NetWitness® Platform XDR

Version 12.0

RSA Endpoint Integration Guide

NETWITNESS

Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

July, 2022

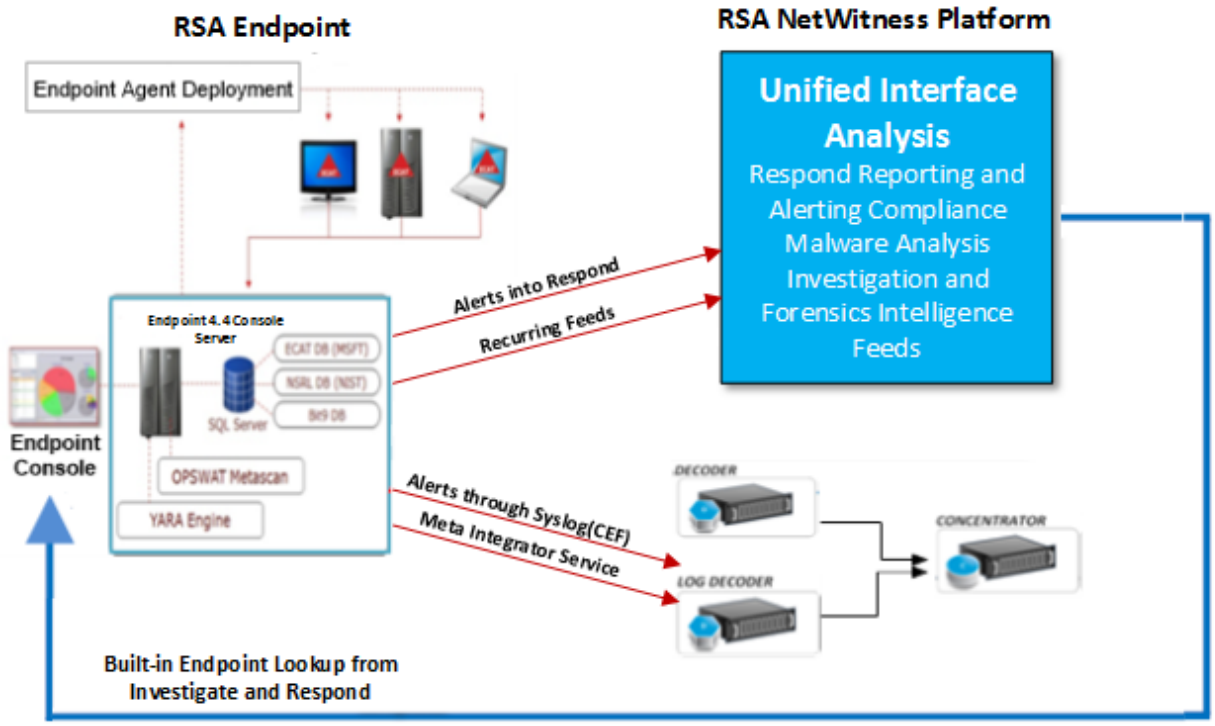
Contents

NetWitness Endpoint Integration

NetWitness customers who are using NetWitness Endpoint 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later can integrate into NetWitness 11.x in several different ways.

Note: In Version 11.2 and later, the following components are rebranded:
- NetWitness Suite to NetWitness Platform
- Packet Decoder to Network Decoder

Integration Options



Integration Methods

The following are the NetWitness Endpoint integration methods:

- Configure Endpoint Alerts through Respond
- Configure Contextual Data from Endpoint through Recurring Feed
- Configure Endpoint Alerts through Syslog into a Log Decoder
- Configuring Meta Integrator service in the NetWitness Endpoint 4.4.0.2 or later directly to a Log Decoder

Endpoint alerts into NetWitness Respond. This integration provides the capability for forwarding Endpoint alerts to Respond.

Contextual data from Endpoint through a NetWitness Live recurring feed. This integration can enrich the session displayed in NetWitness 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.

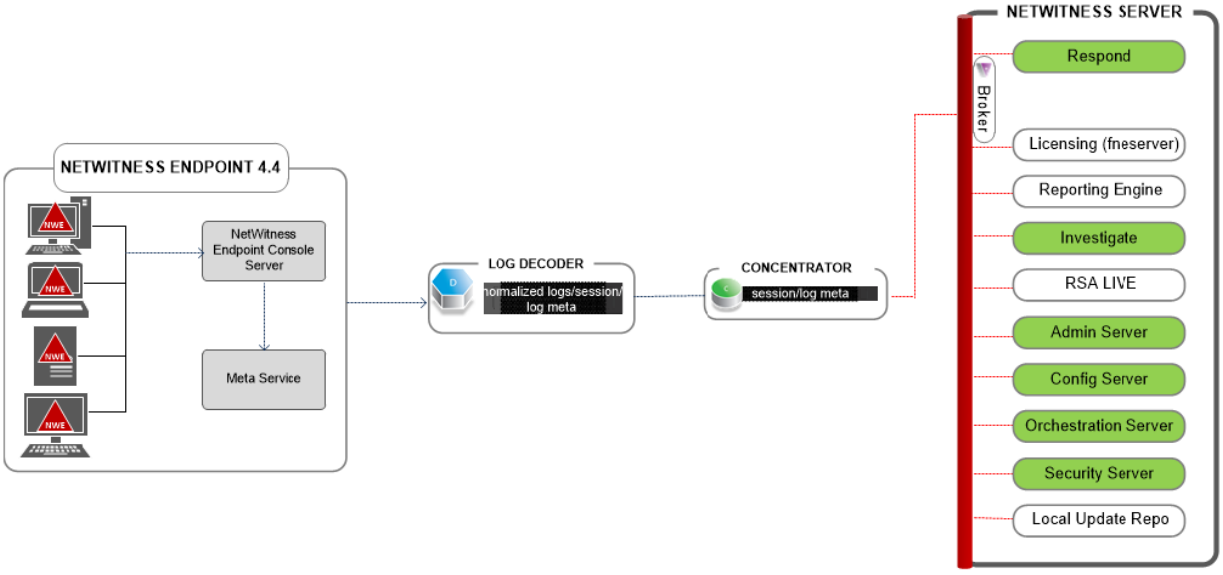
NetWitness Endpoint alerts through Syslog (CEF) into NetWitness Log Decoders. This integration provides the capability to forward Endpoint events through Syslog and to correlate the events with other log or packet metadata in the NetWitness ecosystem.

(For Version 11.1 and later) **NetWitness Endpoint directly to a Log Decoder.** This integration lets you view the Endpoint metadata in the **Investigate > Navigate** and **Event Analysis** view similar to Logs and Packets.

Note: For information on NetWitness Endpoint 4.4.0.x integration with NetWitness, see *NetWitness Endpoint Configuration Guide*.

NetWitness Endpoint Metadata Integration

The NetWitness Platform provides seamless integration allowing Endpoint metadata to be included into the NetWitness work flow. This lets analyst to investigate an incident and respond using packet, log, and endpoint metadata. The endpoint metadata provides further indicators and context related to a host, user, process, or file. It also provides tracking data that provide data of what has transpired with a host, user, process, or file.



Built-in NetWitness Endpoint Lookup

With the NetWitness Endpoint user interface (UI) installed on the same machine where the analyst is using a browser to access NetWitness, the built-in NetWitness Endpoint Lookup from NetWitness Investigation and NetWitness 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 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 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*.

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. NetWitness Endpoint 4.1.2 or later ships with IOCs that users can enable and mark as alertable. 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.

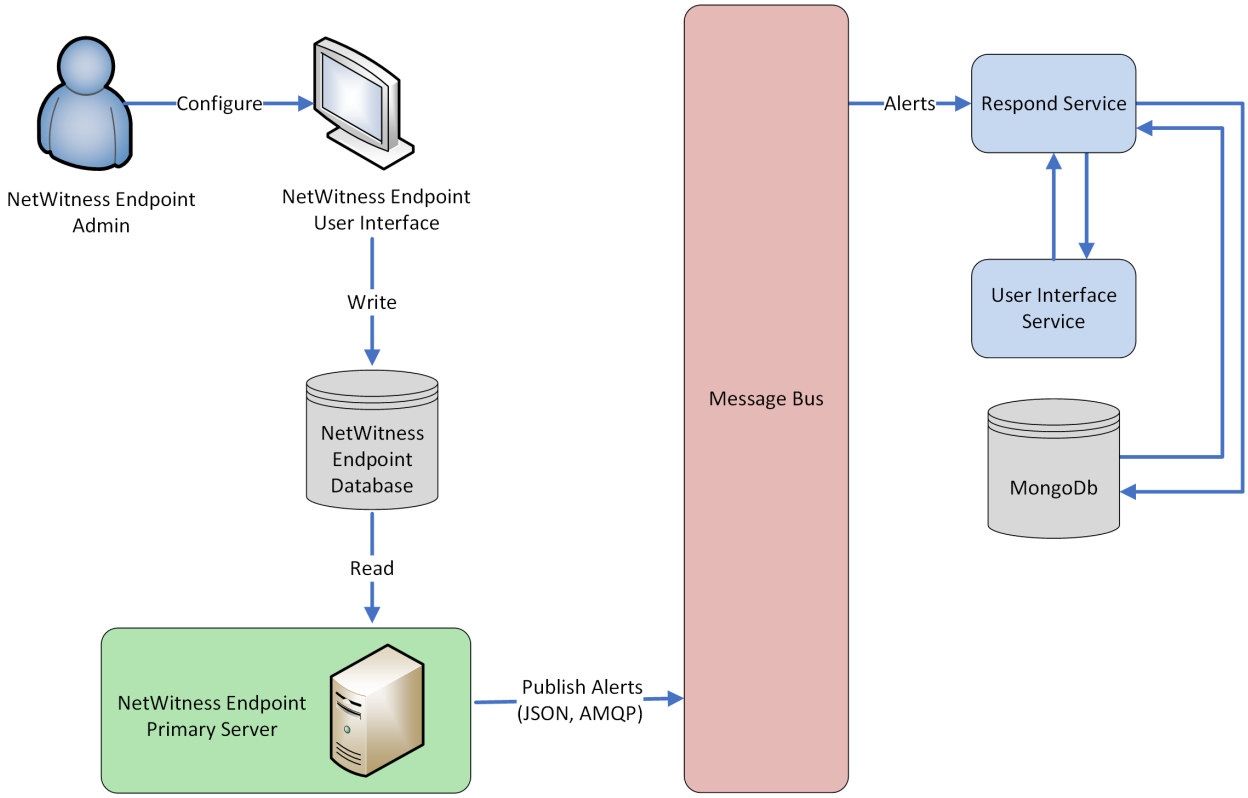
Each of these alert types can be sent to NetWitness.

Configure NetWitness Endpoint Alerts to Respond

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

Note: NetWitness supports NetWitness Endpoint versions 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later for NetWitness Respond integration. For more information, see the "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 and its display in the **Respond > Alerts** view.



Prerequisites

Ensure that you have the following:

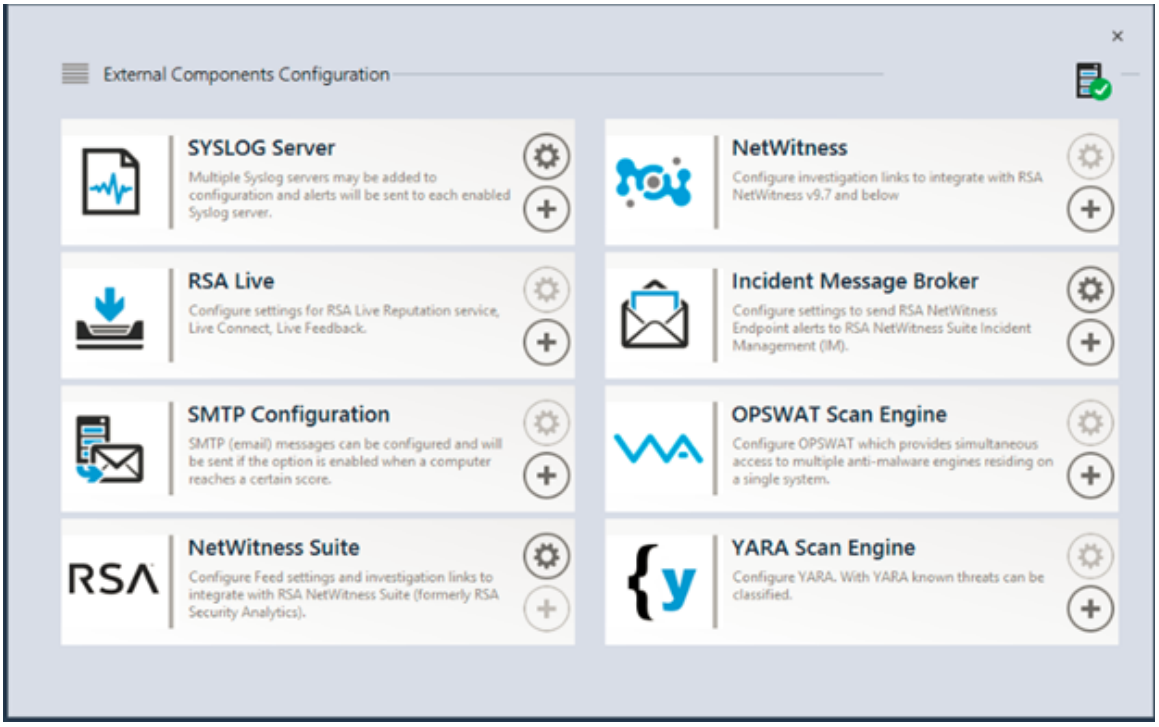
- The Respond service is installed and running on NetWitness.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later is installed and running.

Configure NetWitness Endpoint to Forward NetWitness Endpoint Alerts

To configure NetWitness Endpoint to send alerts to Respond to the NetWitness user interface:

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

   The External Components Configuration dialog is displayed.



2. From the components listed, select **Incident Message Broker** and click + to add a new IM broker.
3. 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.
4. Click **Save**.
5. Navigate to the **ConsoleServer.exe.config** file in **C:\Program Files\RSA\ECAT\Server**.
6. Modify the virtual host configurations in the file as follows:
   `<add key="IMVirtualHost" value="/rsa/system" />`

Note: In NetWitness 11.0 and 11.1, the virtual host is "/rsa/system". For version 10.6.x and below, the virtual host is "/rsa/sa".

7. Restart the API Server and Console Server.
8. 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. Run cmd.exe console with Administrator rights.)

      ```
      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
      c:\client.cer
      ```

      Note: In the previous code sample, if you upgraded to version 4.3 (or later) from a previous version and did not generate new certificates, you should substitute `"EcatCA"` for `"NweCA"`. Or, if your current operating system has PowerShell version 5.1 or later, you can use the following code sample:

      ```
      PS C:\> New-SelfSignedCertificate -KeyExportPolicy Exportable -Subject
      "CN=ecat" -KeyAlgorithm RSA -KeyLength 2048 -CertStoreLocation
      "cert:\LocalMachine\My" -HashAlgorithm SHA256 -KeySpec KeyExchange -
      TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1") -
      Provider "Microsoft RSA SChannel Cryptographic Provider" -KeyUsage
      DigitalSignature, KeyEncipherment, KeyAgreement -Signer (Get-ChildItem -
      Path Cert:\LocalMachine\My\ -DnsName NweCA)-NotAfter (Get-Date).AddYears
      (5); Export-Certificate –Cert (Get-ChildItem –Path
      Cert:\LocalMachine\My\ -DnsName ecat) –FilePath C:\Client.cer
      ```

   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"/>
      ```

9. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format into the import folder:

   `/etc/pki/nw/trust/import`

10. 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.
11. Restart the RabbitMQ server:
    `systemctl restart rabbitmq-server`
    The NetWitness Endpoint account should automatically be available on RabbitMQ.
12. 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 to Respond.

Known Issues	Solutions
Orchestration fails on admin node.	You must copy and paste the content of NweCA or EcatCA certificate in `/etc/rabbitmq/ssl/truststore.pem` and restart the Rabbitmq service.

Configure Contextual Data from NetWitness Endpoint Through Recurring Feed

You can configure NetWitness Endpoint data in NetWitness 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 ecosystem.

Administrators can configure NetWitness to consume system scan contextual data from NetWitness Endpoint through a NetWitness Live recurring feed. This integration can enrich the session from a Decoder or Log Decoder with contextual information displayed in NetWitness 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 Network Decoder, a recurring feed can also be implemented in Log Decoders.

Caution: In an environment with many NetWitness Endpoint hosts, using recurring feed may result in decreased performance on the NetWitness ingest devices (Decoder and Log Decoder).

Prerequisites

- Version 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later NetWitness Endpoint Console server and NetWitness Server Version 10.4 and above installed.
- Version 11.0 or 11.1 NetWitness Decoder and Concentrator connected to the NetWitness Server in the network.

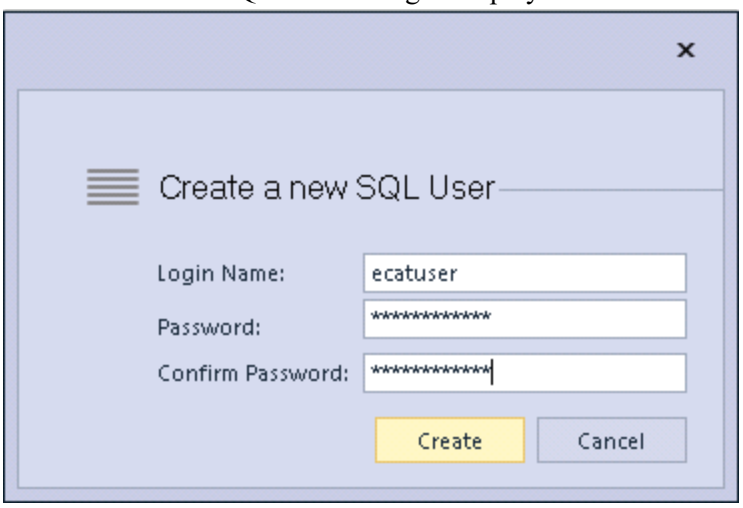
To Configure Contextual Data from NetWitness Endpoint Through Recurring Feed, perform the following:

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

Enable the NetWitness Endpoint Feed for NetWitness

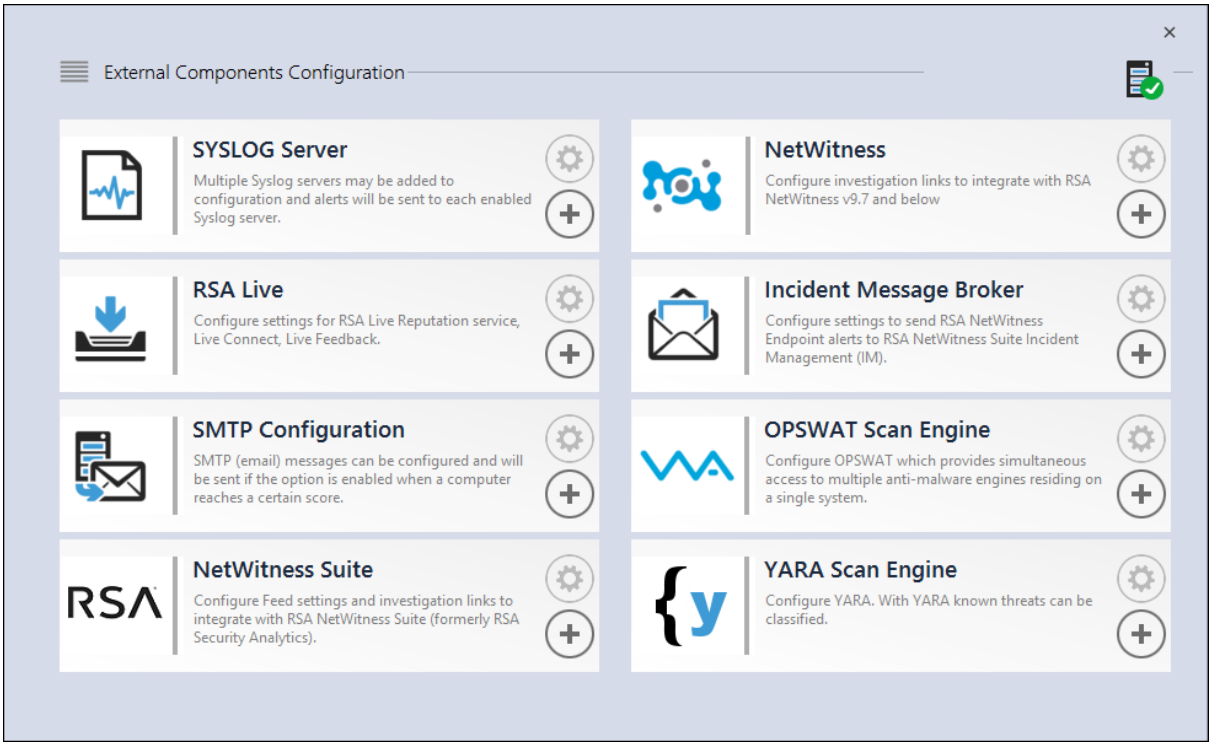
1. In the NetWitness Endpoint user interface, create SQL user in NetWitness Endpoint:
   a. Open the NetWitness Endpoint user interface and log on using the proper credentials.
   b. From the menu bar, select  **(Configure) > Manage Users and Roles**, right-click in the pane, and select **create sql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

The Create a new SQL User dialog is displayed.

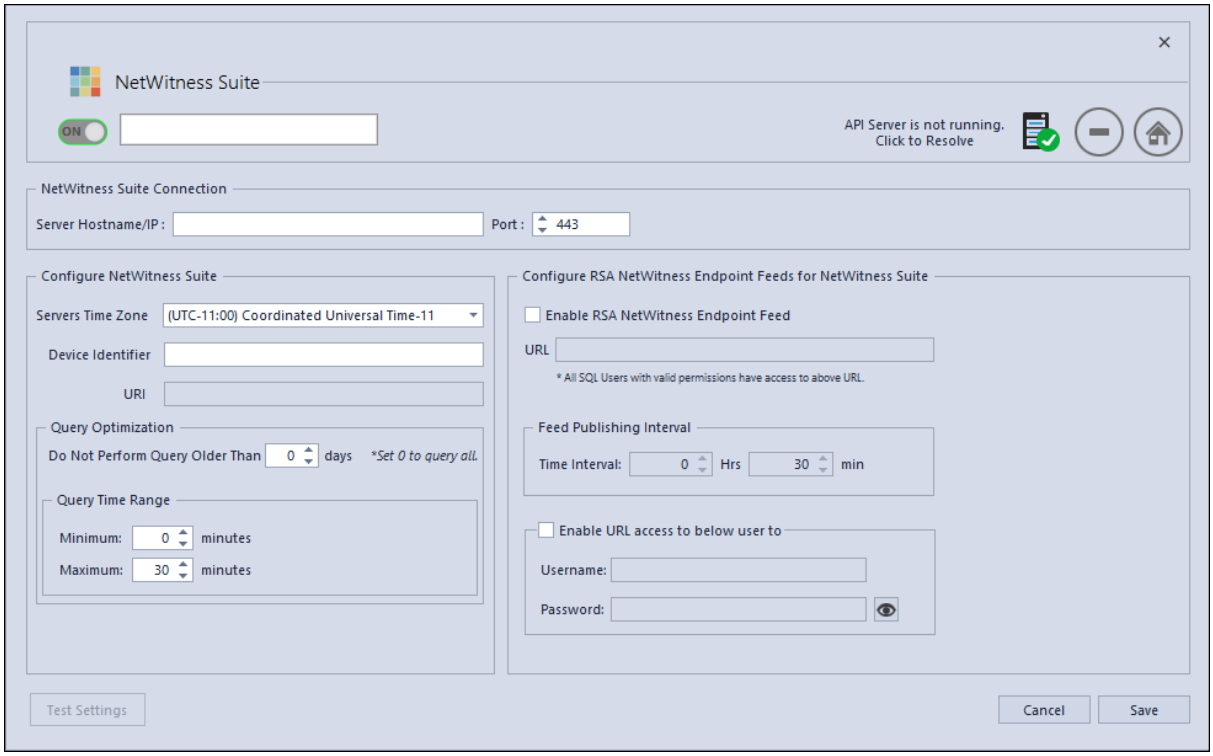


c. Enter the **Login Name** and **Password** and click **Create**.

2. From the menu bar, select **(Configure) > Monitoring and External Components**.
   The External Components Configuration dialog is displayed.



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



4. In the **NetWitness** panel, in **On**, enter the name to identify the NetWitness component.
5. In the **NetWitness 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** 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 concentrator device ID.

   Note: You can find the Device Identifier in NetWitness 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. 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, so that a query does not overload the NetWitness Server.
9. In the **Configure NetWitness Endpoint Feeds for NetWitness** panel, perform the following:
   a. Select **Enable 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 10.5 and above because Java 8 support was added for 10.5. If you are using an earlier version of NetWitness, 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 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 **`NweCA`** (in NetWitness Endpoint 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later fresh install) or **`EcatCA`** (in NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5).
   a. Export without a private key.
   b. Export in DER encoded binary X.509 (`.CER`) format.
   c. Name it **`NweCA.cer`** (in NetWitness Endpoint 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later fresh install) or **`EcatCA.cer`** (in NetWitness Endpoint upgraded from previous version to 4.3.0.4 or 4.3.0.5).

5. Copy the NetWitness Endpoint CA certificate to the NetWitness 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 Endpoint CA certificate into the NetWitness Trusted store, navigate to java directory. Enter the following commands:
   - For NetWitness Endpoint fresh installation:
     `keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore /etc/pki/java/cacerts -storepass changeit`
   - For NetWitness Endpoint upgraded from previous version:
     `keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore /etc/pki/java/cacerts -storepass changeit`

   When prompted for certificate update confirmation, enter **Yes**.
7. Create a file `jetty.user` in the `/etc/default` directory and add the following text.
   `JAVA_OPTIONS="${JAVA_OPTIONS} -Djdk.security.allowNonCaAnchor=true"`
8. On the NetWitness host, do one of the following:
   - For NetWitness Endpoint 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later fresh installation, edit**`/etc/hosts.user`** 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.user`** 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`
9. SSH to ADMIN Server and run the following command.
   `nw-manage --refresh-host --host-all`
10. To restart NetWitness, enter the following command:
    service jetty restart

Configure the NetWitness Concentrator Service

1. Log on to NetWitness 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 Investigation.
level is "IndexValues"
name matches the column name of the CSV file that NetWitness uses while defining the recurring feed (see the table in *Configure the Recuring Custom Feed Task in NetWitness* 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.

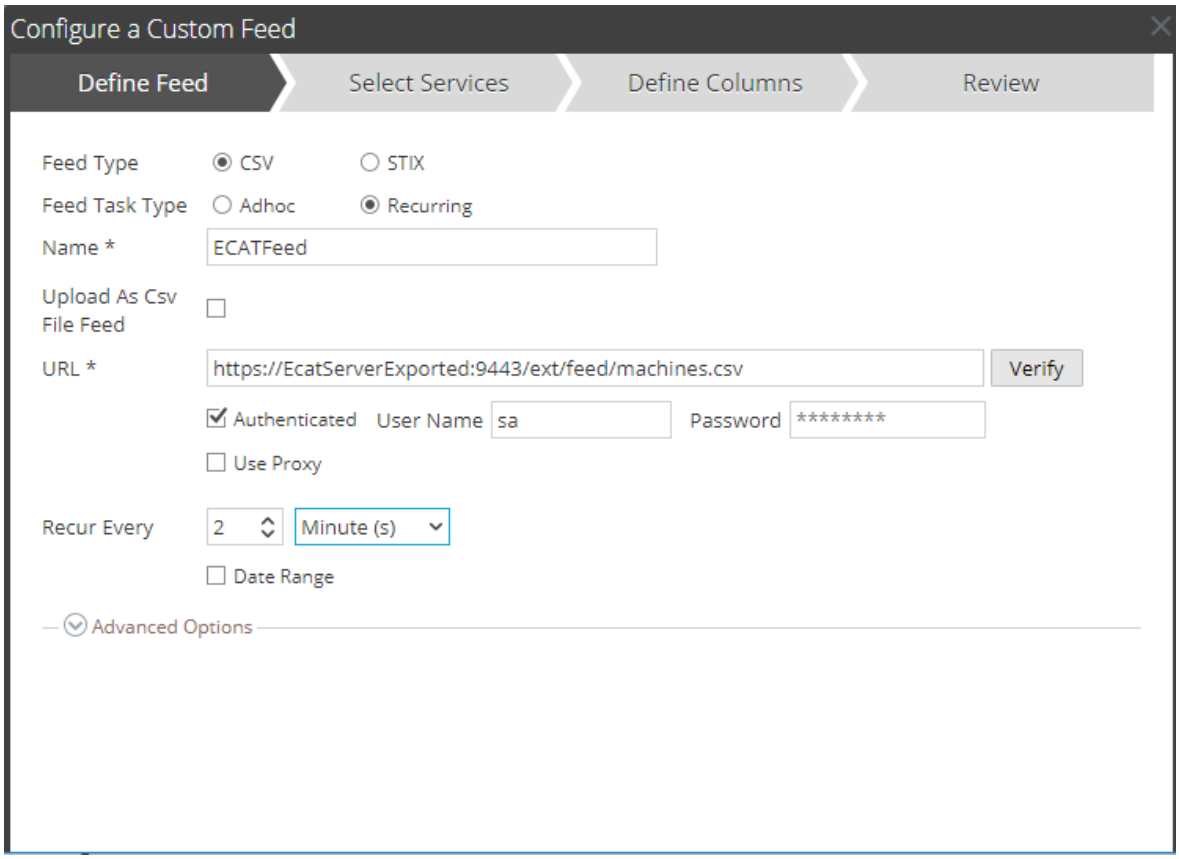
Configure the Recurring Custom Feed Task in NetWitness

1. Log on to NetWitness 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 Type** field, select **CSV**.
   b. In the **Feed Task Type** field, select **Recurring**.
   c. In the **Name** field, enter the name of the feed. For example, EndpointFeed.
   d. Enable the **Upload As Csv File Feed** checkbox to upload the feed as a CSV file.
   e. 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, 4.4, 4.4.0.2, or later 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`**.

f. Enable the **Authenticated**checkbox and enter the username and password as noted in *Enable the ECAT Feed* above.

g. Click **Verify** to check if NetWitness can reach the web resource.

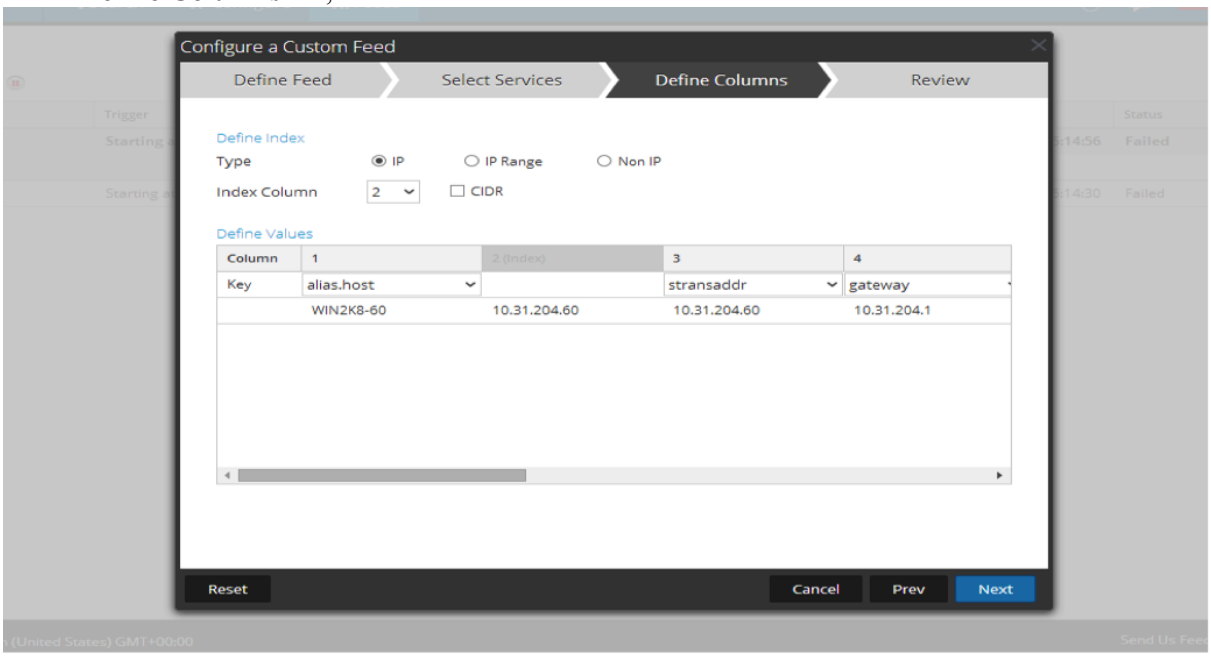
.



h. 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.

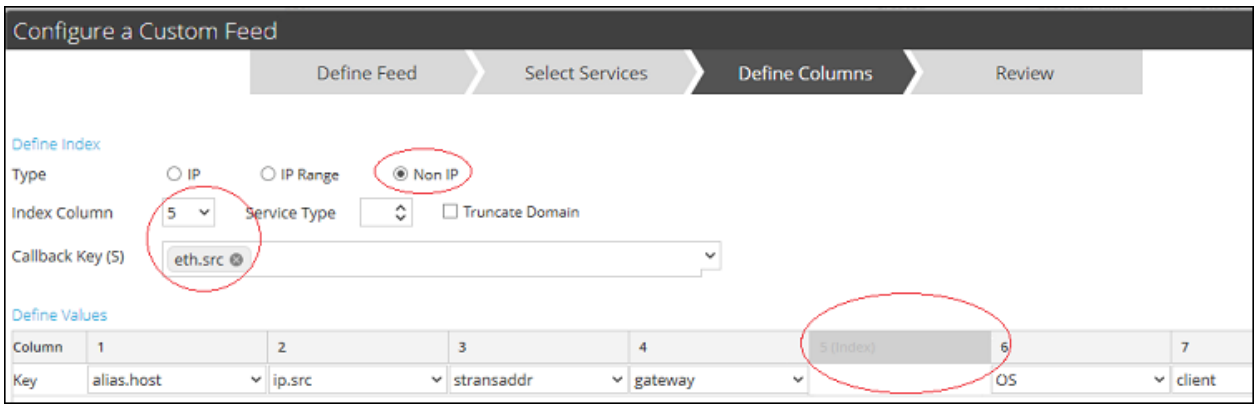


The following table shows the columns in the CSV file for the NetWitness Endpoint feed.

Column	Name	Description	Column Name in NetWitness (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
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

Column	Name	Description	Column Name in NetWitness (Meta Key Name)
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.



Result

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

Configure Endpoint Alerts Through Syslog into a Log Decoder

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

For NetWitness networks that are consuming logs, this integration of NetWitness Endpoint with NetWitness pushes NetWitness Endpoint events to the Log Decoder through common event format (CEF) syslog messages and generates metadata that is used by NetWitness 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 reporting on NetWitness Endpoint events, and NetWitness alerting of NetWitness Endpoint events.

Prerequisites

The following are required for this integration:

- Version 4.3.0.4, 4.3.0.5, 4.4, 4.4.0.2, or later NetWitness Endpoint UI.
- NetWitness Server Version 11.1 is installed.
- Version 10.4 or later NetWitness 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" in the *Malware Analysis Configuration Guide*.

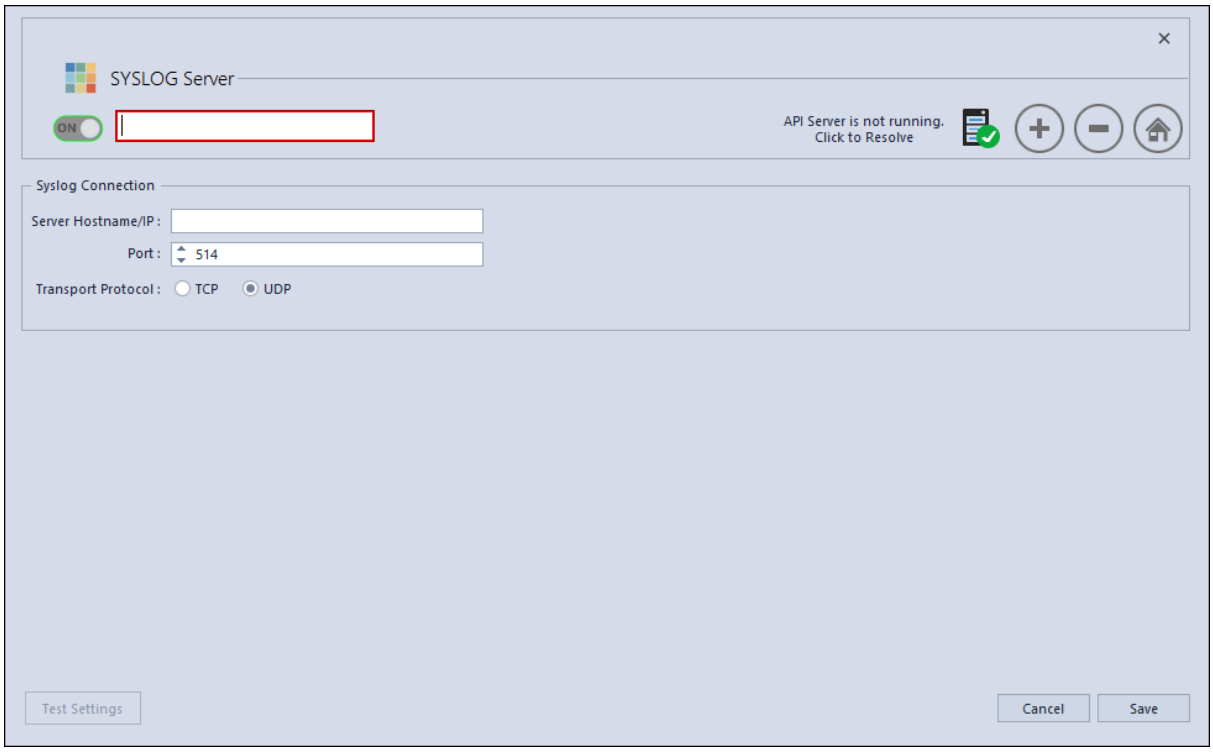
Note: Use only one of these parsers. When the CEF parser is deployed, it supersedes the NetWitness Endpoint parser, and all CEF messages into NetWitness are processed by the CEF parser. Enabling both parsers is an unnecessary burden on performance.

2. Configure NetWitness Endpoint to send syslog output to NetWitness 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.

Configure NetWitness Endpoint to Send Syslog Output to NetWitness

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

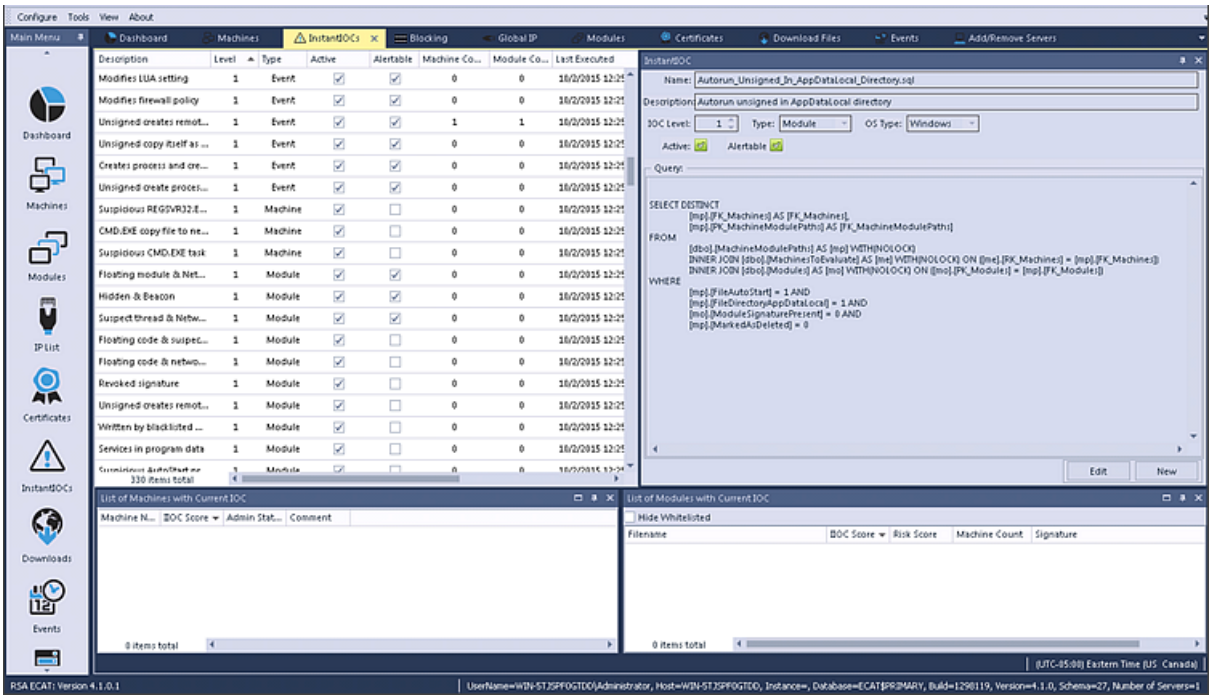
1. Open the NetWitness Endpoint user interface and log on using the proper credentials.
2. From the menu bar, select **(Configure) > Monitoring and External Components**.
   The External Components Configuration dialog is displayed.
3. In **SYSLOG Server**, click .
   The SYSLOG Server dialog is displayed.



4. In the **NetWitness** 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 NetWitness Log Decoder
   Port = 514
   Transport Protocol = Select **UDP** or **TCP** as appropriate for your Syslog server for the transport protocol.

6. Click **Save**.
7. 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 NetWitness table-map.xml provided by NetWitness, 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 Mapping	Transient in NetWitness
agentid	client	No
CEF Header Hostname Field	alias.host	No
CEF Header Product Version	version	No
CEF Header Product Name	Product	Yes
CEF Header Severity	severity	Yes

NetWitness Endpoint Fields	NetWitness Mapping	Transient in NetWitness
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	No
fname	filename	No
fsize	filename.size	No
gatewayip	gateway	Yes
instantIOCLevel	threat.desc	No
instantIOCName	threat.category	No
machineOU	dn	No
machineScore	risk.num	No
md5sum	checksum	No
os	OS	No
port	ip.dstport	No
protocol	protocol	Yes
Raw Message	msg	Yes
remoteip	stransaddr	Yes
rt	alias.host	No
sha256sum	checksum	No
shost	host.src	No
smac	eth.src	No
src	ip.src	No
start	starttime	No
suser	user.dst	No
timezone	timezone	No

NetWitness Endpoint Fields	NetWitness Mapping	Transient in NetWitness
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 you need to add them to `table-map-custom.xml`, and set the flags to `None`.

NetWitness Endpoint Fields	NetWitness Mapping	Transient in NetWitness
moduleScore	cs.modulescore	Yes
moduleSignature	cs.modulesign	Yes
Target module	cs.targetmodule	Yes
YARA result	cs.yararesult	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_yararesult" nwName="cs.yararesult" 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

1. Log on to NetWitness and go to  **(Admin) > Services**.
    1. Select a **Concentrator** from the list and select **View > Config.**
2. Select the **Files** tab, and from the **Files to Edit** drop-down list, select **index-concentrator-custom.xml**.

3. 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.
4. Restart the Concentrator.
5. 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 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="Int32" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Domain OU" 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.yararesult"
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 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 core meta keys as described in the "Conduct an Investigation" topic in *Investigation and Malware Analysis User Guide*.