Cisco Security Analytics and Logging

Security Analytics and Logging On Premises Release Notes

TOC

Introduction

Overview

This document provides information on new features and improvements, bug fixes, and known issues for Cisco Security Analytics and Logging (On Premises). For additional information, go to cisco.com.

Terminology

This guide uses the term "**appliance**" for any Firepower or Stealthwatch product, including virtual products such as the Stealthwatch Management Console Virtual Edition.

Before You Deploy

Before you deploy SAL On Prem, please review the Getting Started with Security Analytics and Logging Guide and the Security Analytics and Logging On Premises: Firepower Event Integration Guide.

⚠ We support installing the Security Analytics and Logging On Prem App only on an SMC as a standalone appliance. You cannot install the App on an SMC if it manages one or more Flow Collectors.

SAL On Prem Version Compatibility

The following table provides a high-level overview of the solution components required to use a Stealthwatch Management Console to store Firepower event data in a SAL (OnPrem) deployment:

Solution Component	**Required Version**	**Licensing for SAL (OnPrem)**	**Notes**
Firepower Management Center (hardware or virtual)	• Firepower 6.4+ for event export via syslog • Firepower 6.4-6.6 for manual cross-launch query configuration • Firepower 6.7+ for automatic cross-launch query configuration	none	• can store syslog on one Stealthwatch Management Console per Firepower Management Center
Firepower Threat Defense	Firepower 6.4+, with Firepower Management	none	• multiple Firepower Threat Defense devices managed

device (hardware or virtual)	Center running that version or greater		by one Firepower Management Center can export syslog to the same Stealthwatch Management Console
Stealthwatch Management Console	Stealthwatch 7.3.0+	none	- can deploy either an SMC 2210 hardware appliance or SMC Virtual Edition (VE) appliance - can receive syslog from multiple Firepower Threat Defense devices, all managed by one Firepower Management Center - must install the Security Analytics and Logging On Prem App for syslog ingest, and for viewing Firepower events in the Stealthwatch Management Console Web App
Security Analytics and Logging On Prem App	Security Analytics and Logging On Prem App 1.0+	Logging and Troubleshooting Smart License, based on GB/day ingested	- install this app on the Stealthwatch Management Console and configure to enable syslog ingest

In addition to these components, you must make sure that all of the appliances can synchronize time using NTP. If you want to remotely access the Firepower or Stealthwatch appliances' consoles, you can enable access over SSH.

Software Download

Note the following:

- **Patches:** Make sure you install the latest rollup patch on your appliances before you upgrade. You can download the files from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
- **Downloading Files:** Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator. In the Download and Upgrade section, select **Software Download**. Select **Security** > **Network Visibility and Segmentation** > **Stealthwatch**.

3rd Party Applications

Stealthwatch does *not* support installing 3rd party applications on appliances.

Browsers

- **Compatible Browsers:** Firepower and Stealthwatch both support the latest version of Google Chrome and Mozilla Firefox.

Security Analytics and Logging On Prem App Installation

To install Security Analytics and Logging On Prem, access Central Management and click the App Manager tab. The Steathwatch Management Console (SMC) begins to run immediately after you install Security Analytics and Logging On Prem. After you complete SAL On Prem deployment, it takes some time before you can view your Firepower events in the Stealthwatch Management Console.

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 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 Security Analytics and Logging On Prem, all files associated with it, including temporary files and Firepower event data, 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	If you desire, go to Cisco Software Central to download and install the latest version (this replaces

Status	Definition	Action to Take
	version of Stealthwatch, but a new version of this app is available.	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 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.
NewApp	This is a new app.	If you desire, install this new app using Central Manager.
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.

See the Stealthwatch Apps Version Compatibility Matrix for more information on Stealthwatch App versions.

Resource usage

The Security Analytics and Logging On Prem app

- can NOT be deployed if your Stealthwatch Management Console manages any Flow Collectors
- requires the following amount of disk space for installation:
    - /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.)
    - See the Cisco Security Analytics and Logging (On Premises): Firepower Event Integration Guide for more information on disk space recommendations for event retention. Note that we have tested event retention against SMCs with 1 TB, 2 TB, and 4 TB disk storage.

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.

After You Deploy

After deploying your Stealthwatch appliances, please install the required patches:

- patch-smc-ROLLUP001-7.3.0-03.swu or later

Review the patch readme files on Cisco Software Central for details.

What's New

These are the new features and improvements for the SAL On Prem initial release:

Firepower Event Storage on a Stealthwatch Management Console Virtual Edition

In a Cisco Security Analytics and Logging (On Premises) deployment, you can use a Stealthwatch appliance to store data from another Cisco product deployment, such as a Firepower appliance deployment. In the case of the Firepower deployment, you can export your Firepower connection (including Security Intelligence), intrusion, file, and malware events as syslog over UDP from your Firepower Threat Defense devices managed by a Firepower Management Center to a Stealthwatch Management Console Virtual Edition (VE) to store that information. You can then review your event data from the Stealthwatch Management Console VE Web App UI. You can also cross-launch from the Firepower Management Center UI to the Stealthwatch Management Console VE Web App UI to view additional context on the information from which you cross-launched.

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
  - For phone support: 1-800-553-2447 (U.S.)
  - For worldwide support numbers: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Known Issues

There are no known issues in this release.

Change Log

Revision	Revision Date	Description
1_0	12 November 2020	Initial version.
1_1	24 November 2020	Clarified app uninstall and app storage requirements.

Copyright Information