RSA® NETWITNESS®
Logs
Implementation Guide

Bayshore Networks SingleKey 6.3

Jeffrey Carlson, RSA Partner Engineering

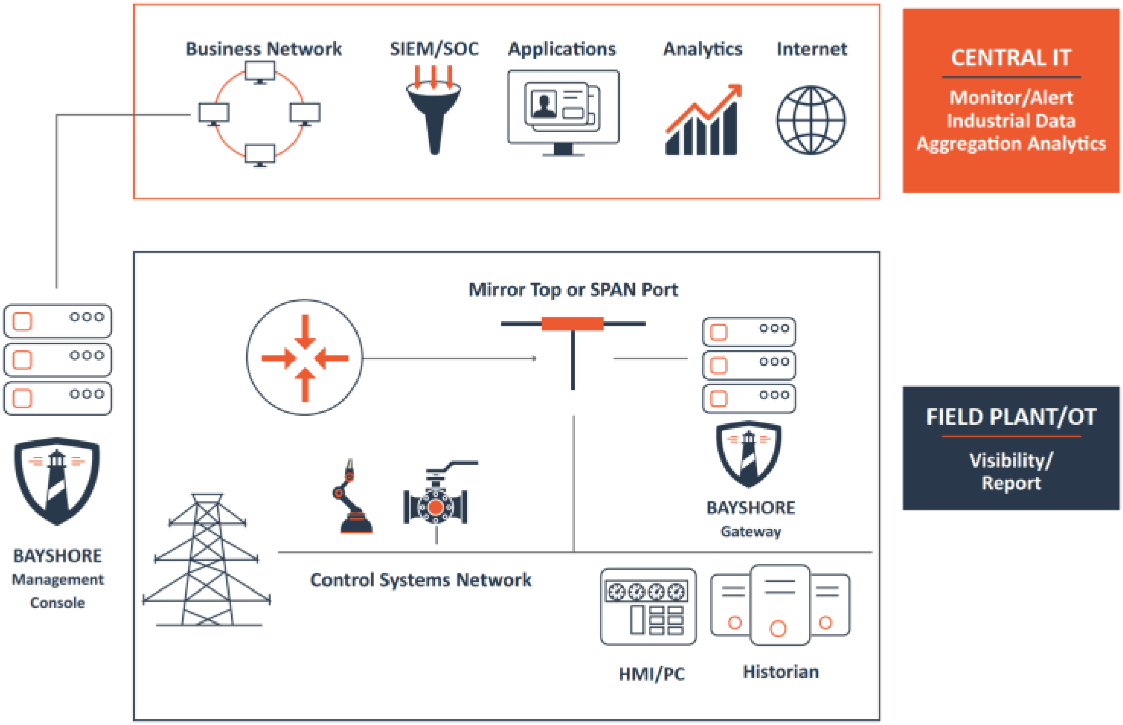
Last Modified: July 25th, 2018

Solution Summary

Today's industrial organizations are undergoing a digital transformation – connecting their informational and operational technologies in order to gain insights, intelligence and efficiencies that ultimately enhance business value. While the convergence of IT and OT environments can offer significant competitive advantages, it also exposes organizations to increased cyber threat.

Bayshore Networks SingleKey integrates with RSA Netwitness to provide IIOT and SCADA related security alerts. This gives organizations visibility into their traditional IT and OT networks, which provides unsurpassed visibility, analytics and automated response capabilities to help security teams detect, prioritize and investigate threats across their organization's entire infrastructure.

RSA NetWitness Features	
Bayshore SingleKey 6.3	
Integration package name	Common Event Format
Device display name within NetWitness	Analysis
Event source class	bayshore_singlekey
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
07/25/2018	Initial support for Bayshore Networks SingleKey.

! Important: The RSA NetWitness CEF parser is dependent on the partner adhering to the CEF Rules outlined in the *ArcSight Common Event Format (CEF) Guide*. A copy of the Common Event Format guide can be found on http://protect724.hp.com/**.**

Eg. Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]

! Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.

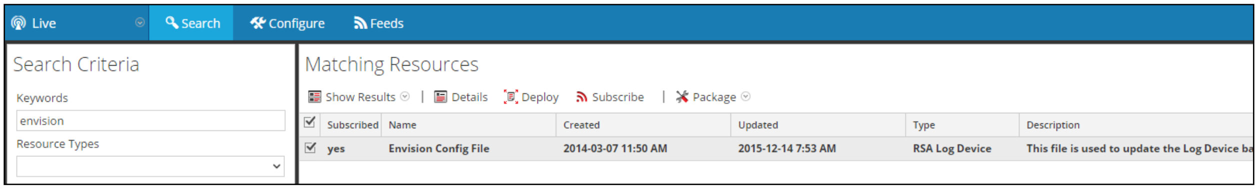
RSA NetWitness Configuration

Deploy the enVision Config File

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

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

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

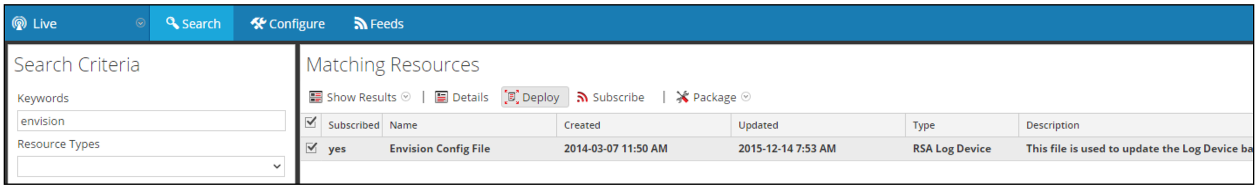


Keywords: envision

Resource Types:

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

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

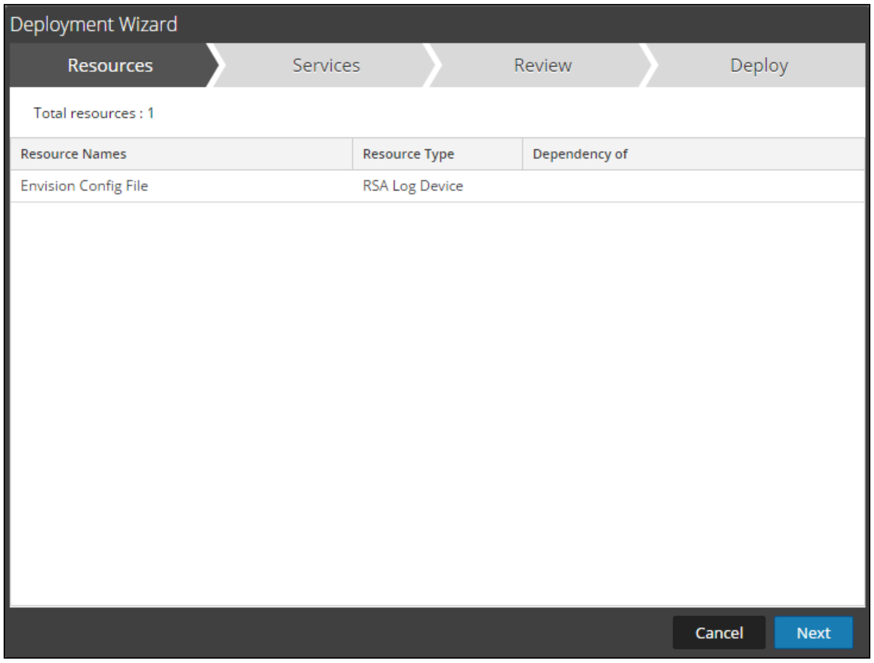


Keywords: envision

Resource Types:

☑	Subscribed	Name	Created	Updated	Type	Description
☑	yes	Envision Config File	2014-03-07 11:50 AM	2015-12-14 7:53 AM	RSA Log Device	This file is used to update the Log Device ba

6. Select **Next**.

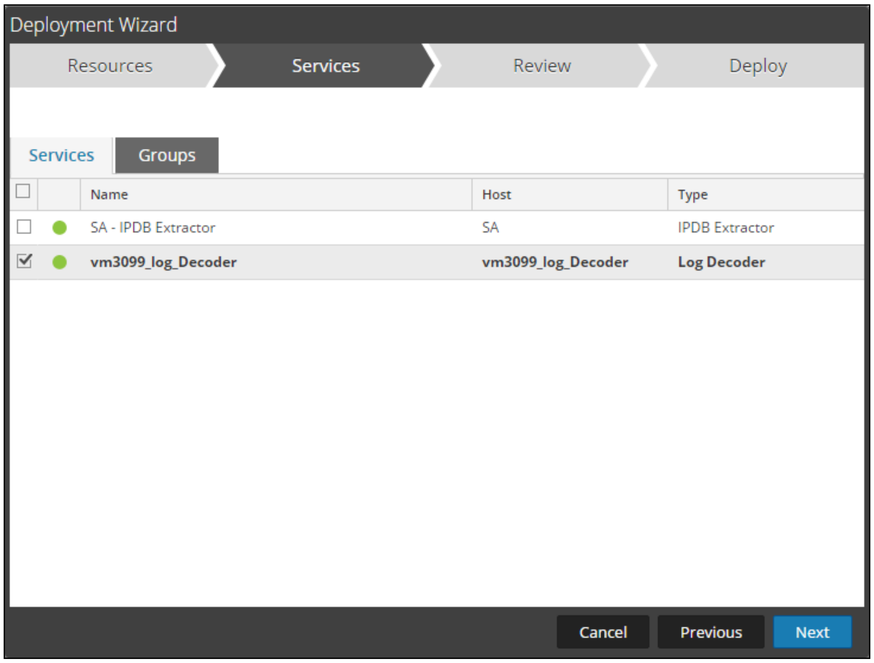


Deployment Wizard

Total resources : 1

Resource Names	Resource Type	Dependency of
Envision Config File	RSA Log Device	

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

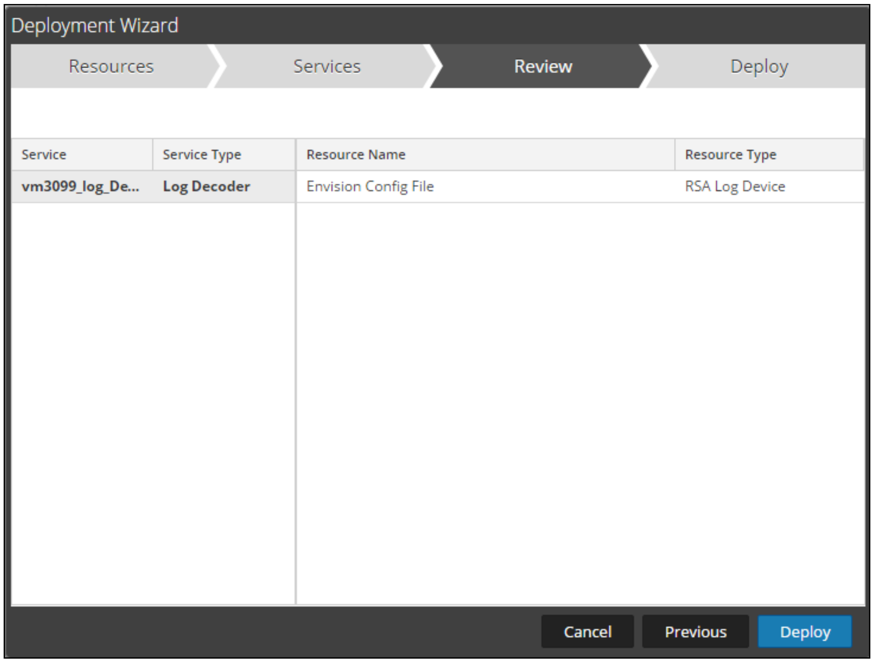


Deployment Wizard

□		Name	Host	Type
□	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	vm3099_log_Decoder	vm3099_log_Decoder	Log Decoder

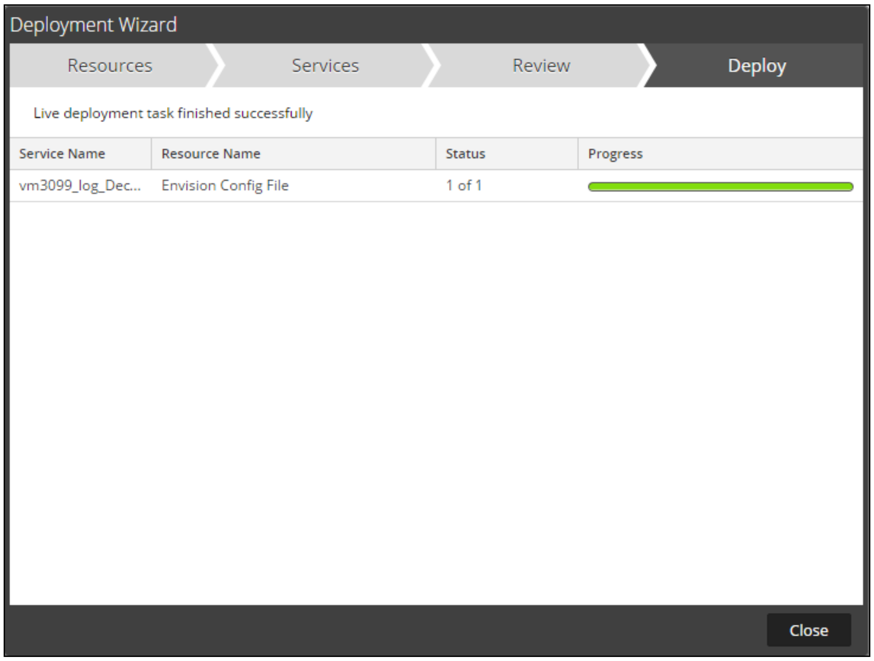
! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	Log Decoder	Envision Config File	RSA Log Device

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



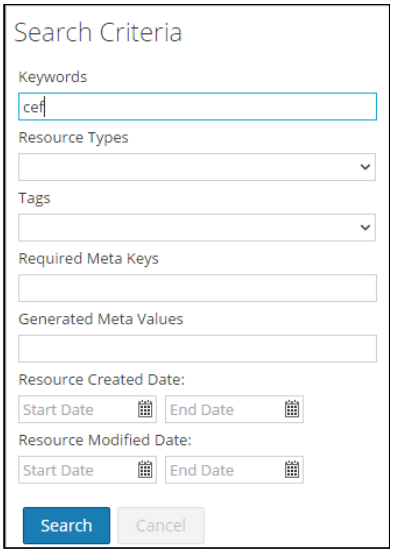
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3099_log_Dec...	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:

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



Keywords: cef

Resource Types:

Tags:

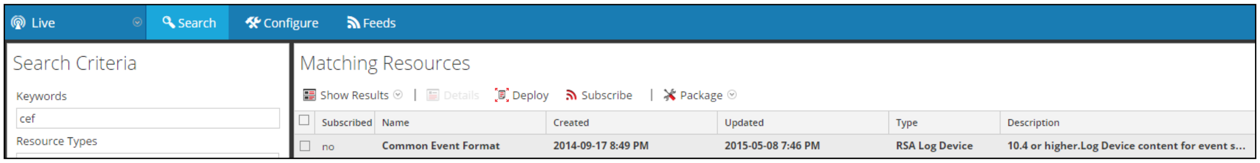
Required Meta Keys:

Generated Meta Values:

Resource Created Date: Start Date / End Date

Resource Modified Date: Start Date / End Date

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

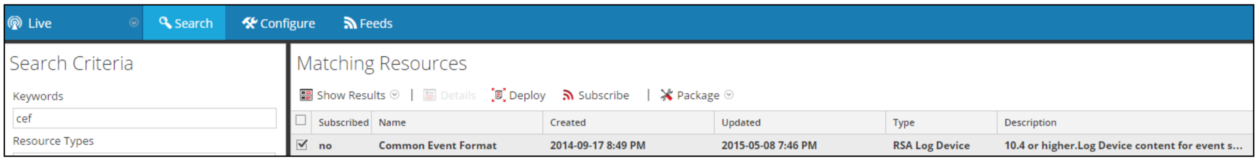


Keywords: cef

Resource Types

☐	Subscribed	Name	Created	Updated	Type	Description
☐	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

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

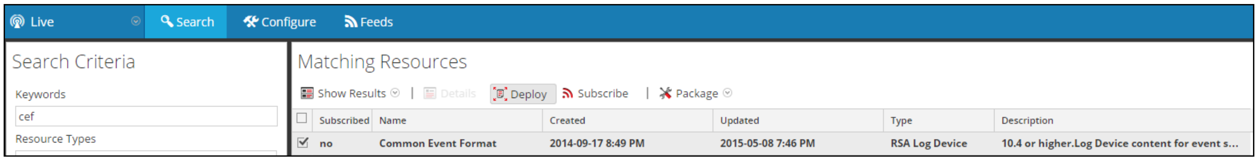


Keywords: cef

Resource Types

☐	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

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

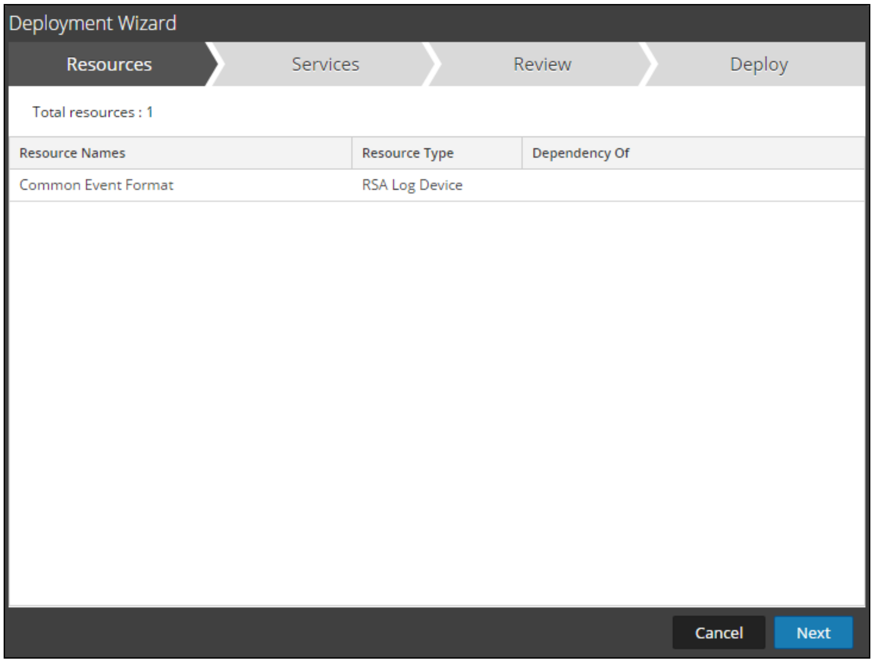


Keywords: cef

Resource Types

☐	Subscribed	Name	Created	Updated	Type	Description
☑	no	Common Event Format	2014-09-17 8:49 PM	2015-05-08 7:46 PM	RSA Log Device	10.4 or higher.Log Device content for event s...

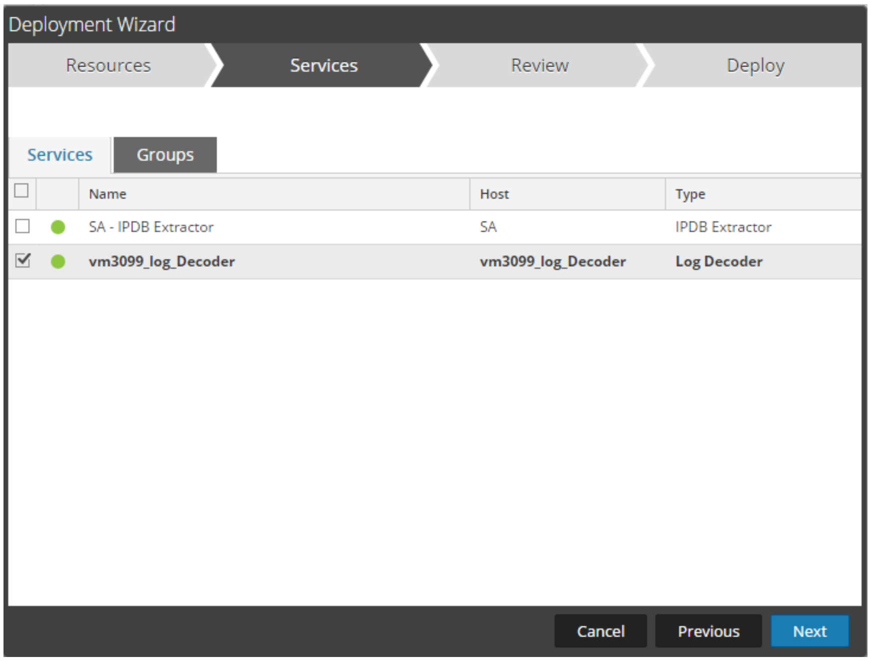
15. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency Of
Common Event Format	RSA Log Device	

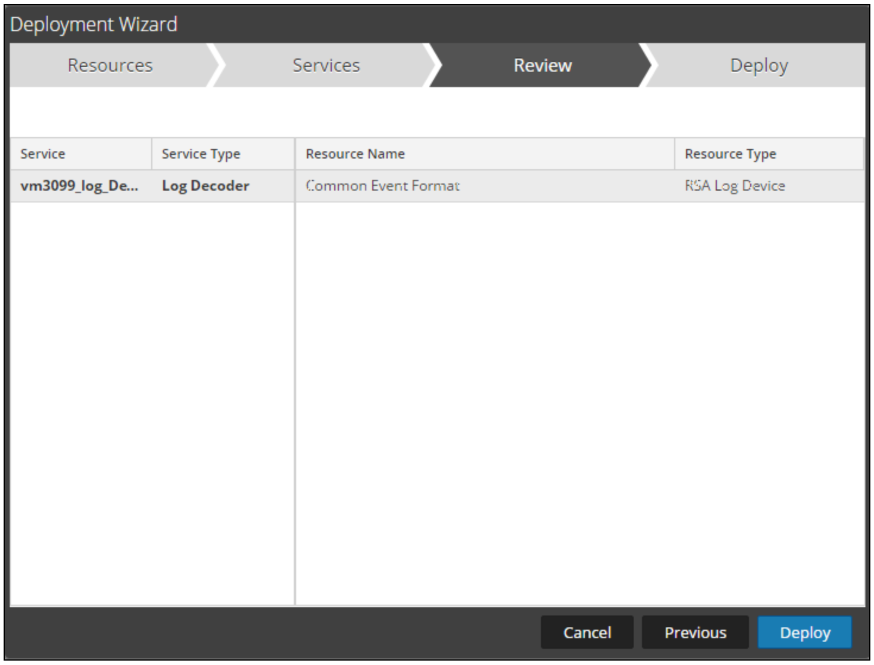
16. Select the **Log Decoder** and Select **Next**.



☐		Name	Host	Type
☐	●	SA - IPDB Extractor	SA	IPDB Extractor
☑	●	**vm3099_log_Decoder**	**vm3099_log_Decoder**	**Log Decoder**

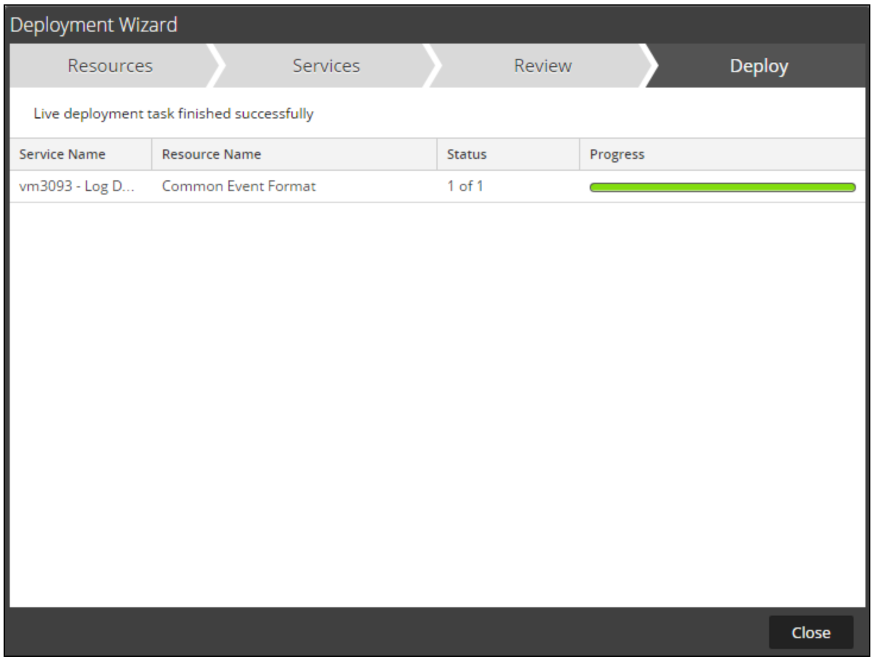
! Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

17. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3099_log_De...	Log Decoder	Common Event Format	RSA Log Device

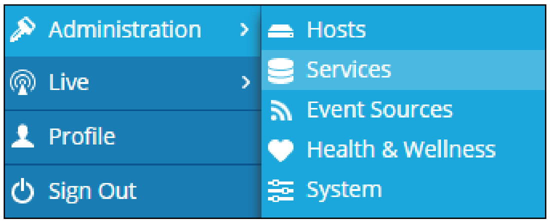
18. Select **Close**, to complete the deployment of the Common Event Format.



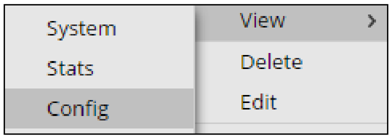
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3093 - Log D...	Common Event Format	1 of 1	🟩

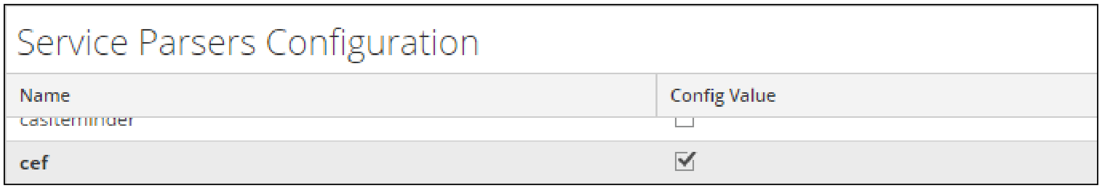
19. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



20. Locate the Log_Decoder and click the gear ⚙ to the right and select **View, Config**.



21. **Check** the box next to the cef Parser within the Service Parsers Configuration and select **Apply**.



Service Parsers Configuration

Name	Config Value
casiteminder	□
cef	☑

22. Restart the **Log Decoder services**.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Bayshore Networks SingleKey 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 Bayshore Networks SingleKey components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

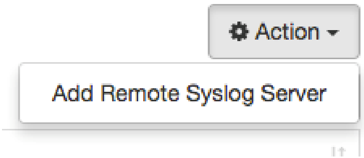
! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure <Partner> <Product> is properly configured and secured before deploying to a production environment. For more information, please refer to the <Partner> <Product> documentation or website.

Bayshore Networks SingleKey Configuration

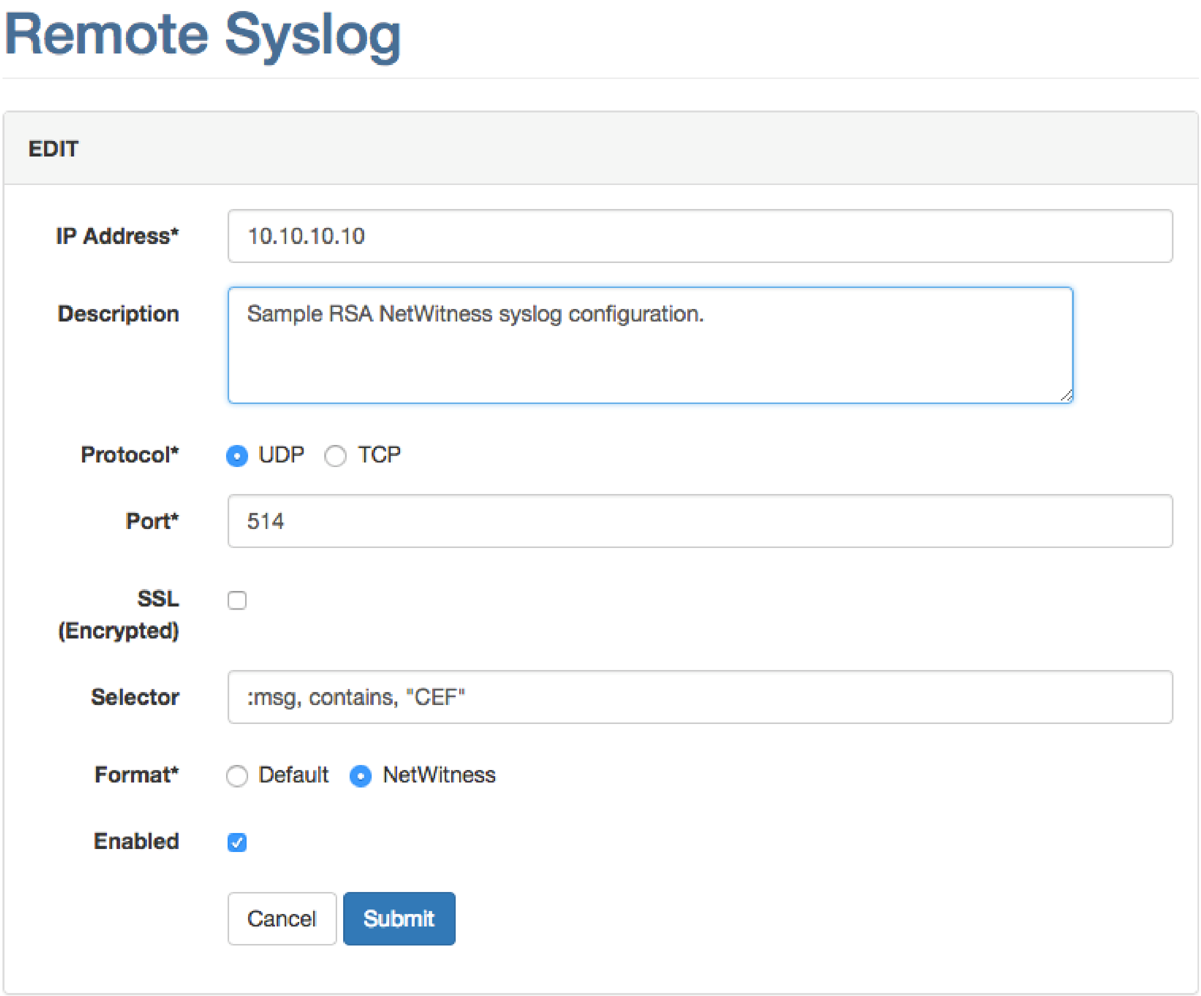
After completing the previous sections, Deploy enVision Config File and Deploy Common Event Format Content File, you can now collect events from most sources supporting the Common Event Format (CEF).

Follow these steps to configure Remote Syslog on SingleKey to send events to NetWitness using the CEF format.

1) Navigate to **External Services -> Remote Syslog** and select **Add Remote Syslog Server** from the **Actions** dropdown on the top right.



2) Fill in the SIEM parameters as followed



Remote Syslog

EDIT

IP Address*	10.10.10.10
Description	Sample RSA NetWitness syslog configuration.
Protocol*	● UDP ○ TCP
Port*	514
SSL (Encrypted)	□
Selector	:msg, contains, "CEF"
Format*	○ Default ● NetWitness
Enabled	☑

- **IP Address**

  The SIEM IPv4 address. Ex: 192.168.1.10

- **Description**

  A short description about the intended recipient of syslog messages. Ex: RSA Netwitness collector

- **Protocol**

  Choose the Protocol to be used. Syslog is typically used over UDP.

- **Port**

  The port in use by the SIEM product. The default port for syslog is 514.

- **SSL(Encrypted)**

  This only applies when TCP protocol is selected. If selected, it will encrypt the TCP stream.

- **Selector**

  You can filter which messages are sent to the SIEM product.

  Please input exactly the following for Netwitness

  :msg, contains, "CEF"

- **Format**

  Select Netwitness as the syslog format.

- **Enabled**

  Signifies if this configuration is enabled or not.

3) Select **Submit**

Edit the following files to collect Bayshore Networks SingleKey events

! Important: The cef.xml file is overwritten by NetWitness Live during updates. Please maintain a backup of the cef.xml, cef-custom.xml and table-map-custom.xml files.

Edit the cef.xml file

Use WinSCP or SSH to access the RSA Netwitness Log Decoder. Make a backup of the cef.xml file before making any edits.

Location: /etc/netwitness/ng/envision/etc/devices/cef/cef.xml

Find the end of <MESSAGE section, copy/paste the lines below and place them after the last <MESSAGE.../> entry.

```
<MESSAGE
        id1="bayshore_singlekey"
        id2="bayshore_singlekey"
        eventcategory="1901000000"
functions="&lt;@event_name:*HDR(event_description)&gt;&lt;@msg:*PARMVAL($MSG)
&gt;&lt;@event_time_string:*PARMVAL(param_event_time)&gt;"
content="&lt;param_event_time&gt;&lt;msghold&gt;"/>
```

Edit the cef-custom.xml file

Use WinSCP or SSH to access the RSA Netwitness Log Decoder. If the file exists, make a backup of the cef-custom.xml file before making any edits, otherwise create the file.

Location: /etc/netwitness/ng/envision/etc/devices/cef/cef-custom.xml

If this is a new file, then copy/paste the entirety of the code below, otherwise, only copy the require sections. Sections needed are bolded.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DEVICEMESSAGES>
    <!-- ** Please insert your custom keys or modifications below this line
** -->
    <VendorProducts>
                <Vendor2Device vendor="Bayshore" product="SingleKey"
device="bayshore_singlekey" group="Analysis"/>
    </VendorProducts>
    <ExtensionKeys>
         <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="bayshore_singlekey" metaName="policyname"
label="Policy"/>
         </ExtensionKey>
         <ExtensionKey cefName="cs2" metaName="cs_fld">
              <device2meta device="bit9" metaName="v_instafname"
              label="installerFilename"/>
              <device2meta device="bayshore_singlekey" metaName="ruleuuid"
label="Rule UID"/>
         </ExtensionKey>
   </ExtensionKeys>

</DEVICEMESSAGES>
```

Edit the table-map-custom.xml file

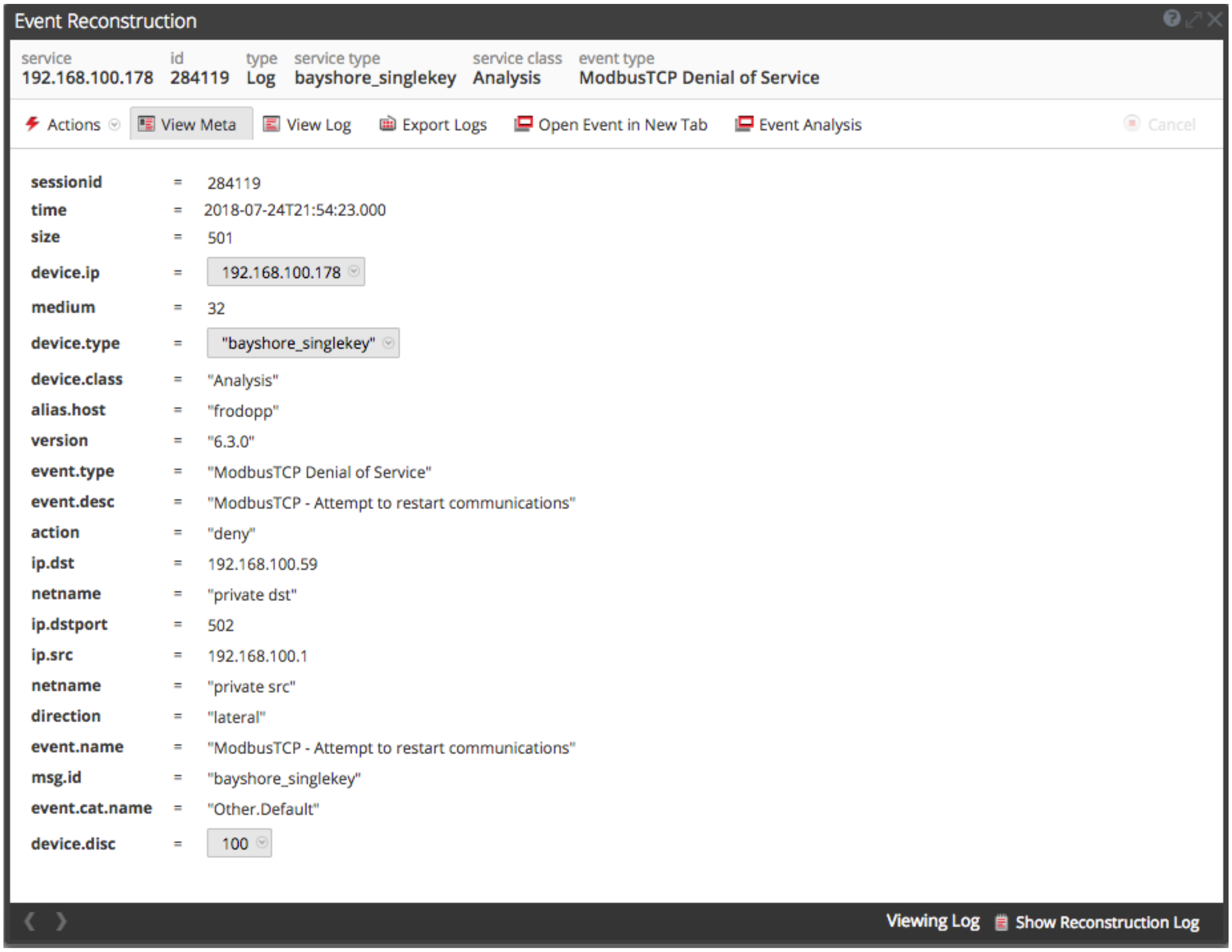
Use WinSCP or SSH to access the RSA Netwitness Log Decoder. If the file exists, make a backup of the table-map-custom.xml file before making any edits, otherwise create the file.

Location: /etc/netwitness/ng/envision/etc/table-map-custom.xml

```
<?xml version="1.0" encoding="utf-8"?>
<mappings>

<!-- Custom keys for Bayshore-->
        <mapping envisionName="BayshoreControl" nwName="BayshoreControl"
format="Text" flags="None" />
        <mapping envisionName="BayshoreOp" nwName="BayshoreOp" format="Text"
flags="None" />
</mappings>
```

RSA NetWitness Collection Example:



Event Reconstruction

service	id	type	service type	service class	event type
192.168.100.178	284119	Log	bayshore_singlekey	Analysis	ModbusTCP Denial of Service

```
sessionid      =  284119
time           =  2018-07-24T21:54:23.000
size           =  501
device.ip      =  192.168.100.178
medium         =  32
device.type    =  "bayshore_singlekey"
device.class   =  "Analysis"
alias.host     =  "frodopp"
version        =  "6.3.0"
event.type     =  "ModbusTCP Denial of Service"
event.desc     =  "ModbusTCP - Attempt to restart communications"
action         =  "deny"
ip.dst         =  192.168.100.59
netname        =  "private dst"
ip.dstport     =  502
ip.src         =  192.168.100.1
netname        =  "private src"
direction      =  "lateral"
event.name     =  "ModbusTCP - Attempt to restart communications"
msg.id         =  "bayshore_singlekey"
event.cat.name =  "Other.Default"
device.disc    =  100
```

Certification Checklist for RSA NetWitness

Date Tested: July 25th, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.1	Virtual Appliance
Bayshore SingleKey	6.3	

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