RSA NetWitness Platform

Event Source Log Configuration Guide

FireEye Endpoint Security (FireEye HX)

Last Modified: Tuesday, June 14, 2022

Event Source Product Information:

Vendor: FireEye
Event Source: FireEye Endpoint Security (HX series)
Versions: 5.1.x

RSA Product Information:

Supported On: NetWitness Platform 11.0 and later
Event Source Log Parser: fireeyehx
Collection Method: Logstash
Event Source Class.Subclass: IPS

To configure the FireEye HX event source, you must complete these tasks:

I. Enable HTTP Notifications on FireEye HX

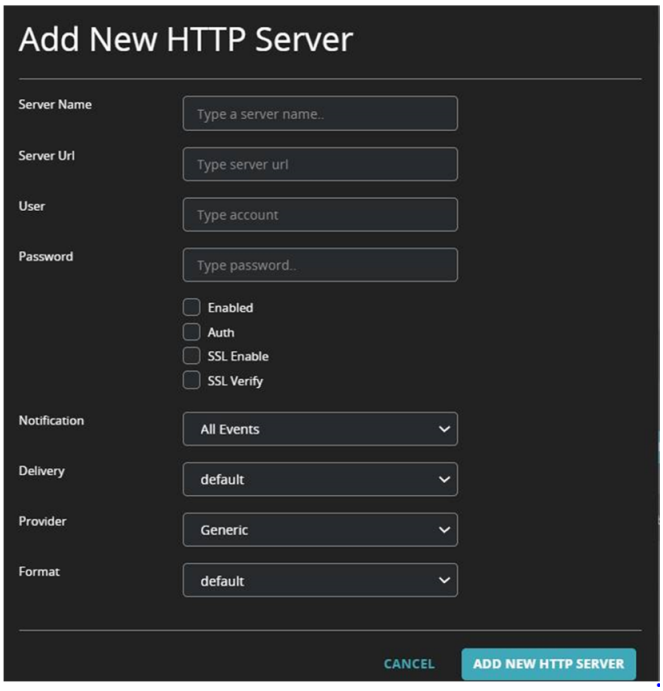
II. Setup the FireEye HX Event Source in the RSA NetWitness Platform

Enable HTTP Notifications on FireEye HX

As the RSA NetWitness Platform supports single - line logs collection, you must enable HTTP notifications to collect single - line logs from FireEye HX.

To enable HTTP Notifications on FireEye HX:

1. Log into the FireEye appliance with an administrator account.
2. Click **Settings**. Click **Notifications**.
3. Click the **http** hyperlink. Make sure the **Event type** check box is selected.
4. Do the following to configure the Global HTTP Settings:
   - Type **NetWitnessHTTP** next to the **Add HTTP Server** tab.
   - Click **Add HTTP Server**.
   - In the newly created **NetWitnessHTTP** entry, make sure the check boxes for **Enabled**, **Auth**, and **SSL Enable** are selected.



5. Enter the following per instance settings. This will override the global settings configured.

   Server URL: `https://<Server URL>:<port>/`

Note:
- Here, **<Server URL>** refers to `http://<your logcollector ip>:<your port>/` and the default port used is **8089**. This port can be changed.
- Make sure the FireEye Appliance and the Log Collector are in the same network.

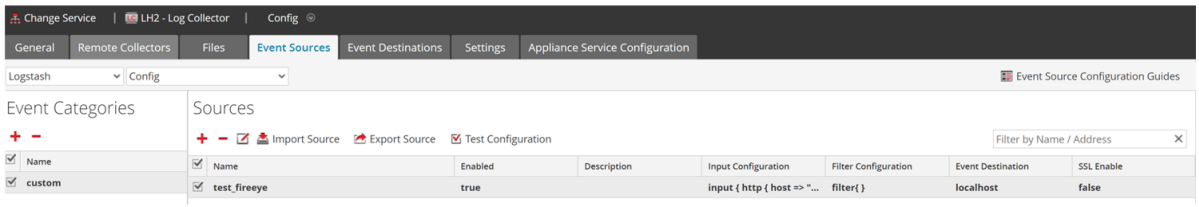
6. Click **Update**.

Note: Ignore the step 5 if the Global HTTP settings are pre-configured.

Setup the FireEye HX Event Source in the RSA NetWitness Platform

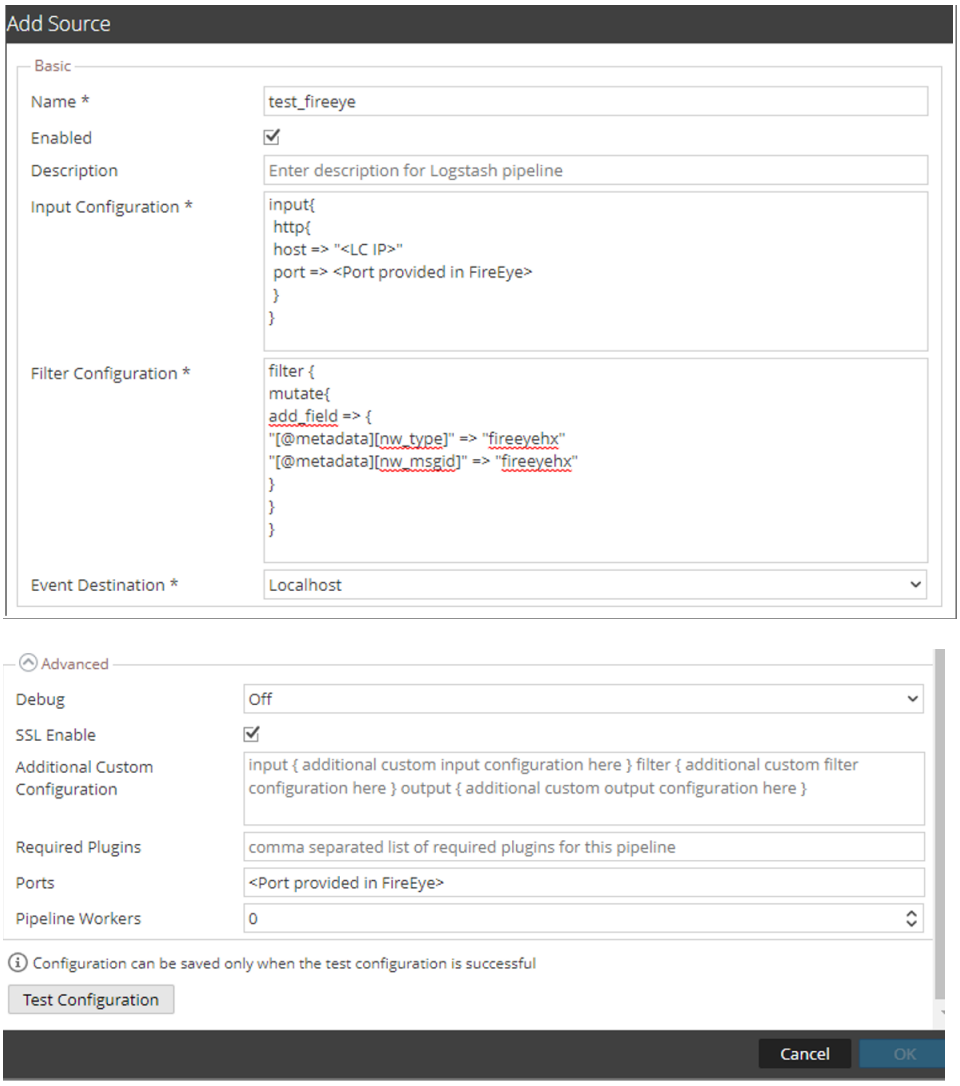
To configure the FireEye HX Event Source:

1. In the RSA NetWitness Platform menu, select **ADMIN** > **Services**.
2. In the **Services** grid, select a Log Collector service, and from the **Actions** menu, choose **View** > **Config**.
3. In the **Event Sources** view, select **Logstash** / **Config** from the drop-down menu.



4. In the **Event Categories** panel toolbar, click  .
5. Select **custom** from the list and in the **Sources** panel, click  .

   The **Add Source** dialog is displayed.



6. Define parameter values, as described in FireEye HX Collection Configuration Parameters.

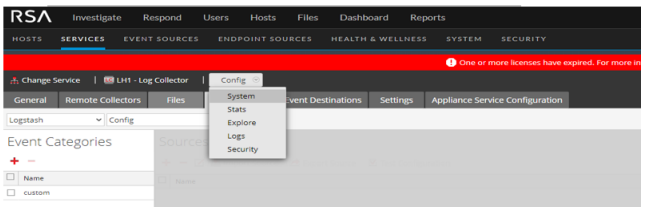
7. Click **Test Configuration**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

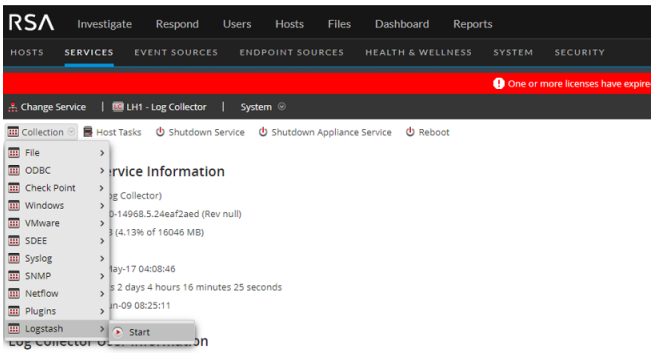
   Note: The Log Collector takes approximately **60** seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

8. If the test is successful, click **OK**. The new event source is displayed in the **Sources** panel.

9. Save the configuration. From the **Actions** menu choose **System**.



10. In the **Collection** drop-down menu, select **Logstash** > **Start**, to start the log collection.



FireEye HX Collection Configuration Parameters

The tables below list the configuration parameters required for integrating FireEye HX with RSA NetWitness Platform.

Note: Fields that are followed by an asterisk (*) are mandatory.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Description	Enter the description for the Logstash pipeline.

Input Configuration *	Enter input configuration for the Logstash pipeline as shown in below.
	`input{`
	`http{`
	`host => "<LC IP>"`
	`port => <Port provided in FireEye>`
	`}`
	`}`

Filter Configuration *	Enter filter configuration for the Logstash pipeline as shown below.
	`filter {`
	`mutate{`
	`add_field => {`

Name	Description
	"[@metadata][nw_type]" => "fireeyehx" "[@metadata][nw_msgid]" => "fireeyehx" } } } **Note:** You should not change **fireeyehx** in "[@metadata][nw_type]" => "fireeyehx" and "[@metadata][nw_msgid]" => "fireeyehx", as they are the names of the parser and message ID respectively.
Event Destination *	The NetWitness Log Collector or Log Decoder to which the event logs have to be sent.

Advanced Parameters

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. **Caution:** Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed for debugging and monitoring isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enable	Uncheck to disable certificate verification.
Additional Custom Con-	Logstash pipeline additional custom configuration for input, filter

Name	Description
figuration	or output sections. This is optional.
Required Plugins	Logstash plugins required by the custom pipeline configurations in a comma separated list.
Ports	Ports required by the custom pipeline configurations (refer the screenshots below step 5 under Setup the FireEye HX Event Source in the RSA NetWitness Platform).
Pipeline Workers	Number of pipeline worker threads allocated for logstash pipeline execution.

Deploy FireEye HX parser from LIVE

To deploy the FireEye HX parser from Live:

1. In the RSA NetWitness Platform menu, select **ADMIN** > **Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** menu, choose **View** > **Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and make sure that the **Config Value** field for your event source is selected.

November 2020

Trademarks