ENDPOINT SECURITY
EVENT STREAMER
GENERAL AVAILABILITY RELEASE NOTES
RELEASE 1.1.8

Endpoint Security Event Streamer

Software Release 1.1.8

Revision 1

FireEye Contact Information:

Website: www.fireeye.com

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

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

Announcements

Thank you for using this FireEye Product. This document provides an overview of the new features, resolved issues, and known issues in the FireEye Endpoint Security Event Streamer 1.1.8 release.

FireEye Customer Security Best Practices

Because our quality assurance process includes continuous security testing, FireEye recommends updating all FireEye products with the latest releases as soon as possible. As an overall strategy to reduce risk exposure, customers are also encouraged to follow best practices, which include:

- Always keep the product version up to date.
- Limit network access to the management interfaces of the appliance using firewalls or similar measures.
- Only issue accounts to trusted administrators.
- Use strong passwords.
- Monitor logs.
- Restrict physical access to the appliance to trusted administrators.

Endpoint Event Streamer

This release of Event Streamer is supported on **Endpoint Security 5.0.0 or later** with **Agent 31 or later** running on **Windows 7 and above**.

Note: This release is supported on Windows platform only. It is not recommended to install Event Streamer release 1.1.8 on Endpoint Security Server 4.9.x with Agent 30 or lower versions. This is not a supported scenario.

Features

Event Streamer is an Endpoint Security Innovation Architecture (IA) module designed to enable Windows Event Log event streaming. This module provides the following features:

- Streaming events to a FireEye Helix server.
- Streaming events to a 3rd party server supporting the Syslog protocol.
- Streaming of the System, Application Experience, Security, AppLocker, PowerShell, Application, Windows Defender, Task Scheduler, Print Service, and Terminal Services event logs.
- Configurable streaming of events based on event log and event ID.

For more details on usage of these features, see the *Endpoint Security Event Streamer module user guide*.

Installation Instructions

Event Streamer is an optional module available for **Endpoint Security 5.0.0** with **Agent 31 or later**. It is installed using your Endpoint Security Web UI by downloading the module installer package (.cms file) from the FireEye Market and then uploading the module .cms file to your Endpoint Security Web UI. The module is disabled by default.

Prior to installing and configuring Event Streamer, see the Event Streamer module user guide for install and configuration steps. You must configure a Helix ID and Helix Token Service URL on the Endpoint Security Server prior to installing Event Streamer. The steps for this are detailed in the section *Configuring the Helix ID and Helix Token Service URL* in the module user guide. Any customer running Endpoint Security version 5.0.0 or 5.0.1 will need to email request.token@fireeye.com to request the Token Service URL. Refer to *Enabling the Event Streamer Module* for steps to enable the server module. After installation, the module appears on the Modules menu tab.

Note: If you have non-Windows hosts, FireEye recommends that you exclude them from Event Streamer module installation because the 1.1.8 release doesn't support mac OS and Linux platforms.

Product Compatibility

This section describes the product compatibility for Event Streamer release 1.1.8

Agent Version	Endpoint Security Server Version	Operating System Requirements		
		Windows	macOS	Linux
31+	5.0.0+	Yes	No	No

Supported Windows operating systems:

Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

Resolved Issues

- Resolved security issue. (ENDPT-75963)

Known Issues

The following issues are known in Event Streamer release 1.1.8.

- 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).
- Event Streamer cannot communicate using TLS version 1.0 (ENDPT-60330).
- 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)

Technical Support

For General Availability modules, contact FireEye through the Support portal https://csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required) https://docs.fireeye.com