



## **Encrypted Traffic Analytics Configuration Guide, Cisco IOS XE Gibraltar 16.11.x**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

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 NON-INFRINGEMENT 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 of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://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](http://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. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

[Read Me First](#) 1

---

### CHAPTER 2

[Encrypted Traffic Analytics](#) 3

[Feature Information for Encrypted Traffic Analytics](#) 3

[Restrictions for Encrypted Traffic Analytics](#) 4

[Information About Encrypted Traffic Analytics](#) 4

[Data Elements for Encrypted Traffic](#) 4

[How to Configure Encrypted Traffic Analytics](#) 5

[Enabling ET-Analytics on an Interface](#) 5

[Applying an ACL for Whitelisting](#) 6

[Verifying the ET-Analytics Configuration](#) 6





# CHAPTER 1

## Read Me First

---

### Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

### Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

### Related References

- [Cisco IOS Command References, All Releases](#)

### Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).





## CHAPTER 2

# Encrypted Traffic Analytics

Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics exports the relevant data elements in the form of NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).

- [Feature Information for Encrypted Traffic Analytics, on page 3](#)
- [Restrictions for Encrypted Traffic Analytics, on page 4](#)
- [Information About Encrypted Traffic Analytics, on page 4](#)
- [How to Configure Encrypted Traffic Analytics, on page 5](#)
- [Verifying the ET-Analytics Configuration, on page 6](#)

## Feature Information for Encrypted Traffic Analytics

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Encrypted Traffic Analytics (ET-Analytics)**

Feature Name	Releases	Feature Information
Encrypted Traffic Analytics	Cisco IOS XE Fuji 16.7.1  Cisco IOS XE Everest 16.6.2	Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics exports the relevant data elements in the form of NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).

Feature Name	Releases	Feature Information
Encrypted Traffic Analytics	Cisco IOS XE Fuji 16.8.1	Support for VRF keyword in flow destinations was added.
Show commands for Encrypted Traffic Analytics	Cisco IOS XE Gibraltar 16.11.1	Simplified <b>show</b> commands to display ETA configurations, flow statistics, and export statistics for quick troubleshooting.
IPFIX support for Encrypted Traffic Analytics	Cisco IOS XE Gibraltar 16.11.1	IP Flow Information Export (IPFIX) protocol is another way for transmitting traffic flow information over the network. Support for <b>ipfix</b> keyword in flow destinations was added.
Source interface support for ETA Netflow records	Cisco IOS XE Gibraltar 16.11.1	Support for <b>source-interface</b> <i>interface-name</i> for ETA Netflow records was added.

## Restrictions for Encrypted Traffic Analytics

ET-Analytics is not supported on management interfaces, VRF-Aware Software Infrastructure (VASI) interface, and internal interfaces.

## Information About Encrypted Traffic Analytics

### Data Elements for Encrypted Traffic

ET-Analytics uses intraflow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for bulk decryption and without compromising on data integrity.

ET-Analytics extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco's Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements.

Transport Layer Security (TLS) is a cryptographic protocol that provides privacy for applications. TLS is usually implemented with common protocols such as HTTP for web browsing or Simple Mail Transfer Protocol (SMTP) for email. HTTPS is the use of TLS over HTTP; this protocol is used to secure communication between a web server and client and is supported by most major web servers.

The TLS template is used to report several of the TLS parameters in use for a flow. These parameters help in finding the use of insecure cipher suites, out-of-date protocol version, and so on.

- Sequence of Packet Lengths and Times (SPLT) - SPLT contains the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the inter-arrival times of those packets. SPLT can be represented as an array of packet sizes (in bytes) along with an array of times (in milliseconds) indicating the time since the previous packet was observed. The SPLT template is used to report packet size and timing information for a flow, which is useful to analyze encrypted traffic and find malicious flows or perform other classifications.



- Initial Data Packet (IDP) - IDP obtains packet data from the first packet of a flow. It allows extraction of data such as an HTTP URL, DNS hostname/address, and other data elements. The TLS handshake is composed of several messages that contain unencrypted metadata used to extract data elements such as cipher suites, TLS versions, and the client's public key length. The IDP template is used to report packet data from the first data packet of a flow. This template allows collectors to perform application classification of a flow (for example, using Snort).

# How to Configure Encrypted Traffic Analytics

## Enabling ET-Analytics on an Interface

### Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>et-analytics</code>	Enters encrypted traffic analytics configuration mode.
Step 4	<code>ip flow-export destination ip-address port [vrf vrf-name] [source-interface interface-name] [ipfix]</code>	Configures the destination IP address optional VRF name. The ETA records are exported to this destination. <p><b>Note</b> Use the <code>ipfix</code> option to export the data in IPFIX format. IP Flow Information Export (IPFIX) protocol is a way for transmitting traffic flow information over the network.</p>
Step 5	<code>exit</code>	Returns to global configuration mode.
Step 6	<code>interface interface-id</code>	Specifies the interface and port number and enters interface configuration mode.
Step 7	<code>et-analytics enable</code>	Enables encrypted traffic analytics on this interface.
Step 8	<code>end</code>	Returns to privileged EXEC mode.

### Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export destination 192.0.2.1 2055 vrf green
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
```

```
Device(config-if) # et-analytics enable
Device(config-if) # end
```

## Applying an ACL for Whitelisting

### Procedure

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>et-analytics</code>	Enters encrypted traffic analytics configuration mode.
Step 4	<code>whitelist acl access-list</code>	Whitelists the specified access list traffic. The access list can be a standard, extended, or named ACL.
Step 5	<code>exit</code>	Returns to global configuration mode.
Step 6	<code>ip access-list extended access-list</code>	Specifies a named extended access list and enters extended access list configuration mode.
Step 7	<code>permit ip {ip-address   any   host   object-group}</code>	Specifies the packets to forward to a source host or source IP address.
Step 8	<code>end</code>	Returns to privileged EXEC mode.

### Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl eta_whitelist
Device(config-et-analytics)# exit
Device(config)# ip access-list extended eta_whitelist
Device(config-ext-nacl)# permit ip host 198.51.100.1 any
Device(config-ext-nacl)# permit ip any host 198.51.100.1
Device(config-ext-nacl)# permit ip host 198.51.200.1 any
Device(config-ext-nacl)# permit ip any host 198.51.200.1
Device(config-ext-nacl)# end
```

## Verifying the ET-Analytics Configuration

The following **show** commands are used to display ETA configurations, flow statistics, and export statistics to allow quick troubleshooting. Given below are the sample outputs of the **show** commands.



**Note** These commands are applicable for Cisco IOS XE Gibraltar 16.11.1 and later.

**Device# show et-analytics configuration**

```
ET-Analytics Global state
=====
All Interfaces      : Off
IP Flow-record Destination: 10.10.10.1 : 2 Format: v9
IP Flow-record Destination: 198.51.100.1 : 1 Format: v9
IP Flow-record Destination: 198.51.100.1 : 3 Format: v9
IP Flow-record Destination: 198.58.100.1 : 1 Format: v9
Source interface: GigabitEthernet0/0/0:148.12.3.4

Inactive timer: 15

ET-Analytics interfaces
=====
GigabitEthernet0/0/0
```

**Device# show et-analytics statistics**

```
ET-Analytics Stats:
  Flow statistics:
    feature object allocs : 0
    feature object frees  : 0
    flow create requests  : 0
    flow create matching   : 0
    flow create successful: 0
    flow create failed, CFT handle: 0
    flow create failed, getting FO: 0
    flow create failed, malloc FO : 0
    flow create failed, attach FO : 0
    flow create failed, match flow: 0
    flow create, aging already set: 0
    flow ageout requests   : 0
    flow ageout failed, freeing FO: 0
    flow ipv4 ageout requests : 0
    flow ipv6 ageout requests : 0
    flow whitelist traffic match : 0
ET-Analytics 10.10.10.1:2 vrf 0 format v9
Stats:
  Export statistics:
    Total records exported      : 0
    Total packets exported     : 0
    Total bytes exported       : 0
    Total dropped records      : 45472778
    Total dropped packets      : 22736389
    Total dropped bytes        : 2273638900
    Total IDP records exported :
      initiator->responder : 0
      responder->initiator : 0
    Total SPLT records exported:
      initiator->responder : 0
      responder->initiator : 0
    Total back pressure        : 0
    Total buffer alloc error   : 0
```

```

ET-Analytics 198.51.100.1:1 vrf 0 format v9
Stats:
  Export statistics:
    Total records exported      : 0
    Total packets exported      : 0
    Total bytes exported        : 0
    Total dropped records       : 45226752
    Total dropped packets       : 22613376
    Total dropped bytes         : 2261337600
    Total IDP records exported :
      initiator->responder : 0
      responder->initiator : 0
    Total SPLT records exported:
      initiator->responder : 0
      responder->initiator : 0
    Total back pressure         : 0
    Total buffer alloc error    : 0
ET-Analytics 198.51.100.1:3 vrf 0 format v9
Stats:
  Export statistics:
    Total records exported      : 0
    Total packets exported      : 0
    Total bytes exported        : 0
    Total dropped records       : 45113838
    Total dropped packets       : 22556919
    Total dropped bytes         : 2255691900
    Total IDP records exported :
      initiator->responder : 0
      responder->initiator : 0
    Total SPLT records exported:
      initiator->responder : 0
      responder->initiator : 0
    Total back pressure         : 0
    Total buffer alloc error    : 0
ET-Analytics 198.58.100.1:1 vrf 0 format v9
Source interface ip:148.12.3.4 Stats:
  Export statistics:
    Total records exported      : 0
    Total packets exported      : 0
    Total bytes exported        : 0
    Total dropped records       : 148864
    Total dropped packets       : 74432
    Total dropped bytes         : 7443200
    Total IDP records exported :
      initiator->responder : 0
      responder->initiator : 0
    Total SPLT records exported:
      initiator->responder : 0
      responder->initiator : 0
    Total back pressure         : 0
    Total buffer alloc error    : 0

```

**Device# show et-analytics statistics export**

```

ET-Analytics 1.1.1.1:22 vrf 0 Stats:
  Export statistics:
    Total records exported      : 0
    Total packets exported      : 0
    Total bytes exported        : 0
    Total dropped records       : 13171887
    Total dropped packets       : 2634378
    Total dropped bytes         : 716551980

```

```

Total IDP records exported :
  initiator->responder : 1
  responder->initiator : 0
Total SPLT records exported:
  initiator->responder : 1
  responder->initiator : 0
Total SALT records exported:
  initiator->responder : 0
  responder->initiator : 0
Total BD records exported :
  initiator->responder : 0
  responder->initiator : 0
Total TLS records exported :
  initiator->responder : 0
  responder->initiator : 0
Total back pressure      : 0
Total buffer alloc error : 0

```

ET-Analytics 2.2.2.2:33 vrf 0 Stats:

```

Export statistics:
Total records exported      : 0
Total packets exported     : 0
Total bytes exported       : 0
Total dropped records      : 13171887
Total dropped packets      : 2634378
Total dropped bytes        : 716551980
Total IDP records exported :
  initiator->responder : 1
  responder->initiator : 0
Total SPLT records exported:
  initiator->responder : 1
  responder->initiator : 0
Total SALT records exported:
  initiator->responder : 0
  responder->initiator : 0
Total BD records exported :
  initiator->responder : 0
  responder->initiator : 0
Total TLS records exported :
  initiator->responder : 0
  responder->initiator : 0
Total back pressure        : 0
Total buffer alloc error   : 0

```

ET-Analytics 1.2.3.4:56 vrf 0 Stats:

```

Export statistics:
Total records exported      : 1792
Total packets exported     : 360
Total bytes exported       : 98812
Total dropped records      : 28010
Total dropped packets      : 5602
Total dropped bytes        : 1523744
Total IDP records exported :
  initiator->responder : 1
  responder->initiator : 0
Total SPLT records exported:
  initiator->responder : 1
  responder->initiator : 0
Total SALT records exported:
  initiator->responder : 0
  responder->initiator : 0
Total BD records exported :
  initiator->responder : 0
  responder->initiator : 0

```

```

Total TLS records exported :
    initiator->responder : 0
    responder->initiator : 0
Total back pressure       : 0
Total buffer alloc error  : 0

```

**Device# show et-analytics statistics flow**

```

ET-Analytics Stats:
  Flow statistics:
    feature object allocs : 1
    feature object frees  : 0
    flow create requests  : 11687
    flow create matching  : 11686
    flow create successful: 1
    flow create failed, CFT handle: 0
    flow create failed, getting FO: 0
    flow create failed, malloc FO : 0
    flow create failed, attach FO : 0
    flow create failed, match flow: 0
    flow create, aging already set: 1
    flow ageout requests   : 0
    flow ageout failed, freeing FO: 0
    flow ipv4 ageout requests : 0
    flow ipv6 ageout requests : 0
    flow whitelist traffic match : 0

```

**Device# show et-analytics flow**

```

GLOBAL CFT ~ Max Flows:50000 Buckets Num:0
+++++
Filtering parameters:
  IP1 : ANY
  Port1 : ANY
  IP2 : ANY
  Port2 : ANY
  Vrf id : ANY
  Application: ANY
  TC id: ANY
  DST Interface id: ANY
  L3 protocol : IPV4/IPV6
  L4 protocol : TCP/UDP/ICMP/ICMPV6
  Flow type : ANY
Output parameters:
  Print CFT internal data ? No
  Only print summary ? No
  Asymmetric : ANY
+++++
=====
+++++
      Number of flows that passed filter: 0
+++++
              FLOWS DUMP DONE.
+++++

```

**Note**

- From Cisco IOS XE Gibraltar 16.11.1 onwards, use the **clear et-analytics statistics export** command instead of the **show platform hardware qfp active feature et-analytics datapath stats export clear** command.
- From Cisco IOS XE Gibraltar 16.11.1 onwards, use the **clear et-analytics statistics flow** command instead of the **show platform hardware qfp active feature et-analytics datapath stats flow clear** command.

Use the following commands for releases earlier to Cisco IOS XE Gibraltar 16.11.1. The following **show** commands are used to see the platform ET-analytics, threat-visibility interfaces, FMAN FP global and interface information, and ET-analytics datapath information. Given below are the sample outputs of the **show** commands.

```
Device# show platform hardware qfp active feature et-analytics data interface gigabitEthernet
2
```

```
uidb handle: 0x3fe
Interface Name: GigabitEthernet2
```

```
Device# show platform hardware qfp active feature et-analytics data memory
```

```
ET-Analytics memory information:

Size of FO           : 3200 bytes
No. of FO allocs    : 952903
No. of FO frees     : 952902
```

```
Device# show platform hardware qfp active feature et-analytics data runtime
```

```
ET-Analytics run-time information:

Feature state       : initialized (0x00000004)
Inactive timeout    : 15 secs (default 15 secs)
Flow CFG information : !Flow Table Infrastructure information internal to ETA!
  instance ID       : 0x0
  feature ID        : 0x0
  feature object ID : 0x0
  chunk ID          : 0x4
```

```
Device# show platform hardware qfp active feature et-analytics datapath stats export
```

```
ET-Analytics 192.168.1.100:2055 vrf 2 Stats:
Export statistics:
  Total records exported      : 2967386
  Total packets exported     : 1885447
  Total bytes exported       : 2056906120
  Total dropped records      : 0
  Total dropped packets      : 0
  Total dropped bytes        : 0
```

```

Total IDP records exported :
    initiator->responder : 805813
    responder->initiator : 418799
Total SPLT records exported:
    initiator->responder : 805813
    responder->initiator : 418799
Total SALT records exported:
    initiator->responder : 0
    responder->initiator : 0
Total BD records exported :
    initiator->responder : 0
    responder->initiator : 0
Total TLS records exported :
    initiator->responder : 171332
    responder->initiator : 174860
ET-Analytics 172.27.56.99:2055 Stats:
  Export statistics:
    Total records exported      : 2967446
    Total packets exported     : 1885448
    Total bytes exported       : 2056909280
    Total dropped records      : 0
    Total dropped packets      : 0
    Total dropped bytes        : 0
    Total IDP records exported :
      initiator->responder : 805813
      responder->initiator : 418799
    Total SPLT records exported:
      initiator->responder : 805813
      responder->initiator : 418799
  Total SALT records exported:
    initiator->responder : 0
    responder->initiator : 0
  Total BD records exported :
    initiator->responder : 0
    responder->initiator : 0
  Total TLS records exported :
    initiator->responder : 171332
    responder->initiator : 174860

```

**Device# show platform hardware qfp active feature et-analytics datapath stats flow**

```

ET-Analytics Stats:
  Flow statistics:
    feature object allocs : 0
    feature object frees  : 0
    flow create requests  : 0
    flow create matching  : 0
    flow create successful: 0
    flow create failed, CFT handle: 0
    flow create failed, getting FO: 0
    flow create failed, malloc FO : 0
    flow create failed, attach FO : 0
    flow create failed, match flow: 0
    flow create, aging already set: 0
    flow ageout requests   : 0
    flow ageout failed, freeing FO: 0
    flow ipv4 ageout requests : 0
    flow ipv6 ageout requests : 0
    flow whitelist traffic match : 0

```



```
Device# show vrf tableid
```

VRF Name	Tableid	Address Family
Mgmt-intf	0x00000001	ipv4 unicast
Mgmt-intf	0x1E000001	ipv6 unicast
blu	0x00000002	ipv4 unicast
red	0x00000003	ipv4 unicast

