Cisco Secure Network Analytics

ETA Cryptographic Audit Release Notes v3.2.1

Table of Contents

Introduction

This document provides general information for ETA Cryptographic Audit (Encrypted Traffic Analytics) 3.2.x. The latest version of ETA Cryptographic Audit is v3.2.1.

The TLS Fingerprinting Report has been replaced with the Client Processes Report, which provides an overview of client processes used by selected host groups that are communicating with one another during a particular time frame.

- ETA Cryptographic Audit now works with Cisco Secure Network Analytics (formerly Stealthwatch) in which the Secure Network Analytics Data Store has been deployed.
- Client Processes does not work with Secure Network Analytics in which the Secure Network Analytics Data Store has been deployed.

Overview

ETA Cryptographic Audit

The ETA Cryptographic Audit Report does the following:

- Investigates the cryptographic parameters between a subject (server) and its peers (clients). Particularly, it shows the
  - Number of encrypted connections made to critical servers that store proprietary data
  - TLS version and cipher suite being used
  - Data volume
  - Key length
- Detects trend changes and "diversions."
- Identifies the servers and applications that are not up to date or are poorly supported.
- Provides an overview of the encrypted traffic traveling from and to key areas of your network.
- Provides a Crypto-compliance overview, which is required for audits and to ensure secure communication in critical network segments.
- Provides proof of compliance (e.g., PCI, FIPS). This shows that for critical parts of your network, the encrypted channels use current, reviewed, and revised policies.

> If you are a Secure Network Analytics user, you can use ETA (Encrypted Traffic Analytics) Cryptographic Audit. However, you see results only for the host groups for which you have user permissions.

Client Processes

The Client Processes Report does the following:

- Identifies client processes initiating secure connections without endpoint security, such as Cisco Identity Services Engine (ISE).
- Provides visibility into host processes initiating secure (TLS) connections, identifying them based on a knowledge base used in the Cisco Mercury research project, capitalizing on ETA technology and TLS fingerprint functionality.
- Allows data exportation to an XLS report.
- Provides an option to pivot to a flow search.

About Apps

We introduced apps in v7.0.0 of Cisco Secure Network Analytics (formerly Stealthwatch). Secure Network Analytics apps are similar in concept to the apps you install on a smartphone. They are optional features that enhance and extend the capabilities of Secure Network Analytics. The release schedule for the apps is independent from the normal Secure Network Analytics upgrade process. Due to this, we can update apps as needed without having to link them with a core Secure Network Analytics release, and you can install apps without having to update your Secure Network Analytics system.

Use the App Manager page to manage your installed Secure Network Analytics apps. From this page you can install, update, uninstall, or view the status of an app. After installing an app, you can access it from the appropriate option on the dashboard in the Secure Network Analytics Web App. Your user permissions determines which apps you can view.

When you update Secure Network Analytics, the app that is currently installed is retained; however, some apps may require you to upgrade to the latest version of Secure Network Analytics. In addition, when you upgrade your Secure Network Analytics system, you may need to upgrade some or all of the apps. To learn which app version is supported by a particular version of Secure Network Analytics, see the Secure Network Analytics Apps Version Compatibility Matrix.

> Only a Primary Admin can install or uninstall an app.

> ⚠ When you update to a later version of an app, simply install the newer version over the existing version. You do not need to uninstall your existing app. If you uninstall an app, all files associated with it, including temporary files, are removed.

Status	Definition	Action to Take
UpToDate	Your installed app is the most current version.	No action is required.
UpdateAvailable	You have upgraded to a new version of Secure Network Analytics. Your existing app is supported by this version of Secure Network Analytics, but a new version of this app is available.	If you desire, go to Cisco Software Central to download and install the latest version (this replaces your existing version).
UpgradeRequired	You have upgraded to a new version of Secure Network Analytics, and your existing app is not supported by the Secure Network Analytics version you are now using.	To continue using this app, go to Cisco Software Central to download and install the latest version (this replaces your existing version).
AppNotSupported	You have upgraded to a new version of Secure Network Analytics. This app may no longer be supported by the version of Secure Network Analytics you are now using. It could be that this app has been deprecated or a newer version of this app has not yet been released.	Go to Cisco Software Central to see if a new version has been released.

Status	Definition	Action to Take
Error	The installation, upgrade, or removal process for the associated app has not successfully completed.	Contact Cisco Support (see the last section in this document for support contact information). A partial installation, upgrade, or removal of this app may have occurred. If so, this must be corrected.

App Compatibility Notice

To simplify the Cisco Secure Network Analytics customer experience, only one version of a Secure Network Analytics app will be available to install at any point in time (similar to the app store model). Although we strive for maximum app compatibility, not all versions of an app will be compatible with all versions of Secure Network Analytics.

Cisco reserves the right to discontinue a Secure Network Analytics app at any time. There may be many reasons for doing so, including but not limited to the following:

1. The equivalent capabilities provided by the app are now provided elsewhere, either via a new version of the app, a new app, or via a feature in Secure Network Analytics.
2. The capabilities provided by the app are no longer considered relevant or useful to our customer base.

If the decision is made to discontinue a Secure Network Analytics app, advance notice will be provided at least sixty days prior to the discontinuation date. Although Secure Network Analytics apps are currently included with your Secure Network Analytics license, Cisco reserves the right to charge license fees for certain Secure Network Analytics apps in the future.

Before You Begin

Before you download and install ETA Cryptographic Audit, please read this notice:

> ETA Cryptographic Audit is subject to export control laws and regulations. By downloading ETA Cryptographic Audit, you agree that you will not knowingly, without prior written authorization from the competent government authorities, export or re-export (directly or indirectly) ETA Cryptographic Audit to any prohibited destination, end user, or for any end use.

To see results containing cryptographic data, you must have ETA-enabled devices sending traffic to your Flow Collector(s).

Client Processes

Before you install the ETA Cryptographic Audit app, you need to do the following:

Enable TLS Fingerprinting in your network environment for each applicable Flow Collector. The client processes feature is disabled by default. To enable it for a Flow Collector, do the following:

1. Log in to the applicable Flow Collector interface.
2. From the navigation pane on the left side of the page, click **Support > Advanced Settings**.
3. At the top of the page, for the enable_tls_fingerprint label, change the 0 (zero) that is displayed in the Option Value field to 1 (0 indicates that the feature is disabled).

Remember that you need to repeat steps 1-3 for each Flow Collector for which you want to enable client processes.

Download the ETA Cryptographic Audit SWU file from Cisco Software Central

1. Go to Cisco Software Central.
2. In the Download and Upgrade section, click **Access downloads**.
3. In the **Select a Product** search bar, enter **Secure Network Analytics** and press **Enter**.
4. Choose **Secure Network Analytics Manager 2210** from the list.
5. Choose **App - ETA Cryptographic Audit** from the list.
6. In the window on the right, click the (**Download**) icon for the ETA SWU file and download to your choice of location.

Upload ETA Cryptographic Audit on Central Manager

- It usually takes a few minutes to upload and install an app.
- Only the system administrator can upload and install apps.

1. Verify that you are installing a version of the app that is compatible with your current version of Secure Network Analytics. See the Secure Network Analytics Apps Version Compatibility Matrix.

2. Go to Central Management.
3. On the App Manager tab, click **Browse** to select the SWU file.
4. Select the app file.

   The upload and installation process automatically begins.

5. (Conditional) If you need to cancel the upload process, click **Cancel** in the Upload dialog.

   After you install the app, you can access it from the main menu under the **Dashboards** menu.

Resource usage

The following is true for ETA Cryptographic Audit:

- Supports multiple Flow Collectors and domains.
- Requires the following amount of disk space:
  - /lancope – 1 MB
  - /lancope/var – 240 MB (Keep in mind that this disk space volume is a starting point, and consumption grows as your system accumulates more data.)

To find the disk usage statistics for an appliance, complete the following steps.

1. In the Web App, from the main menu, click the ⚙ (**Global Settings**) icon and choose **Central Management** from the drop-down menu.
2. Click the **Appliance Manager** tab.
3. Click the **Actions** menu for the appliance and choose **View Appliance Statistics** from the menu.
4. If prompted, log in to the associated interface.
5. Scroll down to the Disk Usage section.

Failover

Upon installation, ETA Cryptographic Audit is installed on both the primary and secondary SMCs. You do not have to wait for a failover situation to use the ETA Cryptographic Audit on the secondary Manager; you can use it on the secondary Manager anytime.

Backup

Refer to the following table to know if ETA Cryptographic Audit data and configuration settings can be backed up.

If I perform this type of backup...	Will the associated data be backed up?
Configuration	• Installation is not backed up. • No app-specific configuration is backed up.
Database	• No app-specific data is backed up.

Install ETA Cryptographic Audit

To install ETA Cryptographic Audit, access Central Management and click the App Manager tab.

- If the available disk space in Secure Network Analytics is between 100–300 MB, a message appears informing you how much remaining disk space Secure Network Analytics has. In this situation, it is possible that the ETA Cryptographic Audit app may require more disk space than is available. See **Resource usage** in this document to verify how much disk space is required for the ETA Cryptographic Audit app.
- If Secure Network Analytics has less than 100 MB of disk space, you cannot install this app.

Online Help

To access the online help for this app, click the (**Help**) icon located in the upper right corner of the page.

What's Been Fixed

This section summarizes fixes made in this release. The Secure Network Analytics defect or story number is provided for reference.

Version 3.0.0

Defect	Description
SWONE-5915	We have increased the maximum number of IP addresses listed in the ETA Cryptographic Audit Report from 100 to 1000.
SWONE-9541	If ETA Cryptographic Audit fails to respond in a way that is not apparent to the user, the user now receives a meaningful error message.
SWONE-9752	You can now use ETA Cryptographic Audit on a secondary SMC.
SWONE-9818	We have fixed an issue which under specific circumstances prevented printing of the entire ETA Cryptographic Audit Report.
SWONE-9869	When a subset of Flow Collectors fails, ETA Cryptographic Audit continues to function.
SWONE-10583	The correct number of connections is now displayed in the Audit Report Results.
SWONE-10960	When you run a flow search from the ETA Cryptographic Audit, you now receive results for TLS v1.3.
SWONE-11106	We improved error logging in the diagnostics pack.
SWONE-11139	ETA Cryptographic Audit now properly specifies charsets for reports.

Version 3.1.0

No fixes were necessary for this version.

Version 3.2.0

Defect	Description
SWONE14575	When a backend error occurs, you now receive an error message that contains a little more detailed information: *FC not reachable/unable to execute a query*.
SWONE-14284	When working in a table that contains 10,000+ rows, there is no longer a lag in response time.
SWONE-15181	When running the Audit Report and you set the End Time so that it matches the Start Time, you now receive a warning and are not able to submit the query until you adjust one of the entries.
SWONE-15822	When choosing a Start Time and End Time in the calendar for the Audit Report, the calendar no longer freezes.
SWONE-16329	The filter function now works correctly.
SWONE-16692	The page numbers at the bottom of the page now display correctly.
SWONE-17450	Various elements on the page are now displaying correctly (Type of Report drop-down list, Subject Host Groups and Peer Host Groups panels).

Version 3.2.1

No fixes were necessary for this version.

Contact Support

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

Call

- Your local Cisco Partner
- Cisco Support
    - (U.S.) 1-800-553-2447
    - Worldwide support number: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Open a case

- By web: http://www.cisco.com/c/en/us/support/index.html
- By email: tac@cisco.com

Copyright Information