



Cisco Stealthwatch

ETA Cryptographic Audit Release Notes v2.0



Table of Contents

Introduction	3
Overview	3
Before You Begin	3
App compatibility with Stealthwatch	4
Resource usage	5
Failover	6
Backup	6
Install ETA Cryptographic Audit	7
App Compatibility Notice	7
Online Help	8
What's Been Fixed	8
Version 2.0.2	8
Version 2.0.3	9
Contact Support	10

Introduction

For v2.0.x, ETA (Encrypted Traffic Analytics) Cryptographic Audit has been refactored so that it is compatible with Stealthwatch v7.2.x. Underlying architectural changes have been made to the Stealthwatch Management Console (SMC) in Stealthwatch v7.2.x.

ETA Cryptographic Audit does not work with Stealthwatch systems in which the Stealthwatch Data Store (available in v7.3.0) has been deployed.

This document provides general information as well as any associated improvements and bug fixes for ETA Cryptographic Audit v2.0.x. The latest version of ETA Cryptographic Audit is v2.0.3.

Overview




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

ETA Cryptographic Audit 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.

Before You Begin

Before you install ETA Cryptographic Audit, please read this section.


 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.

App compatibility with Stealthwatch

When you update Stealthwatch, the app that is currently installed is retained; however, the app may not be compatible with the new Stealthwatch version. Refer to the [Stealthwatch Apps Version Compatibility Matrix](#) to determine which app version is supported by a particular version of Stealthwatch.

You can have only one version of an app installed on your Stealthwatch Management Console (SMC). Use the App Manager page to manage your installed apps. From this page you can install, update, uninstall, or view the status of an app. Refer to the following table to learn about the possible app statuses.

Since it is possible that a newer version of an app exists and is not listed in App Manager, always check to see if a newer version is available in [Cisco Software Central](#).

 When you are updating 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 ETA Cryptographic Audit, 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 Stealthwatch. Your existing app is supported by this version of Stealthwatch, 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).

Status	Definition	Action to Take
UpgradeRequired	You have upgraded to a new version of Stealthwatch, and your existing app is not supported by the Stealthwatch 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 Stealthwatch. This app may no longer be supported by the version of Stealthwatch 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.
Error	The installation, upgrade, or removal process for the associated app has not successfully completed.	Contact Cisco Stealthwatch 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.

Resource usage

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 SMC Web App, 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 context menu.
4. If prompted, log in to the Appliance Administration interface.
5. Scroll down to the Disk Usage section.

Failover

Upon installation, an app is installed on both the primary and secondary SMCs; however, the app works only on the primary SMC. If the secondary SMC becomes the primary SMC, the app functions on the new primary SMC as if it had been newly installed. If the original primary SMC once again becomes the primary SMC, functionality is restored on this original primary SMC.

- If the apps or app versions on your Primary and Secondary Stealthwatch Management Consoles do not match, the apps may not function properly. When there is a mismatch, a message appears prompting you to sync your apps or app versions.

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	<ul style="list-style-type: none">• Installation is not backed up.• No app-specific configuration is backed up.
Database	<ul style="list-style-type: none">• 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 Stealthwatch is between 100–300 MB, a message appears informing you how much remaining disk space Stealthwatch 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 Stealthwatch has less than 100 MB of disk space, you cannot install this app.

App Compatibility Notice

Stealthwatch apps were introduced in v7.0.0 of Cisco Stealthwatch.

Stealthwatch apps are similar in concept to the apps you install on a smartphone. They are optional independently releasable features that enhance and extend the capabilities of Cisco Stealthwatch. You can install, update, and remove Stealthwatch apps using App Manager, which you can access in the SMC Web App under the Central Management menu option.

The release schedule for Stealthwatch apps is independent from the normal Stealthwatch upgrade process. Consequently, we can update Stealthwatch apps as needed without having to link them with a core Stealthwatch release.

To simplify the Stealthwatch customer experience, only one version of a Stealthwatch app is 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 are compatible with all versions of Stealthwatch. To learn which app version is supported by a particular version of Stealthwatch, see the [Stealthwatch Apps Version Compatibility Matrix](#).


Some apps may require you to upgrade to the latest version of Cisco Stealthwatch. In addition, when you upgrade your Stealthwatch system, you may need to upgrade some or all of the apps.

Cisco reserves the right to discontinue a Stealthwatch 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 Stealthwatch.
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 Stealthwatch app, advance notice is provided at least sixty days prior to the discontinuation date. Although Stealthwatch apps are currently included with your Cisco Stealthwatch license, Cisco reserves the right to charge license fees for certain Stealthwatch apps in the future.

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 Stealthwatch defect or story number is provided for reference.

Version 2.0.2

Defect	Description
SWAPP-58	<p>In some instance when installing the ETA Cryptographic Audit app, if the Flow Collector list was out of date, the install would fail.</p> <p>Now the Flow Collector list is loaded from the SMC instead of Central Management, which makes this action more reliable.</p>
SWAPP-291	<p>An extra scroll bar was appearing on the ETA Cryptographic Audit Report.</p> <p>The scroll bar no longer appears.</p>
SWAPP-300	<p>When choosing the host group, you can now specify which traffic orientation to use: client or server. You can also specify the peer host group.</p>
SWAPP-301	<p>Improved DNS processing.</p>
SWAPP-302	<p>There was an issue that prevented you from downloading the ETA Cryptographic Audit Report if you had canceled a previous report download.</p>

Defect	Description
	Now when you cancel a report download it does not prevent you from downloading a subsequent report.
SWAPP-310	<p>You could not sort entries in the table that lists the query results.</p> <p>Now you can sort entries in this table.</p>

Version 2.0.3

Defect	Description
SWAPP-313	<p>The ETA Cryptographic Audit page was cutting off a portion of the Search button.</p> <p>Now you can see the entire button.</p>
SWAPP-366	<p>When generating a report, ETA Cryptographic Audit required 100% CPU.</p> <p>The generation of a report no longer causes significant CPU load.</p>
SWAPP-374	<p>ETA Cryptographic Audit did not detect when the Stealthwatch Data Store was employed.</p> <p>ETA Cryptographic Audit now detects the Stealthwatch Data Store.</p>
SWAPP-5915	<p>ETA Cryptographic Audit did not give users the ability to view incomplete reports. When the report contained more results than could be listed in the report, a warning displayed.</p> <p>We have increased the limit of IP addresses shown on reports to 1000. When results exceed this quantity, users can view the first 1000 results, and the report displays a warning on the second page of the report.</p>

Contact Support

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

Call

- Your local Cisco Partner
- Cisco Stealthwatch 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

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)