RSA® NETWITNESS®
Logs
Implementation Guide

Sentryo ICS CyberVision 2.0.3

Daniel R. Pintal, RSA Partner Engineering

Last Modified: November 12, 2018

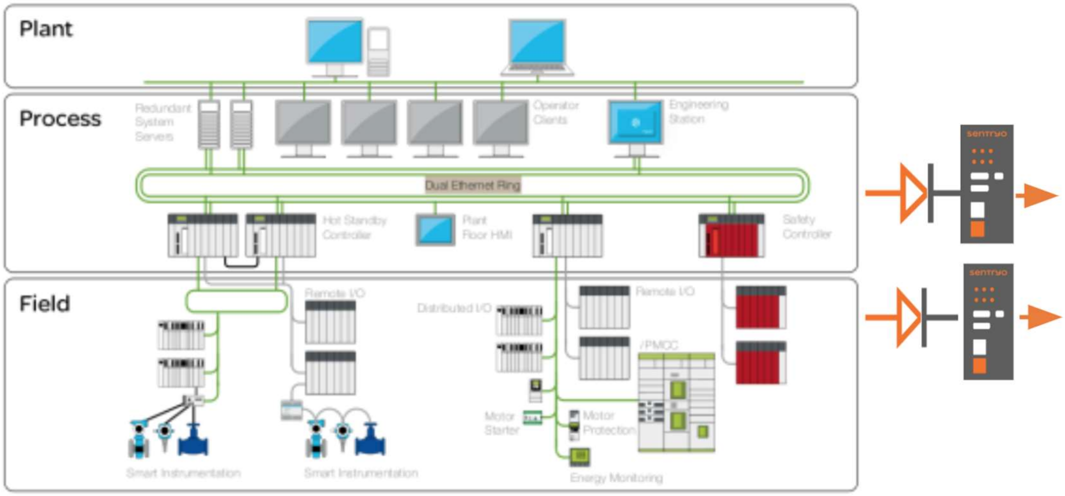
Solution Summary

Sentryo ICS CyberVision is a network monitoring and threat intelligence platform that provides cyber-resilience for Industrial Control Systems (ICS) and SCADA networks.

The solution relies on the use of sensors, and the data processed goes through a central analytics software to provide data visualization. The sensors passively analyze industrial network communications to provide meaningful information about network assets, advanced anomaly detection and alerts in real-time for any threat to operational continuity and system integrity.

Using ICS CyberVision with RSA NetWitness helps SOC and NOC administrators to investigate and remediate anomalies in their network and cloud infrastructures through a single unified interface.

RSA NetWitness Features	
Sentryo ICS CyberVision 2.0.3	
Integration package name	Common Event Format
Device display name within NetWitness	sentryo_cybervision
Event source class	SCADA
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
12/5/2017	Initial support for Sentryo ICS CyberVision.
10/23/2018	Added additional keys, 16 Char NW Key names, NetWitness 11.2 Support

! > 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 Sentryo ICS CyberVision with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

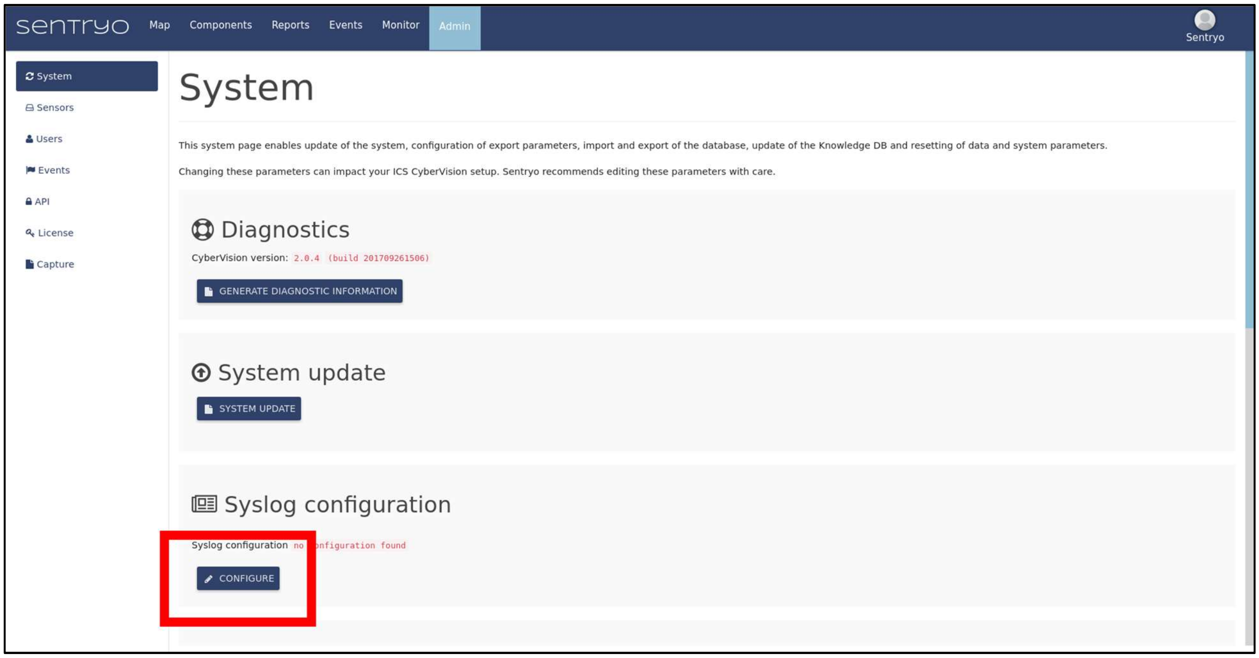
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Note: This document assumes that the user has a working ICS CyberVision installation and solely walks them through the configuration of syslog. If they do not have a working instance or have trouble using the tool itself, they can refer to the official documentation on https://sentryo.zendesk.com/hc/en-us to set up and use ICS CyberVision for their ICS (it is required to register an account on sentryo.zendesk.com before accessing the documentation).

Sentryo ICS CyberVision Configuration

1. In the webapp, the Admin page shows the Syslog configuration panel. Click on **Configure** to expand it.



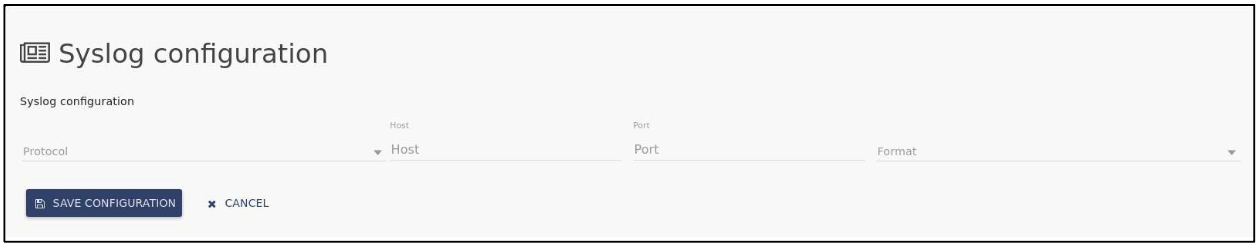
This system page enables update of the system, configuration of export parameters, import and export of the database, update of the Knowledge DB and resetting of data and system parameters.

Changing these parameters can impact your ICS CyberVision setup. Sentryo recommends editing these parameters with care.

CyberVision version: 2.0.4 (build 201709261506)

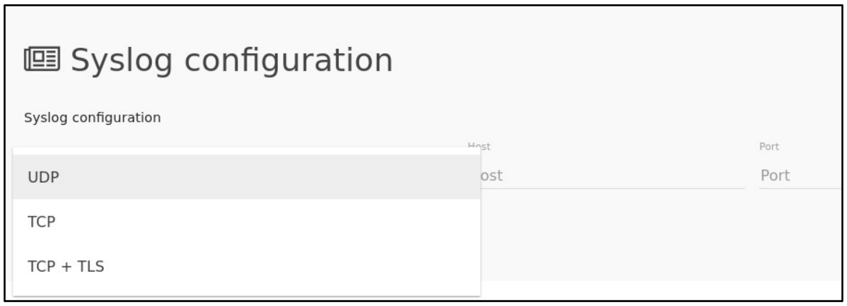
Syslog configuration no configuration found

2. The Syslog configuration panel unfolds and lets the user configure the required parameters for their SIEM.



Protocol selection

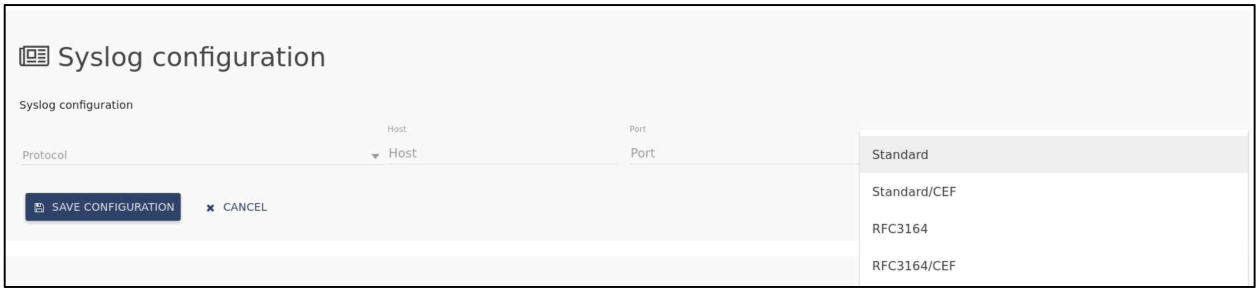
3. The product currently supports three protocols for the network communication with the SIEM: UDP, TCP and TLS over TCP. The user can click on the drop-down menu to select one of the three.



Format selection

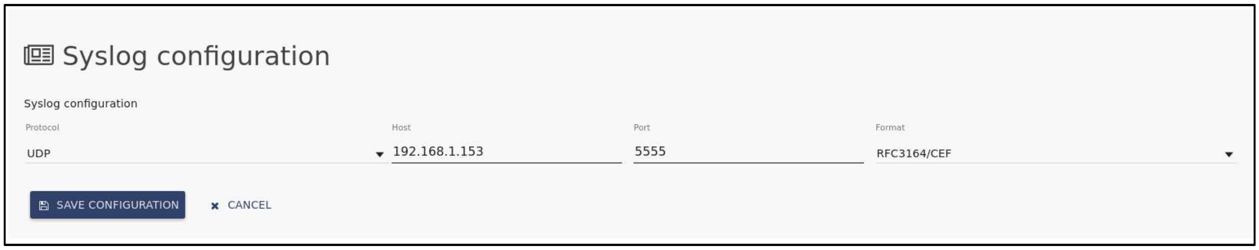
4. The product currently supports four formats for the syslog messages:

- Standard syslog (RFC 5424)
- BSD syslog (RFC 3164)
- CEF-compliant standard syslog
- CEF-compliant BSD syslog



Network

5. The IP/port of the SIEM must also be filled in.



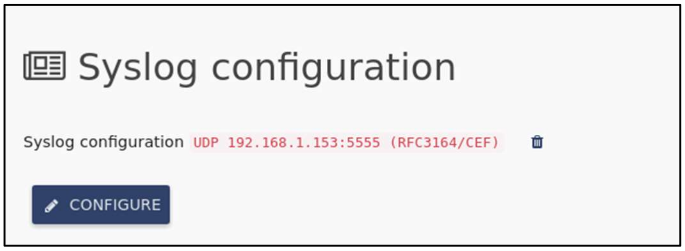
Syslog configuration

Syslog configuration

Protocol: UDP
Host: 192.168.1.153
Port: 5555
Format: RFC3164/CEF

Final steps

6. Clicking on the **Save configuration** button will make the changes effective.
7. The user should then see a line that reflects the configuration they just entered.



Syslog configuration

Syslog configuration `UDP 192.168.1.153:5555 (RFC3164/CEF)`

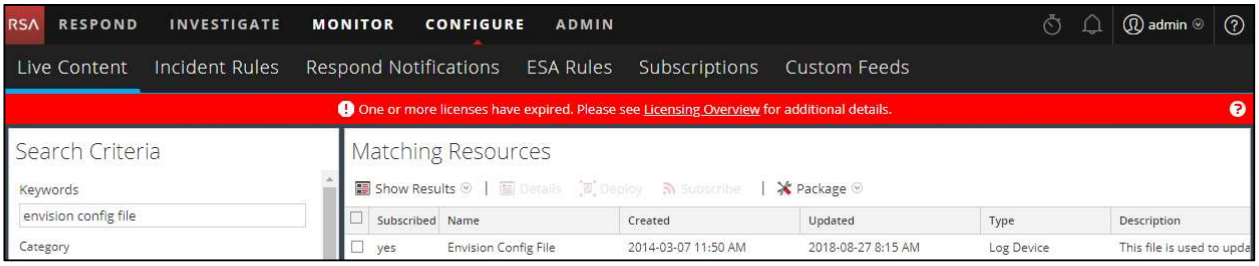
RSA NetWitness Configuration

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 **Configure > Live Content**.
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**.

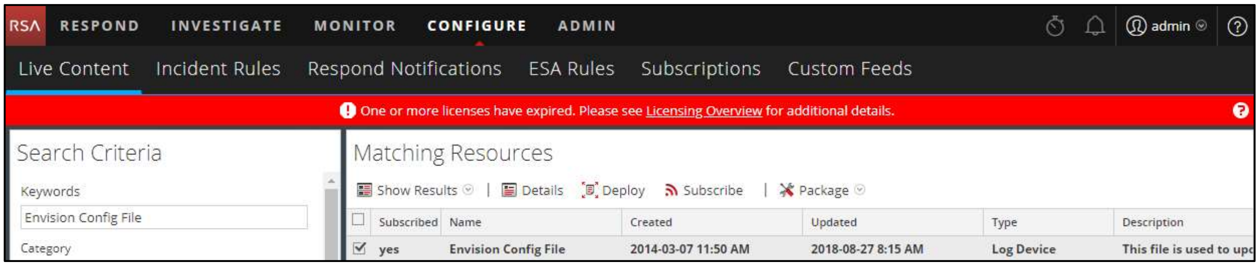


One or more licenses have expired. Please see Licensing Overview for additional details.

Keywords: envision config file

☐ Subscribed	Name	Created	Updated	Type	Description
☐ yes	Envision Config File	2014-03-07 11:50 AM	2018-08-27 8:15 AM	Log Device	This file is used to upda

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

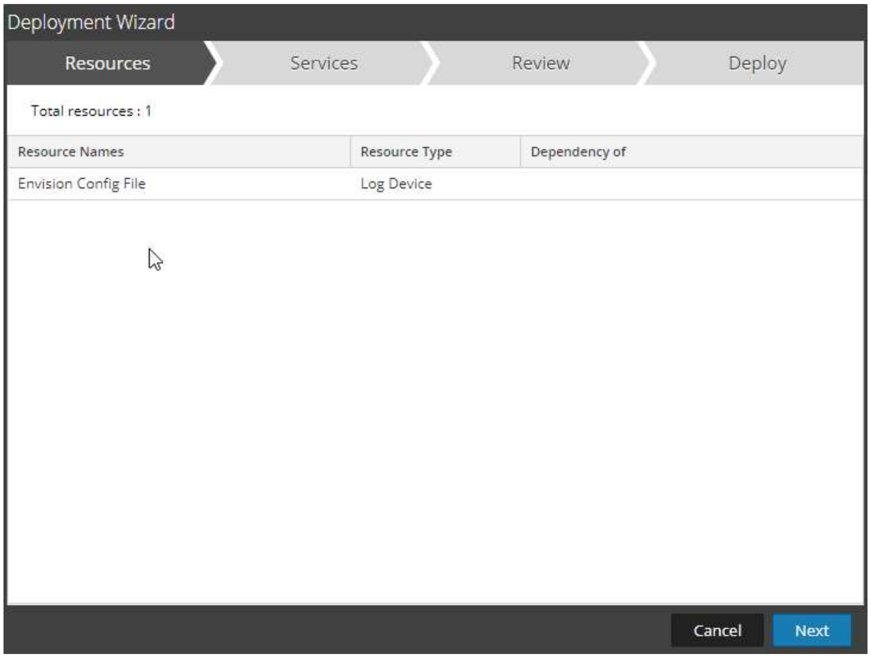


One or more licenses have expired. Please see Licensing Overview for additional details.

Keywords: Envision Config File

☐ Subscribed	Name	Created	Updated	Type	Description
☑ yes	Envision Config File	2014-03-07 11:50 AM	2018-08-27 8:15 AM	Log Device	This file is used to upd

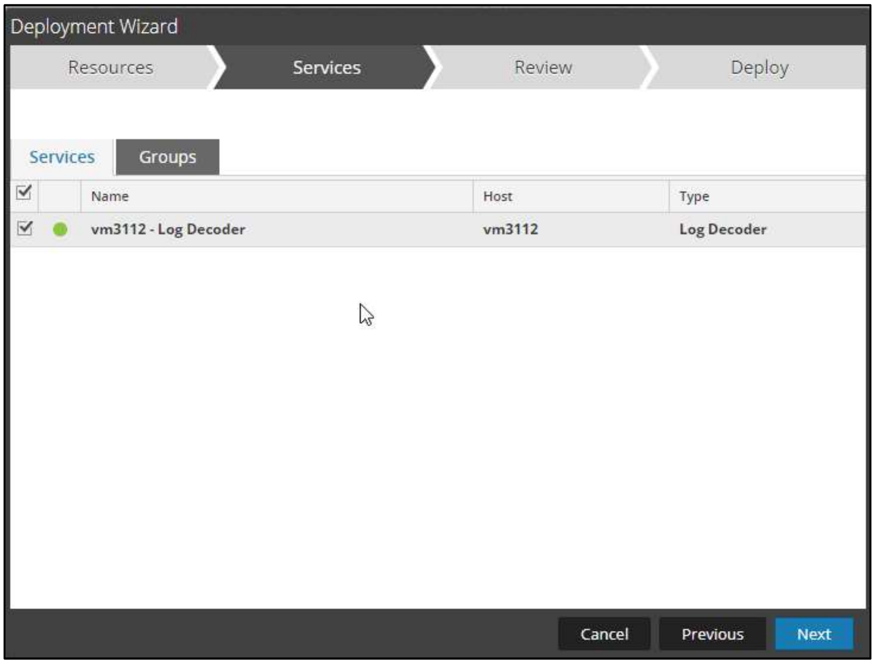
6. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency of
Envision Config File	Log Device	

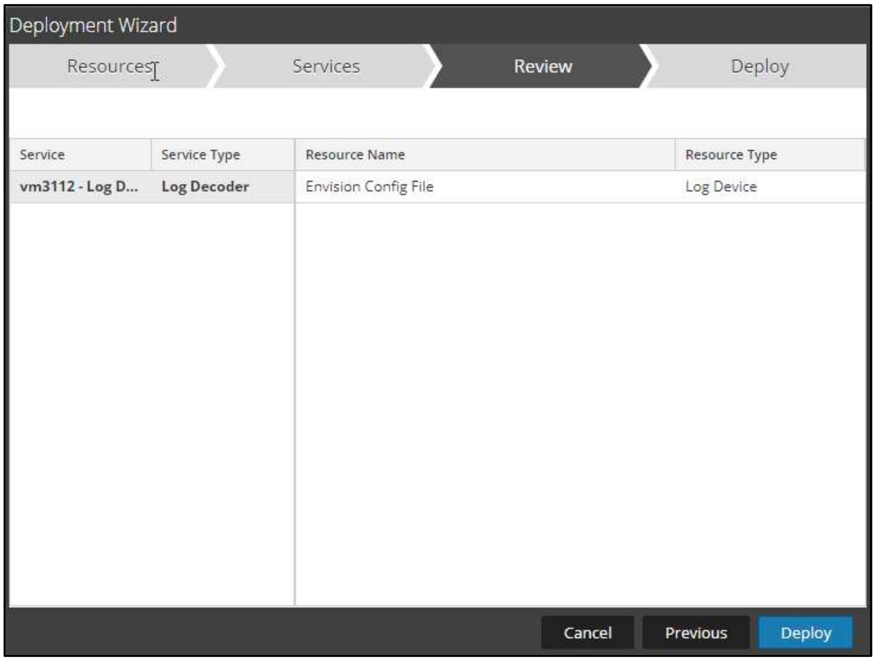
7. Select the **Log Decoder** and select **Next**.



☑		Name	Host	Type
☑	●	vm3112 - Log Decoder	vm3112	Log Decoder

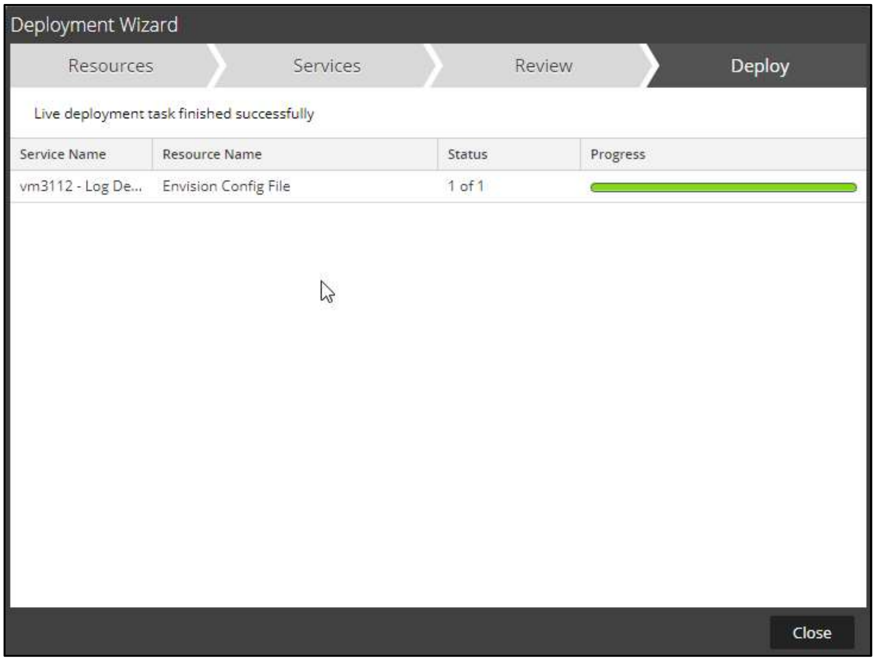
! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3112 - Log D...	Log Decoder	Envision Config File	Log Device

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



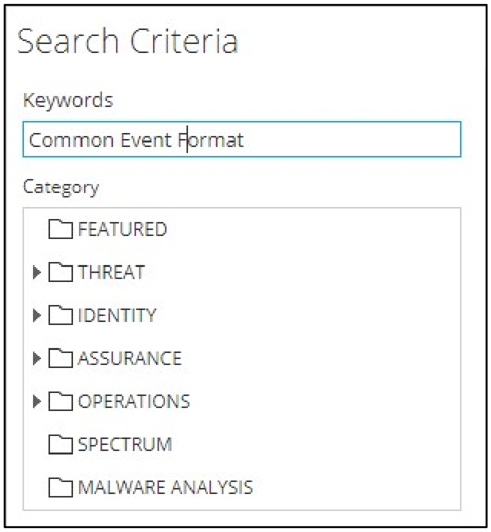
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3112 - Log De...	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:

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

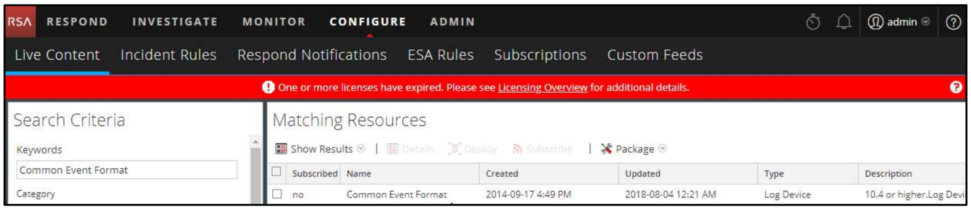


Search Criteria

Keywords: Common Event Format

.

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

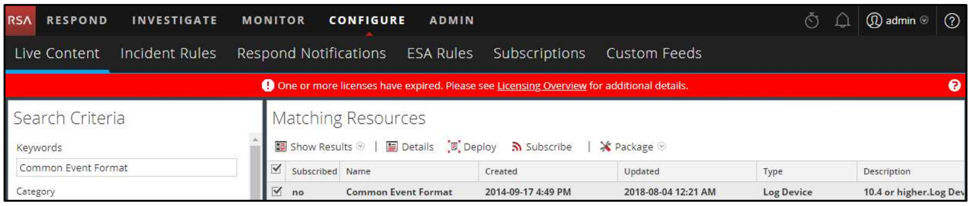


One or more licenses have expired. Please see Licensing Overview for additional details.

Keywords: Common Event Format

□	Subscribed	Name	Created	Updated	Type	Description
□	no	Common Event Format	2014-09-17 4:49 PM	2018-08-04 12:21 AM	Log Device	10.4 or higher.Log Devi

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

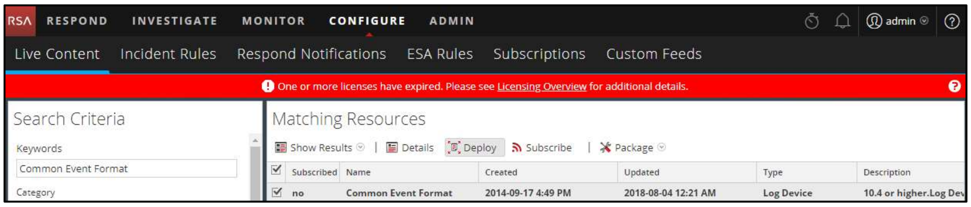


One or more licenses have expired. Please see Licensing Overview for additional details.

Keywords: Common Event Format

☑	Subscribed	Name	Created	Updated	Type	Description
☑	**no**	**Common Event Format**	**2014-09-17 4:49 PM**	**2018-08-04 12:21 AM**	**Log Device**	**10.4 or higher.Log Dev**

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

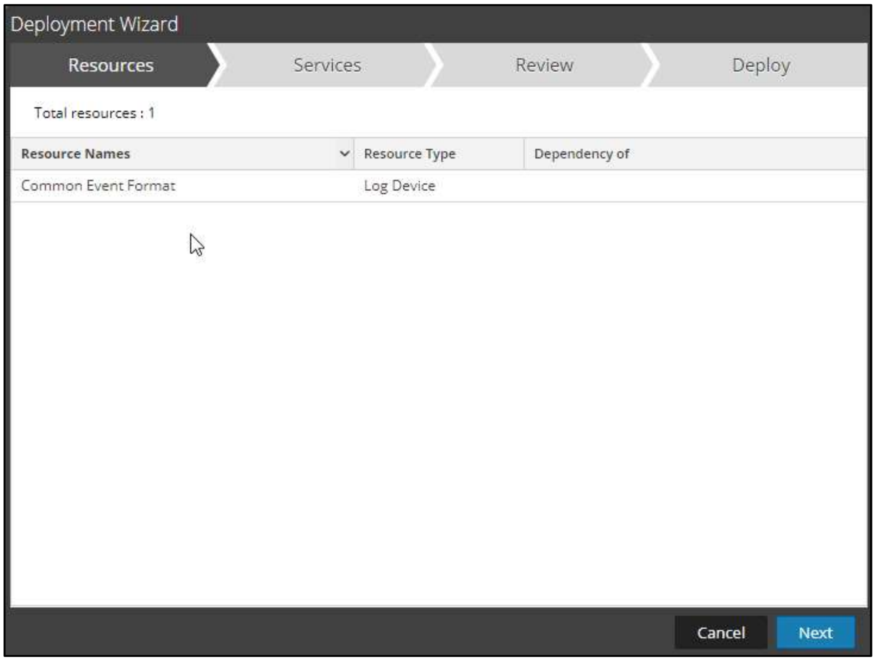


One or more licenses have expired. Please see Licensing Overview for additional details.

Keywords: Common Event Format

☑	Subscribed	Name	Created	Updated	Type	Description
☑	**no**	**Common Event Format**	**2014-09-17 4:49 PM**	**2018-08-04 12:21 AM**	**Log Device**	**10.4 or higher.Log Dev**

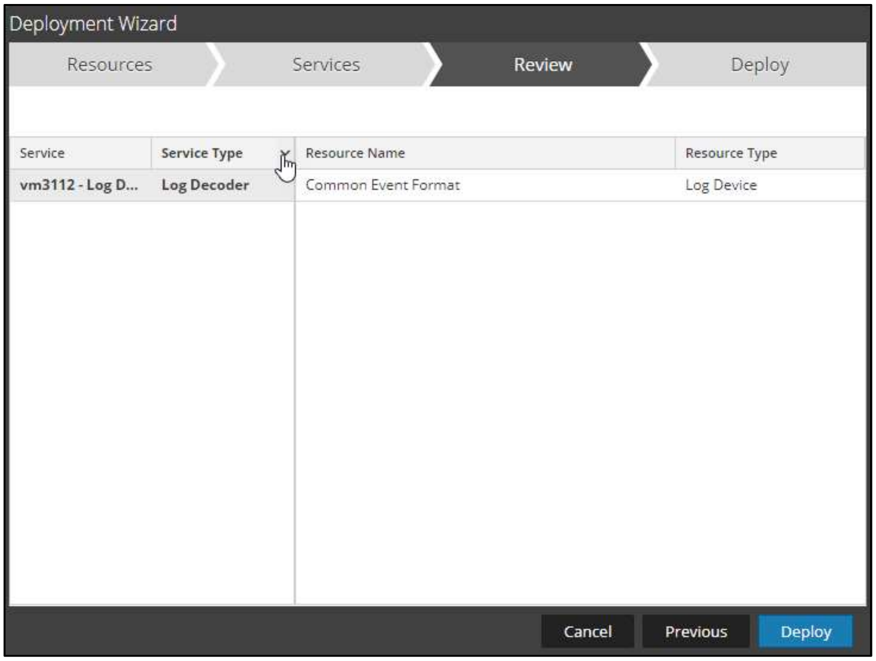
6. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency of
Common Event Format	Log Device	

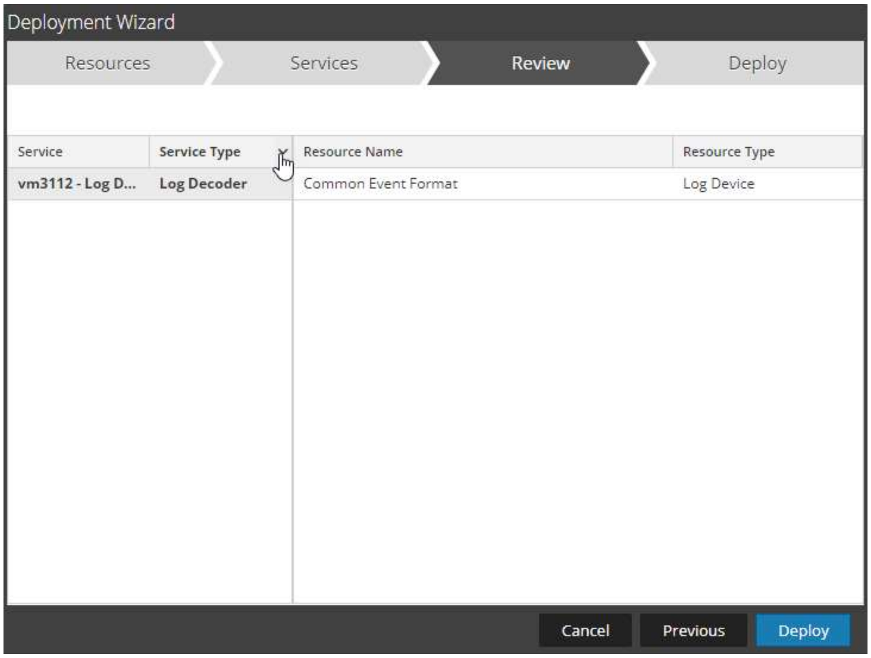
7. Select the **Log Decoder** and Select **Next**.



Service	Service Type	Resource Name	Resource Type
vm3112 - Log D...	Log Decoder	Common Event Format	Log Device

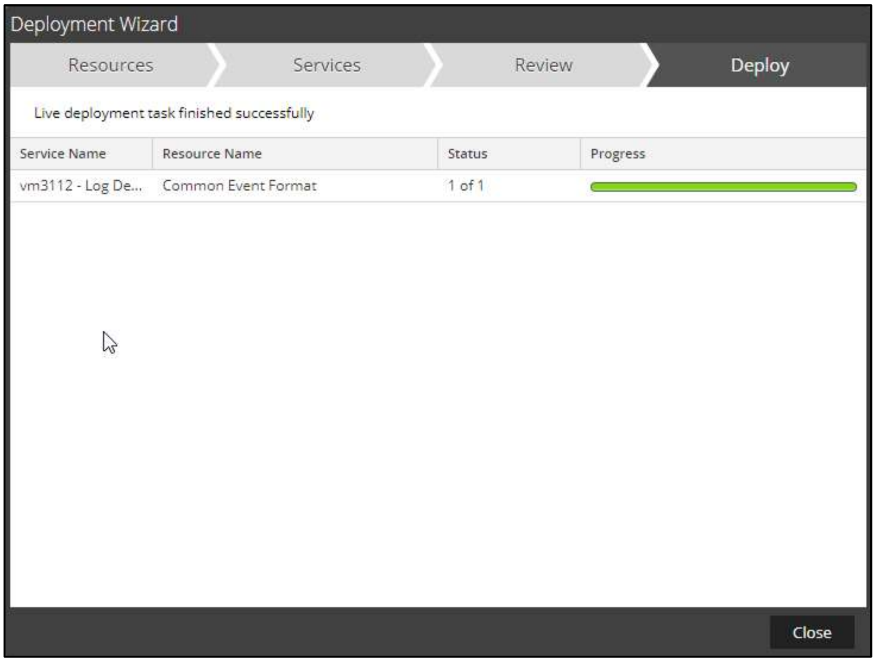
! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3112 - Log D...	Log Decoder	Common Event Format	Log Device

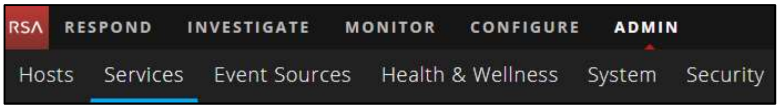
9. Select **Close**, to complete the deployment of the Common Event Format.



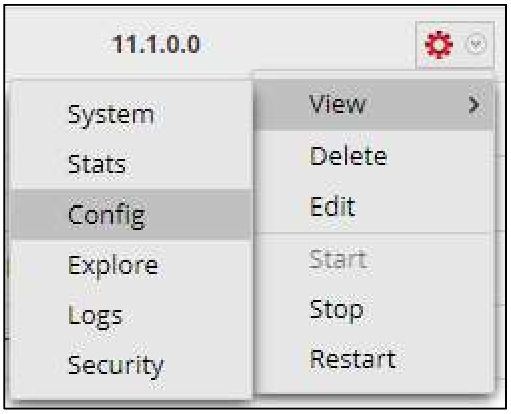
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3112 - Log De...	Common Event Format	1 of 1	🟩

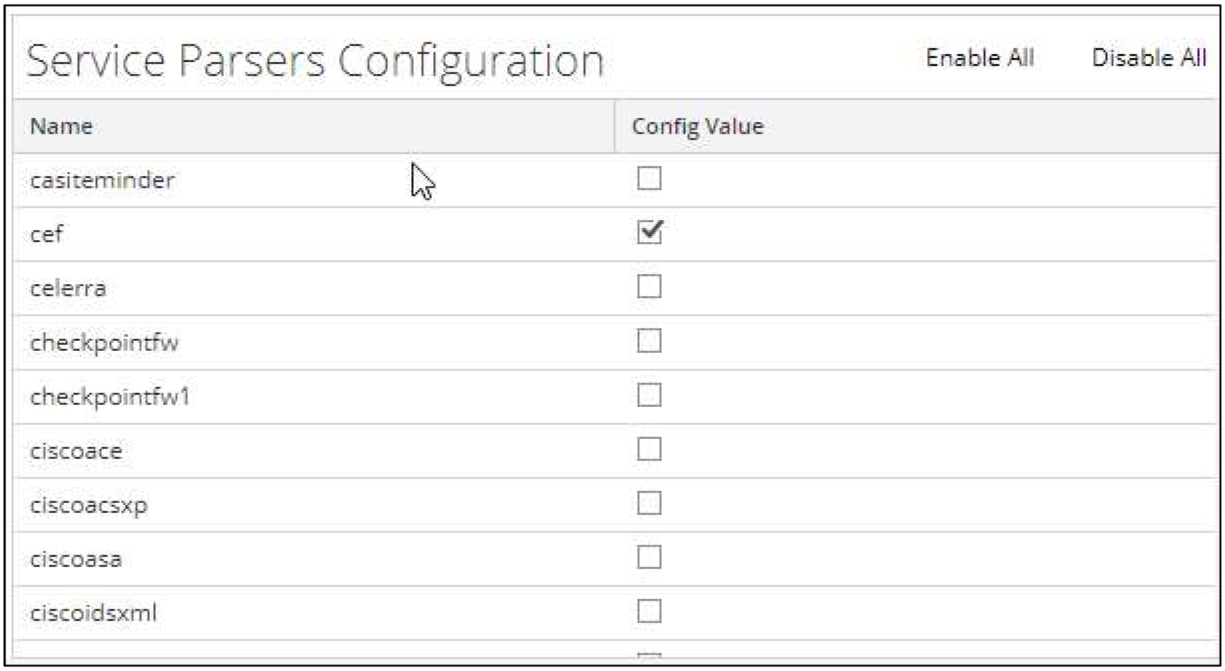
10. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Admin > Services** from the NetWitness Dashboard.



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   Enable All   Disable All

Name	Config Value
casiteminder	☐
cef	☑
celerra	☐
checkpointfw	☐
checkpointfw1	☐
ciscoace	☐
ciscoacsxp	☐
ciscoasa	☐
ciscoidsxml	☐

Edit the Common Event Format to collect Sentryo 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 an SSH connection to the NetWitness Log Decoder.
2. Locate the /etc/netwitness/ng/envision/etc/devices/cef folder. Backup **cef.xml** and edit the existing **CEF.XML** file.
3. 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
       id1="sentryo_cybervision"
       id2="sentryo_cybervision"
       functions="&lt;@event_time:*EVNTTIME($HDR,'%B %F
%Z',event_time_string)&gt;"
       content="&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
-->
<VendorProducts>
        <Vendor2Device vendor="Sentryo" product="Sentryo CyberVision"
device="sentryo_cybervision" group="SCADA"/>
</VendorProducts>
        <ExtensionKeys>
                <ExtensionKey cefName="Version" metaName="version"/>
                <ExtensionKey cefName="severity" metaName="severity"/>
                <ExtensionKey cefName="cat" metaName="category"/>
                <ExtensionKey cefName="msg" metaName="msg"/>

                <ExtensionKey cefName="smac" metaName="smacaddr"/>
                <ExtensionKey cefName="dmac" metaName="dmacaddr"/>
                <ExtensionKey cefName="src" metaName="saddr"/>
                <ExtensionKey cefName="dst" metaName="daddr"/>
                <ExtensionKey cefName="spt" metaName="sport"/>
                <ExtensionKey cefName="dpt" metaName="dport"/>

                <ExtensionKey cefName="spriv" metaName="spriv"/>
                <ExtensionKey cefName="SCVAuthorId" metaName="SCVAuthorId"/>
                <ExtensionKey cefName="SCVEventType" metaName="SCVEventType"/>
                <ExtensionKey cefName="SCVFlowId" metaName="SCVFlowId"/>

                <ExtensionKey cefName="SCVFlowControlActionValue"
metaName="SCVFlowControlActionValue"/>
                <ExtensionKey cefName="SCVFlowControlActionProcessName"
metaName="SCVFlowControlActionProcessName"/>
                <ExtensionKey cefName="SCVFlowSrcComponentId"
metaName="SCVFlowSrcComponentId"/>
                <ExtensionKey cefName="SCVFlowDstComponentId"
metaName="SCVFlowDstComponentId"/>
                <ExtensionKey cefName="SCVFlowControlActionVarName"
metaName="SCVFlowControlActionVarName"/>

                <ExtensionKey cefName="SCVUserNewValue"
metaName="SCVUserNewValue"/>
                <ExtensionKey cefName="SCVUserOldEmailValue"
metaName="SCVUserOldEmailValue"/>
                <ExtensionKey cefName="SCVUserNewAdminValue"
metaName="SCVUserNewAdminValue"/>
                <ExtensionKey cefName="SCVUserAction" metaName="SCVUserAction"/>
                <ExtensionKey cefName="SCVUserOldValue"
metaName="SCVUserOldValue"/>
                <ExtensionKey cefName="SCVUserNewEmailValue"
metaName="SCVUserNewEmailValue"/>
                <ExtensionKey cefName="SCVUserOldAdminValue"
metaName="SCVUserOldAdminValue"/>
```

```
                    <ExtensionKey cefName="SCVFlowForcedVariableVarName"
       metaName="SCVFlowForcedVariableVarName"/>
                    <ExtensionKey cefName="SCVSensorLogFlowId"
       metaName="SCVSensorLogFlowId"/>
                    <ExtensionKey cefName="SCVSensorId" metaName="SCVSensorId"/>
                    <ExtensionKey cefName="SCVSensorOldCaptureMode"
       metaName="SCVSensorOldCaptureMode"/>
                    <ExtensionKey cefName="SCVSensorNewCaptureMode"
       metaName="SCVSensorNewCaptureMode"/>
                    <ExtensionKey cefName="SCVSensorOldCustomInput"
       metaName="SCVSensorOldCustomInput"/>
                    <ExtensionKey cefName="SCVSensorAction"
       metaName="SCVSensorAction"/>
                    <ExtensionKey cefName="SCVSensorNewName"
       metaName="SCVSensorNewName"/>
                    <ExtensionKey cefName="SCVFlowCommunicationType"
       metaName="SCVFlowCommunicationType"/>
                    <ExtensionKey cefName="SCVUserId" metaName="SCVUserId"/>
                    <ExtensionKey cefName="SCVImportDataUpdateSuccess"
       metaName="SCVImportDataUpdateSuccess"/>
                    <ExtensionKey cefName="SCVImportDataMigrationRequired"
       metaName="SCVImportDataMigrationRequired"/>
                    <ExtensionKey cefName="SCVImportDataDumpFilename"
       metaName="SCVImportDataDumpFilename"/>
                    <ExtensionKey cefName="SCVExceptionLabel"
       metaName="SCVExceptionLabel"/>
                    <ExtensionKey cefName="SCVFlowLoginFailureProtocol"
       metaName="SCVFlowLoginFailureProtocol"/>
                    <ExtensionKey cefName="SCVFlowLoginFailureAttempt0"
       metaName="SCVFlowLoginFailureAttempt0"/>
                    <ExtensionKey cefName="SCVFlowLoginFailureNumberOfAttempts"
       metaName="SCVFlowLoginFailureNumberOfAttempts"/>
                    <ExtensionKey cefName="SCVFlowLoginFailureAttempt2"
       metaName="SCVFlowLoginFailureAttempt2"/>
                    <ExtensionKey cefName="SCVComponentOldName"
       metaName="SCVComponentOldName"/>
                    <ExtensionKey cefName="SCVComponentNewName"
       metaName="SCVComponentNewName"/>
                    <ExtensionKey cefName="SCVComponentPropertiesNumber"
       metaName="SCVComponentPropertiesNumber"/>
                    <ExtensionKey cefName="SCVSbsUpdateUpdated"
       metaName="SCVSbsUpdateUpdated"/>
                    <ExtensionKey cefName="SCVTokenName" metaName="SCVTokenName"/>
                    <ExtensionKey cefName="SCVTokenEnable" metaName="SCVTokenEnable"/>
                    <ExtensionKey cefName="SCVTokenAction" metaName="SCVTokenAction"/>
                    <ExtensionKey cefName="SCVTokenTokenName"
       metaName="SCVTokenTokenName"/>
                    <ExtensionKey cefName="SCVTokenTokenEnable"
       metaName="SCVTokenTokenEnable"/>
                    <ExtensionKey cefName="SCVEventMetadataNewSyslogExport"
       metaName="SCVEventMetadataNewSyslogExport"/>
                    <ExtensionKey cefName="SCVEventMetadataIsRetroactive"
       metaName="SCVEventMetadataIsRetroactive"/>
                    <ExtensionKey cefName="SCVEventMetadataOldSeverity"
       metaName="SCVEventMetadataOldSeverity"/>
                    <ExtensionKey cefName="SCVEventMetadataNewSeverity"
       metaName="SCVEventMetadataNewSeverity"/>
                    <ExtensionKey cefName="SCVEventMetadataOldSyslogExport"
       metaName="SCVEventMetadataOldSyslogExport"/>
                    <ExtensionKey cefName="SCVVulnsNumber" metaName="SCVVulnsNumber"/>
                    <ExtensionKey cefName="SCVVulns0VulnId"
       metaName="SCVVulns0VulnId"/>
                    <ExtensionKey cefName="SCVVulnId" metaName="SCVVulnId"/>
                    <ExtensionKey cefName="SCVVulnAction" metaName="SCVVulnAction"/>

             </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="starttime" nwName="start" flags="None"
format="TimeT" envisionDisplayName="StartTime"/>
       <mapping envisionName="endtime" nwName="endtime" flags="None"
format="TimeT" envisionDisplayName="EndTime,rt,end"/>

       <mapping envisionName="cat" nwName="cat" flags="None"
envisionDisplayName="cat"/>
       <mapping envisionName="msg" nwName="msg" flags="None" format="Text"
envisionDisplayName="Message"/>
       <mapping envisionName="severity" nwName="severity" flags="None"
envisionDisplayName="Severity|SeverityLevel"/>
       <mapping envisionName="smacaddr" nwName="eth.src" flags="None"
format="MAC" envisionDisplayName="SourceMacAddress"
nullTokens="Unknown|Irresolvable"/>
       <mapping envisionName="dmacaddr" nwName="eth.dst" flags="None"
format="MAC" envisionDisplayName="DestMacAddress|DestinationMacAddress"/>
       <mapping envisionName="saddr" nwName="ip.src" flags="None" format="IPv4"
envisionDisplayName="ServerAddress|SourceIPAddress|SourceAddress|Address|LocalA
ddress|ClientAddress" failureKey="ipv6.src" nullTokens="(null)|-"/>
       <mapping envisionName="daddr" nwName="ip.dst" flags="None" format="IPv4"
envisionDisplayName="ForeignAddress|DestinationAddress|DestinationIPAddress|Loc
alAddress" failureKey="ipv6.dst" nullTokens="(null)|-"/>
       <mapping envisionName="sport" nwName="ip.srcport" flags="None"
format="UInt16" envisionDisplayName="SourcePort|LocalPort|ServerPort"
nullTokens="-|(null)"/>
       <mapping envisionName="dport" nwName="ip.dstport" flags="None"
format="UInt16" envisionDisplayName="ForeignPort|DestinationPort" nullTokens="-
|(null)|null"/>

       <mapping envisionName="spriv" nwName="spriv" flags="None"/>
       <mapping envisionName="SCVAuthorId" nwName="SCVAuthorId" flags="None"/>
       <mapping envisionName="SCVEventType" nwName="SCVEventType" flags="None"/>
       <mapping envisionName="SCVFlowId" nwName="SCVFlowId" flags="None"
envisionDisplayName="SCVFlowId"/>
```

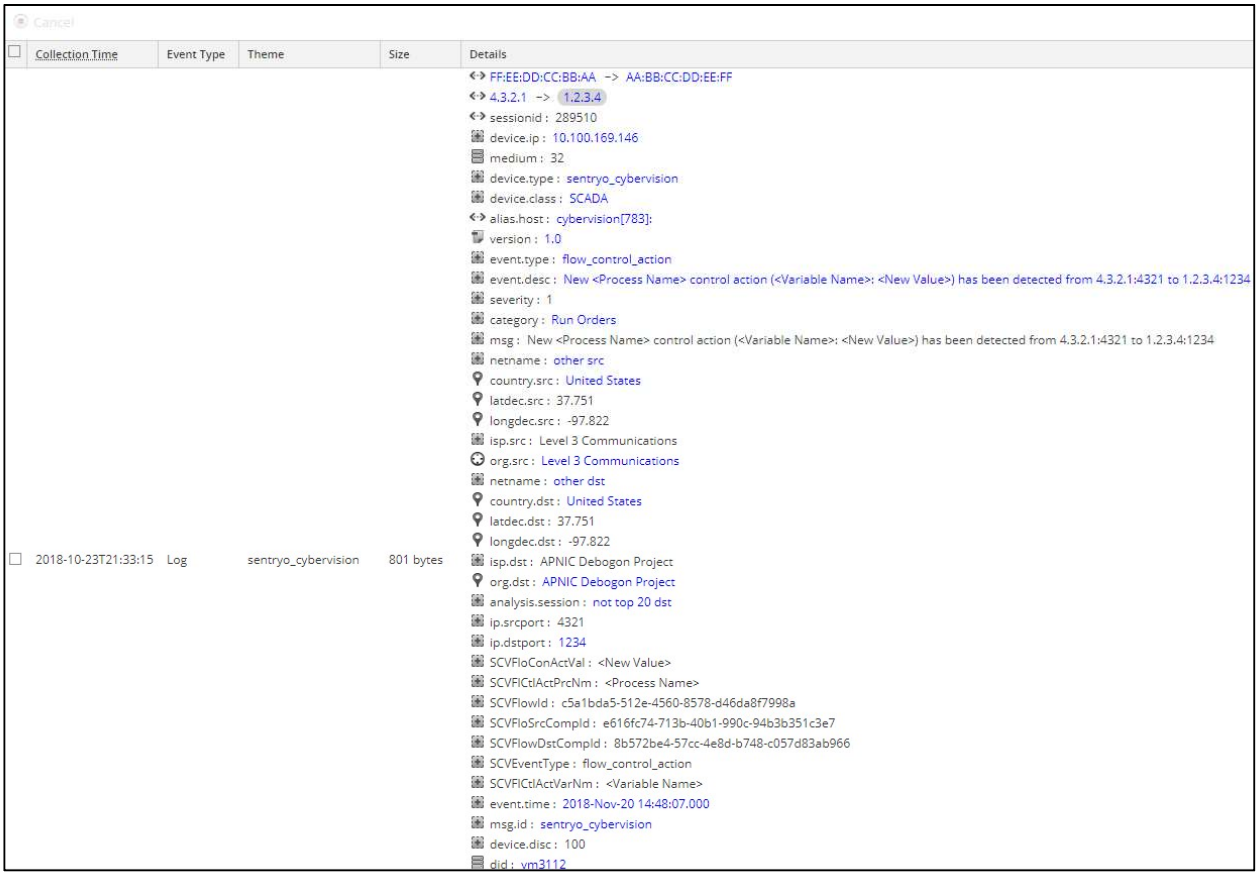
```
        <mapping envisionName="SCVFlowControlActionValue"
nwName="SCVFloConActVal" flags="None"
envisionDisplayName="SCVFlowControlActionValue"/>
        <mapping envisionName="SCVFlowDstComponentId" nwName="SCVFlowDstCompId"
flags="None"/>
        <mapping envisionName="SCVFlowSrcComponentId" nwName="SCVFloSrcCompId"
flags="None"/>
        <mapping envisionName="SCVUserNewValue" nwName="SCVUserNewValue"
flags="None"/>
        <mapping envisionName="SCVUserOldEmailValue" nwName="SCVUsrOldEmlVal"
flags="None"/>
        <mapping envisionName="SCVUserNewAdminValue" nwName="SCVUsrNewAdmVal"
flags="None"/>
        <mapping envisionName="SCVUserAction" nwName="SCVUserAction"
flags="None"/>
        <mapping envisionName="SCVUserOldValue" nwName="SCVUserOldValue"
flags="None"/>
        <mapping envisionName="SCVUserNewEmailValue" nwName="SCVUsrNewEmlVal"
flags="None"/>
        <mapping envisionName="SCVUserOldAdminValue" nwName="SCVUsrOldAdmVal"
flags="None"/>
        <mapping envisionName="SCVFlowForcedVariableVarName"
nwName="SCVFlowFVVNam" flags="None"/>
        <mapping envisionName="SCVSensorLogFlowId" nwName="SCVSnsrLgFlwId"
flags="None"/>
        <mapping envisionName="SCVSensorId" nwName="SCVSensorId" flags="None"/>
        <mapping envisionName="SCVSensorOldCaptureMode" nwName="SCVSnsrOlCapMode"
flags="None"/>
        <mapping envisionName="SCVSensorNewCaptureMode" nwName="SCVSnsrNwCapMode"
flags="None"/>
        <mapping envisionName="SCVSensorOldCustomInput" nwName="SCVSnsrOlCusInpt"
flags="None"/>
        <mapping envisionName="SCVSensorAction" nwName="SCVSensorAction"
flags="None"/>
        <mapping envisionName="SCVSensorNewName" nwName="SCVSensorNewName"
flags="None"/>
        <mapping envisionName="SCVFlowCommunicationType"
nwName="SCVFlowCommunicationType" flags="None"/>
        <mapping envisionName="SCVUserId" nwName="SCVUserId" flags="None"/>
        <mapping envisionName="SCVImportDataUpdateSuccess"
nwName="SCVImprtDUpScs" flags="None"/>
        <mapping envisionName="SCVImportDataMigrationRequired"
nwName="SCVImprtDMigrRqd" flags="None"/>
        <mapping envisionName="SCVImportDataDumpFilename"
nwName="SCVImprtDDmpFnm" flags="None"/>
        <mapping envisionName="SCVExceptionLabel" nwName="SCVExceptionLabel"
flags="None"/>
        <mapping envisionName="SCVFlowLoginFailureProtocol"
nwName="SCVFlwLgnFlPrtcl" flags="None"/>
        <mapping envisionName="SCVFlowLoginFailureAttempt0"
nwName="SCVFlwLgnFlAtmt0" flags="None"/>
        <mapping envisionName="SCVFlowLoginFailureNumberOfAttempts"
nwName="SCVFlwLgnFlNAtmt" flags="None"/>
        <mapping envisionName="SCVFlowLoginFailureAttempt2"
nwName="SCVFlwLgnFlAtmt2" flags="None"/>
        <mapping envisionName="SCVComponentOldName" nwName="SCVComponentOldName"
flags="None"/>
        <mapping envisionName="SCVComponentOldName" nwName="SCVCmpntOldName"
flags="None"/>
        <mapping envisionName="SCVComponentNewName" nwName="SCVCmpntNewName"
flags="None"/>
        <mapping envisionName="SCVComponentPropertiesNumber"
nwName="SCVCmpntPropNum" flags="None"/>
        <mapping envisionName="SCVSbsUpdateUpdated" nwName="SCVSbsUpdateUpdated"
flags="None"/>
        <mapping envisionName="SCVTokenName" nwName="SCVTokenName" flags="None"/>
        <mapping envisionName="SCVTokenEnable" nwName="SCVTokenEnable"
flags="None"/>
        <mapping envisionName="SCVTokenAction" nwName="SCVTokenAction"
flags="None"/>
```

```
        <mapping envisionName="SCVTokenTokenName" nwName="SCVTknTknName"
flags="None"/>
        <mapping envisionName="SCVTokenTokenEnable" nwName="SCVTknTknEnable"
flags="None"/>
        <mapping envisionName="SCVEventMetadataNewSyslogExport"
nwName="SCVEvntMtNwSysEx" flags="None"/>
        <mapping envisionName="SCVEventMetadataIsRetroactive"
nwName="SCVEvntMtIsRetro" flags="None"/>
        <mapping envisionName="SCVEventMetadataOldSeverity"
nwName="SCVEvntMtOlSev" flags="None"/>
        <mapping envisionName="SCVEventMetadataNewSeverity"
nwName="SCVEvntMtNwSev" flags="None"/>
        <mapping envisionName="SCVEventMetadataOldSyslogExport"
nwName="SCVEvntMtOlSyExp" flags="None"/>
        <mapping envisionName="SCVVulnsNumber" nwName="SCVVulnsNumber"
flags="None"/>
        <mapping envisionName="SCVVulns0VulnId" nwName="SCVVulns0VulnId"
flags="None"/>
        <mapping envisionName="SCVVulnId" nwName="SCVVulnId" flags="None"/>
        <mapping envisionName="SCVVulnAction" nwName="SCVVulnAction"
flags="None"/>
        <mapping envisionName="SCVFlowControlActionProcessName"
nwName="SCVFlCtlActPrcNm" flags="None"
envisionDisplayName="SCVFlowControlActionProcessName"/>
        <mapping envisionName="SCVFlowControlActionVarName"
nwName="SCVFlCtlActVarNm" flags="None"/>

</mappings>
```

4. Restart the **Log Decoder services**.

Example: Sentryo Collection Example within NetWitness Investigator:



☐	Collection Time	Event Type	Theme	Size	Details
☐	2018-10-23T21:33:15	Log	sentryo_cybervision	801 bytes	FF:EE:DD:CC:BB:AA -> AA:BB:CC:DD:EE:FF 4.3.2.1 -> 1.2.3.4 sessionid : 289510 device.ip : 10.100.169.146 medium : 32 device.type : sentryo_cybervision device.class : SCADA alias.host : cybervision[783]: version : 1.0 event.type : flow_control_action event.desc : New <Process Name> control action (<Variable Name>: <New Value>) has been detected from 4.3.2.1:4321 to 1.2.3.4:1234 severity : 1 category : Run Orders msg : New <Process Name> control action (<Variable Name>: <New Value>) has been detected from 4.3.2.1:4321 to 1.2.3.4:1234 netname : other src country.src : United States latdec.src : 37.751 longdec.src : -97.822 isp.src : Level 3 Communications org.src : Level 3 Communications netname : other dst country.dst : United States latdec.dst : 37.751 longdec.dst : -97.822 isp.dst : APNIC Debogon Project org.dst : APNIC Debogon Project analysis.session : not top 20 dst ip.srcport : 4321 ip.dstport : 1234 SCVFloConActVal : <New Value> SCVFlCtlActPrcNm : <Process Name> SCVFlowId : c5a1bda5-512e-4560-8578-d46da8f7998a SCVFloSrcCompId : e616fc74-713b-40b1-990c-94b3b351c3e7 SCVFlowDstCompId : 8b572be4-57cc-4e8d-b748-c057d83ab966 SCVEventType : flow_control_action SCVFlCtlActVarNm : <Variable Name> event.time : 2018-Nov-20 14:48:07.000 msg.id : sentryo_cybervision device.disc : 100 did : vm3112

Certification Checklist for RSA NetWitness

Date Tested: November 12, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.2	Virtual Appliance
Sentryo ICS CyberVision	2.0.3	Proprietary

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	✓

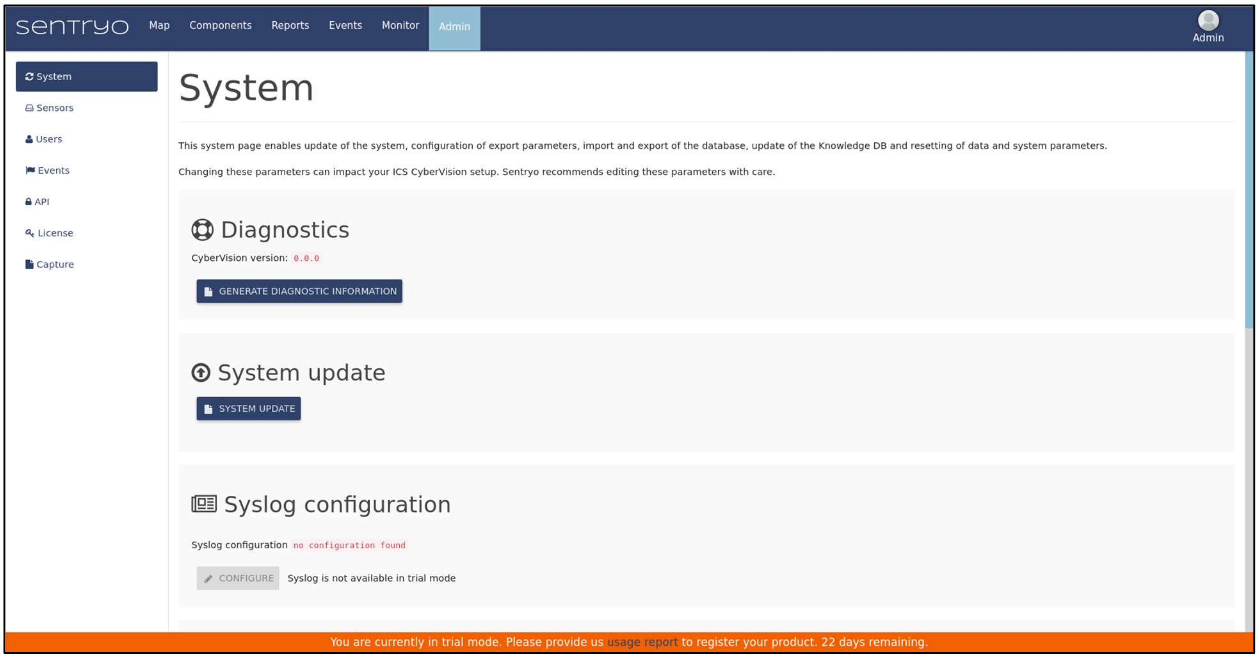
✓ = Pass ✗ = Fail N/A = Non-Available Function

Troubleshooting

If the “Configure” button is greyed out.

- This can happen when the license is not properly installed or does not enable syslog.

  Refer to https://sentryo.zendesk.com/hc/en-us/articles/207923945-Contract-Licenses for further help with licenses.



System

This system page enables update of the system, configuration of export parameters, import and export of the database, update of the Knowledge DB and resetting of data and system parameters.

Changing these parameters can impact your ICS CyberVision setup. Sentryo recommends editing these parameters with care.

Diagnostics

CyberVision version: `0.0.0`

System update

Syslog configuration

Syslog configuration `no configuration found`

Syslog is not available in trial mode

You are currently in trial mode. Please provide us usage report to register your product. 22 days remaining.

Fig 1. Screenshot of ICS CyberVision without a license, thus with syslog disabled.

If RSA NetWitness does not receive any messages from ICS CyberVision

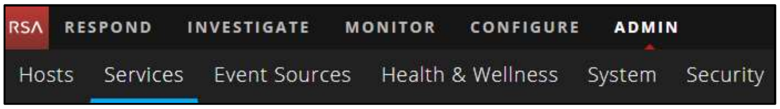
- Make sure the SIEM is connected to and reachable from the Administration interface of ICS CyberVision and not its collection interface.

Appendix

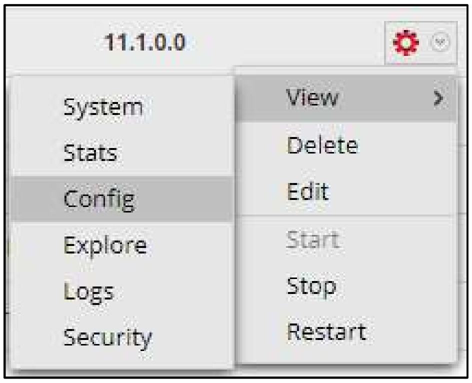
NetWitness Disable the Common Event Format Parser

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

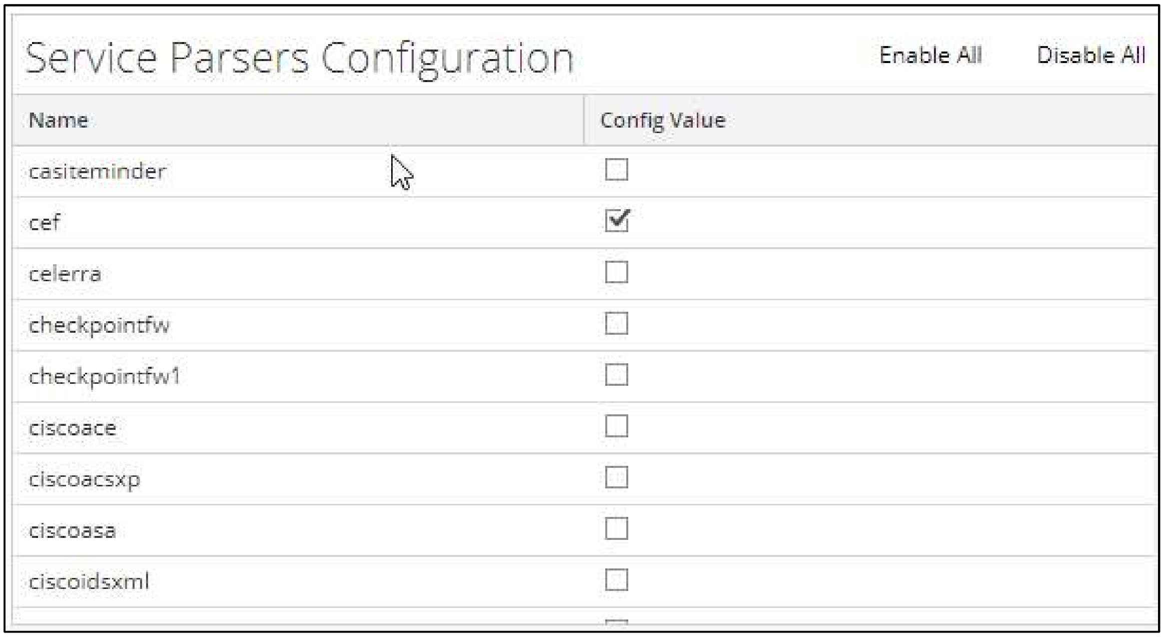
1. Select the NetWitness **Admin > Services**.



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.



Service Parsers Configuration

Enable All Disable All

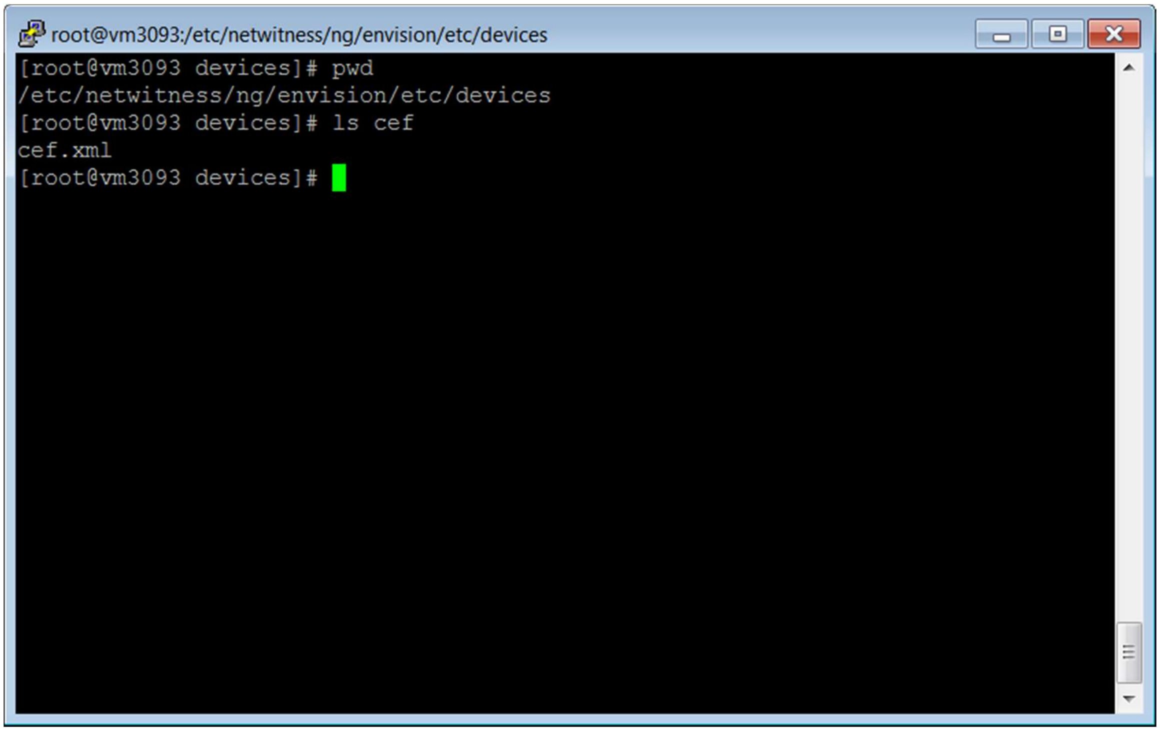
Name	Config Value
casiteminder	☐
cef	☑
celerra	☐
checkpointfw	☐
checkpointfw1	☐
ciscoace	☐
ciscoacsxp	☐
ciscoasa	☐
ciscoidsxml	☐

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.



root@vm3093:/etc/netwitness/ng/envision/etc/devices

```
[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.