# Table of Contents

Table of Contents.......................................................................................................................... 2
About This eStreamer eNcore for Splunk Operations Guide v3.5 ......................................................... 4
Revision History .................................................................................................................................... 4
Conventions ........................................................................................................................................... 4
1 Introduction .......................................................................................................................................... 6
  1.1 Document Purpose ......................................................................................................................... 6
  1.2 Background .................................................................................................................................... 6
  1.3 Application Summary ..................................................................................................................... 6
    1.3.1 Cisco eStreamer eNcore add-on for Splunk (TA-eStreamer) ..................................................... 6
    1.3.2 Cisco eStreamer eNcore Dashboard for Splunk (eStreamer Dashboard) ..................................... 6
2 Prerequisites ......................................................................................................................................... 7
3 Installation .......................................................................................................................................... 7
  3.1 Installing the eNcore add-on for Splunk (TA-eStreamer) ................................................................. 7
  3.2 Installing the eNcore Dashboard for Splunk (eStreamer Dashboard) ............................................... 7
4 eNcore Add-on for Splunk Setup Configuration ................................................................................... 8
  4.1 Enable Data Inputs ......................................................................................................................... 8
  4.2 Enable Scripts ............................................................................................................................... 8
  4.3 eNcore Add-on Setup Page Configuration ..................................................................................... 9
5 Operation ............................................................................................................................................ 12
6 Configuration Options ....................................................................................................................... 13
  6.1 The Monitor .................................................................................................................................... 13
  6.2 Start Time ....................................................................................................................................... 14
  6.3 Outputters ...................................................................................................................................... 14
  6.4 Performance and the workerProcesses Option ............................................................................ 14
  6.5 Batch Size .................................................................................................................................... 15
7 Troubleshooting and questions ........................................................................................................... 16
  7.1 Error messages ............................................................................................................................ 16
  7.2 Frequently Asked Questions .......................................................................................................... 16
8 Cisco Support ..................................................................................................................................... 17
9 Appendix A: Client Certificate Creation and Installation ..................................................................... 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Firepower Management Center eStreamer Client Certificate Creation</td>
<td>18</td>
</tr>
<tr>
<td>10 Appendix B: List of Configuration Options</td>
<td>21</td>
</tr>
<tr>
<td>11 Appendix C: Example Configuration File</td>
<td>24</td>
</tr>
<tr>
<td>Trademarks and Disclaimers</td>
<td>27</td>
</tr>
</tbody>
</table>
About This eStreamer eNcore for Splunk Operations Guide v3.5

<table>
<thead>
<tr>
<th>Author</th>
<th>Sam Strachan (sastrach)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Authority</td>
<td>Cisco Systems Advanced Services, Security &amp; Collaboration IDT, Implementation Americas</td>
</tr>
<tr>
<td>Content ID</td>
<td></td>
</tr>
<tr>
<td>Project ID</td>
<td>868408</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Name or User ID</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>06/01/2017</td>
<td>Michelle Jenkins</td>
<td>Initial Release</td>
</tr>
<tr>
<td>3.0</td>
<td>08/25/2017</td>
<td>Sam Strachan</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>10/15/2018</td>
<td>Richard Clendenning</td>
<td>Updated for v3.5</td>
</tr>
</tbody>
</table>

Conventions

This document uses the following conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><strong>italic</strong></td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <strong>italic</strong> font.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>String</td>
<td>A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier font</strong>.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>
Conventions

**Note:** Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution:** Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Warning:** IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

**Regulatory:** Provided for additional information and to comply with regulatory and customer requirements.
1 Introduction

1.1 Document Purpose

This document outlines the background and usage of the eStreamer eNcore for Splunk client to assist users with installation and execution.

1.2 Background

The Cisco Event Streamer (eStreamer) allows users to stream system intrusion, discovery, and connection data from a Firepower Management Center or managed device (the eStreamer server) to external client applications. eStreamer responds to client requests with terse, compact, binary encoded messages that facilitate high performance.

Historically, the eStreamer SDK has been wrapped with some additional code to create separate Perl applications (e.g., the Cisco eStreamer for Splunk app and the CEF agent).

1.3 Application Summary

eStreamer eNcore is a multi-platform, multi-process Python application that is compatible with Firepower Management Center versions 6.0 and above.

eNcore is an all-purpose client, which requests all possible events from eStreamer, parses the binary content, and outputs events in various formats to support other Security Information and Event Management tools (SIEMs). eNcore was built from scratch in Python with a scalable and fast multi-process architecture. It supports version 6.0 of Firepower Management Center. It was built and tested on CentOS 7, but should work with any Linux distribution that supports the pre-requisites. The software will run on Windows but is not supported.

1.3.1 Cisco eStreamer eNcore add-on for Splunk (TA-eStreamer)

The eStreamer eNcore add-on for Splunk is a technology add-on that contains the core eNcore eStreamer client code as well as:

- A simple set-up screen for configuration
- Data inputs (inputs.conf) for data, logs and status
- Parsing hints (props.conf)
- An extension which allows eNcore to live and die with Splunk

**Note:** The eNcore for Splunk add-on is not supported on Splunk for Windows.

1.3.2 Cisco eStreamer eNcore Dashboard for Splunk (eStreamer Dashboard)

This is an application which includes the same user interface elements as the old Cisco eStreamer for Splunk app (https://splunkbase.splunk.com/app/1629/). The application contains no code or collector elements, however. It is simply a UI application with some pre-defined searches, macros, eventtypes and workflow actions.
2 Prerequisites

The eNcore add-on for Splunk and the eNcore Dashboard for Splunk do not require any special prerequisites. They are downloadable from Splunkbase and they install in the search head in the same way as other add-ons and applications.

The eNcore add-on for Splunk requires Python 2.7 and openSSL, which are part of Splunk’s default installation. If the Splunk install was customized and is missing one or both of these components, they will need to be installed for the add-on to function.

3 Installation

Note: The eNcore for Splunk add-on is not supported on Splunk for Windows.

3.1 Installing the eNcore add-on for Splunk (TA-eStreamer)

To install the eNcore add-on for Splunk, either:

a. Download the add-on from http://apps.splunk.com/app/3662 and use the "Install app from file" feature in Splunk to then upload and install the add-on, or

b. Use the "Browse more apps" feature in Splunk and search for "eNcore", then look for Cisco eStreamer Add-on for Splunk in the search results and click Install for that add-on.

You must install a PKCS12 certificate for your Splunk server, which allows the Firepower Management Center to authenticate the identity of the add-on when the eNcore client contacts the Firepower Management Center and establishes a secure tunnel. You create the PKCS12 certificate on the Firepower Management Center, download it, and copy it to this location on the Splunk server (renaming it client.pkcs12):

$SPLUNK_HOME/etc/apps/TA-eStreamer/bin/encore/client.pkcs12

For more information on creating a PKCS12 certificate and copying it to the Splunk server, see Appendix A.

3.2 Installing the eNcore Dashboard for Splunk (eStreamer Dashboard)

To install the eNcore Dashboard for Splunk, either:

a. Download the app from http://apps.splunk.com/app/3663 and use the "Install app from file" feature in Splunk to then upload and install the add-on, or

b. Use the "Browse more apps" feature in Splunk and search for "eNcore", then look for Cisco Firepower eNcore App for Splunk in the search results and click Install for that app.
4  eNcore Add-on for Splunk Setup Configuration

4.1 Enable Data Inputs

The eNcore add-on for Splunk writes events to log files in the installation’s data directory. Splunk must be configured with a Data Input that reads the events from this directory.

To do this, navigate to Settings > Data Inputs > Files & Directories and enable the data input with the path $SPLUNK_HOME/etc/apps/TA-eStreamer/data and Source type cisco:estreamer:data).

4.2 Enable Scripts

The eNcore add-on for Splunk has three scripts that that perform important operations:

- cisco:estreamer:clean – this script has no output but is used to delete data files older than 12 hours
- cisco:estreamer:log – this script uses the stdout of eNcore to take program log data. This becomes very useful where things are not going to plan. More importantly, it is the script which starts the eStreamer eNcore process.
- cisco:estreamer:status – this script runs periodically to maintain a clear status of whether the program is running

These scripts must be enabled by navigating to Settings > Data Inputs > Scripts and clicking enable for the three TA-eStreamer scripts.
4.3 eNcore Add-on Setup Page Configuration

To configure the eNcore add-on for Splunk setup, navigate to app settings in Splunk by clicking the “cog” icon on the home page:

Find **Cisco eStreamer eNcore for Splunk** and click “Set-up”

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FMC Hostname or IP address</strong></td>
<td>1.2.3.4</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>8302</td>
</tr>
</tbody>
</table>

Check the “Process PKCS12 file?” check box. When you created the PKCS12 file on the Firepower Management Center, you were given an option to encrypt the file with a password. If you configured a password for the file when creating it on the Firepower Management Center, enter that password in the two PKCS12 password fields.

**Note:** Each time you load this page, “Process PKCS12 file” is reset to “no” and the password is not saved. It should be used once to process the PKCS12 file using openSSL and store a public-private key pair.

The Data section of the setup page contains three options. These options are described in the table below and should generally be left unchecked unless there is a need for these items to be written to the Splunk data file.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets? Packet logs can be large and use up storage</td>
<td>By default, when an intrusion event is generated the packet that generated the event is captured. The Firepower Management Center can be configured to stream packet captures (through the Firepower Management Center GUI) if requested. If this &quot;Packets?&quot; option is selected in Splunk, then the Firepower Management Center will stream the packet for each intrusion event immediately after sending the intrusion event. It should be noted that packet captures themselves are not events – they only supply the packet contents associated with an intrusion event. The packet contents are binary information provided in a hex format. This option should only be selected if there is a need to have the packet contents in Splunk.</td>
</tr>
<tr>
<td>Connections? This is a very high-volume option and may consume significant network and storage usage</td>
<td>If managed devices are configured to log most or all connections, then there may be many thousands of connection events per second depending on the number of managed devices and their traffic load.</td>
</tr>
<tr>
<td>Metadata? Metadata logs are not event-driven but can prove informative</td>
<td>The Firepower Management Center sends event records with fields that identify certain items by their ID. For example, an intrusion event record contains a field for ids_policy, and the Firepower Management Center identifies the ids_policy by its ID. The Firepower Management Center sends a separate metadata record to supply the name of the policy that has that ID. eNcore supplies the policy name in the ids_policy field when writing the Splunk output. So there is generally no need for eNcore to write the metadata records to the Splunk data file and this should be left unchecked unless needed for troubleshooting.</td>
</tr>
</tbody>
</table>

The options appear as follows in the add-on setup page:

- [ ] Packets? Packet logs can be large and use up storage
- [ ] Connections? This is a very high-volume option and may consume significant network and storage usage
- [ ] Metadata? Metadata logs are not event-driven but can prove informative
To save the settings on the page without executing eNcore, leave the Is enabled? check box unchecked and click Save.

To execute eNcore, check the Is enabled? check box and click Save.

Control

☐ Is enabled? The eNcore client should remain disabled until configured. If running, it may take a moment or two for the client to stop once disabled.
5 Operation

Once you have fully configured all items as described in section 4, the eNcore add-on for Splunk is started by checking the Is enabled? check box on the add-on setup page and clicking Save as described in section 4.3.

Following execution, the operation of the add-on can be monitored by searching for status, log, and data events:

- To check the status, search for sourcetype="cisco:estreamer:status"
- To check more detailed log output, search for sourcetype="cisco:estreamer:log"
- To look for eStreamer data, search for sourcetype="cisco:estreamer:data"

For further analysis of the Firepower events consider installing either:

- Cisco eStreamer eNcore Dashboard for Splunk
- Splunk Add-on for Cisco FireSIGHT

Please note that at time of writing Splunk Add-on for Cisco FireSIGHT searches Splunk for “cisco:sourcefire” events. To use this add-on with the eNcore add-on, it is recommended to configure a new Sourcetype Rename. To do this, navigate to Settings > Fields > Sourcetype renaming and configure the items as follows:

- Destination app: Splunk_TA_sourcefire
- Original sourcetype name: cisco:estreamer: data
- New sourcetype name: cisco:sourcefire
6 Configuration Options

This default configuration provided by the eNcore for Splunk add-on in the estreamer.conf file provides an optimal configuration for many deployments. However, some options that may need to be adjusted by the user in certain circumstances. This section provides details regarding several of these options. The complete list of settings is provided in Appendix B.

6.1 The Monitor

The monitor is a separate thread that runs monitoring and maintenance tasks. By default, it runs every two minutes. It writes the number of events handled to the eNcore log and checks the status of subprocesses. If are any problems with subprocesses, the monitor places the client into an error state and the client shuts itself down.

An example of messages written to the log by the monitor thread is shown below.

```
2018-03-30 05:09:15,026 Monitor INFO Running. 2296400 handled; average rate 578.86 ev/sec;
2018-03-30 05:11:15,684 Monitor INFO Running. 2296400 handled; average rate 561.87 ev/sec;
2018-03-30 05:13:15,384 Monitor INFO Running. 2296400 handled; average rate 545.86 ev/sec;
```

Several aspects of the log messages can be configured in the monitor section of the estreamer.conf configuration file, which is located in $SPLUNK_HOME/etc/apps/TA-eStreamer/bin/encore/estreamer.conf.

The aspects that can be configured are:

- `period`: The interval in seconds at which the monitor performs its check of subprocesses and writes status messages to the log.
- `bookmark`: If true, the bookmark (the time of the latest event in Unix time format) is included in each monitor log message.
- `handled`: If true, the number of events that eNcore has handled since being started.
- `details`: If true, then in addition to the brief status message that the monitor writes to the log, it will also write a detailed message containing many status items related to the operation of the eNcore client.

An example of the configuration of these parameters in the estreamer.conf file is shown here:

```
"monitor": {
    "period": 120,
    "bookmark": false,
    "handled": true,
    "details": true
}
```
6.2 Start Time

The eStreamer server expects the client request to state the start time, which specifies that the Firepower Management Center should only send events that occurred after the start time. There are three options:

- **0**: Send all events from the earliest point available on the Firepower Management Center
- **1**: Send all events that occur after receiving the client request
- **2**: Use a bookmark to pick up where we left off. First run is from 0

An example of the start configuration in the estreamer.conf file is shown here:

```
"@startComment": "0 for genesis, 1 for now, 2 for bookmark",
"start": 2,
```

6.3 Outputters

By default, only the Splunk outputter is enabled. It writes its data to a relative file location, but you may want to output the data to a different location. To change this, alter the `stream.uri` property to `file:///absolute/file/path/filename{0}.ext` where `{0}` is the timestamp placeholder.

An example of the outputters configuration in the estreamer.conf file is shown here:

```
"outputters": [
    {
        "name": "Splunk default",
        "adapter": "splunk",
        "enabled": true,
        "stream": {
            "uri": "relfile:///data/splunk/encore.log{0}",
            "options": {
                "rotate": true,
                "maxLogs": 9999
            }
        }
    }
]
```

6.4 Performance Tuning

The performance of the eNcore for Splunk add-on has been improved in version 3.5 with the addition of multi-processing. By default, four worker processes operate on the incoming messages to achieve higher throughput. While multiple processes can provide significant performance gains, these gains are highly dependent on the platform because for each platform, the processing bottlenecks may be different. Multiple processes also require additional overhead for managing task distribution, so that increasing the number of processes could actually decrease the performance on platforms with a low number of CPU cores.
The number of worker processes is configurable through the workerProcesses parameter in the estreamer.conf configuration file. The number can be set from 1 to 12. Generally, the more capable the platform (i.e., more CPU cores, better I/O, etc.), more throughput is achieved through a higher number of worker processes. However, the only reliable approach is to test performance with various settings such as 1, 2, 4, 8, and 12, and in many cases the best performance may be gained with just one worker process because no process marshalling is required.

One scenario for testing is to:

1. Disable the add-on's Data Input in Splunk, because the same events will be requested multiple times during the testing.
2. Configure a set number of workerProcesses (such as 8) and then start eNcore with a start parameter of 0 (for genesis) or at least an old start time.
3. Request connection events from the Firepower Management Center (or in some other way request the Firepower Management Center send millions of backlogged events).
4. Observe the event rate reported by the monitor process in the estreamer.log file.
5. Repeat the test with a different number of workerProcesses.
6. When the optimal number has been determined, set the workerProcesses to that number and enable the add-on's Data Input to resume production operations.

An example of the workerProcesses configuration in the estreamer.conf file is shown here:

```
"workerProcesses": 12
```

### 6.5 Batch Size

The eNcore for Splunk add-on also attempts to improve performance by batching received events and only writing them to output when the threshold for the batch has been reached. The default batch size is 100 events.

If the event rate is very low, then a batch size of 100 events could cause an unwanted delay in the appearance of events in Splunk. For example, if intrusion events are the only events that are handled and the intrusion event rate averages 100 events per hour, then the first event in a batch will often be delayed an hour or more while the batch completes and is written to disk. To reduce such delays the batchSize can be set to a lower value, or to eliminate them entirely, the batchSize can be set to 1.

The disadvantage of setting batchSize to 1, is that in high-throughput environments, the overall event rate will be lower.

An example of the batchSize configuration in the estreamer.conf file is shown here:

```
"batchSize": 50
```
7 Troubleshooting

7.1 Error messages

The eNcore for Splunk add-on is engineered to provide meaningful error messages. Below is an example error message.

The eStreamer service has closed the connection. There are a number of possible causes which may show above in the error log.

If you see no errors then this could be that
* the server is shutting down
* there has been a client authentication failure (please check that your outbound IP address matches that associated with your certificate - note that if your device is subject to NAT then the certificate IP must match the upstream NAT IP)
* there is a problem with the server. If you are running Firepower Management Center v6.0, you may need to install "Sourcefire 3D Defense Center S3 Hotfix AZ 6.1.0.3-1"

If you encounter errors that do not make sense or require further explanation, then please contact support so that we can fix the problem and improve the error messages.

7.2 Frequently Asked Questions

Can I connect to more than one Firepower Management Center?
Currently, not within a single instance.

Can eNcore de-duplicate data to keep my SIEM costs lower?
Not today. It is on the roadmap.

Can I run two instances of eNcore in a HA pair?
Yes and no. It is technically possible to run two side-by-side, but they will be completely ignorant of each other and output double the data. It may be preferable to run them in a hot-stand-by configuration where the primary client’s state and configuration data is regularly copied to the secondary client. The state and configuration data in question are comprised of:

- estreamer.conf
- x.x.x.x-port_bookmark.dat
- x.x.x.x-port_cache.dat
- x.x.x.x-port_pkcs.cert
- x.x.x.x-port_pkcs.key
- x.x.x.x-port_status.dat
Can I increase the logging granularity?
Yes, by changing `logging.level` in the estreamer.conf file. Please note that while it is possible to increase this level to VERBOSE, the performance impact will be crippling. DEBUG may be useful but slow. We strongly recommend not going above INFO for standard production execution.

8 Cisco Support
Support is provided by Cisco TAC.
9 Appendix A: Client Certificate Creation and Installation

9.1 Firepower Management Center eStreamer Client Certificate Creation

The steps to generate an eStreamer client certificate are as follows:

1. Navigate to the web interface of the Firepower Management Center at https://fmc-ip-address and log in with your Firepower Management Center credentials.

2. In the Firepower Management Center 6.x GUI, navigate to **System > Integration > eStreamer**.

   ![Firepower Management Center eStreamer Certificate Creation](image)

3. Click **Create Client**.

4. Provide the Hostname and password.

   **Note:** This should be the IP of the client, which will be collecting the event data from the Firepower Management Center. The password you enter here will be required when you first execute eStreamer eNcore.

Please note that the IP address you enter here must be the IP address of the eStreamer-eNcore client from the perspective of the Firepower Management Center. In other words, if the client is behind a NAT device, then the IP address must be that of the upstream NAT interface.
5. Click **Save**.

**Create Client Save Screen**

6. Download the PKCS12 file by clicking the Download icon at the right.
7. Copy the PKCS12 file to the desired location in the target device. By default, eStreamer-eNcore will look for `/path/eStreamer_eNcore/client.pkcs12`. If you wish to use a different filename, then you must edit the `eStreamer.conf` file.
# Appendix B: List of Configuration Options

The following table provides a comprehensive list of configuration options for the eNcore for Splunk add-on.

<table>
<thead>
<tr>
<th>Key</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>true</td>
</tr>
<tr>
<td>connectTimeout</td>
<td>The duration in seconds the client will wait for a connection to establish before failing.</td>
</tr>
<tr>
<td>responseTimeout</td>
<td>The duration in seconds the client will wait for a response before timing out.</td>
</tr>
<tr>
<td>monitor.details</td>
<td>true</td>
</tr>
<tr>
<td>monitor.period</td>
<td>The period in seconds between each execution of monitor tasks. Default is 120. Lower numbers are useful for debugging but will create more log traffic.</td>
</tr>
<tr>
<td>monitor.bookmark</td>
<td>true</td>
</tr>
<tr>
<td>monitor.handled</td>
<td>true</td>
</tr>
</tbody>
</table>
| Start                | 0 specifies oldest data available  
1 specifies data as of now  
2 specifies use of bookmark |
<p>| logging.level        | Levels include FATAL, ERROR, WARNING, INFO, DEBUG, VERBOSE, and TRACE. Select the level of logging as per your requirement. It is strongly recommended that you do not use anything above INFO for production environments. DEBUG will generate very large log files and TRACE will significantly affect performance. |
| logging.format       | This describes the format of the log and how they are stored. Default configuration setting for message format is “{date-time} {name of module} {level of logging-message}”. |
| logging.stdOut       | true | false. This determines whether log output is also shown in Standard Output. |</p>
<table>
<thead>
<tr>
<th>Key</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging.filepath</td>
<td>This specifies the location of the application log.</td>
</tr>
<tr>
<td>subscription.servers[]</td>
<td>While this is an array, eNcore can only currently support one server. The array is to support the future ability to connect to multiple hosts.</td>
</tr>
<tr>
<td>server.host</td>
<td>The IP address of the Firepower Management Center (eStreamer Server). Default configuration is 1.2.3.4. If you change the host entry after having run eNcore then new cache, bookmark and metadata files will be generated.</td>
</tr>
<tr>
<td>server.port</td>
<td>The server port to connect to. Default 8302.</td>
</tr>
<tr>
<td>server.pkcs12Filepath</td>
<td>The PKCS12 file path location. If you change this having already run eNcore, then you must also delete the cached public and private key otherwise eNcore will continue to use those. They are called <code>{host}-</code> <code>{port}</code> _pkcs.cert and <code>{host}-</code> <code>{port}</code> _pkcs.key.</td>
</tr>
<tr>
<td>server.tlsVersion</td>
<td>Valid options are 1.0 and 1.2.</td>
</tr>
<tr>
<td>subscription.records</td>
<td>Do not change these values.</td>
</tr>
<tr>
<td>handler.records.metadata</td>
<td>true</td>
</tr>
<tr>
<td>handler.records.flows</td>
<td>true</td>
</tr>
<tr>
<td>handler.outputters[]</td>
<td>An array of outputter controllers which define the behavior and format of what gets written by eNcore.</td>
</tr>
<tr>
<td>outputter.name</td>
<td>This is a human readable name for your convenience. It is unused by the code.</td>
</tr>
<tr>
<td>outputter.adapter</td>
<td>Data is read from eStreamer and stored in a structured internal format. The adapter transforms the data to a desired format. Recognized values are:</td>
</tr>
<tr>
<td></td>
<td>- splunk</td>
</tr>
<tr>
<td></td>
<td>- json</td>
</tr>
</tbody>
</table>
### Appendix B: List of Configuration Options

<table>
<thead>
<tr>
<th>Key</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>outputter.enabled</code></td>
<td>true</td>
</tr>
<tr>
<td><code>outputter.passthru</code></td>
<td>true</td>
</tr>
<tr>
<td><code>outputter.stream.uri</code></td>
<td>Specify the location where the output will be stored. You can specify a file URI as normal (e.g., file:///absolute/path/to/file) or a relative filepath (relative:path/to/file). Only file URLs are supported currently.</td>
</tr>
<tr>
<td><code>outputter.stream.options</code></td>
<td>File-based streams require additional options.</td>
</tr>
</tbody>
</table>
| `option.rotate`          | true | false. Set if you want log rotation. Default configuration setting for this is true. Please note that eNcore will not delete any old files. If you wish to do that, you will need to script it separately and schedule it. Example: Call this from a cron job. 
```bash
#!/bin/bash
find /opt/splunk/etc/apps/eStreamer/log/* -mmin +1440 -exec rm {};
```
| `option.maxLogs`         | Specify the size of the log (number of lines). Default configuration for this is 10,000. You can have fewer, larger files (e.g, 50,000). |
| `workerProcesses`        | Specify the number of worker processes, from 1 to 12, to optimize performance. See section 6.4 for guidance on setting this option. |
| `batchSize`              | Specify the threshold for a batch. See section 6.5 for guidance on setting the batch size. |
11 Appendix C: Example Configuration File

The eNcore for Splunk add-on comes with a default estreamer.conf configuration file. For reference purposes, an example configuration file is provided below.

Example estreamer.conf Configuration File

```json
{
    "connectTimeout": 10,
    "responseTimeout": 10,

    "@startComment": "0 for genesis, 1 for now, 2 for bookmark",
    "start": 2,

    "monitor": {
        "period": 120,
        "bookmark": false,
        "handled": true,
        "details": true
    },

    "logging": {
        "@comment": "Levels include FATAL, ERROR, WARNING, INFO, DEBUG, VERBOSE and TRACE",
        "level": "INFO",
        "format": "%asctime\s%\level\s-%\message\s",
        "stdOut": true,
        "filepath": "estreamer.log"
    },

    "@queueComment": [
        "Maximum number of messages buffered before throttling takes place. The more powerful",
        "your CPU and more RAM you have, the larger this number can be. It's essentially a",
        "buffer size. Beyond a certain size you won't see any performance gain and it will",
        "just take longer to stop"
    ],

    "maxQueueSize": 100,

    "subscription": {
        "servers": [
            {
                "host": "1.2.3.4",
                "port": 8302,
                "pkcs12Filepath": "client.pkcs12",
                "@comment": "Valid values are 1.0 and 1.2",
                "tlsVersion": 1.2
            }
        ]
    }
}
```
"records": {
   "@comment": [
      "Just because we subscribe doesn’t mean the server is sending. Nor does it mean,
      we are writing the records either. See handler.records[]"
   ],
   "packetData": true,
   "extended": true,
   "metadata": true,
   "eventExtraData": true,
   "impactEventAlerts": true,
   "intrusion": true,
   "archiveTimestamps": true
}

"handler": {
   "records": {
      "core": true,
      "metadata": true,
      "flows": true,
      "packets": true,
      "intrusion": true,
      "rua": true,
      "rna": true,

      "@includeComment": "These records will be included regardless of above",
      "include": []
   }

   "@excludeComment": [
      "These records will be excluded regardless of above (overrides ‘include’)",
      "e.g. to exclude flow and IPS events use [ 71, 400 ]"
   ],
   "exclude": []
}

"@comment": "If you disable all outputters it behaves as a sink",
"outputters": [
   {
      "name": "Splunk default",
      "adapter": "splunk",
      "enabled": true,
      "stream": {
         "uri": "relfile:///data/splunk/encore.log(0)",
         "options": {
            "rotate": true,
            "maxLogs": 9999
         }
      }
   }
]
```json
{
    "name": "JSON",
    "adapter": "json",
    "enabled": false,
    "stream": {
        "uri": "relfile:///data/json/log{0}.json",
        "options": {
            "rotate": true,
            "maxLogs": 9999
        }
    }
}
```
Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.