployment of the Envision Config file.



Deploy the Common Event Format

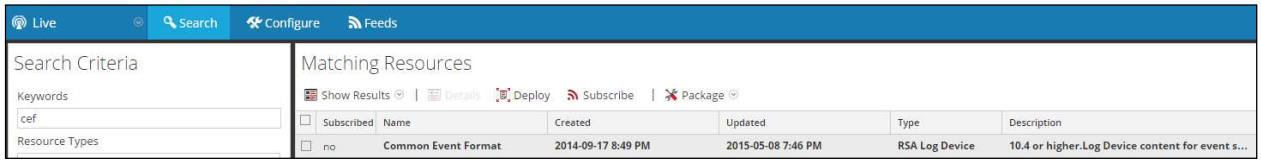
Next, you will need to deploy the *Common Event Format file* from the **NetWitness Live** module. Log into NetWitness and perform the following actions:

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

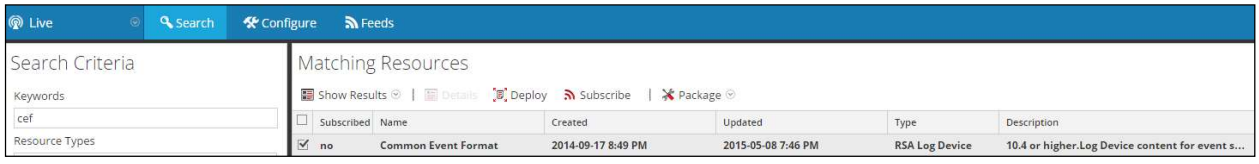


.

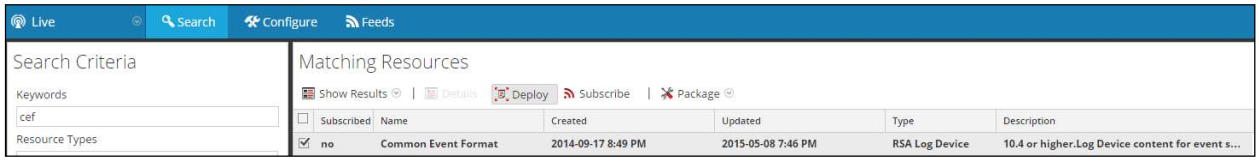
3. RSA NetWitness will display the **Common Event Format** in Matching Resources.



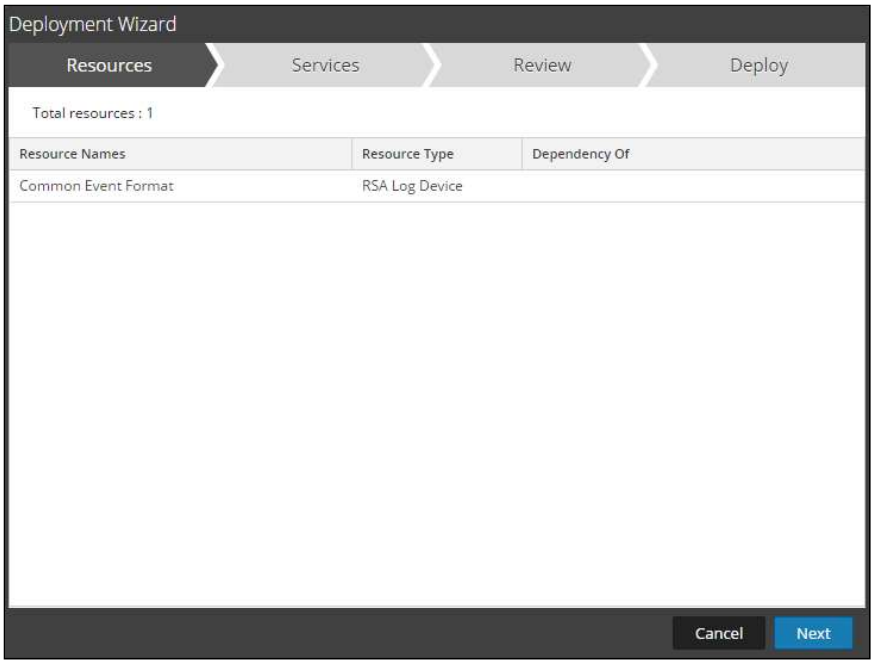
4. Select the checkbox next to **Common Event Format**.



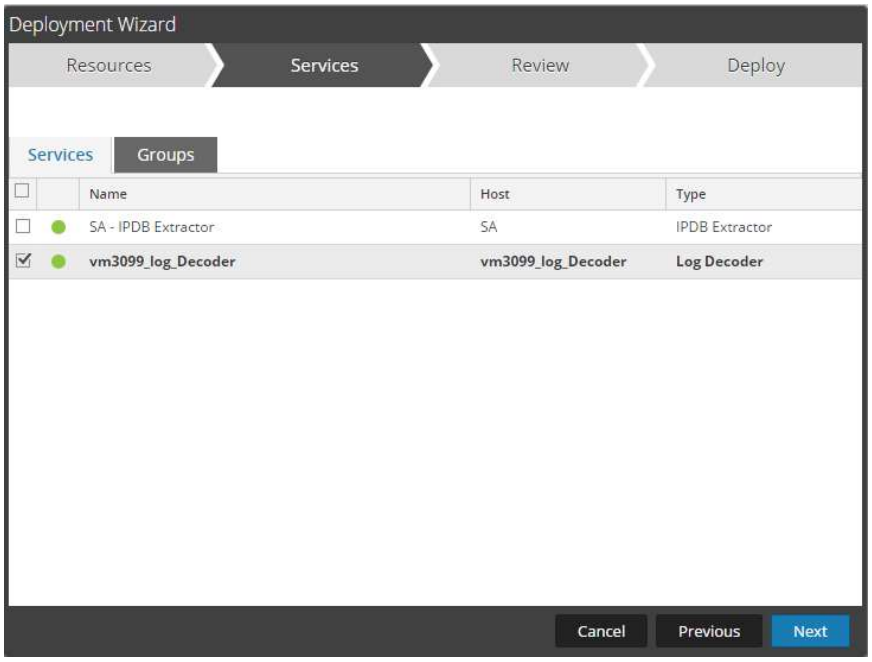
5. Click **Deploy** in the menu bar.



6. Select **Next**.

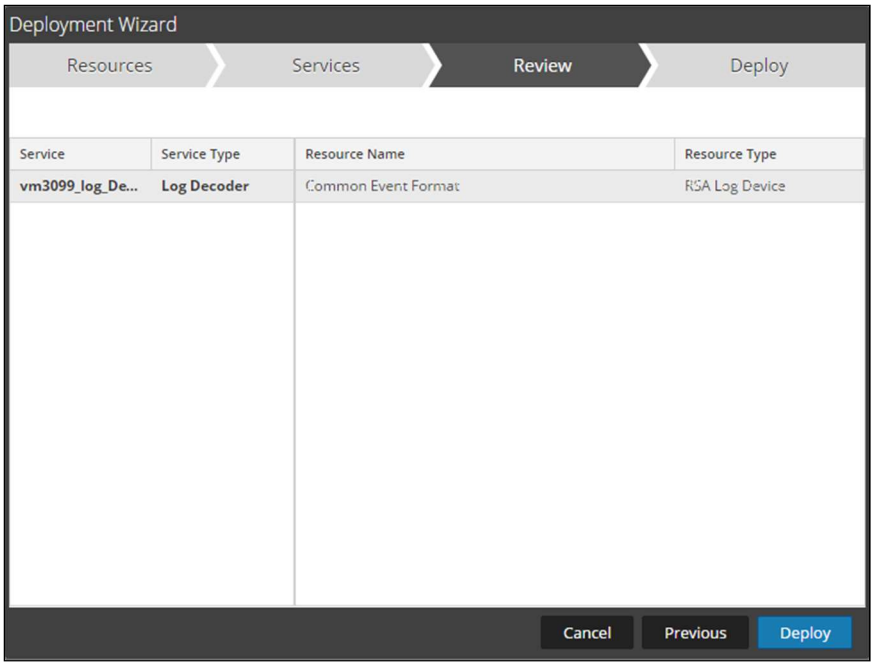


7. Select the **Log Decoder** and Select **Next**.

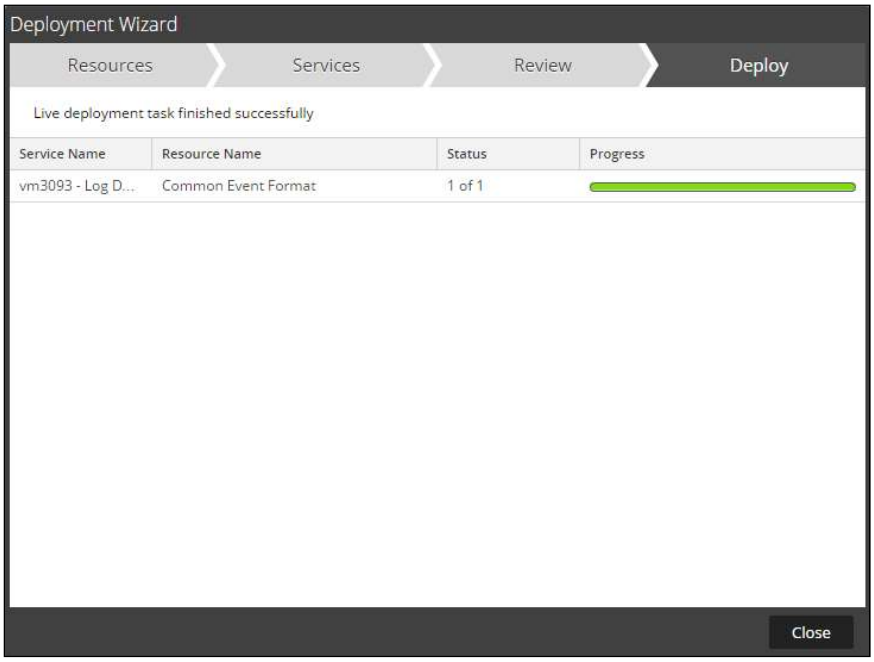


! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

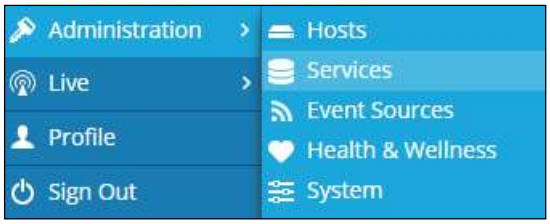
8. Select **Deploy**.



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 Morphisec 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
        id1="morphisec_eptp"
        id2="morphisec_eptp"
        eventcategory="1901000000"

functions="&lt;@starttime:*EVNTTIME($MSG,'%B<space>%F<space>%W<space>%Z<space>%
L',param_starttime)&gt;"
        content="&lt;param_starttime&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.
   Example.

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

<MESSAGE
       id1="morphisec_eptp"
       id2="morphisec_eptp"
       eventcategory="1901000000"

functions="&lt;@starttime:*EVNTTIME($MSG,'%B<space>%F<space>%W<space>%Z<space>%
L',param_starttime)&gt;"
       content="&lt;param_starttime&gt;&lt;msghold&gt;" />

<VendorProducts>
       <Vendor2Device vendor="Morphisec" product="Morphisec Endpoint Threat
Prevention" device="morphisec_eptp" group="Analysis"/>
</VendorProducts>

           <ExtensionKeys>

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

              <ExtensionKey cefName="AttackedModule" metaName="AttackedModule"/>
              <ExtensionKey cefName="LastStackFunctionCall"
metaName="LastStackFunctionCall"/>
              <ExtensionKey cefName="LastModuleLoaded"
metaName="LastModuleLoaded"/>
              <ExtensionKey cefName="CommandLine" metaName="CommandLine"/>
              <ExtensionKey cefName="ParentProcessCommandLine"
metaName="ParentProcessCommandLine"/>
              <ExtensionKey cefName="CodeProcessed" metaName="CodeProcessed"/>
              <ExtensionKey cefName="ParentSignature"
metaName="ParentSignature"/>
              <ExtensionKey cefName="ProcessSignature"
metaName="ProcessSignature"/>

              <ExtensionKey cefName="msg" metaName="msg">
                     <device2meta device="trendmicrodsa" metaName="info"/>
                     <device2meta device="morphisec_eptp" metaName="info"/>
              </ExtensionKey>

              </ExtensionKeys>

       -->

</DEVICEMESSAGES>
```

Edit the NetWtness 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.

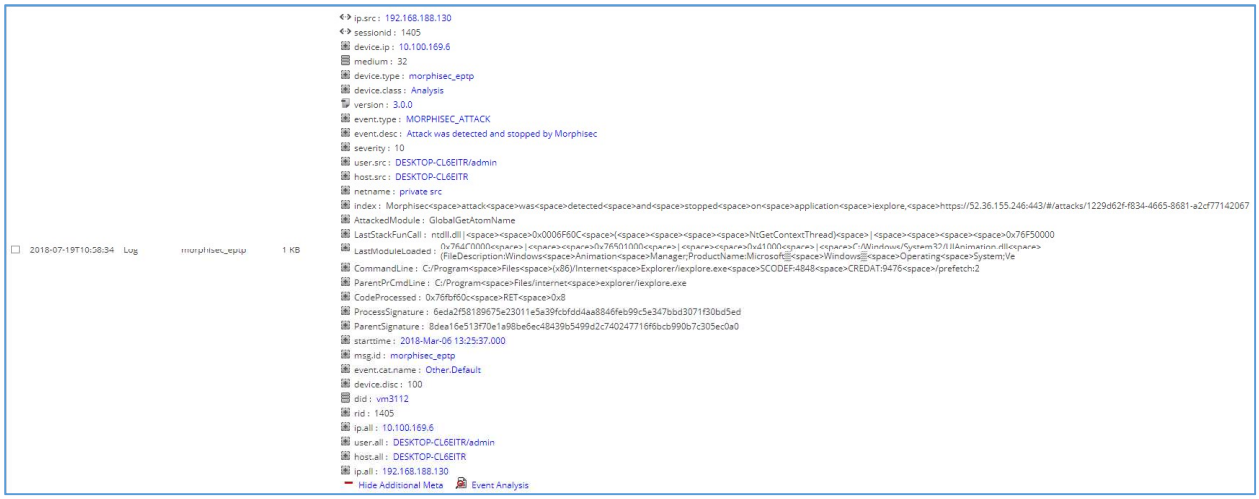
```
<?xml version="1.0" encoding="utf-8"?>
<!--
# attributes:
#      envisionName: The name of the column in the universal table
#      nwName:                    The name of the NetWitness meta field
#      format:                    Optional. The language key data type. See
LanguageManager. Defaults 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="AttackedModule" nwName="AttackedModule"
flags="None"/>
       <mapping envisionName="LastStackFunctionCall" nwName="LastStackFunCall"
flags="None"/>
       <mapping envisionName="LastModuleLoaded" nwName="LastModuleLoaded"
flags="None"/>
       <mapping envisionName="CommandLine" nwName="CommandLine" flags="None"/>
       <mapping envisionName="ParentProcessCommandLine" nwName="ParentPrCmdLine"
flags="None"/>
       <mapping envisionName="CodeProcessed" nwName="CodeProcessed"
flags="None"/>
       <mapping envisionName="ParentSignature" nwName="ParentSignature"
flags="None"/>
       <mapping envisionName="ProcessSignature" nwName="ProcessSignature"
flags="None"/>
       <mapping envisionName="info" nwName="index" flags="None"/>
       <mapping envisionName="severity" nwName="severity" flags="None"
envisionDisplayName="Severity|SeverityLevel"/>

</mappings>
```

4. Restart the **Log Decoder services** to begin log collection.

Morphisec Collection Example from NetWitness Investigator:



Certification Checklist for RSA NetWitness

Date Tested: July 27, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.1	Virtual Appliance
Morphisec Endpoint Threat Prevention	2.7	

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	✓

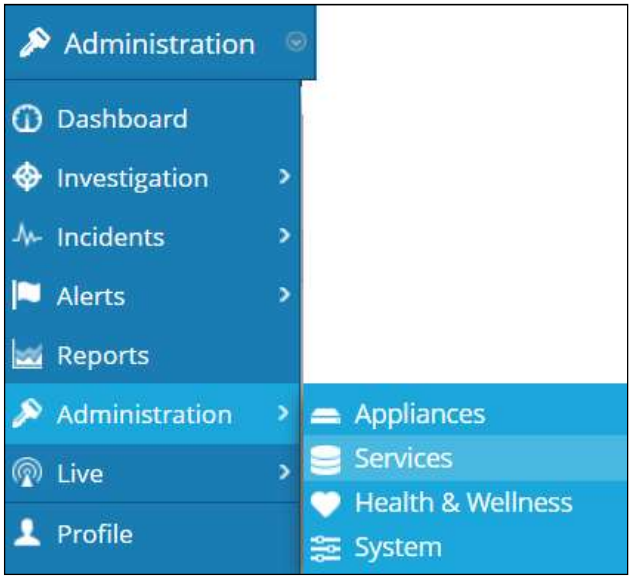
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

NetWitness Disable the Common Event Format Parser

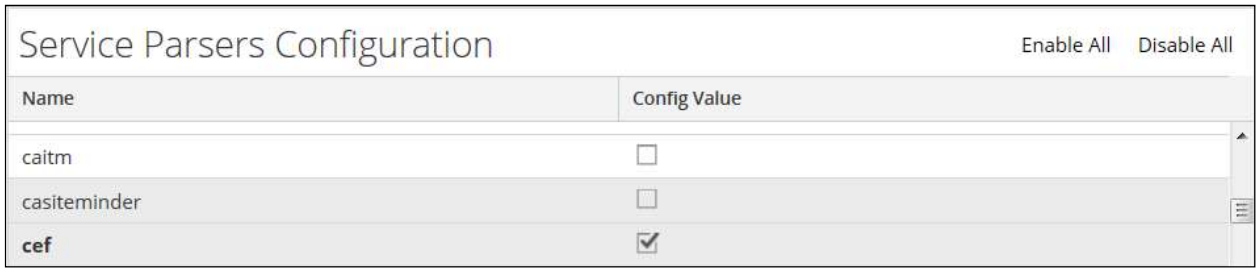
To disable the NetWitness Common Event Format Parser and not delete it perform the following:

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.

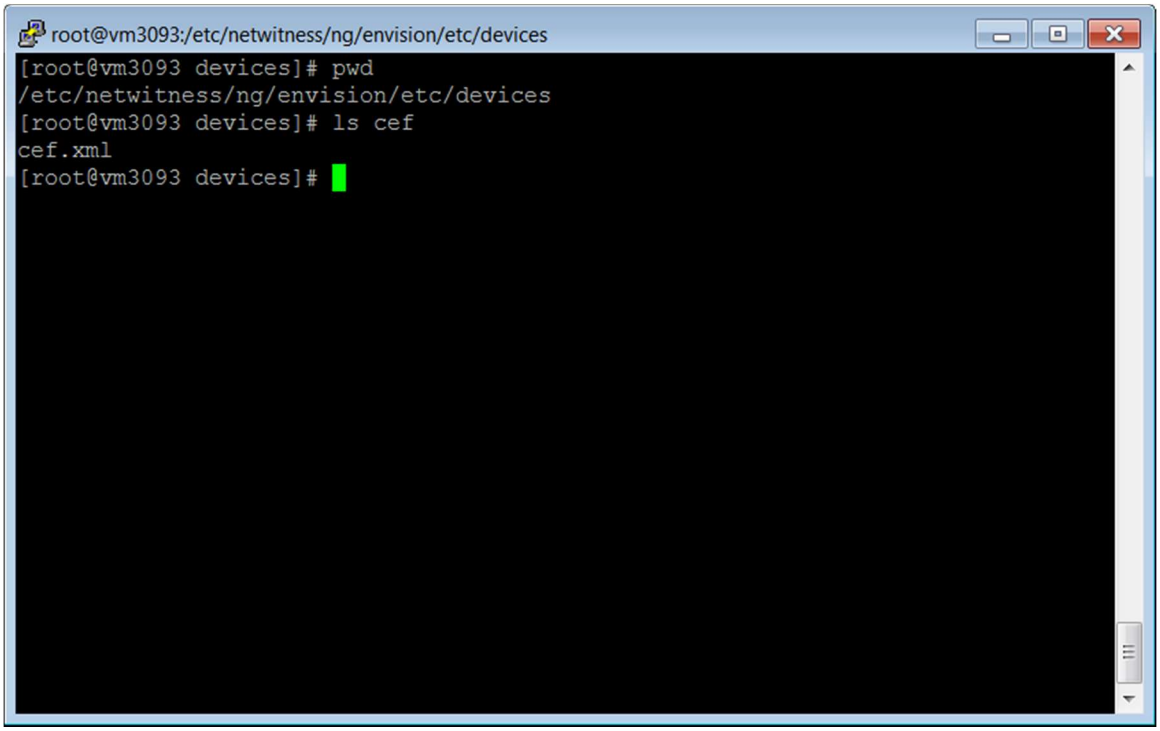


4. Click **Apply** to save settings.

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.