



# Cisco Secure Cloud Analytics

Configuration Guide for Enhanced NetFlow



---

# Table of Contents

<b>Configuration for Enhanced NetFlow Overview</b> .....	<b>3</b>
Data .....	3
Network Flow Records .....	3
Encrypted Traffic Analytics Flow Records .....	4
<b>Configuring Enhanced NetFlow Reception</b> .....	<b>5</b>
Download the Latest Cersion of the Sensor Install File .....	5
Configure Your Sensor to Pass Enhanced NetFlow Telemetry .....	5
Verifying Sensor Health Status .....	6
<b>Enhanced NetFlow - Related Detections</b> .....	<b>7</b>
<b>Encrypted Traffic Report</b> .....	<b>8</b>
Encrypted Traffic Analytics Report Fields .....	8
Using the Encrypted Traffic Report .....	9
View the Encrypted Traffic Report .....	9
Update the Data Displayed in the Encrypted Traffic Report .....	9
View Additional Information on a Source Entity .....	9
View Additional Information on a Connected Entity .....	10
Download a Comma-Separated File Containing the Information .....	10
<b>Additional Resources</b> .....	<b>11</b>
<b>Contacting Support</b> .....	<b>12</b>
<b>Change History</b> .....	<b>13</b>

# Configuration for Enhanced NetFlow Overview

Recent Cisco switches and routers can export Enhanced NetFlow as part of encrypted traffic analytics capabilities. You can configure Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) to collect this telemetry. This enables new types of observations and alerts. See the [Encrypted Traffic Analytics white paper](#) for more information.

No additional licenses are required to send network flow data or telemetry to the cloud.

## Data

Two categories of data are sent to the cloud over HTTPS, and stored encrypted while at rest:

- Network flow records
- Records for encrypted traffic analytics, if you have an encrypted traffic analytics enabled switch and router and configure the Cisco Secure Cloud Analytics sensor (formerly Stealthwatch Cloud Sensor) to pass the records

## Network Flow Records

The network flow records can include:

<ul style="list-style-type: none"> <li>• IP address of host endpoint</li> </ul>	<ul style="list-style-type: none"> <li>• start time</li> </ul>	<ul style="list-style-type: none"> <li>• last active time</li> </ul>
<ul style="list-style-type: none"> <li>• TCP or UDP port</li> </ul>	<ul style="list-style-type: none"> <li>• port range</li> </ul>	<ul style="list-style-type: none"> <li>• autonomous system number</li> </ul>
<ul style="list-style-type: none"> <li>• mac address</li> </ul>	<ul style="list-style-type: none"> <li>• group IDs</li> </ul>	<ul style="list-style-type: none"> <li>• VM ID</li> </ul>
<ul style="list-style-type: none"> <li>• protocol data*</li> </ul>	<ul style="list-style-type: none"> <li>• SYN packet count</li> </ul>	<ul style="list-style-type: none"> <li>• RST packet count</li> </ul>
<ul style="list-style-type: none"> <li>• number of bytes and packets sourced per period</li> </ul>	<ul style="list-style-type: none"> <li>• TrustSec security group tag id and name</li> </ul>	<ul style="list-style-type: none"> <li>• number of total bytes and packets since flow started</li> </ul>
<ul style="list-style-type: none"> <li>• FIN packet count</li> </ul>	<ul style="list-style-type: none"> <li>• well-known service port</li> </ul>	<ul style="list-style-type: none"> <li>• protocol</li> </ul>
<ul style="list-style-type: none"> <li>• flow identifier</li> </ul>	<ul style="list-style-type: none"> <li>• application ID</li> </ul>	<ul style="list-style-type: none"> <li>• packet shaper application ID</li> </ul>

<ul style="list-style-type: none"> <li>• service ID</li> </ul>	<ul style="list-style-type: none"> <li>• sensor application ID</li> </ul>	<ul style="list-style-type: none"> <li>• NBAR application ID</li> </ul>
<ul style="list-style-type: none"> <li>• Palo Alto application ID</li> </ul>	<ul style="list-style-type: none"> <li>• VLAN ID</li> </ul>	<ul style="list-style-type: none"> <li>• connection count</li> </ul>
<ul style="list-style-type: none"> <li>• username</li> </ul>	<ul style="list-style-type: none"> <li>• retransmit count</li> </ul>	<ul style="list-style-type: none"> <li>• server response time</li> </ul>
<ul style="list-style-type: none"> <li>• MPLS label</li> </ul>	<ul style="list-style-type: none"> <li>• list of exporters</li> </ul>	<ul style="list-style-type: none"> <li>• flow sequence number</li> </ul>
<ul style="list-style-type: none"> <li>• round trip time</li> </ul>	<ul style="list-style-type: none"> <li>• sensor IP Address</li> </ul>	<ul style="list-style-type: none"> <li>• SVRD metric</li> </ul>

\* The protocol data field contains miscellaneous data, such as URLs, SSL certificates, and special characters for header data.

### Encrypted Traffic Analytics Flow Records

Encrypted traffic analytics flow records are only sent if you have an encrypted traffic analytics enabled switch or router, and configure the sensor to collect Enhanced NetFlow. For more information about encrypted traffic analytics, refer to the [Encrypted Traffic Analytics white paper](#) and the [Encrypted Traffic Analytics deployment guides](#).

The encrypted traffic analytics flow records include:

<ul style="list-style-type: none"> <li>• initial data packet (IDP) *</li> </ul>	<ul style="list-style-type: none"> <li>• sequence of packet lengths and times (SPLT)</li> </ul>	<ul style="list-style-type: none"> <li>• transport layer security (TLS) version</li> </ul>
<ul style="list-style-type: none"> <li>• TLS session ID</li> </ul>	<ul style="list-style-type: none"> <li>• selected cipher suite</li> </ul>	

\* The Initial Data Packet (IDP) contains mostly protocol related data and headers, such as Server Name Indication (SNI), protocol versions, offered and selected cypher suite and HTTP header fields (in case of unencrypted HTTP traffic). For protocols other than HTTPS/HTTP, it contains the protocol headers for the first 1500 bytes of the client/server communication (usually encrypted on the protocol level without the possibility of decryption without the rest of the data).

# Configuring Enhanced NetFlow Reception

If you deploy a sensor version 4.0 or greater, you can configure it to collect Enhanced NetFlow telemetry, which enables new types of observations and alerts. See the [Encrypted Traffic Analytics deployment guides](#) for information on how to configure encrypted traffic analytics telemetry exporters.

Download the latest version of the sensor install file from your Secure Cloud Analytics web UI. See the [Sensor Installation Guide](#) for more information on sensor deployment.

## Download the Latest Version of the Sensor Install File

1. Log in to your Secure Cloud Analytics web UI.
2. Select the **? (Help) icon > Sensor Install**.
3. Click the download button to download the latest version of the sensor .iso file.
4. Go to the [Sensor Installation Guide](#) for instructions on how to deploy the sensor.

After you deploy the sensor, you can log in to your Secure Cloud Analytics web UI, review the ports your sensor is configured to use, and configure the sensor with a different port to pass Enhanced NetFlow telemetry to the cloud.

## Configure Your Sensor to Pass Enhanced NetFlow Telemetry

1. Configure your encrypted traffic analytics capable device to export telemetry to the sensor's IP address.



We recommend that you configure Enhanced NetFlow to use a different destination UDP port than the Flexible NetFlow destination UDP port. For example, configure port 2055/UDP for Enhanced NetFlow, and port 9995/UDP for Flexible NetFlow.

2. Log in to your Secure Cloud Analytics web UI.
3. Select the **☁ (Cloud) icon > Sensors** to view the Sensor List.
4. Click **Change Settings** for the sensor you want to configure.
5. Select the NetFlow/IPFIX tab. Note the list of ports used, especially for (Flexible) NetFlow. Do not configure these ports for Enhanced NetFlow.
6. Click **Add New Probe**.
7. Select the `Enhanced NetFlow (et-analytics)` **Probe Type**.

8. Enter the UDP **Port** you configured for your encrypted traffic analytics capable device.





Ensure that the UDP port you configure is not one that is also configured for Flexible NetFlow or IPFIX in your sensor configuration. If it is, update your configuration to ensure that the port configured for Enhanced NetFlow is dedicated to only Enhanced NetFlow.

9. Select the **UDP Protocol**.
10. Select the **Standard Source**.
11. Click **Save**.

## Verifying Sensor Health Status

You can verify a sensor's configuration by checking the sensor's health status from the Sensor List page.

1. Log in to your Secure Cloud Analytics web UI.
2. Select the  **(Cloud) icon > Sensors** to view the Sensor List.
3. Locate your configured sensor. If the sensor displays a green up arrow  **(Cloud) icon**, your sensor is properly configured. Otherwise, review your sensor configuration.

## Enhanced NetFlow - Related Detections

Based on Enhanced NetFlow telemetry, Secure Cloud Analytics can detect threats based on:

- DNS domain name queries
- Hostnames in HTTPS requests
- URL patterns in HTTP requests

Secure Cloud Analytics generates observations and alerts when the telemetry matches known threats.

# Encrypted Traffic Report

The Encrypted Traffic Report uses encrypted traffic analytics to display detailed information about encrypted traffic that the system monitored, including source and destination entities, and encryption method details. By default, the system displays information from the past 24 hours. You can change the timeframe of displayed information, and filter the displayed encrypted connections. You can also download a comma-separated value (CSV) file containing details about the encrypted connections.

You must configure your sensor to pass Enhanced NetFlow data to the cloud in order to populate this model. See [Secure Cloud Analytics Configuration Guide for Enhanced NetFlow](#) for more information.

## Encrypted Traffic Analytics Report Fields

Field	Description
Time	The timestamp that the system detected the session.
IP	The IP address that originated the session.
Port	The port over which the originating IP address sent traffic.
Remote IP	The IP that the originating IP address established a session with.
Remote Port	The port over which the Remote IP address sent traffic.
Connected Port	The port over which the Connected IP address sent traffic.
Encryption Protocol	The encrypted session protocol.
Encryption Key Exchange	The method of cryptographic key exchange used to establish the encrypted connection.
Encryption Key Length	The length in bits of the cryptographic keys exchanged.
Encryption Algorithm	The encryption algorithm used to secure the connection.



Encryption MAC	The encryption message authentication code used to authenticate the connection.
----------------	---

## Using the Encrypted Traffic Report

### View the Encrypted Traffic Report

1. Log in to your Secure Cloud Analytics web UI.
2. Select **Models > Encrypted Traffic Analytics**.

### Update the Data Displayed in the Encrypted Traffic Report

1. Expand the filters pane.
2. If you want to filter on an originating host, enter an originating **IP** address.
3. If you want to filter on a connected host, enter a **Remote IP** address.
4. If you want to filter on an originating host port, enter an originating **Port**.
5. If you want to filter on a connected host port, enter a **Remote Port**.
6. If you want to filter on an encryption protocol, select a **Protocol** from the drop-down.
7. If you want to filter on the encryption algorithm used, enter an **Algorithm**.
8. If you want to filter on the message authentication code, select a **MAC** from the drop-down.
9. If you want to filter on the encryption key exchange method, enter a **Key Exchange**.
10. If you want to filter on the encryption key length, enter a minimum and maximum **Key Length**.
11. Enter a new **Start Date** and **Start Time**.
12. Enter a new **End Date** and **End Time**.
13. Click **Update**.

### View Additional Information on a Source Entity

1. Select **Alerts** from the IP address or hostname drop-down to view all alerts related to the entity.
2. Select **Observations** from the IP address or hostname drop-down to view all observations related to the entity.
3. Select **Device** from the IP address or hostname drop-down to view information about the device.

4. Select **Session Traffic** from the IP address or hostname drop-down to view session traffic related to this entity.
5. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
6. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

## View Additional Information on a Connected Entity

1. Select **IP Traffic** from the IP address or hostname drop-down to view recent traffic information for this entity.
2. Select **Session Traffic** from the IP address or hostname drop-down to view recent session traffic information for this entity.
3. Select **AbuseIPDB** from the IP address or hostname drop-down to view information about this entity on AbuseIPDB's website.
4. Select **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
5. Select **Google Search** from the IP address or hostname drop-down to search for this IP address on Google.
6. Select **Talos Intelligence** from the IP address or hostname drop-down to view information on Talos's website.
7. Select **Add IP to watchlist** from the IP address or hostname drop-down to add this entity to the watchlist.
8. Select **Find IP on multiple days** from the IP address or hostname drop-down to search for this entity's traffic from the past month.
9. Select **Copy** from the IP address or hostname drop-down to copy the IP address or hostname.
10. Expand **More with SecureX** to take action in other Cisco products based on this IP, depending on your SecureX integration.

 You must be logged into the SecureX ribbon to enable this.

## Download a Comma-Separated File Containing the Information

- Click **CSV** for the table that you want to download.

# Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for a 60-day Free Trial
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

# Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: [tac@cisco.com](mailto:tac@cisco.com)
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:  
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>
- For Secure Cloud Analytics Free Trial customers, open a case by email: [swatchc-support@cisco.com](mailto:swatchc-support@cisco.com)

---

## Change History

<b>Revision</b>	<b>Revision Date</b>	<b>Description</b>
1.0	8 October 2019	Initial version.
1.1	24 October 2019	Miscellaneous updates and corrections.
1.2	5 November 2019	Updated sensor configuration instructions.
2.0	3 November 2021	Updated product branding.
2.1	4 August 2022	Added Contacting Support section.
2.2	17 January 2023	Updated links to the Sensor Installation Guide.

---

# Copyright Information

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: <https://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)

