Endace Fusion Connector Guide

EDM09-99 - Version 6

Website

www.endace.com

Disclaimer

This document is provided on an "AS IS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND" basis, including (without limitation) any warranties or conditions as to accuracy, non-infringement, merchantability or fitness or a particular purpose. The documentation is subject to change without notice.

In no event shall Endace Technology Limited be liable for damages, losses (direct or indirect) or costs incurred as a result of the use of this documentation or any inaccuracies or errors contained in the documentation, and use of the documentation is at your own risk.

This document, or any part thereof, may not be copied, modified or distributed without the express written authorization of Endace Technology Limited and may be used only in connection with Endace Technology Limited products and services.

Contents

Introduction **1**

Related Documents 1

Installation and Configuration **3**

Software Requirements 3
Installing the Endace Fusion Connector App 3
Configure the Connection to an EndaceProbe 4
Upgrading the Endace Fusion Connector App 5

Using the Endace Fusion Connector App **7**

Preparing a Search Request 8
  Search Parameters 8
Search Results 9
Downloading Search Results 10
Use of Common Information Model Fields 11

Creative Commons License **13**

Attribution-ShareAlike 3.0 Unported 14

Version History **19**

Introduction

Splunk® software is a powerful platform for analysis and visualization of machine data. In the network and security monitoring context this data is typically in the form of log events that are emitted by network elements and perimeter security devices. While the Splunk® software provides a broad overview of the network and correlation capabilities, occasionally a deep dive is needed and often the log event is not granular enough. EndaceProbes capture and index every packet and these packets are the "ground truth" from which network elements and security devices derive the information in the logs sent to the Splunk® software. In cases where the logs are insufficient, an analyst's only recourse for determining the root cause of the event (to resolve or mitigate the upstream issue) is to look at the packets provided by an EndaceProbe.

The Endace Fusion Connector App enables users to rapidly extract packets from an EndaceProbe that are related to a network or security event displayed by the Splunk® software. When a log event is selected in the Splunk® software dashboard the connector automatically extracts the date, time and IP tuple information that identifies the packets underpinning the event. A REST API request is sent to search for and then download these packets from any EndaceProbe.

This document is applicable to Endace Fusion Connector version 1.0.

Related Documents

- *EDM09-100 REST API V0 Reference*
- *EDM09-101 REST API V1 Reference*
- *EDM09-102 REST API V2 Reference*
- *EDM09-111 REST API V4 Reference*

Installation and Configuration

This section details how to install, upgrade and configure the Endace Fusion Connector App.

Software Requirements

This version of the Endace Fusion Connector App requires the following software:

- EndaceProbe OSm 6.2.1 or greater
- Splunk® software version 6.2, 6.0, 5.0

Note:
Use the appropriate version of the Endace Fusion Connector App for the version of the EndaceProbe OSm to ensure that the REST API versions match.

Installing the Endace Fusion Connector App

The Endace Fusion Connector App can be installed from a supplied file or from the SplunkBase website. After the initial installation, you must configure the connection to the EndaceProbe.
See Configure the Connection to the EndaceProbe (page 4).

To install from a supplied file

1. Login to your Splunk® software instance using an administration level user.
2. Navigate to the Manager > Apps page.
3. Click Install app from file.
   The Upload an app window displays.
4. Click the Browse... button and locate the Endace Fusion Connector App install file and then click Open.
5. Click Upload to install the selected install file.
6. When prompted, restart the Splunk® software and login.

To Install from the Splunkbase Website

1. Login to your Splunk® software instance using an administration level user.
2. Navigate to the Manager > Apps page.
3. Click Find more apps.
4. Locate the Endace Fusion Connector App.
5. Click Install and follow the on-screen instructions.
6. When prompted, restart the Splunk® software and login.

Configure the Connection to an EndaceProbe

The Endace Fusion Connector App connects to an EndaceProbe so it can retrieve the requested packets of interest. Each request for information is submitted to the EndaceProbe using the specified IP Address, port and user credentials entered on this page.

Field	Description
Hostname or IP Address	The hostname or IP address of the EndaceProbe that is to process the REST API requests.
Port	The port number on which the EndaceProbe is to receive requests. The connection to the EndaceProbe uses SSL. The entered port number must match the HTTPS port configured on the EndaceProbe. The default port number is 443.
Username	The user name to use to submit the request to the EndaceProbe. This user account must be configured on the EndaceProbe and must have the RBAC role of "app_user". Multiple users can be added. All configured users are listed in *$SPLUNK_HOME/etc/apps/endace/local/app.conf* file - the password is encrypted.
Password	The password for this EndaceProbe user. Once entered the actual password is stored encrypted.

Note:
Once entered, the user name and password are no longer displayed and the fields are shown as blank.

To configure the connection:

1. In the Splunk® software, navigate to the Manager > Apps page.
2. Select the Set up option for the Endace Fusion Connector App.
3. Enter the IP address and port number of the EndaceProbe to which the request will be sent.
4. Enter a valid EndaceProbe user name and password.
   This must have been previously configured on the EndaceProbe.
5. Click Save.
6. Restart the Splunk® software.

   Note:
   Changing the username or password, requires a restart of the Splunk® software.
7. Check the Splunk® software connects correctly to the defined EndaceProbe by completing a manual search on the Endace Fusion Connector App page.
   - If the entered details are incorrect, a message displays indicating which details are incorrect.
   - Correctly entered details will return either the search results or a message indicating no matching packets of interest were found

Upgrading the Endace Fusion Connector App

To upgrade the Endace Fusion Connector App from a file, complete the following steps:

1. Login to your Splunk® software instance using an administration level user.
2. Navigate to the Manager > Apps page.
3. Click Install app from file.
   The Upload an app window displays.
4. Click the Browse... button to locate the Endace Fusion Connector App install file, then click Open.
5. Check the Upgrade app... option.
6. Click Upload to install the selected install file.
7. When prompted, restart the Splunk® software and login.
   The installation overwrites the existing version.

The EndaceProbe connection details and user credentials are retained through the upgrade.

Note:
Once the upgrade is complete, we recommend you clear the browser cache.
This ensures that any changes to the page layout, etc., are loaded. Refer to your respective browser documentation for specific details.

Using the Endace Fusion Connector App

This section describes how to use the Endace Fusion Connector App to retrieve metadata and packets of interest from the connected EndaceProbe or Central Management Server (CMS). These packets are typically identified by attributes present in a Splunk® software log event. Valid attributes are:

- the source or destination IP addresses
- date and time range of interest
- IP Protocol of interest

Once the Endace Fusion Connector App has submitted a search request for packets to the EndaceProbe or CMS, a summary displays the number, location and size (in bytes) of matching packets. This enables the user to determine if the download size is manageable, or if the search parameters need to be refined to produce a smaller data set.

Note:
Metadata is only generated for RotationFiles that are vision enabled.

Preparing a Search Request

A search request can be created in two ways:

- automatically - using a Splunk® software log event to populate the Endace Fusion Connector App page, or
- manually - entering the appropriate information into the Endace Fusion Connector App page.

For details on the Endace Fusion Connector App Search Parameters page, see the Search Parameters table below.

Automatic Population of Endace Flow Search Page

1. Use the Splunk® software search to locate a log event.
2. From the event's drop-down menu select Endace Flow Search.
   The Endace Flow Search page opens and pre-populates the search fields with the details from the log event.
3. Check the pre-populated search page and add or alter the information as required
4. Click Search to send the REST API request to the EndaceProbe and display the search results.
   Depending on the size of the request and the number of EndaceProbes in the monitored network the results may take time to return.

Manual Population of Endace Flow Search Page

1. Open the Endace Flow Search page.
2. Enter the details into the search fields.
3. Click Search to send the REST API request to the EndaceProbe and display the search results.
   Depending on the size of the request and the number of EndaceProbes in the monitored network the results may take time to return.

Search Parameters

The search parameter values are either automatically populated from the Splunk® software log event or entered manually. The REST API request is sent to the configured EndaceProbe or CMS to locate packets of interest.

Field	Description
Event	The date and time of the log event.
From & To	Select or enter the required time range around the log event. • Click the radio buttons next to the date and time to manually enter the required date and time range. • Click the radio buttons next to the selected time range to select a time range. The default is 30 seconds before and after.
Source IP & Destination IP	The source and destination IP addresses and port number (optional) from the log event. The port number may be present if available in the log event. These are required parameters to execute the search. The value must be given in CIDR notation (<IP address>/<prefix length>:<port number>).
Protocol	The IP protocol to use in the search. This field is pre-populated if the log event includes this information, otherwise enter a protocol.

Search Results

Once the search results are returned from the EndaceProbe, an option is provided to download them in PCAP or ERF format. Review each set of results and determine which set to download.

It is important to consider the size of the download as large downloads:

- may take a long time to complete,
- could saturate the management network, and
- may exceed the available memory of the local computer.

The results returned for each REST API request include:

- a combined set with all results found, and
- a set per RotationFile that contains relevant data.

Each set of results lists the following information:

Field	Description
Name	The name of the result set. The *All files* result set is a combined result and contains all the packets of interest for all RotationFiles available on the EndaceProbe. All other result sets are per RotationFile available on the EndaceProbe. The name includes details of the RotationFile host EndaceProbe. Applicable when connecting to a Central Management Server.
Matched Bytes	The number of bytes that match the REST API request out of the total number of bytes available within the specified time range.
Matched Packets	The number of packets that match the REST API request out of the total number of packets available within the specified time range.
TCP Dump Filter	The TCP Dump filter used to create the result set.
Filename	The default name of the download file. This can be changed if required.
Download	PCAP or ERF. Click on the required format button to star the download.

Notes:

- *Search results are collated using the RotationFile metadata. If the packets associated with this metadata have been removed from the RotationFile they will not be available to download. This may mean the number of packets actually downloaded is less than the search results indicated.*
- *Metadata is only generated for RotationFiles that are vision enabled.*

Downloading Search Results

Once you have determined which result set you want to download:

1. Check the default filename and update if required.
2. Click the required download format button (PCAP or ERF).

   A popup window displays requesting user credentials.

   Note:
   Depending on how your internet browser is configured to handle popup windows, the popup window may be blocked. Select the appropriate option to allow the popup window.
3. Enter a valid EndaceProbe user credentials.

   This user credential prompt is separate from those used by the Endace Fusion Connector App to request information from the EndaceProbe. You may use the same user credentials or use different ones as required.

   Note:
   If you incorrectly enter the user credentials, the browser will remember those details until you close the browser (all windows). To be able to re-enter the user credentials, you must recreate the download.
4. Open or save the result set.

Once the download is complete, the packets of interest will be available for inspection using your preferred application.

Use of Common Information Model Fields

The Endace Fusion Connector App conforms to the Splunk® software's Common Information Model (CIM) and interprets the Splunk® software log event to determine whether to display the Endace Flow Search option in the event menu. If at least one field is present in the log event, then the menu selection is displayed and the labeled fields are automatically pre-populated into the search fields in the Endace Flow Search page.

The fields used by the Endace Fusion Connector App are:

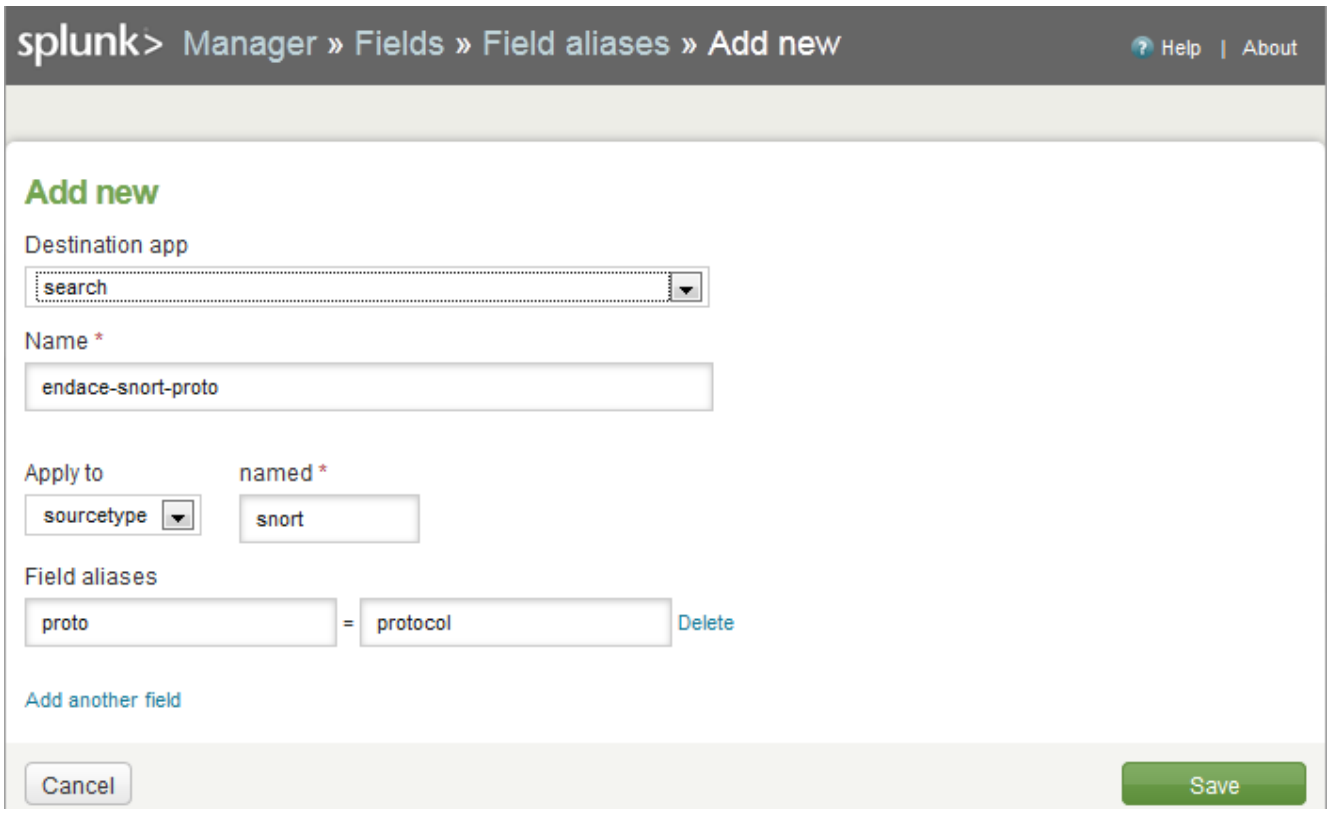
- src_ip
- src_port
- protocol
- dest_ip (optional)
- dest_port (optional)

If the log event contains any of the above fields but they are labeled using non-CIM field labeling, the Endace Fusion Connector App cannot interpret the fields appropriately and therefore will not pre-populate the Endace Flow Search page. To work around this, non-conforming fields can be manually added to the CIM using the Splunk® software field aliases.

For example

Within the SNORT® application the only field of concern is the protocol. By default, the SNORT® application names the field "proto". If left with the default field names the protocol will not automatically pass to the Endace Flow Search page. To get the protocol field to automatically populate the Endace Flow Search page, create a field alias for "proto" to the CIM field "protocol".

Use the Splunk® software field alias screen, to create a field alias:



Creative Commons License

Terms of Use

You are free:

- to Share — to copy, distribute and transmit the work
- to Remix — to adapt the work
- to make commercial use of the work

Under the following conditions:

- Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

With the understanding that:

- Waiver — Any of the above conditions can be waived if you get permission from the copyright holder.
- Public Domain — Where the work or any of its elements is in the public domain under applicable law, that status is in no way affected by the license.
- Other Rights — In no way are any of the following rights affected by the license:
  - Your fair dealing or fair use rights, or other applicable copyright exceptions and limitations;
  - The author's moral rights;
  - Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.
- Notice — For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.

Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions
    a. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.
    b. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.
    c. "Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.
    d. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.
    e. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.
    f. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.
    g. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

h. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

i. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

j. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

k. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;

b. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";

c. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,

d. to Distribute and Publicly Perform Adaptations.

e. For the avoidance of doubt:

f. i. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

g. ii. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,

h. iii. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:
   a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.
   b. You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US)); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the "Applicable License"), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with every copy of the Work as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

c. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Ssection 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

d. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer

   UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability.

   EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous
   a. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.
   b. Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.
   c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
   d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
   e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.
   f. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at http://creativecommons.org/.

Version History

Version	Date	Reason
1	June 2013	First release.
2	August 2013	Minor updates
3	September 2013	Altered reference to Splunk® software & SNORT®.
4	October 2013	Updated field alias graphic
5	September 2015	Updating supported OSM release and Splunk version.
6	February 2016	Rebrand back to Endace.to


endace