Cisco Secure Network Analytics

Host Classifier Release Notes v3.1.0

Table of Contents

Introduction

This document provides general information as well as any associated improvements and bug fixes for Host Classifier v3.x.x. The latest version of Host Classifier is v3.1.0.

> Host Classifier does not work with Secure Network Analytics in which the Secure Network Analytics Data Store (available in v7.3.0) has been deployed.

Overview

> If an individual classifier's associated host group (unique ID) does not exist in Secure Network Analytics, that classifier does 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 Secure Network Analytics does 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 is defined by the domain for which you are reviewing. You can configure individual classification types separately for each domain.

What's New

These are the new features and improvements for Host Classifier v3.1.0.

New Host Classifier Types

The following two host classifier types have been added to Host Classifier:

- Trusted Internet Hosts
- Unclassified Top Servers

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 or 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 Secure Network Analytics

When you update Secure Network Analytics, the app that is currently installed is retained; however, the app may not be compatible with the new Secure Network Analytics version. Refer to the Secure Network Analytics Apps Version Compatibility Matrix to determine which app version is supported by a particular version of Secure Network Analytics.

You can have only one version of an app installed on Manager. 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 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 Secure Network Analytics. Your existing app is supported by this version of Secure Network Analytics, but a	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
	new version of this app is available.	
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.
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.

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 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, 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, an app is installed on both the primary and secondary SMCs; however, the app works only on the primary Manager. If the secondary Manager becomes the primary Manager, the app functions on the new primary Manager 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 Manager once again becomes the primary Manager, functionality is restored on this original primary Manager. It retains only the historical data it contained before it became the secondary Manager.

- If the apps or app versions on your Primary and Secondary Managers 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 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	• Installation is not backed up. • Any host group modifications made using Secure Network Analytics are backed up, whether or not the change was made through Host Classifier.

If I perform this type of backup...	Will the associated data be backed up?
	• No app-specific configuration is backed up.
Database	• 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 Manager begins to run immediately after you install Host Classifier. It takes some time for any results to be displayed. After the results are displayed, Host Classifier begins 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 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 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 Secure Network Analytics has less than 100 MB of disk space, you cannot install this app.

App Compatibility Notice

Secure Network Analytics apps were introduced in v7.0.0 of Secure Network Analytics.

Secure Network Analytics 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 Secure Network Analytics. You can install, update, and remove Secure Network Analytics apps using App Manager, which you can access in the Web App under the Central Management menu option.

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

To simplify the Secure Network Analytics customer experience, only one version of a Secure Network Analytics 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 Secure Network Analytics. To learn which app version is supported by a particular version of Secure Network Analytics, see the Secure Network Analytics Apps Version Compatibility Matrix.

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

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 is 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.

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 story number is provided for reference.

Version 3.0.0

Defect	Description
SWAPP-460	Check boxes are now displayed on the Classification page.

Defect	Description
SWONE-12914	Host Classifier now validates software signatures upon installation.

Version 3.1.0

Defect	Description
LVA-2372	Fixed vulnerability in package zlib.
LVA-2373	Fixed vulnerability in package bzip2.
LVA-2375	Fixed vulnerability in package libbsd.
LVA-2377	Fixed vulnerability in package avahi.
LVA-2379	Fixed vulnerability in package openssl.
LVA-2654	Updated library to v1.8.4-5 + deb10u1. It now contains exponent binding so that it can prevent side-channel attacks against mpi-pown.
LVA-2657	The library has been upgraded to a non-vulnerable version of E2fsprogs 1.45.3 so that an out-of-bounds write on the stack can no longer occur (attackers can no longer corrupt a partition to trigger this vulnerability).
LVA-2763	Fixed vulnerability in package akka.
SWAPP-423	Multiple transfer-encoding headers are now allowed by package.comtypesafe.akka-http-core.
SWAPP-445	Have eased the restrictions for the Domain Controllers query regarding password policy.
SWAPP-452	Fixed vulnerability in package commons-io.
SWAPP-453	Fixed vulnerability in package guava.

Defect	Description
SWONE-6998	The script has been upgraded and now uses Python 3.
SWONE-18556	Updated base image in order to meet FIPS certification requirement.
SWONE-19907	The following two host classifier types have been added to Host Classifier: • Trusted Internet Hosts • Unclassified Top Servers
SWONE-20090	When a user attempts to use Host Classifier with a Data Store domain, Host Classifier now provides a message in the user interface stating that Host Classifier does not work with systems in which the Data Store has been deployed.

Contact

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