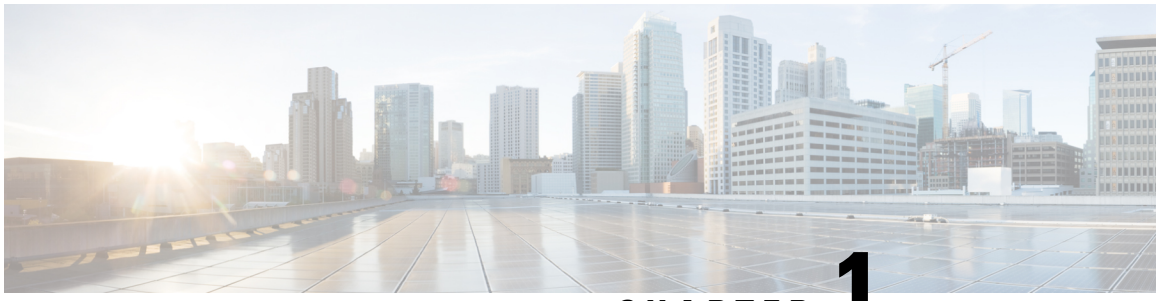
Getting Started with Cisco Security Analytics and Logging (On Premises) v3.2

First Published: 2023-02-15

Last Modified: 2023-02-15

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

Getting Started with Security Analytics and Logging (On Premises) v3.2

Note If you want to store Firewall event data in the Cisco cloud, as opposed to on-premises, see the Cisco Security Analytics and Logging (SaaS) documentation for more information.

Concepts and Architecture

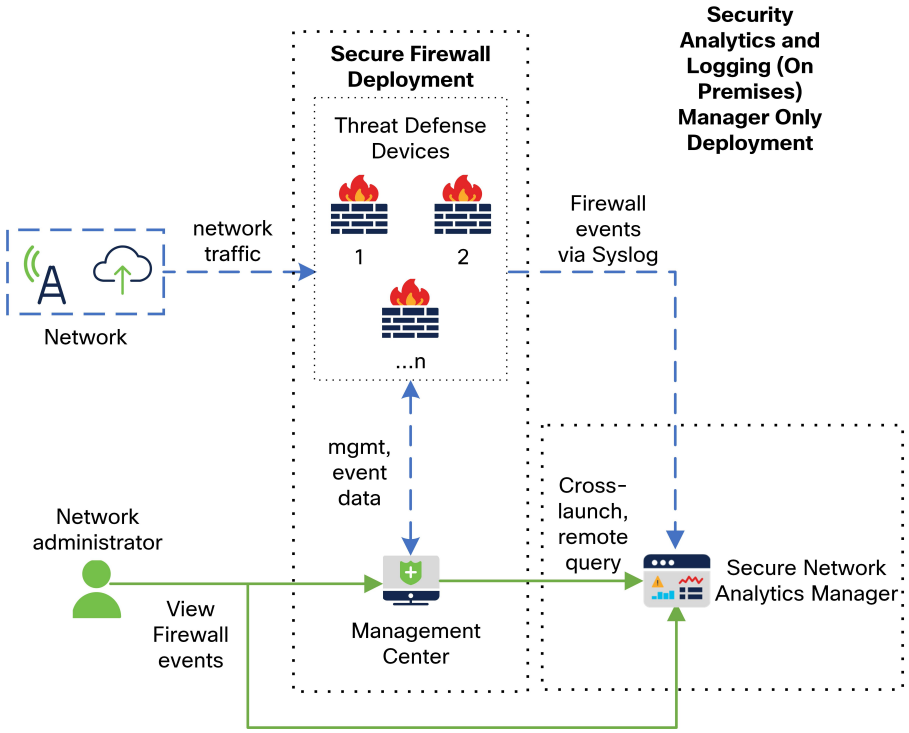
In a Security Analytics and Logging (OnPrem) deployment, you can use a Secure Network Analytics appliance to store data from another Cisco product deployment. In the case of the Secure Firewall deployment, you can export your Security Events and data plane events from your Secure Firewall Threat Defense devices managed by the management center to a Manager to store that information.

You have two options for Secure Network Analytics deployment:

- Manager only - Deploy a standalone Manager to receive and store events, and from which you can review and query events
- Data Store - Deploy Cisco Secure Network Analytics Flow Collectors (up to 5) to receive events, a Cisco Secure Network Analytics Data Store containing 1, 3, or more (in sets of 3) Cisco Secure Network Analytics Data Nodes to store events, and a Manager from which you can review and query events

Manager Only

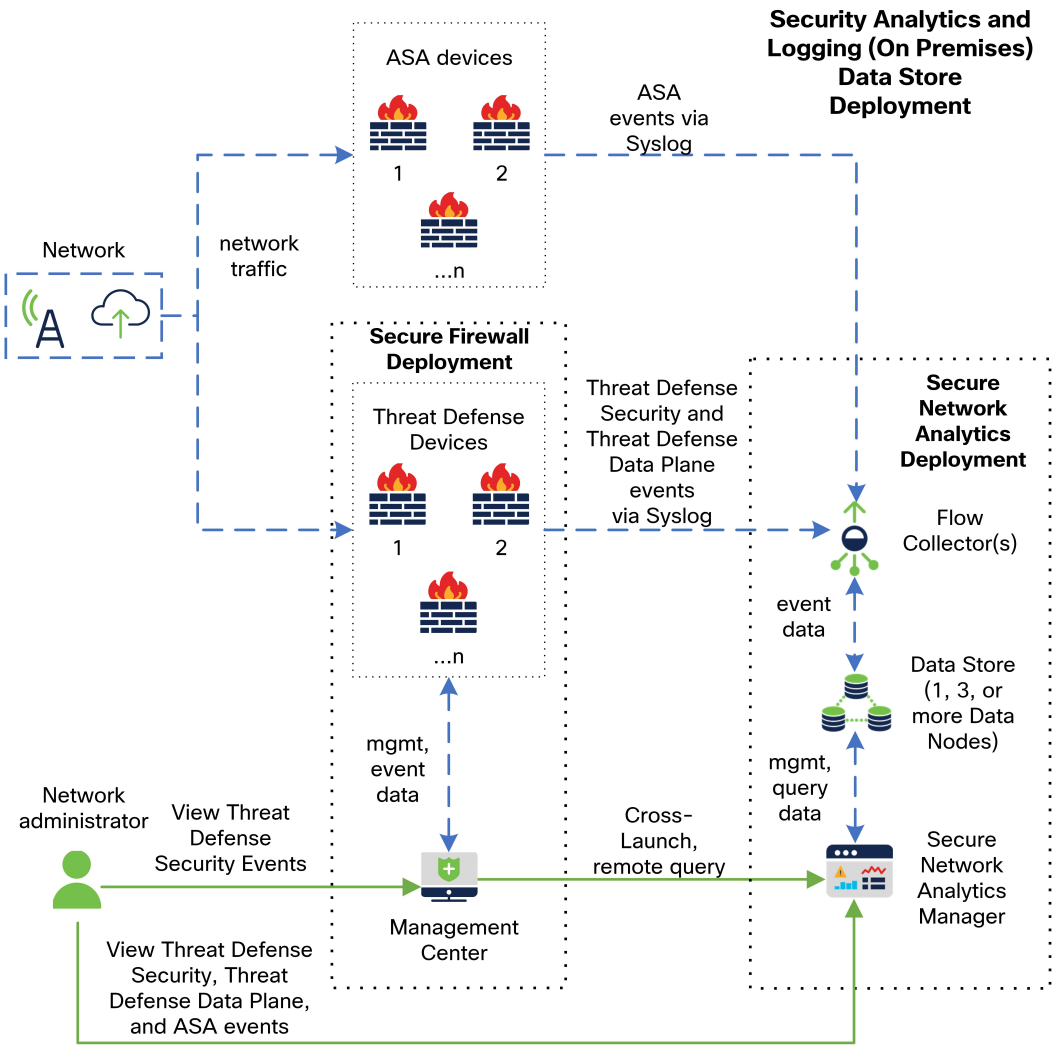
See the following diagram for an example of a Manager only deployment:



In this deployment, the threat defense devices send Secure Firewall events to the Manager, and the Manager stores these events. From the management center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the management center.

Data Store

See the following diagram for an example of a Data Store deployment with a Manager, Data Nodes, and Flow Collector(s):



In this deployment, the threat defense and Secure Firewall ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store for storage. From the management center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the management center.

Reference Documentation

The following table describes relevant reference documentation for Security Analytics and Logging (OnPrem) appliance compatibility, deployment, and use:

Table 1:

Document	Description
Secure Firewall Release Notes	Review the Secure Firewall Release Notes to understand the latest information about the current Secure Firewall release, including last-minute information.
Secure Network Analytics Smart Licensing Guide	Review the Secure Network Analytics Smart Licensing Guide to understand how to register your Secure Network Analytics product instance and license your Secure Network Analytics appliances.
Secure Network Analytics Installation Guide	Review the Secure Network Analytics Installation Guide to understand how to deploy your Secure Network Analytics appliances.
Secure Network Analytics Configuration Guide	Review the Secure Network Analytics Configuration Guide to understand how to configure your Secure Network Analytics appliances.
Secure Network Analytics Release Notes	Review the Secure Network Analytics Release Notes to understand the latest information about the current Secure Network Analytics release, including last-minute information.
Security Analytics and Logging (OnPrem) Release Notes	Review the Security Analytics and Logging (OnPrem) Release Notes to understand the latest information about the current Security Analytics and Logging (OnPrem) release and Security Analytics and Logging (OnPrem) app, including last-minute information.

If you have not already deployed Secure Firewall or configured your Secure Firewall deployment to generate the expected connection, intrusion, file, and malware events, see the following:

Table 2:

Document	Description
Secure Firewall Compatibility Guide	Review the Secure Firewall Compatibility Guide to understand the version support for Secure Firewall Management Center and Secure Firewall Threat Defense device appliance models.
Secure Firewall Installation and Configuration Guides	Review the Secure Firewall Installation and Configuration Guides to understand how to install and configure your Secure Firewall appliances.

Document	Description
Secure Firewall Management Center Configuration Guide	Review the Secure Firewall Management Center Configuration Guide to understand Secure Firewall appliance licensing and configuration of your Secure Firewall Threat Defense devices managed by your Secure Firewall Management Center, access control policies, intrusion policies, and file policies.

Requirements

The following lists the appliance requirements for deploying Security Analytics and Logging (OnPrem) to store your Firewall event data.

Firewall Appliances

You must deploy the following Firewall appliances:

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Secure Firewall Management Center (hardware or virtual)	v7.2+ For the management center running earlier versions, see https://cisco.com/go/sal-on-prem-docs.	none	• You can deploy one Manager per management center, and optionally multiple Flow Collectors and Data Nodes.
Secure Firewall managed devices	v7.0+ using the wizard Threat Defense v6.4 or later using syslog NGIPS v6.4 using syslog	none	• For instructions on how to use syslog for the threat defense v6.4 or later, see Sending Events from Threat Defense Devices On Earlier Versions.
ASA devices	v9.12+	none	

Secure Network Analytics Appliances

You have the following options for deploying Secure Network Analytics:

- Manager only - Deploy only a Manager to ingest and store events, and review and query events
- Data Store - Deploy Flow Collector(s) to ingest events, Data Store to store events, and Manager to review and query events

Table 3: Manager only

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.4.2	none	• The Manager can receive events from multiple threat defense devices, all managed by one management center. • Make sure to install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events on the Manager.
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v3.2.x	Logging and Troubleshooting Smart License, based on GB/day	• Install this app on the Manager and configure to enable event ingest.

Table 4: Data Store

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Manager	Secure Network Analytics v7.4.2	none	• Make sure to install theSecurity Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events on the Manager. • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry,

Solution Component	Required Version	Licensing for Security Analytics and Logging (OnPrem)	Notes
Flow Collector	Secure Network Analytics v7.4.2	none	• You can deploy up to 5 Flow Collectors that are configured for Data Store. • The Flow Collector can receive events from multiple threat defense devices, all managed by one management center. • The Flow Collector can receive ASA events from multiple ASA devices. • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry.
Data Store	Secure Network Analytics v7.4.2	none	• You can deploy either 1, 3, or more (in sets of 3) Data Nodes. • Stores Firewall events received by Flow Collector(s). • Secure Network Analytics v7.4.1+ is required for Single Node Data Store and multi-telemetry.
Security Analytics and Logging (OnPrem) app	Security Analytics and Logging (OnPrem) app v3.2.x	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 Secure Firewall or Secure Network Analytics appliances' consoles, you can enable access over SSH.

Secure Network Analytics Licensing

You can use Security Analytics and Logging (OnPrem) for 90 days without a license in Evaluation Mode. To continue using Security Analytics and Logging (OnPrem) after the 90 day period, you must obtain a Logging and Troubleshooting Smart License for Smart Licensing, based on the GB per day you anticipate sending in syslog data from your Firewall deployment to your Secure Network Analytics appliance.

Note For license calculation purposes, the amount of data is reported to the nearest whole GB, truncated. For example, If you send 4.9 GB in a day, it is reported as 4 GB.

See the Secure Network Analytics Smart Software Licensing Guide for more information on licensing your Secure Network Analytics appliances.

Secure Network Analytics Resource Allocation

Secure Network Analytics offers the following ingest rates when deployed for Security Analytics and Logging (OnPrem):

- a hardware or virtual edition (VE) Manager only deployment can ingest up to roughly 20k events per second (EPS) on average, with short bursts of up to 35k EPS
- a virtual edition (VE) Data Store deployment, with 3 Data Nodes, can ingest up to roughly 50k EPS on average, with short bursts of up to 175k EPS
- a hardware Data Store deployment, with 3 Data Nodes, can ingest up to roughly 100k EPS on average, with short bursts of up to 350k EPS

Based on the allocated hard drive storage, you can store the data for several weeks or months. These estimates are subject to various factors, including network load, traffic spikes, and information transmitted per event.

Note At higher EPS ingest rates, the Security Analytics and Logging (OnPrem) app may drop data. In addition, if you send all event types, instead of only connection, intrusion, file, and malware events, the app may drop data as your overall EPS rises. Review the log files in this case.

Manager Only Recommendations

Manager VE Resources

For optimum performance, allocate the following resources if you deploy a Manager VE:

Resource	Recommendation
CPUs	12
RAM	64 GB
Hard drive storage	2 TB

Manager 2210 Specifications

For hardware specifications, see the Manager 2210 Specification Sheet.

Estimated Retention

Based on the storage space that you allocate for your Manager VE or if you have a Manager 2210, you can store your data for roughly the following time frames on a Manager only deployment:

Average EPS	Average Daily Events	Estimated Retention Period for 1 TB Storage	Estimated Retention Period for 2 TB Storage	Estimated Retention Period for 4 TB Storage (Hardware)
1,000	86.5 million	250 days	500 days	1000 days
5,000	430 million	50 days	100 days	200 days
10,000	865 million	25 days	50 days	100 days
20,000	1.73 billion	12.5 days	25 days	50 days

When the Manager reaches maximum storage capacity, it deletes the oldest data first to make room for incoming data.

Note We have tested the Manager VE with these resource allocations for this estimated ingest and storage period. You may note unanticipated errors due to insufficient resource allocation if you do not assign enough CPUs or RAM to the virtual appliance. If you increase the storage allocation beyond 2 TB, you may note unanticipated errors due to insufficient resource allocation.

Data Store Recommendations

For optimum performance, allocate the following resources if you deploy a Manager VE, Flow Collector VE, and Data Store VE:

Note If you are using a Single Node Data Store or if you have enabled multi-telemetry in Secure Network Analytics, your resource allocation and storage capacity may be different from the following recommendations. For more information, refer to the Secure Network Analytics Appliance Installation Guide (Hardware or Virtual Edition) and the System Configuration Guide v7.4.1.

Table 5: Manager VE

Resource	Recommendation
CPUs	8
RAM	64 GB
Hard drive storage	480 GB

Table 6: Flow Collector VE

Resource	Recommendation
CPUs	8
RAM	70 GB
Hard drive storage	480 GB

Table 7: Data Nodes VE (as part of a Data Store)

Resource	Recommendation
CPUs	12 per Data Node
RAM	32 GB per Data Node
Hard drive storage	5 TB per Data Node VE, or 15 TB total across 3 Data Nodes

Hardware Specifications

For hardware specifications, refer to the appliance specification sheets.

Estimated Retention (3 Data Nodes)

Based on the storage space that you allocate for your Data Store VE or if you have a hardware deployment, you can store your data for roughly the following time frames on your Data Store deployment:

Average EPS	Average Daily Events	Virtual	Hardware
1,000	86.5 million	1,500 days	3,000 days
5,000	430 million	300 days	600 days
10,000	865 million	150 days	300 days
20,000	1.73 billion	75 days	150 days
25,000	2.16 billion	60 days	120 days
50,000	4.32 billion	30 days	60 days
75,000	6.48 billion	Not supported	40 days
100,000	8.64 billion	Not supported	30 days

When the Data Store reaches maximum storage capacity, it deletes the oldest data first to make room for incoming data. To increase your storage capacity, add more Data Nodes using the Secure Network Analytics System Configuration Guide.

Note We have tested the virtual appliances with these resource allocations for this estimated ingest and storage period. You may note unanticipated errors due to insufficient resource allocation if you do not assign enough CPUs or RAM to the virtual appliance. If you increase the Data Node storage allocation beyond 5 TB, you may note unanticipated errors due to insufficient resource allocation.

Communication Ports

The following table lists the communication ports you must open for the Security Analytics and Logging (OnPrem) integration for a Manager only deployment.

Table 8: Manager only

From (Client)	To (Server)	Port	Protocol or Purpose
Management Center, Threat Defense devices, and Manager	External internet (NTP server)	123/UDP	NTP time synchronization, all to the same NTP server
User workstations	Management Center and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser
Threat Defense devices managed by a management center	Manager	8514/UDP	Syslog export from the threat defense devices, ingest to the Manager
Management Center	Manager	443/TCP	remote query from management center to the Manager

The following table lists the communication ports you must open for the Security Analytics and Logging (OnPrem) integration for a Data Store deployment. In addition, see the x2xx Series Hardware Appliance Installation Guide or the Virtual Edition Appliance Installation Guide for the ports you must open for your Secure Network Analytics deployment.

Table 9: Data Store

From (Client)	To (Server)	Port	Protocol or Purpose
Management Center, Threat Defense devices, Manager, Flow Collector, and Data Store	External internet (NTP server)	123/UDP	NTP time synchronization, all to the same NTP server
user workstations	Management Center and Manager	443/TCP	Logging into the appliances' web interfaces over HTTPS using a web browser

From (Client)	To (Server)	Port	Protocol or Purpose
Threat Defense devices managed by a management center	Flow Collector	8514/UDP	Syslog export from the threat defense devices, ingest to Flow Collector
ASA devices	Flow Collector	8514/UDP	Syslog export from ASA devices, ingest to Flow Collector
Management Center	Manager	443/TCP	Remote query from the management center to the Manager

Configuration Overview

The following describes the high-level steps for configuring your deployment to store firewall event data.

Review these tasks before starting your deployment.

Component and Task	Steps
Deploy Manager only	You have the following options: • Deploy a Manager 2210 to your network, and perform initial configuration, including assigning an eth0 management interface IP address and other information. See the x2xx Series Hardware Appliance Installation Guide and Secure Network Analytics System Configuration Guide for more information. • Download the Manager VE ISO, and deploy the Manager VE to your hypervisor. Perform initial configuration, and assign an eth0 management interface IP address and other information. See the Secure Network Analytics Virtual Edition Appliance Installation Guide and Secure Network Analytics System Configuration Guide for more information.
Deploy Data Store	• Deploy a Manager, Flow Collector(s), and 1, 3 or more (in sets of 3) Data Nodes to your network. Perform initial configuration for each appliance, and initialize the Data Store. See x2xx Series Hardware Appliance Installation Guide, Virtual Edition Appliance Installation Guide and Secure Network Analytics System Configuration Guide for more information.
Download and install the Security Analytics and Logging (OnPrem) app on your Manager, and configure your Secure Network Analytics deployment to receive and store Firewall events.	• Download the app file, app-smc-sal-3.2.0-v2.swu from https://software.cisco.com. • On the Manager, go to App Manager in Central Management and install the app. See the Security Analytics and Logging (OnPrem) release notes and app help for more information on the app.

Component and Task	Steps
Configure the Secure Firewall Management Center to send events to Security Analytics and Logging (OnPrem)	You have the following options: • Configure the Secure Firewall Management Center to send events to your Secure Network Analytics appliance. • Configure Data Plane event logging using the *Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog* section in the Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide. • Reduce logging load on the Secure Firewall Management Center using Stop Storing Low-Priority Connection Events on the Secure Firewall Management Center.
Configure ASA devices to send events to Security Analytics and Logging (OnPrem)	• Configure your ASA devices to send events to your Secure Network Analytics appliance using the *ASA Devices Configuration* section of the Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide.
Review Next Steps	Review the Next Steps: • Review the Secure Firewall online help for more information. See the *Work in the Management Center with Connection Events Stored on a Secure Network Analytics Appliance* section of the Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide. • Review the Manager Web App online help for more information on how to use Secure Network Analytics.

Next Steps

After you configure your Firewall devices to send event data to your Secure Network Analytics appliance as part of Security Analytics and Logging (OnPrem), you can take the following steps:

- Review the management center online help.
- Review the Manager Web App online help to learn more about Secure Network Analytics.