



Cisco Stealthwatch

Host Classifier Release Notes v1.0



Table of Contents

Introduction	3
Overview	3
Before You Begin	3
Host Groups	3
App compatibility with Stealthwatch	3
Resource usage	5
Failover	6
Backup	6
Install Host Classifier	6
App Compatibility Notice	7
Online Help	8
What's Been Fixed	8
Version 1.0.9	8
Version 1.0.11	9
Version 1.0.13	10
Contact Support	10

Introduction

This document provides general information as well as improvements and bug fixes for all feature and maintenance releases of Host Classifier v1.0.x. The latest version of Host Classifier is v1.0.13.

Overview

-  If an individual classifier's associated host group (unique ID) does not exist in Stealthwatch, that classifier will not function.

Host Classifier helps you to categorize your hosts into logical groups by observing traffic and providing suggested host group matches for specific queries. You can then confirm, exclude, or ignore any suggestion(s). If you click **Exclude Selected**, then for the next 30 days Stealthwatch will not include this host in future suggestions for the host group you selected in the Classification Searches navigation pane. After 30 days has passed, this host may be suggested again in future queries for reevaluation.

Host Classifier monitors all your domains, but your web view will be defined by the domain for which you are reviewing. You can configure individual classification types separately for each domain.

Before You Begin

Before you install Host Classifier, please read this section.

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

Host Groups

Each classifier requires its default "by function" host group to exist in order for the classifier to return suggestions. The name of each default host group corresponds to the name of the classifier with the exception of the Exchange Server classifier, whose default host group is named *Mail Servers*.

App compatibility with Stealthwatch

When you update Stealthwatch, the app that is currently installed will be 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 Flexera.



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 Host Classifier, 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 Flexera to download and install the latest version (this will replace your existing version).
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 Flexera to download and install the latest version (this will replace 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	Go to Flexera to see if a new version has been released.

Status	Definition	Action to Take
	are now using. It could be that this app has been deprecated or a newer version of this app has not yet 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

Host Classifier

- supports multiple Flow Collectors and domains
- requires the following amount of disk space:
 - /lancope - 50 MB
 - /lancope/var - 10 MB (Keep in mind that this disk space volume is a starting point, and consumption will grow 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.
2. Select **Central Management**.
3. Select the **Appliance Manager** tab.
4. Click the **Actions** menu for the appliance.
5. Select **View Appliance Statistics**.
6. If prompted, log in to the Appliance Administration interface.
7. 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. No historical data is retained, since no app-related data is transferred between the failover pair. If the original primary SMC once again becomes the primary SMC, functionality is restored on this original primary SMC. It retains only the historical data it contained before it became the secondary 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 will be displayed prompting you to sync your apps or app versions.

Backup

Refer to the following table to know if Host Classifier 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. • Any host group modifications made using Stealthwatch are backed up, whether or not the change was made through Host Classifier. • No app-specific configuration is backed up.
Database	<ul style="list-style-type: none"> • All suggestions, confirmations, and exclusions are backed up. • Classifier-specific configuration is backed up (e.g., on/off, auto or manual).

Install Host Classifier

To install Host Classifier, access Central Management and click the App Manager tab. The Stealthwatch Management Console (SMC) will begin to run immediately after you install Host Classifier. It will take some time for any results to be displayed. After the

results are displayed, Host Classifier will begin to query each classifier every six hours, one at a time, with each start time staggered by 10 minutes. To stop the queries, simply change the Enabled status of each classifier from *ON* to *OFF*, or uninstall the app.

- If the available disk space in Stealthwatch is between 100–300 MB, a message will appear informing you how much remaining disk space Stealthwatch has. In this situation, it is possible that the Host Classifier 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 Host Classifier app.
- If Stealthwatch has less than 100 MB of disk space, you will not be able to 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 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 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 will be 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 story number is provided for reference.

Version 1.0.9

Defect	Description
SWAPP-186	Host Classifier was not compatible with 7.0.2 nginx routes. Host Classifier is now compatible with 7.0.2 nginx routes.
US31452	When trying to install Host Classifier v1.0.4 with Stealthwatch v7.1.0 , there was a conflict with the SWU loader and the app was not able to be installed. The SWU loader conflict has been resolved, and Host Classifier v1.0.9 can be installed on Stealthwatch v7.1.0.
US31503	When you clicked the check box in the header row to select all records, all of the records were selected, even if they were not displayed on the current page. Now when you the click the check box in the header row to select all records, only the records displayed on the current page will be selected.
US31563	Previous versions of the app did not provide mechanisms to remove all of its artifacts when being uninstalled from an UpgradeRequired or AppNotSupported state. The app now ensures that all of its artifacts are removed when

Defect	Description
	uninstalled from these states.
US31885	There was a delay when confirming or excluding a host or switching to another tab within Host Classifier. Now minimal delays are experienced when performing these actions.
US32782	Cisco cryptographic primitives and parameters were not being enforced. Cisco cryptographic primitives and parameters are now enforced.
US32784	Random number generation was not in adherence to Cisco cryptography standards. Random number generation is now in adherence to Cisco cryptography standards.
US32785	Cisco TLS standards were not being enforced. Cisco TLS standards are now enforced.
US32788	Logging operations were not in adherence to Cisco standards. Logging operations are now in adherence to Cisco standards.
CSCvo66930	Host Classifier was using a version of jackson-databind that had reported vulnerabilities. Host Classifier now uses an updated version of jackson-databind that has no reported vulnerabilities.

Version 1.0.11

Defect	Description
SWAPP-186	Host Classifier was not compatible with 7.0.2 nginx routes. Host Classifier is now compatible with 7.0.2 nginx routes.

Version 1.0.13

Defect	Description
CSCvq89616 CSCvq80551	<p>Host Classifier was using a version of jackson-databind that had reported vulnerabilities related to the subcomponent FasterXML.</p> <p>Host Classifier now uses an updated version of jackson-databind that has resolved the related FasterXML vulnerabilities.</p>
US35741	<p>Google Analytics telemetry collection has been added to Host Classifier.</p> <p>To disable Google Analytics, in Central Management go to the General tab, scroll down to the External Services section, and uncheck the Enable Google Analytics check box.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> You can disable Google Analytics beginning with v7.1.x.</p> </div>

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)

