RSA® NETWITNESS®
Logs
Implementation Guide

BluVector Cortex 3.1

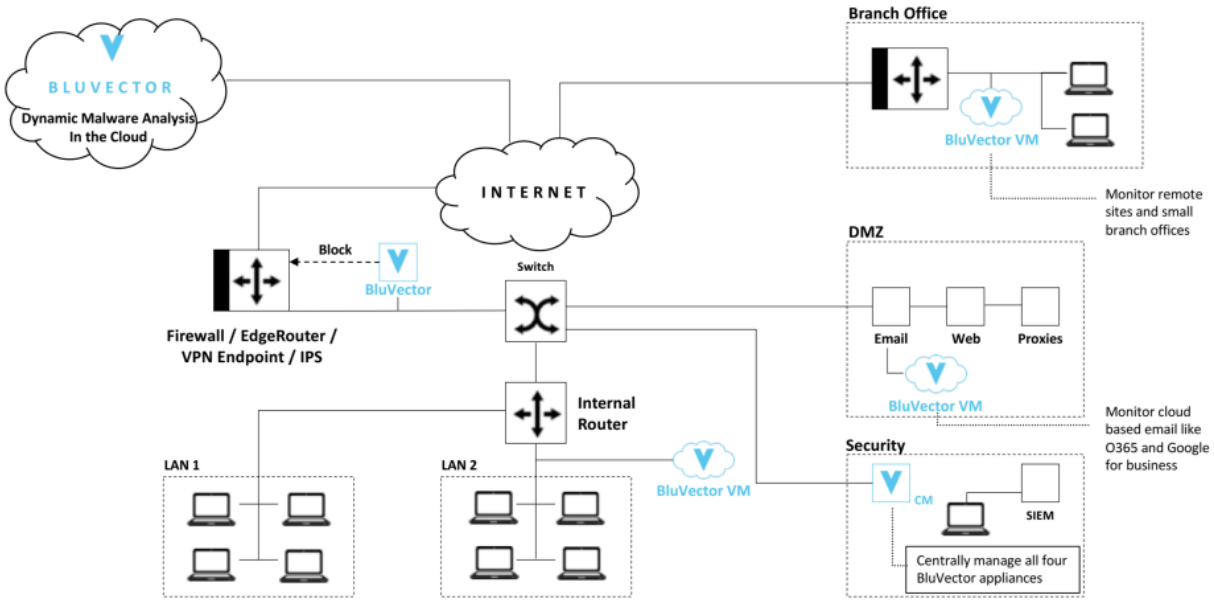
Jeffrey Carlson, RSA Partner Engineering
Last Modified: April 5th, 2017

RSA READY

Solution Summary

BluVector® Cortex™ is an AI-driven sense and response network security platform. Designed for mid-sized to very large organizations, the platform makes it possible to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware, and ransomware in real time.

RSA NetWitness Features	
BluVector Cortex	
Integration package name	Common Event Format
Device display name within NetWitness	bluvector_sensor
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
04/05/2018	Initial support for BluVector Cortex

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*.

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

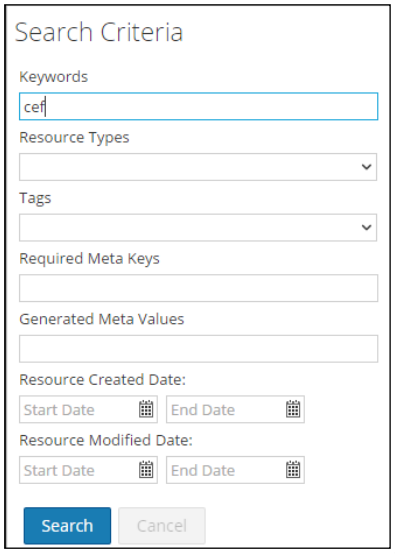
Important: The time displayed in the CEF log header is parsed into evt.time.str. No other time formats are parsed by default.

RSA NetWitness Configuration

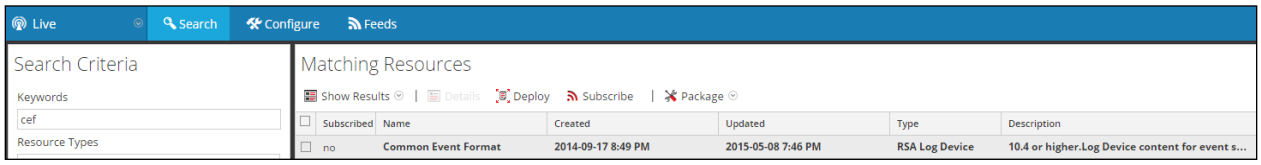
Deploy the Common Event Format (CEF) Parser

In a default installation of RSA NetWitness, the Common Event Parser (CEF) will normally already be present. If it is not installed and enabled on your Log Decoder appliance, you will need to deploy it from **RSA NetWitness Live**. To do this, log into NetWitness and perform the following actions:

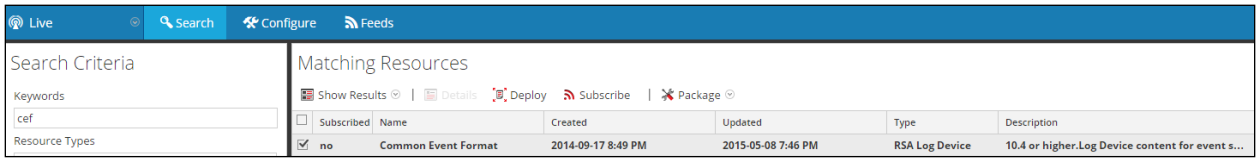
1. From the NetWitness menu, select **Live > Search**.
1. In the keywords field, enter: **CEF**



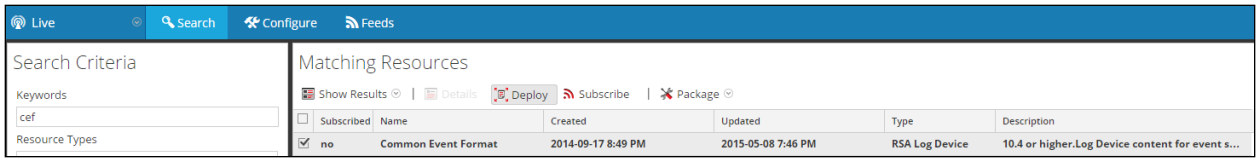
2. RSA NetWitness will display the **Common Event Format** in Matching Resources.



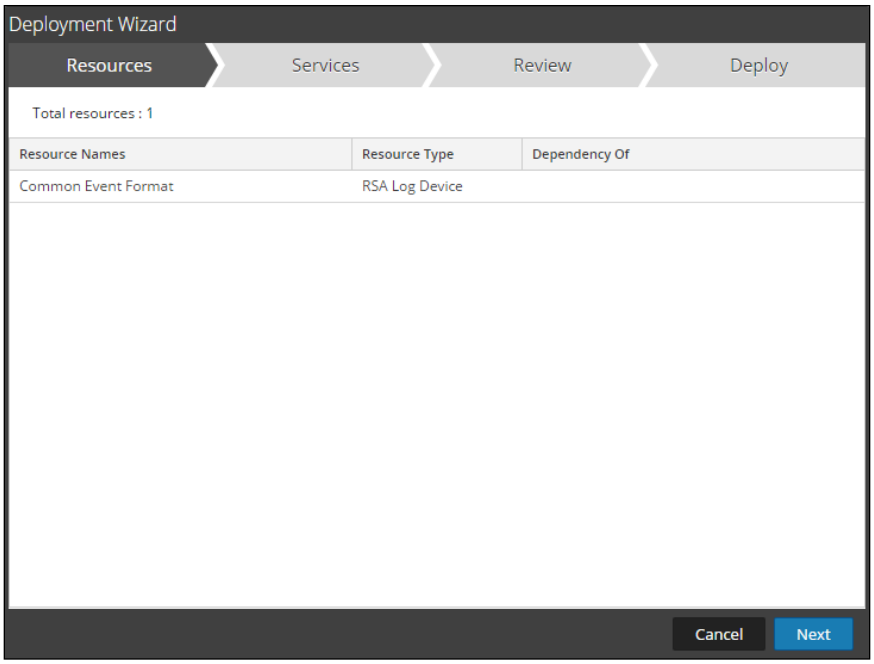
3. Select the checkbox next to **Common Event Format**.



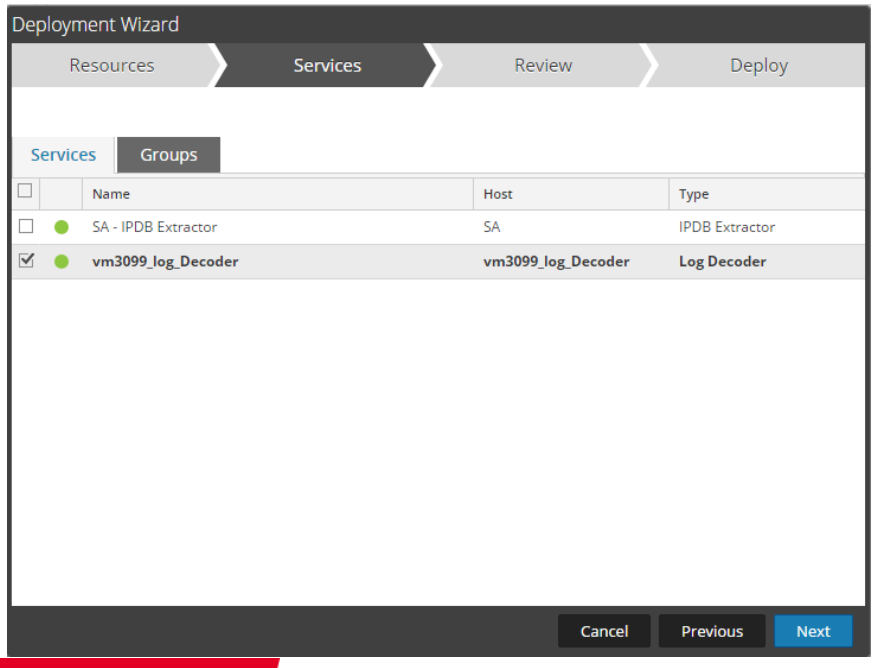
4. Click **Deploy** in the menu bar.



5. Select **Next**.

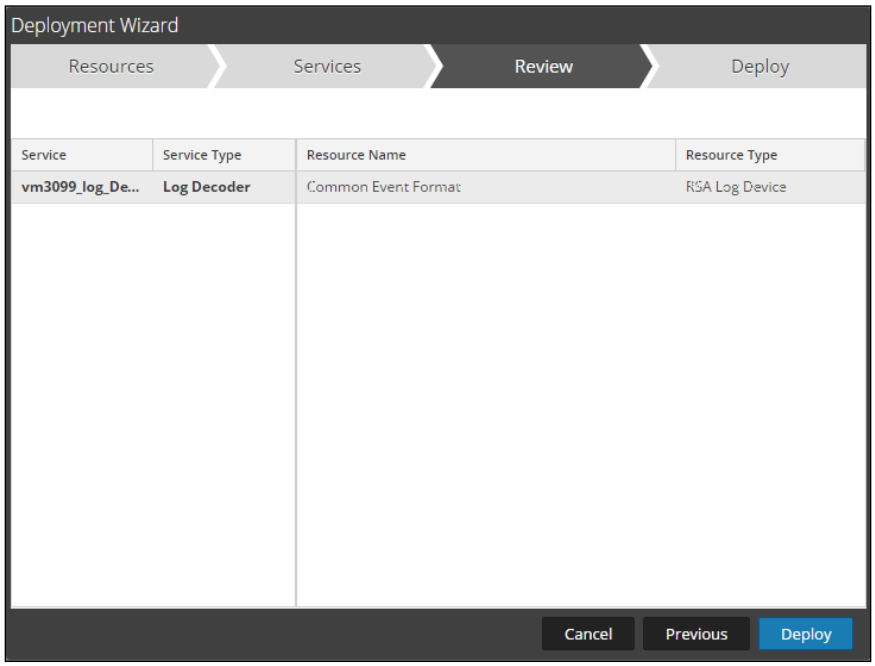


6. Select the **Log Decoder** and Select **Next**.

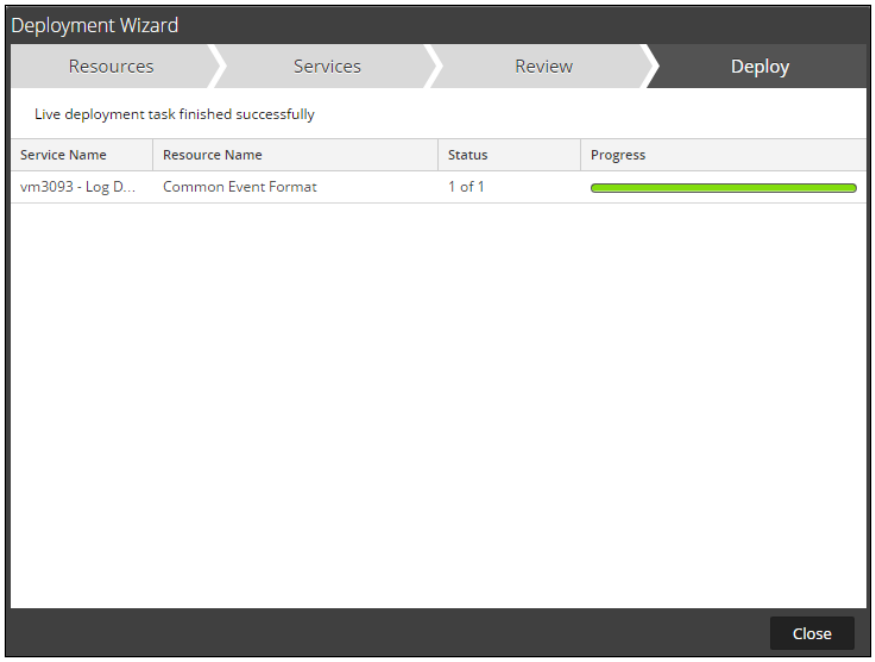


Important: In an environment with multiple Log Decoders, deploy the Common Event Format to each Log Decoder in your network.

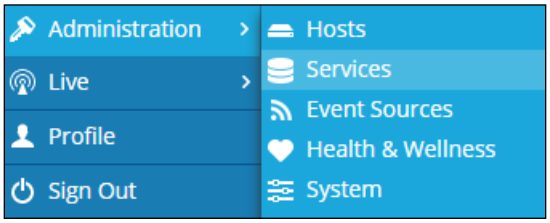
7. Select **Deploy**.



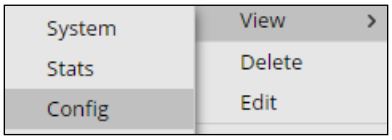
8. Select **Close**, to complete the deployment of the Common Event Format parser.



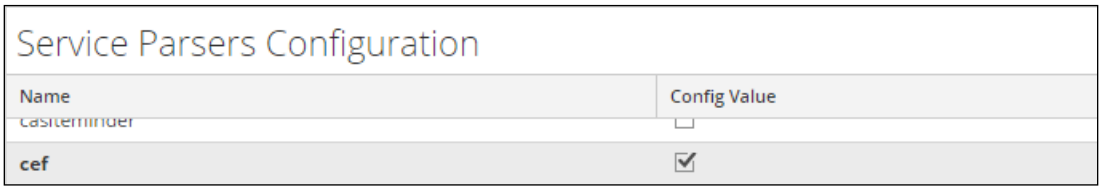
9. Ensure that the CEF Parser is enabled on the Log Decoder(s) by selecting **Administration, Services** from the NetWitness Dashboard.



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



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



12. Restart the **Log Decoder services**.

Edit the cef.xml File to add BluVector Cortex

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 add the following entry for BluVector Cortex:

```
<MESSAGE
   id1="bluvector_sensor"
   id2="bluvector_sensor"
   eventcategory="1612000000"
   functions="&lt;@msg:*PARMVAL($MSG)&gt;&lt;@event_time:*EVNTTIME($MSG,'%
   X',param_event_time)&gt;"
   content="&lt;param_event_time&gt;&lt;msghold&gt;" />
```

Edit the cef-custom.xml 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.

3. 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.
4. If this is a new **cef-custom.xml** file, copy the following into the file, otherwise copy only the required sections.

Example:

```
<VendorProducts>
      <Vendor2Device vendor="BluVector" product="Sensor"
      device="bluvector_sensor" 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="bluvector_sensor"
            metaName="collector.id" label="Collector ID"/>
      </ExtensionKey>
      <ExtensionKey cefName="cs1Label" metaName="cs_fld" />


      <ExtensionKey cefName="cs2" metaName="cs_fld">
            <device2meta device="bit9" metaName="v_instafname"
            label="installerFilename"/>
            <device2meta device="bluvector_sensor"
            metaName="mal.indicators" label="Malware Indicators"/>
```

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

<ExtensionKey cefName="cs3" metaName="cs_fld">
      <device2meta device="websense" metaName="content_type"
      label="ContentType"/>
      <device2meta device="bit9" metaName="policyname"/>
      <device2meta device="mcafeereconnex"
      metaName="content_type"/>
      <device2meta device="bluvector_sensor"
      metaName="indicator.status" label="Detailed Indicator
      Status"/>
</ExtensionKey>
<ExtensionKey cefName="cs3Label" metaName="cs_fld"/>

<ExtensionKey cefName="cs4" metaName="cs_fld">
      <device2meta device="mcafeewg" metaName="info" label="URL
      Categories"/>
      <device2meta device="bluvector_sensor" metaName="event_id"
      label="Event ID"/>
</ExtensionKey>
<ExtensionKey cefName="cs4Label" metaName="cs_fld"/>

<ExtensionKey cefName="categoryObject" metaName="cat_object"/>
<ExtensionKey cefName="categorySignificance"
metaName="cat_signif"/>
<ExtensionKey cefName="categoryDeviceGroup"
metaName="cat_device"/>
<ExtensionKey cefName="categoryOutcome" metaName="cat_outcome"/>
<ExtensionKey cefName="categoryBehavior"
metaName="cat_behavior"/>

</ExtensionKeys>
```

Edit the 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. Add the following entries to the table map to bring in the values from the `cs1` through `cs4` keys (and other custom keys):

```
<!-- Custom keys for BluVector -->
<mapping envisionName="collector.id" nwName="collector.id" flags="None"
format="Text"/>
<mapping envisionName="mal.indicators" nwName="mal.indicators" flags="None"
format="Text"/>
<mapping envisionName="indicator.status" nwName="indicator.status"
flags="None" format="Text"/>
<mapping envisionName="event_id" nwName="event.id" flags="None"
format="Text"/>
<mapping envisionName="cat_object" nwName="cat.object" flags="None"
format="Text"/>
<mapping envisionName="cat_signif" nwName="cat.signif" flags="None"
format="Text"/>
<mapping envisionName="cat_device" nwName="cat.device" flags="None"
format="Text"/>
<mapping envisionName="cat_outcome" nwName="cat.outcome" flags="None"
format="Text"/>
<mapping envisionName="cat_behavior" nwName="cat.behavior" flags="None"
format="Text"/>
```

4. There may be a number of keys that are marked as **Transient** by default that will not show up in an event unless they are changed to **None**. For example, `msg`, and `severity` are all keys that may need to be modified depending on your environment.

Edit the index-concentrator-custom.xml File

1. Using WinSCP or other application to access the RSA NetWitness Concentrator, open a connection and locate the /etc/netwitness/ng/ folder.
2. If one exists, backup the index-conecntrator-custom.xml and then edit the existing file.
3. Add the following entry to the file:

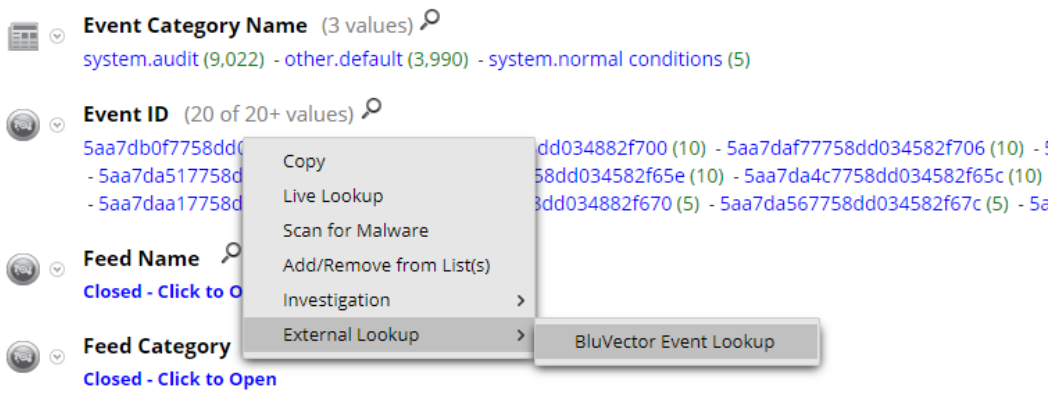
```
<!-- *** Please insert your custom keys or modifications below this line ***
-->
<key description="Event ID" format="Text" level="IndexValues" name="event.id"
valueMax="10000" defaultAction="Open"/>
```

4. This will create a custom key named **Event ID** that will be available in the Investigate -> Navigate view. By including this key, an analyst can right-click on this piece of metadata to redirect to the BluVector UI for further event details. This is done via a custom Context Menu Action for BluVector.

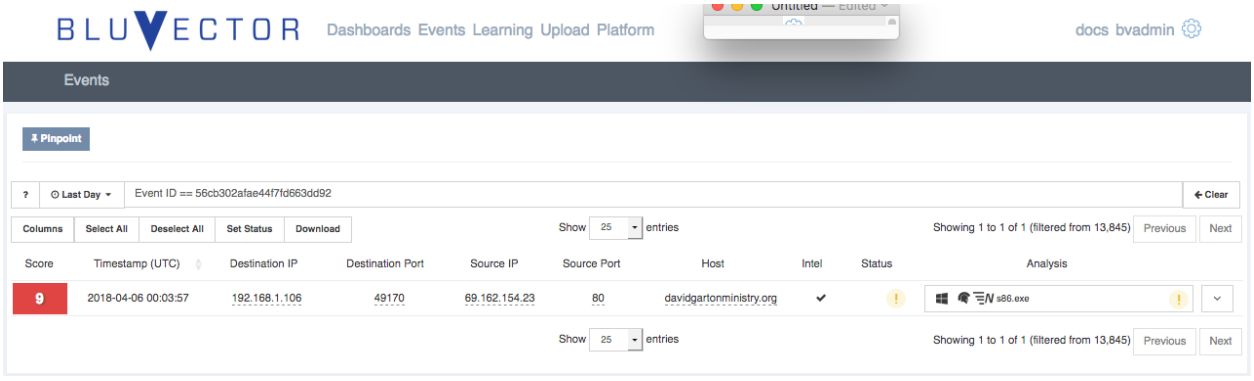
Adding a Context Menu Action for BluVector Event Lookup

In the Context Menu Actions panel of RSA NetWitness, administrators can view, add, and edit context menu actions for the current instance of NetWitness. Each context menu action applies to a specific context in the NetWitness user interface and appears as an option when you right-click a specific location in the user interface.

After a context menu action for BluVector Event Lookup is added to RSA NetWitness, users can select the Event ID of any event and right-click it to perform lookup in the BluVector UI, as shown in the figure below:



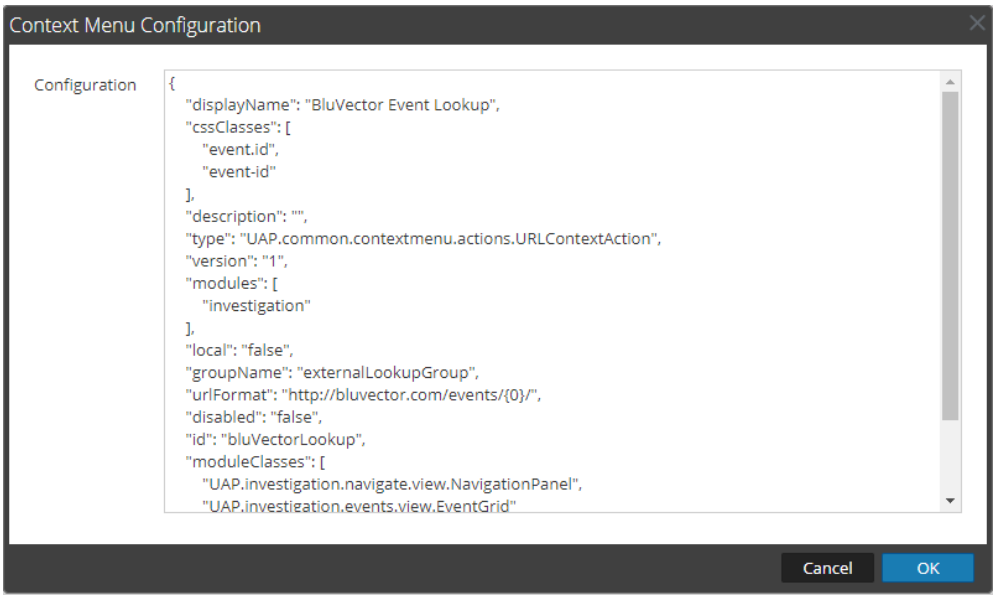
A new window will be opened in the default browser. This window will contain a lookup result for the requested Event ID within the BluVector Cortex interface:



To add this context menu action in RSA NetWitness, perform the following steps:

1. In the NetWitness menu, select **Administration > System**.
2. In the options panel, select **Context Menu Actions**.
3. In the toolbar, click the **Add** button (+).
4. The **Context Menu Configuration** dialog is displayed.

5. Enter the CSS code for the Context Menu Action (see **Appendix A**). Replace <YOUR_BLUVECTOR_SERVER_HOST> with the hostname of your BluVector server:



6. Click **OK**. The new context menu action is created and added to the end of the list of context menu actions.
7. To activate the new context menu action, reload the RSA NetWitness page in the browser. The context menu action becomes available in the form with events or in the main **Investigation** panel.

BluVector Cortex Configuration

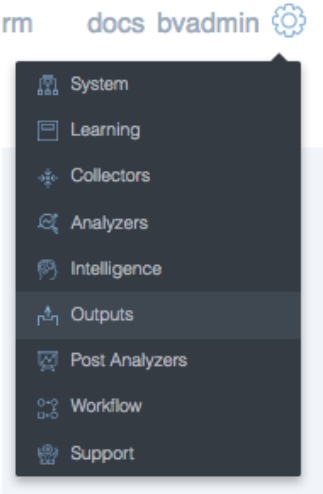
Before You Begin

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

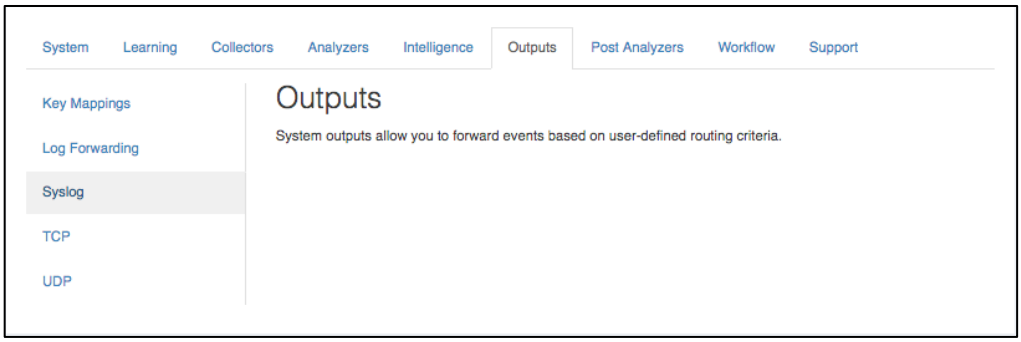
> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure BluVector Cortex is properly configured and secured before deploying to a production environment.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

Procedure: Configuring Syslog Output on BluVector Cortex

1. From the BluVector GUI, click the **Config Icon** to access the **Config Menu**, and then click the **Outputs** selection.



2. Click **Syslog** in the menu on the left



3. Enter the following configuration for the Configured Outputs:

   a. Check **Send Events** to enable the output

   b. Enter an **Output Name** for the file [*Example: BV-For-NetWitness]*

   c. Choose the **Format** option CEF

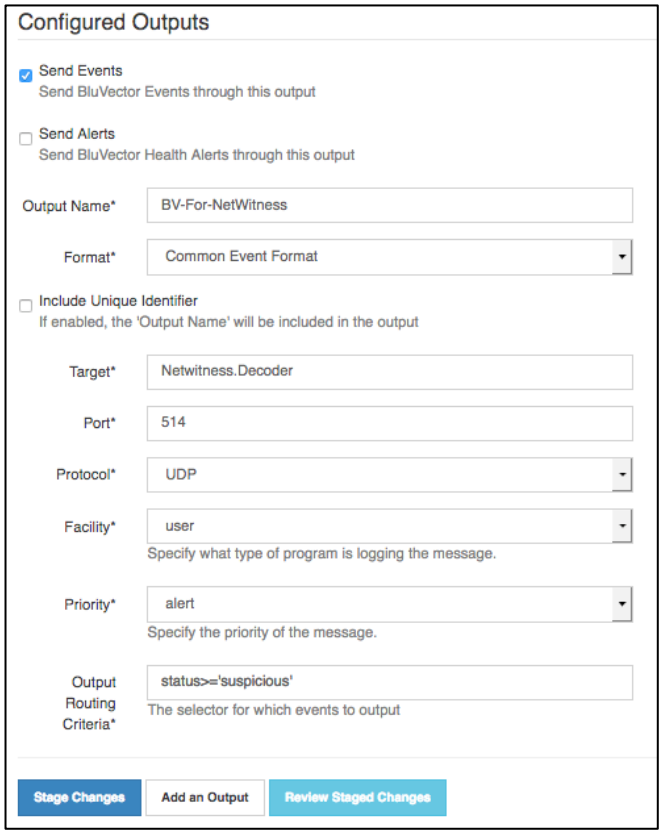
   d. Do not select **Include Unique Identifier**

   e. Enter into the **Target** field the destination for the file. This should be the hostname or IP address for the RSA NetWitness log decoder which will be receiving the generated Syslog messages.

   f. To define a port number, enter the desired port into the **Port** field

   g. Select a transport **Protocol** [*Recommended: UDP*]

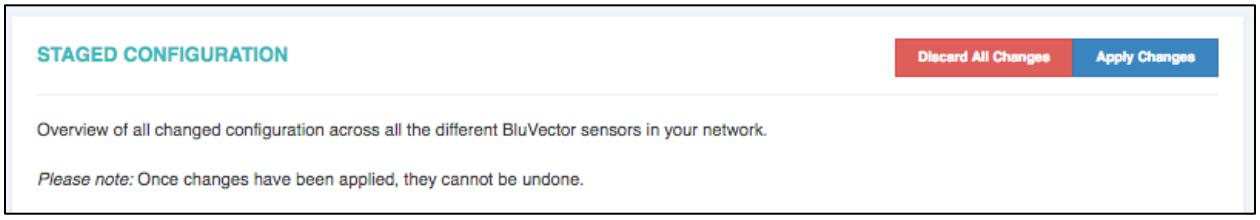
   h. The **Facility** field determines what type of program is logging the message. [*Recommended: user*]



   i. Define the Syslog priority in the **Priority** dropdown menu. [*Recommended: Alert*]

   j. Select the determination of what events to publish to syslog through the **Output Routing Criteria** option. [*Recommended: status>='suspicious'*]

4. Apply and save the new settings by clicking the **Stage Changes** button at the bottom.
5. Select **Stage Changes** when all options are selected
6. Click **Review Staged Changes** to look at all changes to be implemented in the system
7. Select **Apply Changes** to implement the new Syslog output.



Certification Checklist for RSA NetWitness

Date Tested: April 4th, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.1	Virtual Appliance
BluVector Cortex	3.1	

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 A

BluVector Context Menu Action CSS Code

```
{
    "displayName": "BluVector Event Lookup",
    "cssClasses": [
        "event.id",
        "event-id"
    ],
    "description": "",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "1",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "externalLookupGroup",
    "urlFormat": "https://<YOUR_BLUVECTOR_SERVER_HOST>/events/{0}/",
    "disabled": "false",
    "id": "bluVectorLookup",
    "moduleClasses": [
        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
    ],
    "openInNewTab": "true",
    "order": "11"
}
```