# 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 (Manager only), or a Manager that manages a Cisco Secure Network Analytics Flow Collector NetFlow and Cisco Secure Network Analytics Data Nodes (Data Store). You cannot install the app on a 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 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+<br>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. |

| Solution Component | Required Version | Licensing for Security Analytics and Logging (OnPrem) | Notes |
|---|---|---|---|
| Secure Firewall managed devices | v7.0+ using the wizard<br>Threat Defense v6.4 or later using syslog<br>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 1: Manager only***

| Solution Component | Required Version | Licensing for Security Analytics and Logging (OnPrem) | Notes |
|---|---|---|---|
| Manager | Secure Network Analytics v7.5.0 | none | • The Manager can receive events from multiple threat defense devices, all managed by one management center.<br>• 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 v3.3.0 | Logging and Troubleshooting Smart License, based on GB/day | • Install this app on the Manager and configure to enable event ingest. |

*Table 2: Data Store*

| Solution Component | Required Version | Licensing for Security Analytics and Logging (OnPrem) | Notes |
|---|---|---|---|
| Manager | Secure Network Analytics v7.5.0 | none | • Make sure to install the Security Analytics and Logging (OnPrem) app for event ingest, and for viewing Firewall events on the Manager. |
| Flow Collector | Secure Network Analytics v7.5.0 | none | • You can deploy up to 5 Flow Collectors that are configured for Data Store.<br>• The Flow Collector can receive events from multiple threat defense devices, all managed by one management center.<br>• The Flow Collector can receive ASA events from multiple ASA devices. |
| Data Store | Secure Network Analytics v7.5.0 | none | • You can deploy either 1, 3, or more (in sets of 3) Data Nodes.<br>• Stores Firewall events received by Flow Collector(s). |
| Security Analytics and Logging (OnPrem) app | Security Analytics and Logging (OnPrem) app v3.3.0 | 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 Secure Firewall 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-3.3.0-v2.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.