ENDPOINT SECURITY

EVENT STREAMER v1.1.8

MODULE USER GUIDE

GENERAL AVAILABILITY RELEASE

FireEye and the FireEye logo are registered trademarks of FireEye, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

FireEye assumes no responsibility for any inaccuracies in this document. FireEye reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Endpoint Security Event Streamer Module

Software Release 1.1.8

Revision 2

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: https://csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

CONTENTS

PART I: Module Overview

Event Streamer is an Endpoint Security Innovation Architecture (IA) module designed to forward Windows Event Log data to Helix and third-party servers supporting the Syslog protocol. This module supports configurable streaming of the System, Application Experience, Security, AppLocker, PowerShell, Application, Windows Defender, Task Scheduler, Print Service, and Terminal Services event logs using the Syslog protocol as defined by RFC 5424.

Event Log data is recorded locally by an Endpoint Agent module, and then streamed to a Helix instance, a Syslog server, or both, based on its configuration. It utilizes communication with an Endpoint Security server for module settings.

Prerequisites

This release of Event Streamer is supported on **Endpoint Security 5.0.0** with **Endpoint Security Agent software version 31 or later** running on **Windows 7 and above**. FireEye recommends running with the latest Windows updates applied. Please review *Appendix A* for dependencies, limitations and known issues for the current release.

Note: It is not recommended to install Event Streamer on Endpoint Security 4.9.x with Endpoint Agent 30 or lower. This is not a supported scenario.

PART II: Installing Event Streamer Module

Event Streamer is an optional module available for **Endpoint Security 5.0.0** with **Endpoint Security Agent 31 or later**. It is installed by downloading the module installer package (.cms file) from the FireEye Market and then uploading it using the Endpoint Security Web UI. The module is disabled by default. Refer to *Part IV: Enabling the Event Streamer Module* for steps to enable the server module. After you have installed it, the module appears on the Modules menu tab.

Downloading the Installer Package

To download the module installer package:

1. Log in to the Endpoint Security Web UI with your administrator credentials.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, click **Find Modules** to access the FireEye Market. The FireEye Market opens in a new browser tab.
4. In the **Types** filter list on the FireEye Market, select **Endpoint Security Modules**.
5. In the Search Results, click the **Event Streamer** module.
6. On the FireEye Market page for the **Event Streamer** module, click **Download** to download the module .cms file to your local drive.

   Be sure to note the navigation path to the directory where you downloaded the .cms file.

Uploading the Installer Package

To upload the Event Streamer module installer package to your Endpoint Security Web UI:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, click **Upload Modules** to upload the module .cms file from your local drive. The .cms file includes the **server module** and **agent module** of Event Streamer.
4. In the **Upload Module** dialog box, click **Select File.**
5. Navigate to the downloaded module .cms file, select the .cms file, and click **Open**.

   The selected .cms file appears in the **Upload Module** dialog box.
6. In the **Upload Module** dialog box, click **Upload**.

   A message at the top of the page tells you that module installation has been initiated. After you have uploaded the module successfully, it appears in the list of modules on the Modules page.

7. If the module is installed successfully, it must be enabled before use as described in the section *Part IV: Enabling the Event Streamer Module* below.

NOTE: You may need to refresh the Endpoint Security Web UI before the new module appears on the Modules page.

Configuring the Helix ID and Helix Token Service URL

You need to configure a token server and Helix ID on the **Endpoint Security Server** to enable the **Event Streamer** module to communicate with **Helix**. The token server must be configured separately on the DMZ, if applicable.

Configuring the Token Service URL manually is only necessary if you're running Endpoint Security 5.0.0 or 5.0.1. It is configured by default in 5.0.2 and above. To configure the token server through the command line interface:

1. Establish an SSH connection to the HX server and log in using administrator credentials.
2. Type the command: **en**
3. Type the command: **config terminal**
4. For customers running Endpoint Security version 5.0.0 or 5.0.1 (not required for 5.0.2 and above), the customer must send an email to request.token@fireeye.com to request the Token Service URL before running the following command. Note that this Token Service is not the same as the fenet token service required by a Virtual HX.
5. For customers running Endpoint Security version 5.0.0 or 5.0.1 (not required for 5.0.2 and above), type the command: **hx server fe-token-service url <Token Service URL>**

Where <Token Service URL> is the URL of the Helix token server.

To configure the Helix ID through the command line interface:

1. Establish an SSH connection to the HX server and log in using administrator credentials.
2. Type the command: **en**
3. Type the command: **config terminal**
4. Type the command: **helix mode cloud**
5. Type the command: **helix console url <Helix URL>**
6. Type the command: **aaa authentication oidc web policy allowed**

Where <Helix URL> is the URL of the Helix instance (https://apps.fireeye.com/helix/id/<HELIX_ID>).

Installing the Event Streamer Agent Module

The **Event Streamer** module consists of a **server module** and an **agent module**. The above section provided steps to upload the Event Streamer module to the Endpoint Security server. To install the **agent module** on a given host set:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Admin** menu, select **Policies** to access the **Policies** page.

3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to activate Event Streamer, and select **Edit Policy**.

4. Click on the **Categories** button in the **Edit Policy** page and select ***Event Streamer – <version number>*** (e.g., Event Streamer – 1.1.8) and click **Apply**.

5. On the **Edit Policy** page, click the **Save** button.

The above steps will inform the endpoints (local systems) to download the agent module and install it during configuration update. Please review the *Configuring Event Streamer Agent Policy* section below to understand various policy options.

PART III: Uninstalling Event Streamer Module

To uninstall the Event Streamer module from your Endpoint Security Web UI:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.

3. On the **Modules** page, locate the **Event Streamer** module and click the **Actions** icon (the gear icon) and select *Uninstall* to uninstall the module. A confirmation window appears before uninstallation can proceed. Click Uninstall to start the uninstallation of the module.

   A message at the top of the page tells you that module uninstallation succeeded.

The **Event Streamer** module consists of a **server module** and an **agent module**. Uninstalling the **Event Streamer** module removes Event Streamer policy settings from all policies and ensures that both **server module** and the **agent module** are removed from endpoints (local systems).

Uninstalling the Event Streamer Agent Module

The **Event Streamer** module consists of a **server module** and an **agent module**. The above section provided steps to uninstall the Event Streamer module completely from the Endpoint Security server and managed FireEye endpoints. To remove only the **agent module** on a given host set:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Admin** menu, select **Policies** to access the **Policies** page.

3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to remove the **Event Streamer**, and select **Edit Policy**.

4. Click on the **Categories** button in the **Edit Policy** page and unselect ***Event Streamer – <version number>*** (e.g., Event Streamer – 1.1.8) and click **Apply**.

5. On the **Edit Policy** page, click the **Save** button.

PART IV: Configuring Event Streamer Module

The Event Streamer module consists of a **server module** and an **agent module**. It is important to understand the following relationships between the server and agent modules:

- You install and enable the Event Streamer module on agents using the Event Streamer policy section.
- After you enable the **server module**, disabling the **server module disables** the **agent module** in **all policies**.
- Uninstalling the **Event Streamer** module removes the Event Streamer section from all policies and ensures that both **server module** and the **agent module** are removed from endpoints (local systems).

Enabling the Event Streamer Module

You can perform these tasks from the Modules and Policies pages in the Endpoint Security Web UI.

Before proceeding, please review the *Configuring Event Streamer Agent* Policy section below. You should understand the implications of these settings before enabling Event Streamer on endpoint agents.

To enable the Event Streamer server module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, locate the **Event Streamer** module and click the **Actions** icon (the gear symbol) and select **Enable** to enable the module.

To enable the Event Streamer agent module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the **Admin** menu, select **Policies** to access the **Policies** page.
3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to activate Event Streamer, and select **Edit Policy**.
4. In the **Configurations** area of the **Edit Policy** page, click the button labeled **Categories**. This will open a dropdown, with a checkbox labeled **Event Streamer**. Make sure this is checked, and then click the **Apply** button to add the Event Streamer section to the policy.
5. In the **Event Streamer** policy section, toggle the **Enable Event Streamer on the host** selector to **ON**.
6. If you are editing Agent Default Policy, leave all other settings at the default value. If you want to make any adjustments, please review the *Configuring Event Streamer Agent Policy* section below first.
7. On the **Edit Policy** page, click the **Save** button.

Disabling the Event Streamer Module

To disable the <u>server module</u>:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.

3. On the **Modules** page, locate the **Event Streamer** module and click the **Actions** icon (the gear icon) and select **Disable** to disable the module.

Disabling the Event Streamer **server module** (once enabled) will disable the **agent module** in all the policies, causing it to be disabled on associated endpoints (local systems).

To disable the <u>agent module</u>:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Admin** menu, select **Policies** to access the **Policies** page.

3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to disable Event Streamer, and select **Edit Policy.**

4. In the **Configurations** area of the **Edit Policy** page, click **Event Streamer**.

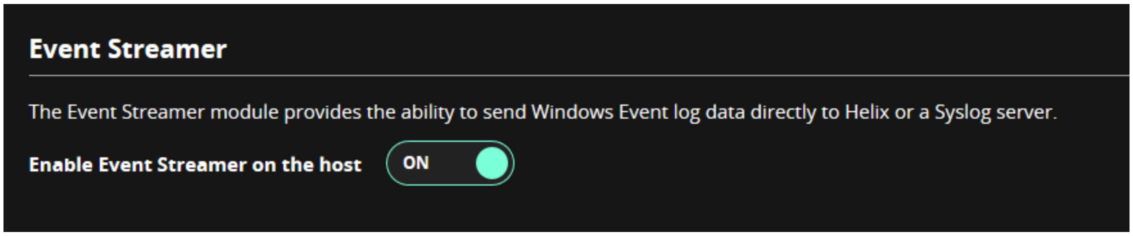
5. Toggle the **Enable Event Streamer on the host** selector to **OFF**.

6. On the **Edit Policy** page, click the **Save** button.

Note: When enabling or disabling the server module in the **HX Module Administration** page, a message will appear at the top of the page to confirm that the Event Streamer module has been enabled or disabled**.** The Status column for the Event Streamer module will also update to display **Enabled** or **Disabled**.

Configuring Event Streamer Agent Policy

This section describes the various configuration settings provided in the Event Streamer policy.



Event Streamer

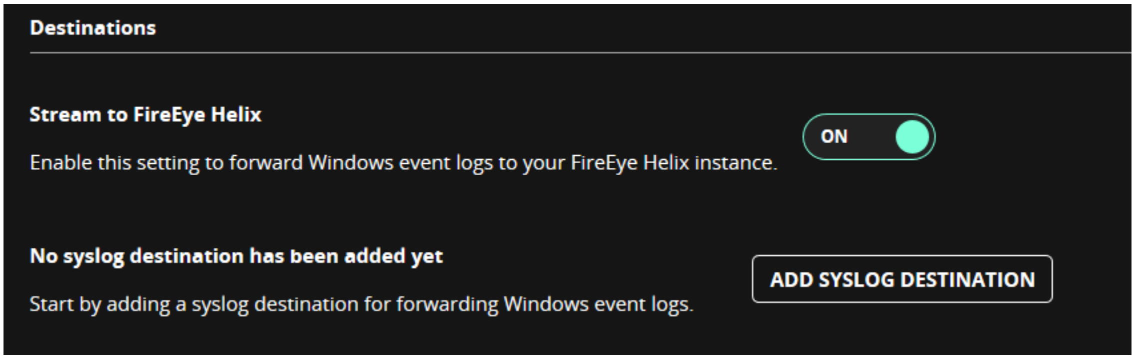
The Event Streamer module provides the ability to send Windows Event log data directly to Helix or a Syslog server.

Enable Event Streamer on the host ON

Figure 1 Event Streamer Policy on HX Server

To enable Event Streamer for the current policy, toggle the setting **Enable Event Streamer on the host** to **ON** and save the policy changes.

Destinations



Destinations

Stream to FireEye Helix

Enable this setting to forward Windows event logs to your FireEye Helix instance. ON

No syslog destination has been added yet

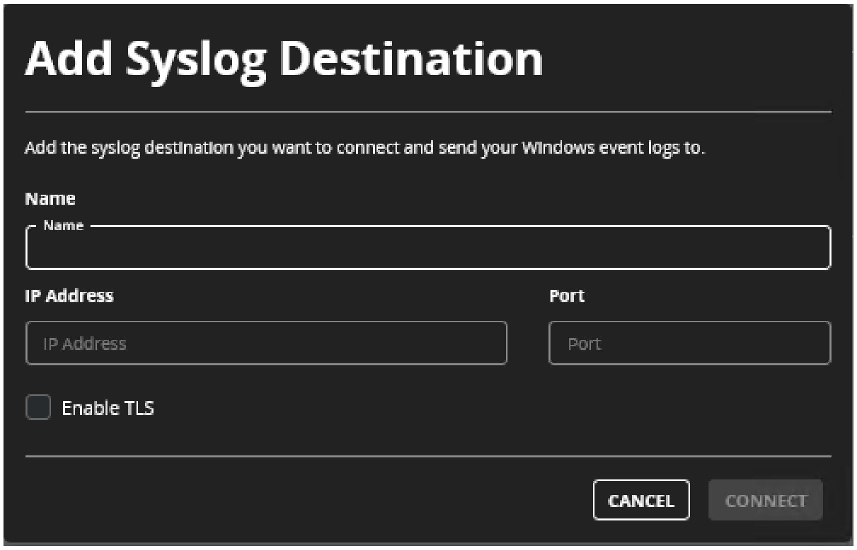
Start by adding a syslog destination for forwarding Windows event logs.

Figure 2 Event Streamer Destinations

To enable event streaming to your Helix instance, toggle the setting **Stream to FireEye Helix** to **ON**.

To configure a Syslog server for Event Streamer communication, input the server settings under **Destinations**. To add a server, click the button **Add Syslog Destination**. Refer to *Figure 3* below for an example of what this interface looks like. This section contains **Name**, which allows you to record a name for the server, **IP Address**, which should be the IPv4 address of the intended server, and **Port**, which should be the port number used by Event Streamer to connect to the server. Lastly, there's a checkbox labeled **TLS Enabled**, which indicates that Event Streamer should establish a secure connection using TLS when connecting to the server.

Note: When enabling this setting, make sure that the configured port accepts TLS connections. Event Streamer supports only TLS 1.1 and 1.2.



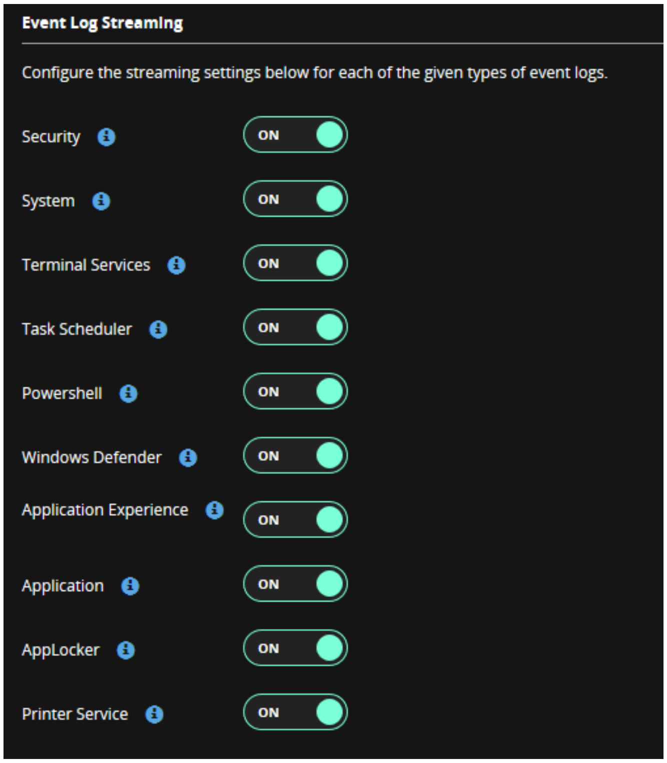
Add Syslog Destination

Add the syslog destination you want to connect and send your Windows event logs to.

□ Enable TLS

Figure 3 Event Streamer Syslog Destination Configuration

Event Log Streaming



Event Log Streaming

Configure the streaming settings below for each of the given types of event logs.

Security	ON
System	ON
Terminal Services	ON
Task Scheduler	ON
Powershell	ON
Windows Defender	ON
Application Experience	ON
Application	ON
AppLocker	ON
Printer Service	ON

Figure 4 Event Streamer Event Log Streaming

Event Log Streaming settings allow an admin to configure which Windows event logs will be monitored. When any of these settings is **ON**, Event Streamer will be configured to record events from the selected event log and stream them. These settings apply to both Helix and Syslog event streaming.

Additional settings are present only in the Endpoint Agent configuration to control monitoring for specific event IDs, advanced logging options, and event recording. These can only be configured through the Endpoint Server API. See the section *Configuring Event Streamer Policy Using the HX API* for more details.

Configuring Event Streamer Policy Using the HX API

Event Streamer makes use of some configuration which doesn’t correspond to any setting currently in the User Interface, to allow fine tuning of event collection. These settings can be updated using the HX API **/hx/api/v3/policies/**

Consult the *HX API Guide* for more information on how to use the API to update these settings.

Event Streamer does not introduce any new API, it’s only possible to use existing HX APIs to configure Event Streamer policy.

The following table lists important settings which can be configured using this method. Note that changing any of these settings to an invalid value (such as a negative number) may cause unexpected behavior in Event Streamer.

General Settings

Setting Name	Description	Default
maxEventsInDB	Maximum number of events to be stored in the cache database before being sent to a Helix instance or Syslog server. Events are removed from the database when they’re successfully sent to the server. Once the maximum number of events is hit, the oldest events are purged from the database. This value is a positive integer but must be passed down as a string.	"10000"
deleteBatchCount	How many events should be deleted when the cache database reaches the configured maximum. This is only used when Event Streamer hits the maximum value specified by the maxEventsInDB setting. This value is a positive integer but must be passed down as a string.	"100"
sendEventsTimeout	How long (in seconds) Event Streamer will wait before sending a new batch of events in the database to the server. This value is a positive integer but must be passed down as a string.	"20"
maxEventsPerTimeout	Maximum number of events that will be sent to the Helix instance or Syslog server at once. If more events are in the database than this value, only the oldest entries are sent up to this limit. Together with sendEventsTimeout, this value can be used to control the maximum throughput of events sent to the server. This value is a positive integer but must be passed down as a string.	"250"
filters	A listing of executables and event IDs from those executables that should not be collected or sent to the Helix instance or Syslog server. This setting can be used to avoid sending data that is not useful or causing excessive noise. This is an array of string values. Refer to the section *Updating Filters (Event Exclusions)* below for an example.	<empty>

Event Log Settings

Setting Name	Description	Default
systemEventIds	The System event IDs, in a comma delimited list, that Event Streamer should monitor.	"7036, 7045, 104, 6, 1125, 1127, 1129, 41, 219, 100, 20, 24, 25, 31, 34, 35, 7022, 7023, 7024, 7026, 7031, 7032, 7034, 7040"
appExperEventIds	The Application Experience event IDs, in a comma delimited list, that Event Streamer should monitor.	"903, 904"
securityEventIds	The Security event IDs, in a comma delimited list, that Event Streamer should monitor.	"5145, 4697, 601, 4688, 592, 4689, 1102, 4720, 4624, 540, 602, 4652, 529, 624, 517, 4768, 4769,4732, 636, 4622, 4771, 4776, 4657, 4663, 4704, 4728, 4756, 5152, 5038, 4946, 4947, 4948, 4950, 4951, 4952, 4954, 4957, 4958, 632, 657, 660, 663, 675, 676, 680, 849, 850, 851, 852, 853, 854, 855, 857, 859, 860, 861, 5025, 5027, 5028, 5029, 5030, 5034, 5035, 5037, 6281, 4953, 5031, 5050"
appLockerEventIds	The App Locker event IDs, in a comma delimited list, that Event Streamer should monitor.	"8003, 8004, 8005, 8006"
powershellEventIds	The Powershell event IDs, in a comma delimited list, that Event Streamer should monitor.	"4103, 4104"
applicationEventIds	The Application event IDs, in a comma delimited list, that Event Streamer should monitor.	"11707, 4097, 2, 1, 1033, 8194, 1001"
winDefenderEventIds	The Windows Defender event IDs, in a comma delimited list, that Event Streamer should monitor.	"1005, 1006, 1010, 2001, 2003, 2004, 3002, 5008"
taskSchedulerEventIds	The Task Scheduler event IDs, in a comma delimited list, that Event Streamer should monitor.	"106, 200, 203"
terminalServicesEventIds	The Terminal Services event IDs, in a comma delimited list, that Event Streamer should monitor.	"21, 22, 23, 24, 25, 1149"
printerSvcEventIds	The Printer Service event IDs, in a comma delimited list, that Event Streamer should monitor.	"307"

Updating Filters (Event Exclusions)

The **filters** setting allows you to exclude events from processing by Event Streamer. These filters are based on executable path and will apply to any process instance of the configured executable. For each executable specified, you can provide a list of one or more event IDs which will not be recorded. This can be utilized to remove noisy or unimportant events.

The executable path included in a filter must be an exact match, there is currently no support for pattern matching or wildcards. Also note that these filters are not guaranteed to filter all events. Some events triggered by a process do not contain the process executable path field, meaning it's not possible to filter based on that criteria.

Here is an example of a possible set of exclusions configured using the API:

[“C:\\Program Files (x86)\\FireEye\\xagt\\xagt.exe:: 7036, 7045, 104”, “C:\\example.exe:: 903, 904”]

This configuration for the **filters** setting would remove monitoring for the System event IDs 7036, 7045, and 104 for the FireEye process xagt.exe, as well as the Application Experience IDs 903 and 904 for example.exe at the specified path.

APPENDIX A: Frequently Asked Questions

How do I verify if the Event Streamer installation succeeded?

Once Event Streamer is installed and enabled, it will run without any user interaction. To verify that it's installed, look for the file EventStreamer.dll under the FireEye ProgramData folder at this location:

%PROGRAMDATA%\FireEye\xagt\exts\plugin\EventStreamer\EventStreamer.dll

How do I verify if Event Streamer is running after install?

To verify that Event Streamer is running and recording events for an Endpoint Agent, check for the following additional file:

%PROGRAMDATA%\FireEye\xagt\exts\EventStreamer\sandbox\events.db

Another way to verify that EventStreamer is running is by checking the full contents of an Agent sysinfo, which can be acquired using the HX API **/hx/api/v3/hosts/<agent_id>/sysinfo** or by checking the sysinfo contents using HXTool (downloaded in the FireEye Market). You should see the fields **EventStreamerStatus** as *running*. Several other fields should be populated, including **EventStreamer/plugin_start** which indicates the last start time of Event Streamer. This requires an account with the api_admin role.

Does Event Streamer support streaming events to Helix and a Syslog server simultaneously?

Yes, Event Streamer can be configured to send events to only Helix, only a Syslog server, or both simultaneously. If both are configured, each event generated will be sent to both Helix and Syslog. Note that events are stored separately prior to being sent to these servers, so each event will be recorded in the Event Streamer database once for Helix and again for Syslog.

Is it possible for Event Streamer to miss some events?

Event Streamer sends events in batches periodically. The time period and maximum number of events sent at each iteration is controlled by configuration. If the number of events recorded exceeds the rate of events sent based on this configuration on average, it's likely that some events will be dropped without being sent. This can be resolved by adjusting the settings that configure the time limit and maximum number of events. Note that the time period between sending batches of events is a minimum, there may be some extra time in between events being sent.

Will Event Streamer have a large impact on system performance?

The Event Streamer agent module should not have a significant impact on CPU, disk, or memory utilization. The number of events recorded and sent to a Helix instance or Syslog server may vary in different environments and on different systems. If the number of events is too high, you can reduce the load by disabling specific Windows Event logs (See the section *Event Log Streaming* above) or configuring exclusions (See the section *Updating Filters (Event Exclusions)* above).

Are there any log files created during installation on the Endpoint Agents?

The Event Streamer **agent module** does not create any additional log files during install, upgrade, or uninstall.

What processes are created when Event Streamer is installed and enabled?

After installation, Event Streamer spawns an instance of xagt.exe with *EventStreamer* in its command line. This is a container application to interact with agent services. This process runs under the System account like any other agent instances.

Does Event Streamer depend on any other Endpoint Security modules?

No, the Event Streamer **server** and **agent modules** have no dependencies.

What is the expected behavior if the Endpoint Security server goes offline?

Event Streamer will be unable to receive configuration updates but should continue to record events and send them to the configured Helix instance or Syslog server.

Can I install Event Streamer on an earlier version of the Endpoint Agent (e.g. 29, 30) and then upgrade to a supported version?

This is not a supported scenario. It’s recommended to upgrade to supported versions of the Endpoint Security server and agent prior to deploying Event Streamer.

How can I check if Event Streamer is sending events successfully or failing to send events?

Event Streamer will log information in the Agent logs when sending events. When attempting to send events, it will log the following lines for Helix and Syslog:

Attempting to send # events to Helix.

Attempting to send # syslog events (TCP).

Where # is the number of events it's attempting to send at once. If some number of Syslog events were successfully sent, but some failed, it will log:

Successfully sent # syslog events. Failed to send # syslog events.

As Helix sends many events all at once, any failure will mean that none of the events are delivered. If all events failed to send, it will log:

Failed to send events to Helix, error: #

Failure to send syslog data, will try again at next timer callback

Additionally, you can view Event Streamer Sysinfo data to check how many events have been sent successfully or failed within the last Sysinfo period. Using the HX API **/hx/api/v3/hosts/<agent_id>/sysinfo** or HXTool (downloaded in the FireEye Market), you can view the following Event Streamer fields:

events_in_db	Number of events remaining in the Event Streamer database.
total_helix_events_sent	Total number of events sent to Helix since the last Sysinfo.
total_helix_events_failed	Total number of events that failed when being sent to Helix since the last Sysinfo. Note that these are not unique events. A batch of events failing to send multiple times will count towards this total for each failure.
total_syslog_events_sent	Total number of events sent to the Syslog server since the last Sysinfo.
total_syslog_events_failed	Total number of events that failed when being sent to the Syslog server.
last_helix_try	Time indicating the last attempted communication with Helix.
last_helix_success	Time indicating the last successful communication with Helix.
last_syslog_try	Time indicating the last attempted communication with the Syslog server.
last_syslog_success	Time indicating the last successful communication with the Syslog server.
total_events_generated	Total unique events generated since the last Sysinfo.
total_events_dropped	Total number of events that were dropped without being sent since the last Sysinfo.

How can I check if Helix is receiving events from Event Streamer?

You can search for Event Streamer events in Helix by running the following query:

program=EventStreamer | *groupby source*

Why does the "Module Administration" page in the Endpoint Security Server UI show the "State" of the plugin as "Failed"?

When this occurs, the **Status Information** column for the module will show a more detailed error message indicating the cause of the failure. This could occur for several reasons, including (but not limited to):

1. Attempting to re-upload an already installed package.
2. Attempting to upload a corrupted package.
3. Network connection issues, in which case re-attempting install may resolve the failure.

How can I control the rate of events being streamed?

Event Streamer has several configuration options which are not controllable via the Endpoint Security Server Web UI. Several of these settings can be used to control the frequency and number of events that are streamed. These settings are controllable using the HX API. For more information, refer to the section *Configuring Event Streamer Policy Using the HX API*.

Can I filter out unnecessary or unimportant events?

Aside from the ability to monitor specific events logs, it's also possible to control the monitored event ID's, and to configure filters to drop events coming from specific processes (See the section *Updating Filters (Event Exclusions)* above).

Why do some Syslog events show up broken into smaller portions?

Events may appear in several smaller portions due to limitations on message size defined in the Syslog protocol, or message size settings configured for a Syslog server.

How does Event Streamer record events when you have both Helix and Syslog enabled and how does this impact the setting maxEventsInDB?

When both are enabled, Event Streamer records each event twice – once for Helix, and once for Syslog. This does not impact the setting *maxEventsInDB*, so any event recorded will still count as two events towards the maximum limit. When events are sent, the limit set by *maxEventsPerTimeout* applies to Helix and Syslog separately, so Event Streamer should send up to *maxEventsPerTimeout* to Helix and the same amount to Syslog.

What versions of TLS does Event Streamer support?

Event Streamer supports TLS 1.1 and 1.2. It does not support communication using TLS 1.0.

Do I need to whitelist any URL in my firewall?

Make sure to whitelist the Helix Token Service URL for your Endpoint Security server. The Endpoint Security server must be able to reach this Token Service URL for any events to be sent to a Helix instance. For the Endpoint Security Agent, you must whitelist the Helix Ingest URL (<helixid>.ingest.apps.fireeye.com) and Syslog server address, depending on whether the Agent is configured to send events to a Helix instance, a Syslog server, or both.

Does Event Streamer need to communicate with Helix directly or can it go through a Commbroker or Cloud Collector?

Once configured, Event Streamer sends Windows Event Log events directly to Helix. No other component is needed between the Endpoint Agent and Helix. Sending via a Commbroker or Cloud Collector is not supported.

Is there a limit to the number of event IDs Event Streamer can monitor?

Windows limits the number of event IDs you can monitor from a single event log to 80. This means that you cannot include more than 80 event IDs in a single category. This is not a limit on the total number of event IDs monitored, only for each category (e.g. securityEventIds).

Does Event Streamer support streaming to IBM QRadar?

No, Syslog streaming through Event Streamer cannot be configured for use with IBM QRadar SIEM.

Dependencies / Limitations / Known Issues

- This release of the Event Streamer module is supported on Endpoint Security 5.0.0 with Endpoint Security Agent software version 31 or later running on the Windows Operating System, Windows 7 and above only. Mac OS and Linux platforms are not supported. Event Streamer is not supported with Endpoint Security version 4.9.x or lower, or Endpoint Agent version 30 or lower.
- Upgrade is only valid going from the currently installed release, to the next release of Event Streamer. Upgrades from older versions, which skip some intermediate versions, are not valid.
- It is not possible to use an IPv6 address when configuring a Syslog server. If an IPv6 address is used, Event Streamer will be unable to connect to the server (ENDPT-58399).
- It is not possible to specify a host name for the Syslog server, only an IPv4 address (ENDPT-61043).
- If any event log is enabled after Event Streamer is started, Event Streamer will not record events from that source until after it's restarted (ENDPT-62977).
- If the Helix configuration is added or changed after the Event Streamer agent module is installed, you will need to disable and then re-enable the module before the new Helix configuration is applied (ENDPT-66084)
- Syslog port field in the Endpoint Security server UI incorrectly accepts space characters and includes them in the port (ENDPT-65884)