



# RSA NetWitness Endpoint Integration Guide

for Version 11.0



## **Contact Information**

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## **Trademarks**

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

## **Third-Party Licenses**

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

## **Note on Encryption Technologies**

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## **Distribution**

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

November 2017

# Contents

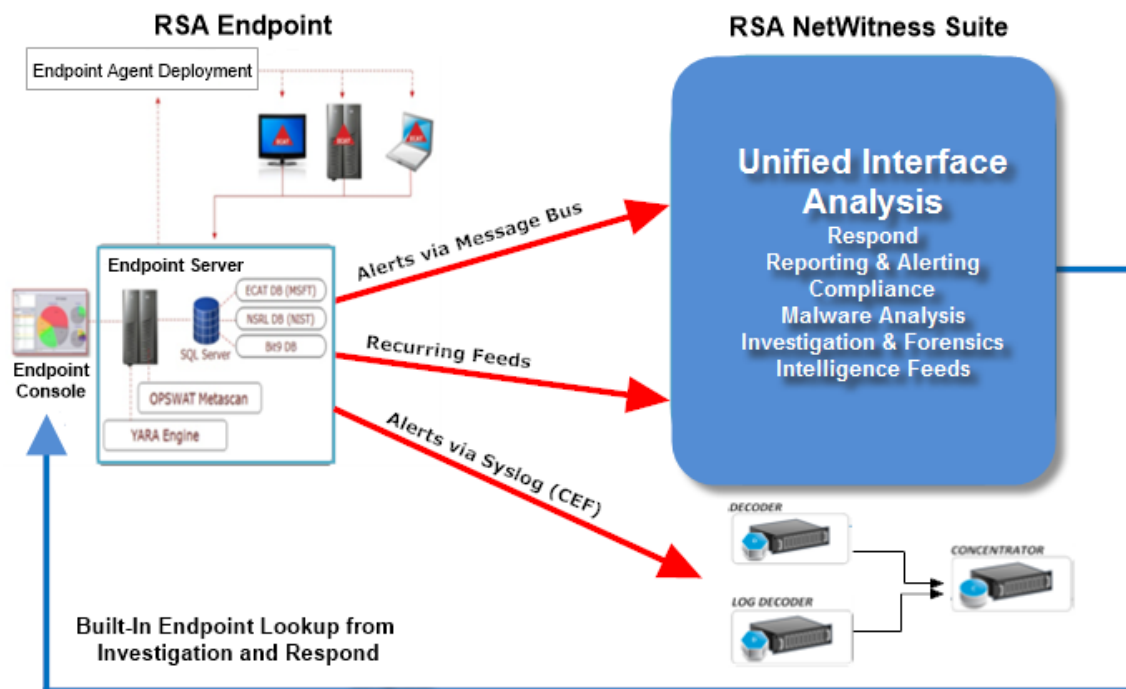
---

<b>RSA NetWitness Endpoint Integration .....</b>	<b>4</b>
Integration Options .....	4
Built-in NetWitness Endpoint Lookup .....	4
Integration Methods .....	5
NetWitness Endpoint Meta Integration .....	6
NetWitness Endpoint Alerts and Indicators of Compromise .....	6
<b>Configure NetWitness Endpoint Alerts via Message Bus .....</b>	<b>7</b>
Configure NetWitness Endpoint to Forward NetWitness Endpoint Alerts .....	8
<b>Configure Contextual Data from NetWitness Endpoint via Recurring Feed .....</b>	<b>11</b>
Enable the NetWitness Endpoint Feed for NetWitness Suite .....	12
Export the NetWitness Endpoint SSL Certificate .....	15
Configure the NetWitness Suite Concentrator Service .....	16
Configure the Recurring Custom Feed Task in NetWitness Suite .....	17
<b>Configure Endpoint Alerts via Syslog into a Log Decoder .....</b>	<b>22</b>
Configure NetWitness Endpoint to Send Syslog Output to NetWitness Suite .....	23
Edit the Table Mapping in table-map-custom.xml .....	24
Configure the NetWitness Suite Concentrator Service .....	27

# RSA NetWitness Endpoint Integration

RSA customers who are using RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 can integrate NetWitness Endpoint and RSA NetWitness Suite in several different ways. This guide is for RSA NetWitness Suite version 11.0.

## Integration Options



## Built-in NetWitness Endpoint Lookup

With the RSA NetWitness Endpoint user interface (UI) installed on the same machine where the analyst is using a browser to access NetWitness Suite, the built-in NetWitness Endpoint Lookup from NetWitness Suite Investigation and NetWitness Suite Respond provides right-click access to the NetWitness Endpoint console server for the following meta keys: IP address (ip-src, ip-dst, ipv6-src, ipv6-dst, orig\_ip), host (alias-host, domain.dst), client, and file-hash. These are described in the "Launch an External Lookup of a Meta Key" topic in *Investigation and Malware Analysis User Guide* and the "View Alerts" topic in *NetWitness Respond User Guide*.

NetWitness Suite configuration is not required for endpoint lookup when you are using one of the built-in parsers, NetWitness Endpoint or CEF, and you have not customized the default meta keys used when loading metadata in Investigation. For more information, see "Manage and Apply Default Meta Keys in an Investigation" topic in the *Investigation and Malware Analysis User Guide*.

**Note:** The exception occurs if you customize NetWitness Suite by editing the display setting for the default meta keys in Investigation, add meta keys to the table-map-custom.xml file, or customize NetWitness Endpoint feeds. Some configuration is required to add the custom meta keys to the context menu NetWitness Endpoint Lookup in the **ADMIN > System** view as described in the "Add Custom Context Menu Actions" topic in the *System Configuration Guide*.

## Integration Methods

With an RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 console server installed on a Windows host and proper configuration of NetWitness Endpoint and NetWitness Suite by an administrator, three additional integrations of NetWitness Endpoint analysis data are possible.

The following are the RSA NetWitness Endpoint integration methods:

- Configure Endpoint Alerts via Message Bus
- Configure Contextual Data from Endpoint via Recurring Feed
- Configure Endpoint Alerts via Syslog into a Log Decoder

**Endpoint alerts via message bus into NetWitness Respond.** This integration provides the capability for forwarding Endpoint alerts to Respond via message bus.

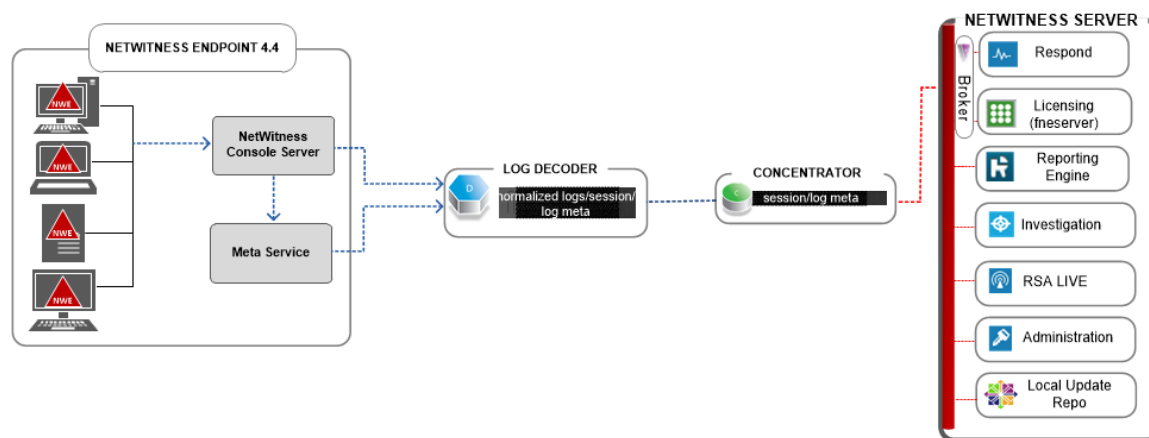
**Contextual data from Endpoint via a NetWitness Suite Live recurring feed.** This integration can enrich the session displayed in NetWitness Suite Investigation with contextual information; some examples include the host operating system, MAC address, IIOC score, and other data that may not be present in the log or packet data.

**NetWitness Endpoint alerts via Syslog (CEF) into NetWitness Suite Log Decoders.** This integration provides the capability to forward Endpoint events via Syslog and to correlate the events with other log or packet metadata in the NetWitness Suite ecosystem.

## NetWitness Endpoint Meta Integration

The NetWitness Endpoint Meta Integration with RSA NetWitness Suite offers customers that have both products a way to more easily take advantage of their products in a single user interface. The following diagram illustrates how NetWitness Endpoint integrates with the NetWitness Suite. The NetWitness Endpoint metadata is collected and published from all machines where NetWitness Endpoint agents are deployed, and then sent to the NetWitness Suite Log Decoder.

The meta can then be viewed in the associated NetWitness Suite Concentrator and also in NetWitness Suite Investigate.



## NetWitness Endpoint Alerts and Indicators of Compromise

NetWitness Endpoint IIOC (Instant Indicator of Compromise) is a database query that NetWitness Endpoint runs on collected NetWitness Endpoint scan data to determine the presence of potential malware on scanned hosts. RSA NetWitness Endpoint 4.1.2 or later ships with IOCs that users can enable and mark as alertable. RSA NetWitness Endpoint runs IOC queries regularly on new scan data, which is collected and stored in the database. If the IOC query is satisfied, this indicates a potential indicator of compromise, and the event can be reported to a user or sent to an external system as an alert.

Possible types of alerts are:

- Machine alert: This alert indicates that the machine in question is suspicious.
- Module alert: This alert indicates that a module, such as a file, a DLL, or an executable, is suspicious. It contains details about the module in question.
- Event alert: This alert represents any other suspicious activity detected by NetWitness Endpoint that does not fall into the above categories.

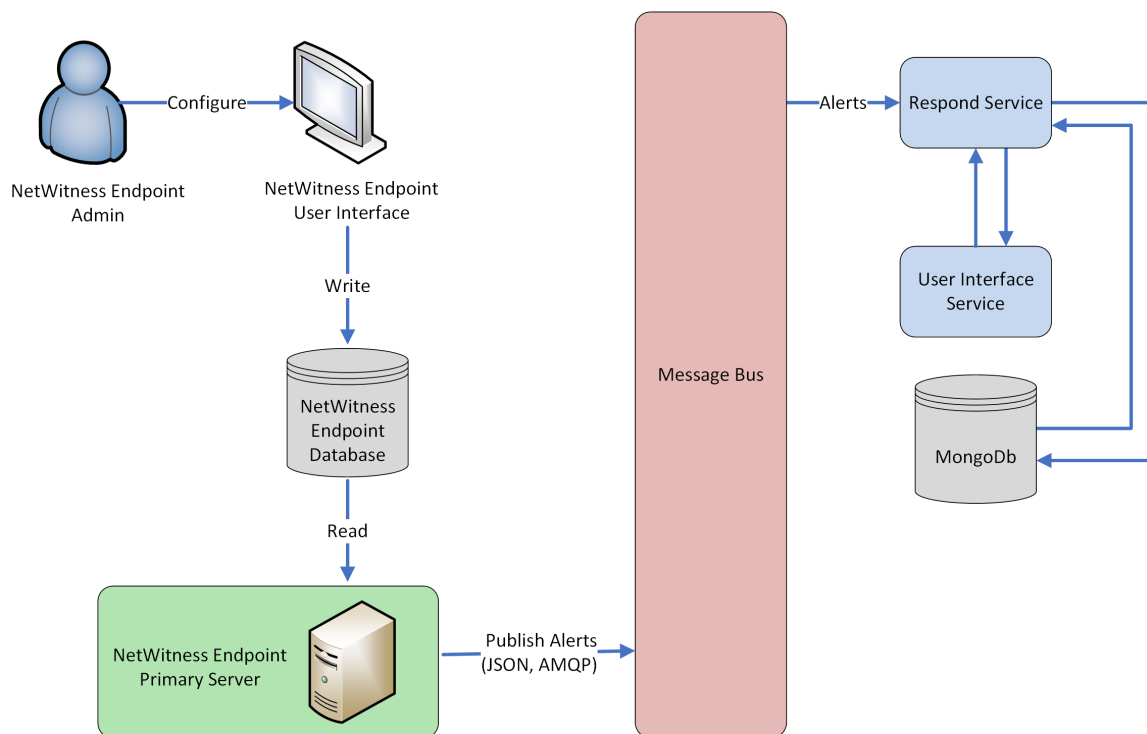
Each of these alert types can be sent to NetWitness Suite.

## Configure NetWitness Endpoint Alerts via Message Bus

This procedure is required to integrate NetWitness Endpoint with NetWitness Suite so that the NetWitness Endpoint alerts are picked up by the Respond component of NetWitness Suite and displayed in the **RESPOND > Alerts** view.

**Note:** RSA supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, or 4.4 for NetWitness Respond integration. For more information, see the "RSA NetWitness Suite Integration" topic in the *NetWitness Endpoint User Guide*.

The diagram below represents the flow of NetWitness Endpoint alerts to the Respond Incident List view of NetWitness Suite and its display in the **RESPOND > Alerts** view.



## Prerequisites

Ensure that you have the following:

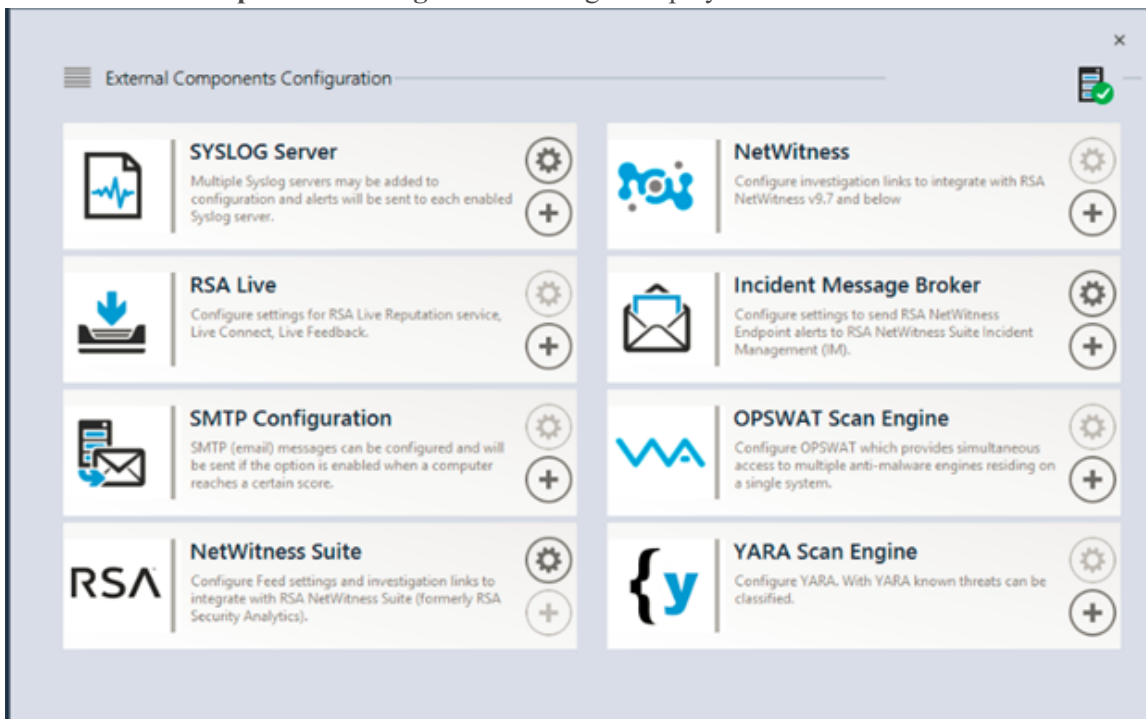
- The Respond service is installed and running on NetWitness Suite 11.0.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 is installed and running.

## Configure NetWitness Endpoint to Forward NetWitness Endpoint Alerts

To configure NetWitness Endpoint to send alerts over the message bus to the NetWitness Suite user interface:

1. In the NetWitness Endpoint user interface, click **Configure > Monitoring and External Components**.

The **External Components Configuration** dialog is displayed.



1. From the components listed, select **Incident Message Broker** and click + to add a new IM broker.
2. Enter the following fields:
  - a. **Instance Name**: Enter a unique name to identify the IM broker.
  - b. **Server Hostname/IP address**: Enter the Host DNS or IP address of the IM broker (NetWitness Server).
  - c. **Port number**: The default port is 5671.
3. Click **Save**.
4. Navigate to the **ConsoleServer.exe.config** file in **C:\Program Files\RSA\ECAT\Server**.



5. Modify the virtual host configurations in the file as follows:

```
<add key="IMVirtualHost" value="/rsa/system" />
```

**Note:** In NetWitness Suite 11.0, the virtual host is “/rsa/system”. For version 10.6.x and below, the virtual host is “/rsa/sa”.

6. Restart the API Server and Console Server.
7. To set up SSL for Respond Alerts, perform the following steps on the NetWitness Endpoint primary console server to set the SSL communications:
  - a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key).
  - b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You MUST set the CN name to ecat.)

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
cy end -sy 12 client.cer
```

**Note:** In the above code sample, if you upgraded to Endpoint version 4.3 from a previous version and did not generate new certificates, you should substitute "EcatCA" for "NweCA".

- c. Make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the IMBrokerClientCertificateThumbprint section of the ConsoleServer.Exe.Config file as shown.
- ```
<add key="IMBrokerClientCertificateThumbprint"
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```
8. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:
 

```
/etc/pki/nw/trust/import
```
  9. Issue the following command to initiate the necessary Chef run:
 

```
orchestration-cli-client --update-admin-node
```

 This appends all of those certificates into the truststore.
  10. Restart the RabbitMQ server:
 

```
systemctl restart rabbitmq-server
```

 The NetWitness Endpoint account should automatically be available on RabbitMQ.
  11. Import the /etc/pki/nw/ca/nwca-cert.pem and /etc/pki/nw/ca/ssca-cert.pem files from the NetWitness Server and add them to the Trusted Root Certification stores in the Endpoint Server.

## Troubleshooting

This section suggests how to resolve problems you may encounter when you configure NetWitness Endpoint alerts via Message Bus.

| Known Issues                       | Solutions                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Orchestration fails on admin node. | You must copy and paste the content of EcatCA certificate in <code>/etc/rabbitmq/ssl/truststore.pem</code> and restart the Rabbitmq service. |

## Configure Contextual Data from NetWitness Endpoint via Recurring Feed

---

You can configure RSA NetWitness Endpoint data in RSA NetWitness Suite to provide contextual data from NetWitness Endpoint to Decoder and Log Decoder sessions. This configuration adds contextual meta values in addition to the instant IOC alerts that can be used to build correlations to other metadata in the NetWitness Suite ecosystem.

Administrators can configure NetWitness Suite to consume system scan contextual data from NetWitness Endpoint via a NetWitness Suite Live recurring feed. This integration can enrich the session from a Decoder or Log Decoder with contextual information displayed in NetWitness Suite Investigation; some examples include the host operating system, MAC address, IIOC score, and other data that may not be present in the log or packet data into sessions from a Decoder or Log Decoder.

**Note:** Although this feature is targeted for customers with a packet Decoder, a recurring feed can also be implemented in Log Decoders.

**Caution:** In environments with many NetWitness Endpoint hosts, use of this recurring feed may result in decreased performance on the NetWitness Suite ingest devices (Decoder and Log Decoder).

### Prerequisites

- Version 4.3.0.4, 4.3.0.5, or 4.4 NetWitness Endpoint Console server and NetWitness Server Version 10.4 and above installed.
- Version 11.0 RSA Decoder and Concentrator connected to the NetWitness Server in the network.

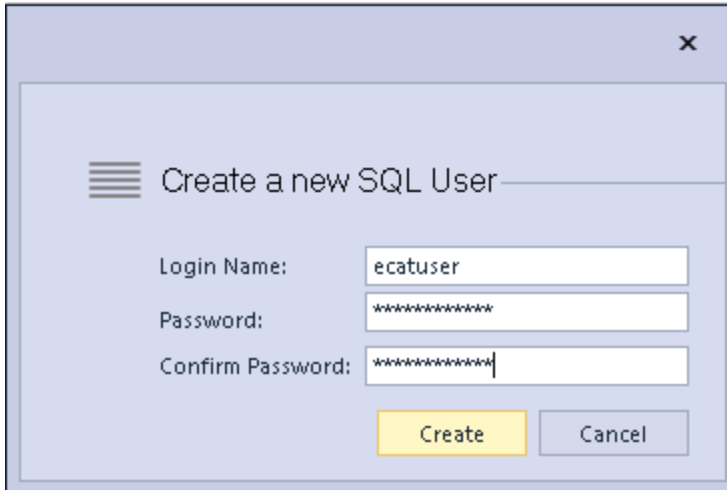
**To Configure Contextual Data from NetWitness Endpoint via Recurring Feed, perform the following:**

1. Enable the NetWitness Endpoint Feed for NetWitness Suite in the NetWitness Endpoint User Interface.
2. Export the NetWitness Endpoint CA Certificate from the NetWitness Endpoint Console server and Import it into NetWitness Suite trust store.
3. Configure the NetWitness Suite Concentrator service to define which meta keys are indexed.
4. Create a recurring feed in NetWitness Suite Live.

## Enable the NetWitness Endpoint Feed for NetWitness Suite

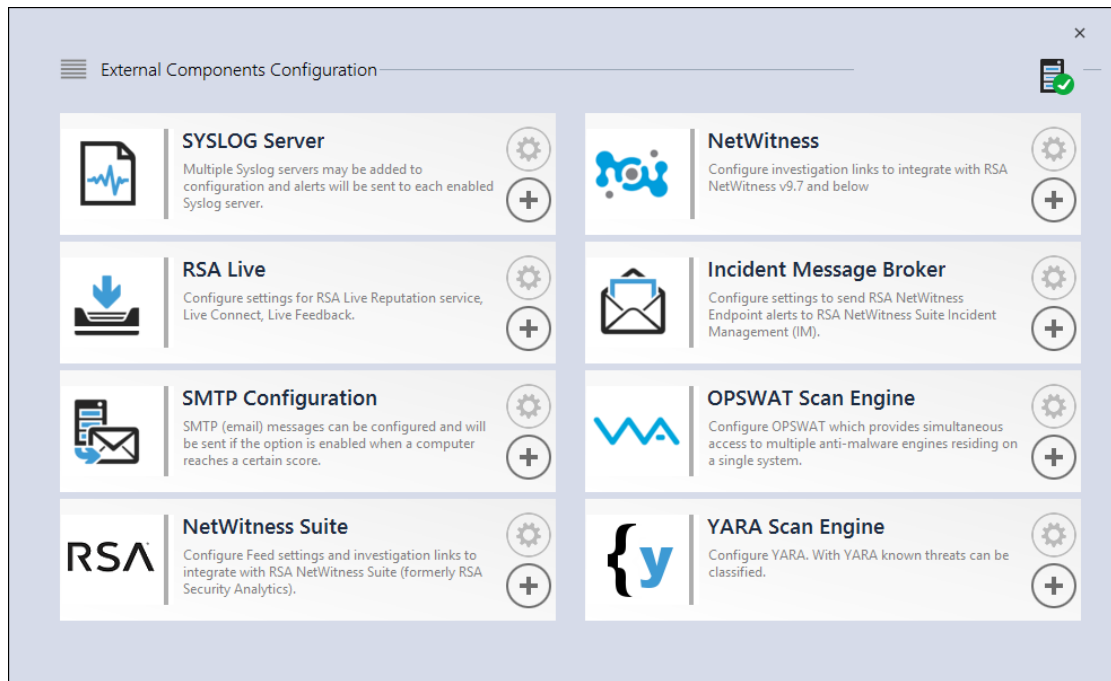
1. In the NetWitness Endpoint user interface, create SQL user in NetWitness Endpoint:
  - a. Open the NetWitness Endpoint user interface and log on using the proper credentials.
  - b. From the menu bar, select **Configure > Manage Users and Roles**, right-click in the pane, and select **create sql user**.

The Create a new SQL User dialog is displayed.

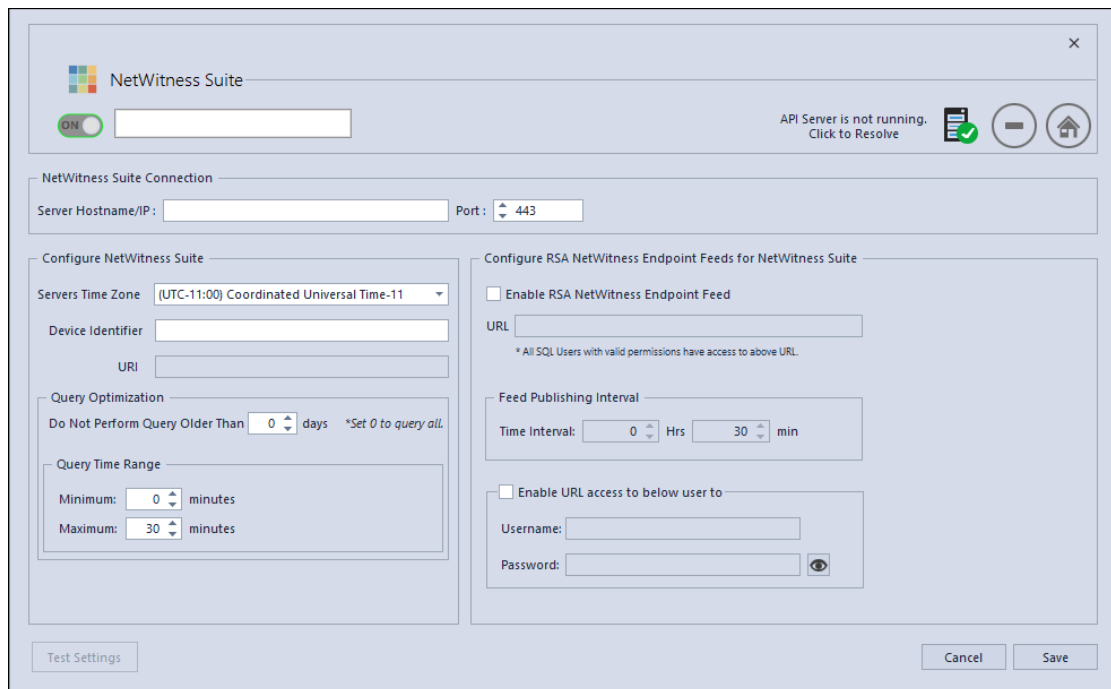


- c. Enter the **Login Name** and **Password** and click **Create**.
2. From the menu bar, select **Configure > Monitoring External Components**.

The External Components Configuration dialog is displayed.



3. In NetWitness Suite, click +.  
The NetWitness Suite dialog is displayed.



4. In the **NetWitness Suite** panel, in **On**, enter the name to identify the NetWitness Suite component.

5. In the **NetWitness Suite Connection** panel, perform the following.
  - a. In the **Server Hostname/IP** field, enter the host name or IP address of the NetWitness Server.
  - b. In the **Port** field, enter the port number. By default port number is 443.
6. In the **Configure NetWitness Suite** panel, perform the following:
  - a. In the **Servers Time Zone** field, select the time zone for the component from the drop-down list.
  - b. In the **Device Identifier** field, enter the NetWitness Suite concentrator device ID.

**Note:** You can find the Device Identifier in NetWitness Suite when you look up a Concentrator or Broker in **Investigation > Navigate ><Concentrator or Broker Name>**. The Device Identifier is the number in the URL after "investigation." For example, in the URL `https://<IP address>investigation/319/navigate/values`, the Device Identifier is **319**.

The **URI** field is populated when you click **Save**.

7. In the **Query Optimization** panel, in the **Do Not Perform Query Older Than** field, enter the number of days to limit the query period. Enter **0** if you want to discard this feature.
8. In the **Query Time Range** panel, perform the following:
  - a. In the **Minimum** field, enter the number of minutes for the minimum query time range. This value is used to automatically increase the time range submitted to NetWitness Suite. This ensures that a query returns a positive response if the NetWitness Endpoint Agent's reported time is slightly different than NetWitness Endpoint's time.
  - b. In the **Maximum** field, enter the number of minutes to limit the time range. This value is used to automatically limit the time range submitted to NetWitness Suite, so that a query does not overload the NetWitness Server.
9. In the **Configure RSA NetWitness Endpoint Feeds for NetWitness Suite** panel, perform the following:
  - a. Select **Enable RSA NetWitness Endpoint Feed**.
  - b. In the **URL** field, enter the SQL **Username** and **Password** (configured in step 1) to access the location of the feed.

The **URL** field is populated when you click **Save**.
  - c. Enter the time interval for the frequency at which feeds are published.

10. In the **Feed Publishing Interval** panel, in the **Time Interval** field, select the time interval in **hrs** and **mins** for the frequency at which feeds are published.
11. In the **Enable URL access to below user to** panel, enter the **Username** and **Password** of the NetWitness Endpoint user.
12. Click **Save**.  
A feed is created.

## Export the NetWitness Endpoint SSL Certificate

**Note:** This procedure works only for NetWitness Suite 10.5 and above because Java 8 support was added for 10.5. If you are using an earlier version of NetWitness Suite, refer to the applicable version of this guide.

**To export the NetWitness Endpoint CA certificate from the NetWitness Endpoint Console server and copy it to the NetWitness Suite host:**

1. Log on to the NetWitness Endpoint Console.
2. Open MMC.
3. Add a certificate snap-in for **Computer account**.
4. Export the certificate named **EcatCA**.
  - a. Export without a private key.
  - b. Export in DER encoded binary X.509 (.CER) format.
  - c. Name it **EcatCA.cer**.
5. Copy the NetWitness Endpoint CA certificate to the NetWitness Suite host:
  - For NetWitness Endpoint 4.3.0.4, 4.3.0.5 or 4.4 fresh installation:  
`scp NweCA.cer root@<sa-machine>:.`
  - For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5:  
`scp EcatCA.cer root@<sa-machine>:.`
6. To import the NetWitness Endpoint CA certificate into the NetWitness Suite Trusted store, perform the following:
  - a. Check the Java version installed on your NetWitness Suite using the following command:  

```
java -version
```

 The openjdk version is displayed. For example, openjdk version "1.8.0\_71"
  - b. To set the JDK parameter, navigate to java directory. Enter the following commands:

- `JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/`
- For NetWitness Endpoint fresh installation:  
`$JDK/bin/keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit`
- For NetWitness Endpoint upgraded from previous version:  
`$JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit`

When prompted for certificate update confirmation, enter **Yes**.

7. On the NetWitness Suite host, do one of the following:
  - For NetWitness Endpoint 4.3.0.4, 4.3.0.5, or 4.4 fresh installation, edit `/etc/hosts` to map the IP address of the NetWitness Endpoint Console server to the name **NweServerCertificate** by adding the following line to the file:  
`<ip-address-ecat-cs> NweServerCertificate`
  - For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5, edit `/etc/hosts` to map the IP address of the upgraded NetWitness Endpoint Console server to the name **ecatserverexported** by adding the following line to the file:  
`<ip-address-ecat-cs> ecatserverexported`
8. To restart NetWitness Suite, enter the following command:  
`service jetty restart`

## Configure the NetWitness Suite Concentrator Service

1. Log on to NetWitness Suite and go to **ADMIN > Services**.
2. Select a Concentrator from the list and select **View > Config**.
3. Select the **Files** tab, and from the **Files to Edit** drop-down menu, select **index-concentrator-custom.xml**.
4. Add the following NetWitness Endpoint meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them. The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:  
**description** is the name of the meta key you want to display in NetWitness Suite



Investigation.

**level** is "IndexValues"

**name** matches the column name of the CSV file that NetWitness Suite uses while defining the recurring feed (see the table in *Configure the Recurring Custom Feed Task in NetWitness Suite* below).

```
<key description="Gateway" format="Text" level="IndexValues" name="gateway" valueMax="250000" defaultAction="Open"/>
```

```
<key description="Risk Number" format="Float64" level="IndexValues" name="risk.num" valueMax="250000" defaultAction="Open"/>
```

```
<key description="Strans Addr" format="Text" level="IndexValues" name="stransaddr" valueMax="250000" defaultAction="Open"/>
```

```
<key description="Domain" format="Text" level="IndexValues" name="domain" valueMax="250000" defaultAction="Open"/>
```


```
<key description="User Account" format="Text" level="IndexValues" name="username" valueMax="250000" defaultAction="Open"/>
```

```
<key description="Ecat Connectiontime" format="Text" level="IndexValues" name="ecat.ctime" valueMax="250000" defaultAction="Open"/>
```

```
<key description="Ecat Scantime" format="Text" level="IndexValues" name="ecat.stime" valueMax="250000" defaultAction="Open"/>
```

5. Restart the Concentrator to activate the custom key updates.

## Configure the Recurring Custom Feed Task in NetWitness Suite

1. Log on to NetWitness Suite and go to **CONFIGURE > Custom Feeds**.  
The Feeds view is displayed.
2. In the toolbar, click .  
The Setup Feed dialog is displayed.
3. In the Setup Feed dialog, select **Custom Feed** and click **Next**.  
The Configure a Custom Feed wizard is displayed, with the Define Feed form open.
4. In the **Define Feed**, perform the following:
  - a. In the **Feed Task Type** field, select **Recurring**.
  - b. In the **Name** field, enter the name of the feed. For example, EndpointFeed.
  - c. In the **URL** field, enter the URL with the hostname of the Windows server on which NetWitness Endpoint is installed:

- For NetWitness Endpoint 4.3.0.4, 4.3.0.5 or 4.4 fresh installation, use the URL **`https://NweServerCertificate:9443/api/v2/feed/machines.csv`**.
  - For NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5, use the URL **`https://ecatserverexported:9443/api/v2/feed/machines.csv`**.
- d. Enable the checkbox **Authenticated** and enter the username and password as noted in *Enable the ECAT Feed* above.
  - e. Click **Verify** to check if NetWitness Suite can reach the web resource.
  - f. Define the schedule and click **Next**.

5. In the **Select Services** tab, select the Decoder or groups to consume the feed. Click **Next**.

6. In the **Define Columns** tab, enter the column names as shown in the table below and save the feed.

The following table shows the columns in the CSV file for the NetWitness Endpoint feed.

Column	Name	Description	Column Name in NetWitness Suite (Meta Key Name)
1	MachineName	Host name of the Windows agent	alias.host
2	LocalIp	IPv4 address	IP type (indexed column)
3	RemoteIp	Far end IP as seen by the router	stransaddr
4	GatewayIp	IP of the gateway	gateway
5	MacAddress	MAC address	eth.src
6	OperatingSystem	Operating system used by the Windows Agent	OS

Column	Name	Description	Column Name in NetWitness Suite (Meta Key Name)
7	AgentID	Agent ID of the host (unique ID assigned to the agent)	client
8	ConnectionUTCTime	Last time when the agent connected to NetWitness Endpoint server	ecat.ctime
9	Source Domain	Domain	domain.src
10	ScanUTC time	Last time when the agent was scanned	ecat.stime
11	UserName	Username of the client machine	username
12	Machine Score	Score of the agent indicating the suspicious level	risk.num

**Note:** In the table, the recommended index setting is LocalIp. However, if the LocalIp for NetWitness Endpoint Agent PC is allocated by a DHCP Server and the DHCP lease has expired, and if the IP is then re-allocated to another PC, the metadata created by the feed will be incorrect. To avoid this risk, use the machine name or the Mac address instead of the localIP address as the Feed's index. For example, to use a Mac address, you could enter the values as shown in the following figure.

**Configure a Custom Feed**

Define Feed > Select Services > **Define Columns** > Review

**Define Index**

Type: ☐ IP ☐ IP Range ☒ Non IP

Index Column: 5 Service Type:  ☐ Truncate Domain

Callback Key (5): eth.src

**Define Values**

Column	1	2	3	4	5 (Index)	6	7
Key	alias.host	ip.src	stransaddr	gateway	OS		client

## Result

When viewing feed data in NetWitness Suite, upon a match of the indexed value (ip.src), meta data is populated in Investigation, Reporting, and Alerting Interfaces.

## Configure Endpoint Alerts via Syslog into a Log Decoder

---

You can configure the use of RSA NetWitness Endpoint data in RSA NetWitness Suite to provide NetWitness Endpoint alerts via Syslog into Log Decoder sessions. This generates metadata that is used by NetWitness Suite Investigation, Alerts, and Reporting Engine.

For NetWitness Suite networks that are consuming logs, this integration of NetWitness Endpoint with NetWitness Suite pushes NetWitness Endpoint events to the Log Decoder via common event format (CEF) syslog messages and generates metadata that is used by NetWitness Suite Investigation, Alerts, and Reporting Engine. The use case for this integration is SIEM Integration to allow centralized event management, correlation of NetWitness Endpoint events with other Log Decoder data, NetWitness Suite reporting on NetWitness Endpoint events, and NetWitness Suite alerting of NetWitness Endpoint events.

### Prerequisites

The following are required for this integration:

- Version 4.3.0.4, 4.3.0.5, or 4.4 NetWitness Endpoint UI.
- NetWitness Server Version 11.0 is installed.
- Version 10.4 or later RSA Log Decoder and Concentrator connected to the NetWitness Server in the network.
- Port UDP- 514 or TCP - 1514 open from NetWitness Endpoint server to Log Decoder in the firewall.

### Procedure

1. Deploy the required parser (CEF or rsaecat) to the Log Decoder as described in the "Manage Live Resources" topic in *Live Services Management*. After you deploy the parser, make sure the parser is enabled. For more information, see Services Config View - General Tab.

**Note:** Use only one of these parsers. When the CEF parser is deployed, it supersedes the NetWitness Endpoint parser, and all CEF messages into NetWitness Suite are processed by the CEF parser. Enabling both parsers is an unnecessary burden on performance.

2. Configure NetWitness Endpoint to send syslog output to NetWitness Suite and generate NetWitness Endpoint alerts to the Log Decoder.

3. (Optional) Edit the table mapping in `table-map-custom.xml` and the `index-concentrator-custom.xml` to add fields based on user preferences for metadata to be mapped to NetWitness Suite.

## Configure NetWitness Endpoint to Send Syslog Output to NetWitness Suite

**To add the Log Decoder as a Syslog external component and generate NetWitness Endpoint alerts to the Log Decoder:**

1. Open the NetWitness Endpoint user interface and log on using the proper credentials.
2. From the menu bar, select **Configure > Monitoring and External Components**.

The External Components Configuration dialog is displayed.

3. In **SYSLOG Server**, click **+**.

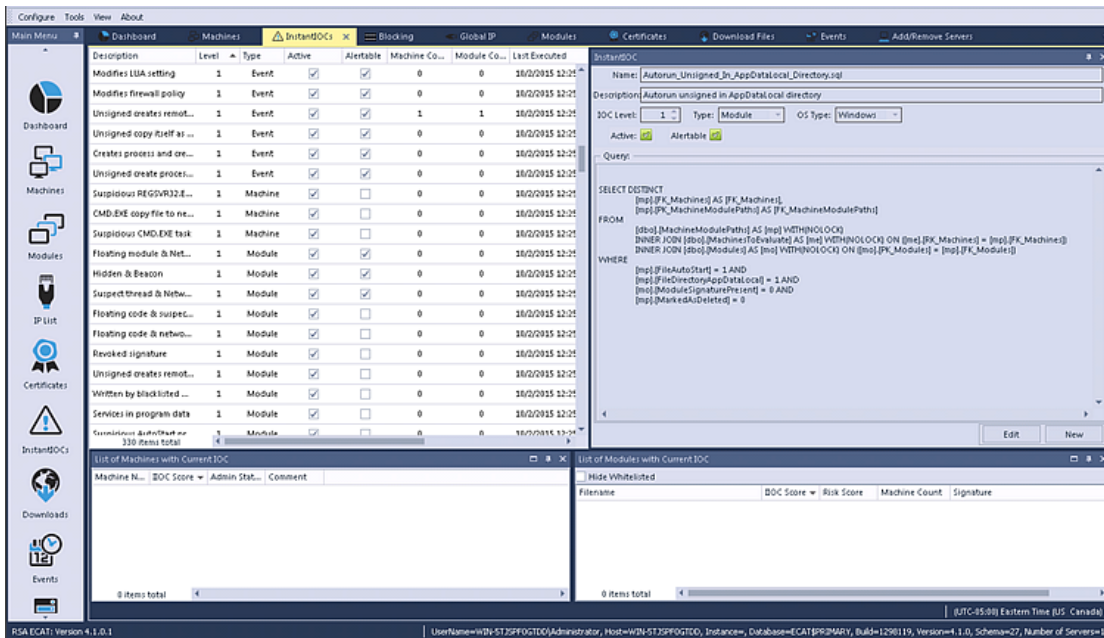
The SYSLOG Server dialog is displayed.

4. In the **NetWitness Suite** panel, in **On**, enter the descriptive name for the Log Decoder.
5. In the **Syslog Connection** panel, perform the following to enable Syslog messaging:

**Server Hostname/IP** = The hostname DNS or IP address of the RSA Log Decoder  
**Port** = 514

**Transport Protocol** = Select **UDP** or **TCP** as appropriate for your Syslog server for the transport protocol.

- Click **Save**.
- Open the **InstantIOCs** window in the NetWitness Endpoint UI and, in the **Alertable** column, click to enable each IIOC for which you want alerts sent to the Log Decoder.



When the instant IOCs are triggered, Syslog alerts from the NetWitness Endpoint server are sent to the Log Decoder. Log Decoder alerts are then aggregated to the Concentrator. These events are injected into the Concentrator as metadata.

## Edit the Table Mapping in table-map-custom.xml

In the default RSA table-map.xml provided by RSA, the meta keys in the table-map.xml file are set to Transient. In order to view the meta keys in Investigation, the keys must be set to None. To make changes to the mapping, you must add the entries to the table-map-custom.xml on the Log Decoder.

This is the list of meta keys in table-map.xml.

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
agentid	client	No
CEF Header Hostname Field	alias.host	No



NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
CEF Header Product Version	version	Yes
CEF Header Product Name	Product	Yes
CEF Header Severity	severity	Yes
CEF Header Signature ID	event.type	No
CEF Header Signature Name	event.desc	No
destinationDnsDomain	ddomain	Yes
deviceDnsDomain	domain	Yes
dhost	host.dst	No
dst	ip.dst	No
end	endtime	Yes
fileHash	checksum	Yes
fname	filename	No
fsize	filename.size	Yes
gatewayip	gateway	Yes
instantIOCLLevel	threat.desc	No
instantIOCName	threat.category	No
machineOU	dn	Yes
machineScore	risk.num	No
md5sum	checksum	Yes
os	OS	Yes

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
port	ip.dstport	No
protocol	protocol	Yes
Raw Message	msg	Yes
remoteip	stransaddr	Yes
rt	alias.host	No
sha256sum	checksum	Yes
shost	host.src	No
smac	eth.src	Yes
src	ip.src	No
start	starttime	Yes
suser	user.dst	No
timezone	timezone	Yes
totalreceived	rbytes	Yes
totalsent	bytes.src	No
useragent	user.agent	No
userOU	org	Yes

The following seven keys are not in `table-map.xml`; to use these keys in NetWitness Suite you need to add them to `table-map-custom.xml`, and set the flags to `None`.

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
moduleScore	cs.modulescore	Yes

NetWitness Endpoint Fields	NetWitness Suite Mapping	Transient in NetWitness Suite
moduleSignature	cs.modulesign	Yes
Target module	cs.targetmodule	Yes
YARA result	cs.yarareult	Yes
Source module	cs.sourcemodule	Yes
OPSWATResult	cs.opswatresult	Yes
ReputationResult	cs.represult	Yes

Here are the entries to be added to the `table-map-custom.xml` if required.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
  <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
  <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
  <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
  <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
  <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
  <mapping envisionName="cs_yarareult" nwName="cs.yarareult" flags="None"
envisionDisplayName="YaraResult"/>
```

**Note:** Restart the Log Decoder or reload the log parsers for the changes to take effect.

## Configure the NetWitness Suite Concentrator Service

- Log on to NetWitness Suite and go to **ADMIN > Services**.
  - Select a Concentrator from the list and select **View > Config**.
- Select the **Files** tab, and from the **Files to Edit** drop-down list, select **index-concentrator-custom.xml**.
- Add the NetWitness Endpoint meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them.
- Restart the Concentrator.

- To add the Concentrator as a data source in the Reporting Engine, in the **ADMIN > Services** view, select the Reporting Engine and Select **View> Config > Sources**.  
NetWitness Endpoint meta is populated in Reporting Engine, and you can run reports by selecting the appropriate meta keys.

## Example

**Note:** The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:

**description** is the name of the meta key you want to display in NetWitness Suite

Investigation.

**level** is "IndexValues"

**name** is the NetWitness Endpoint meta key name from the table below

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
  <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
  <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
  <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
  <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
  <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
  <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
  <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
  <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
  <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
  <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
  <key description="Module Sign" format="Text" level="IndexValues"
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
  <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
  <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
  <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
  <key description="yara result" format="Text" level="IndexValues"
```

```
name="cs.yarareult" valueMax="250000" defaultAction="Open"/>
  <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
  <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
  <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
  <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
  <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
  <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
  <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
  <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
  <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
</language>
```

## Result

Analysts can:

- Create NetWitness Suite alerts based on NetWitness Endpoint events by configuring NetWitness Endpoint events as an enrichment source.
- Create ESA rules using NetWitness Endpoint meta as described in the "Add Rules to the Rules Library" topic in the *Alerting Using ESA Guide*.
- Report on NetWitness Endpoint events using NetWitness Endpoint meta as described in the "Configure a Rule" topic in the *Reporting Guide*.
- View NetWitness Endpoint alerts in NetWitness Respond as described in the "View Alerts" topic in *NetWitness Respond User Guide*.
- View NetWitness Endpoint meta keys in Investigation along with standard NetWitness Suite core meta keys as described in the "Conduct an Investigation" topic in *Investigation and Malware Analysis User Guide*.

