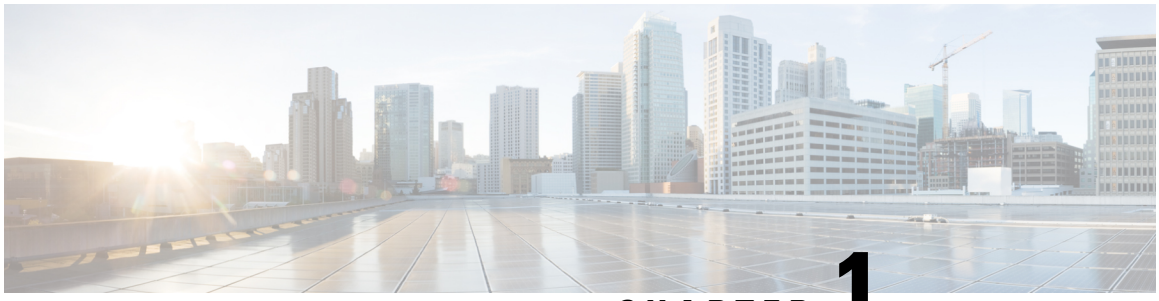
Cisco Security Analytics and Logging (On Premises) Release Notes v2.0.2

First Published: 2021-05-26

Last Modified: 2021-12-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

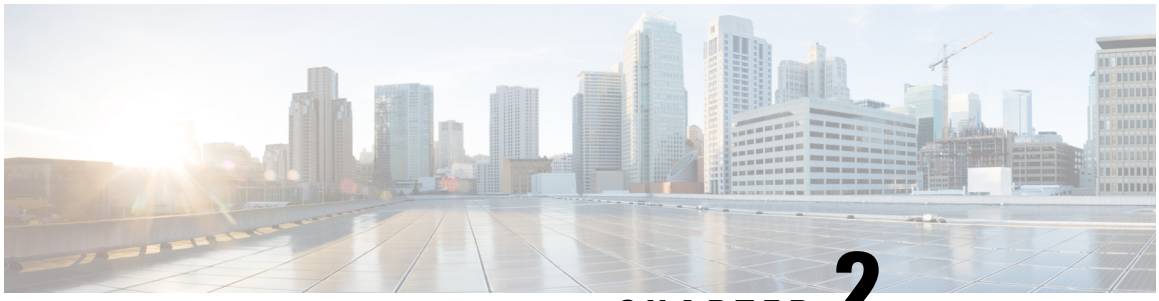
Introduction

Overview

This document provides information on new features and improvements, bug fixes, and known issues for Cisco Security Analytics and Logging (On Premises) v2.0.2. For additional information, go to cisco.com.

Terminology

This guide uses the term "**appliance**" for any Firewall or Cisco Secure Network Analytics (formerly Stealthwatch) product, including virtual products such as the Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) Virtual Edition.



CHAPTER 2

Before You Deploy

Before you deploy Security Analytics and Logging (OnPrem), please review the Getting Started with Security Analytics and Logging Guide and the Security Analytics and Logging On Premises: Firewall Event Integration Guide.

Important We support installing the app on a Manager as a standalone appliance (Single-node), or a Manager that manages a Cisco Secure Network Analytics Flow Collector NetFlow and Cisco Secure Network Analytics Data Nodes (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing Data Nodes.

Version Compatibility

The following tables provide a high-level overview of the solution components required to use Secure Network Analytics to store Firewall event data in a Security Analytics and Logging (OnPrem) deployment.

Firewall Appliances

You can deploy the following Firewall appliances:

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Firepower Management Center (hardware or virtual)	v7.0+ For FMC running earlier versions, see https://cisco.com/go/sal-on-prem-docs.	none	• can deploy one Manager per Firepower Management Center, and optionally one Flow Collector and one Cisco Secure Network Analytics Data Store (3 Data Nodes)
Firepower managed devices	v7.0+ using the wizard FTD v6.4+ using syslog NGIPS v6.4	none	

Secure Network Analytics Appliances

You have the following options for deploying Secure Network Analytics:

- Single-node - Deploy only a Manager to ingest and store events, and review and query events
- Multi-node - Deploy a Flow Collector to ingest events, Data Store to store events, and Manager to review and query events

Note You cannot deploy a mix of Secure Network Analytics hardware and Secure Network Analytics VE appliances.

Table 1: Single-node

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.3.1+	none	• can deploy either an Manager 2210 hardware appliance or Manager Virtual Edition (VE) appliance • can receive events from multiple Firepower Threat Defense devices, all managed by one Firepower Management Center • must install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events in the Manager Web App
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v2.0+	Logging and Troubleshooting Smart License, based on GB/day	Install this app on the Manager and configure to enable event ingest

Table 2: Multi-node

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.3.2+	none	• can deploy either an Manager 2210 hardware appliance or Manager Virtual Edition (VE) appliance • must install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events in the Secure Network Analytics Web App
Flow Collector	Secure Network Analytics v7.3.2+	none	• can deploy either a Flow Collector 4210 hardware appliance or Flow Collector VE appliance • can receive events from multiple Firepower Threat Defense devices, all managed by one Firepower Management Center
Data Store (3 Data Nodes)	Secure Network Analytics v7.3.2+	none	• can deploy either a Data Store 6200 (3 Data Nodes) hardware or Data Store VE (3 Data Nodes VE) • can store Firewall events received by the Flow Collector
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v2.0+	Logging and Troubleshooting Smart License, based on GB/day	Install this app on the Manager and configure to enable event 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 Secure Network Analytics appliances' consoles, you can enable access over SSH.

Software Download

Note the following:

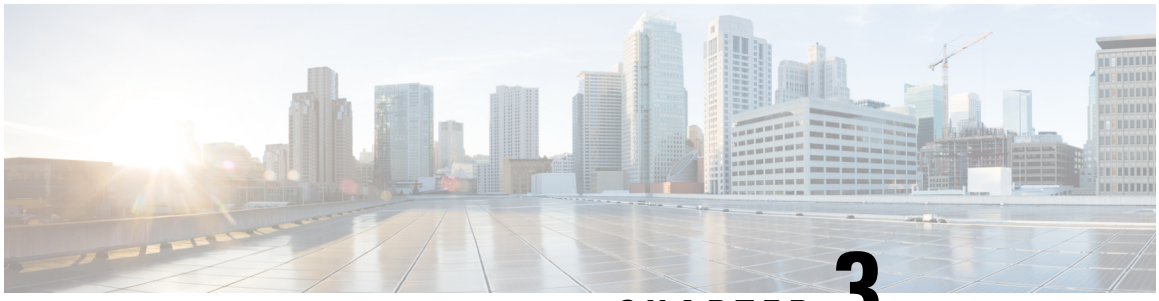
- **Patches**: Make sure you install the latest rollup patch on your appliances before you upgrade. You can download the files from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
- **Downloading Files**:
  1. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.
  2. In the Download and Upgrade section, select **Software Download**.
  3. Select **Security > Network Visibility and Segmentation > Secure Analytics (Stealthwatch) > Secure Network Analytics Virtual Manager > App - Security Analytics and Logging On Prem**.
  4. Download the Security Analytics and Logging On Prem app file, app-smc-sal-2.0.2.swu.

Third-party Applications

We do *not* support installing third-party applications on appliances.

Browsers

Secure Firewall and Secure Network Analytics both support the latest version of Google Chrome and Mozilla Firefox.



CHAPTER 3

Security Analytics and Logging (OnPrem) App Installation

Use the App Manager in Central Management to install Security Analytics and Logging (OnPrem). We recommend that you use Chrome or Firefox for your browser.

1. Log in to your Manager.
2. Click the **Global Settings** icon.
3. Select **Central Management**.
4. Click the **App Manager** tab.
5. Click **Browse**.
6. Follow the on-screen prompts to upload the app file.

Important We support installing the app on an Manager as a standalone appliance (Single-node), or an Manager that manages a Flow Collector and Data Node(s) (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing Data Node(s).

- App Compatibility with Secure Network Analytics, on page 9
- Resource Usage, on page 11

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 a 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.

Important 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.

Table 3:

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.
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 Secure Network Analytics 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 Secure Network Analytics Apps Version Compatibility Matrix for more information on Secure Network Analytics App versions.

Resource Usage

The Security Analytics and Logging (OnPrem) app

- can only be deployed if your Manager
  - does not manage any Flow Collectors, or
  - manages Flow Collectors and Data Nodes
- 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 Security Analytics and Logging (On Premises): Firewall Event Integration Guide for more information on disk space recommendations for event retention.

Finding Disk Usage Statistics

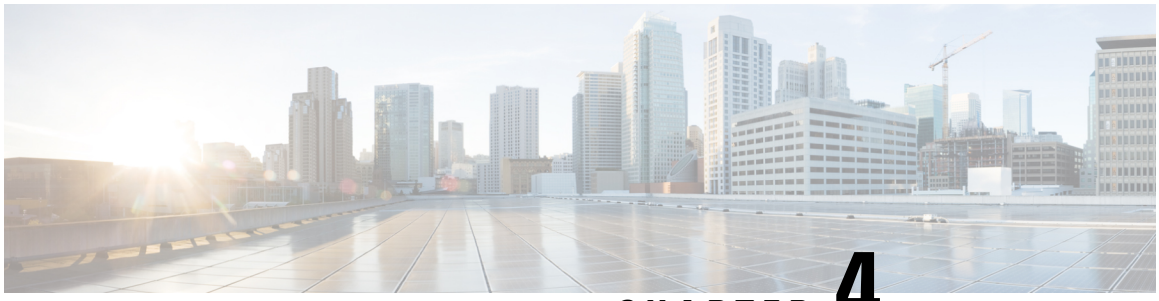
To find the disk usage statistics for an appliance, complete the following steps.

Before you begin

- Log into the Secure Network Analytics Web App as an administrator.

Procedure

Step 1 Click the Global Settings icon, and choose **Central Management** from the drop-down menu.
Step 2 Click the **Appliance Manager** tab.
Step 3 Click the **Actions** menu for the appliance and choose **View Appliance Statistics** from the context menu.
Step 4 If prompted, log in to the Appliance Administration interface.
Step 5 Scroll down to the Disk Usage section.



CHAPTER 4

What's New

These are the new features and improvements in the Security Analytics and Logging (OnPrem) release v2.0.2:

New Features and Functionality

Expanded Storage with the Secure Network Analytics Data Store

You can now deploy a hardware or virtual Secure Network Analytics Data Store and Flow Collector with your Secure Network Analytics Manager for expanded Firepower event storage capacity. When you deploy your Secure Network Analytics appliances, during First Time Setup, you can choose to configure your appliances for deployment with a Data Store, and for use as part of a Cisco Security Analytics and Logging (On Premises) deployment.

Important After you choose to configure your Secure Network Analytics Manager or Flow Collector for use with Cisco Security Analytics and Logging (On Premises), you cannot update the appliance's configuration to change this. You must RFD the appliance if you select the wrong choice. Enable this only if you plan to use Secure Network Analytics for Cisco Security Analytics and Logging (On Premises) to store your Firepower event information.

See the Security Analytics and Logging (On Premises): Firewall Event Integration Guide for more information on the integration, Install Version 7.3.x with Hardware Appliances for more information on deploying Secure Network Analytics hardware with a Data Store, and Install Version 7.3.x with Virtual Appliances for more information on deploying virtual Secure Network Analytics appliances with a Data Store.

Remote Query from the Firepower Management Center

You can now query your events stored within Secure Network Analytics from your Firepower Management Center. See the Security Analytics and Logging (On Premises): Firewall Event Integration Guide for more information on configuring this, and the Firepower Management Center OLH for more information on remote query functionality.

Configuration Wizard in the Firepower Management Center

You can now use a wizard in the Firepower Management Center to set up Cisco Security Analytics and Logging (On Premises) for all Firepower Management Center users. See the Security Analytics and Logging (On Premises): Firewall Event Integration Guide for more information on how to use the wizard.

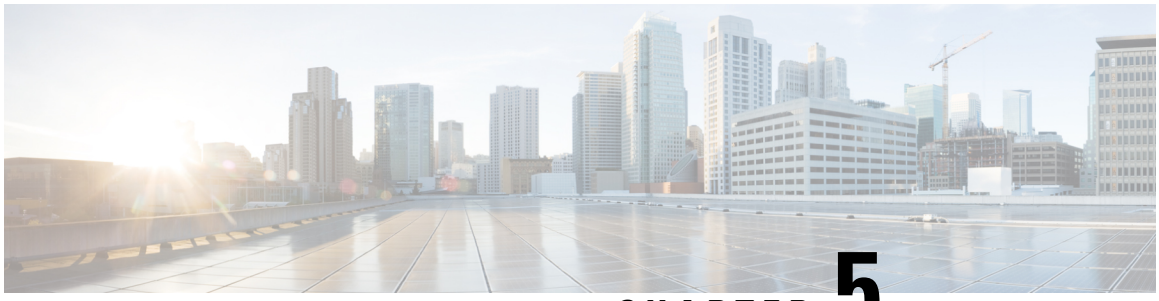
Event Viewer Search

The Cisco Security Analytics and Logging (On Premises) app event viewer now allows you to search for strings within events, to more quickly find specific events.

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: https://www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html



CHAPTER 5

Resolved and Known Issues

Resolved Issues

Table 4: v2.0.2

Defect	Description
LVA-2811	Updated Apache Log4J 2 to v2.15.

Table 5: v2.0.1

Defect	Description
SWONE-14331	Fixed an issue where Firepower was intermittently sending incorrect SyslogIDs for File and Malware events.
SWONE-15345	Updated processing on timestamps from Firepower on a Single-node deployment.

Known Issues

v2.0.2

None