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.