Cisco Secure Network Analytics

x2xx Series Hardware Appliance Installation Guide

Table of Contents

Introduction **5**

Overview 5

Audience 5

Installing Appliances and Configuring Your System 6

Related Information 6

Terminology 6

Common Abbreviations 7

About Secure Network Analytics Appliances **8**

Manager 2210 8

Data Store 6200 8

Flow Collector 4210 and 5210 9

UDP Director 2210 9

Flow Sensor 1210, 3210, and 4240 10

Secure Network Analytics without Data Store **11**

Secure Network Analytics with Data Store **12**

Queries 13

Data Store Storage and Fault Tolerance 13

Telemetry Storage Example 14

General Deployment Requirements **15**

Hardware and Software Version Release Matrix 15

Specifications 15

Cisco Integrated Management Controller (CIMC) 15

Standard Appliance Requirements (without Data Store) 16

Manager and Flow Collector Deployment Requirements 16

Data Store Deployment Requirements **17**

Appliance Requirements (with Data Store) 17

Manager and Flow Collector Deployment Requirements 17

Data Node Deployment Requirements 18

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Multi-Data Node Deployment 18
Supported Hardware Metrics (with Analytics enabled) 19
Supported Hardware Metrics (without Analytics enabled) 19
Single Data Node Deployment 19
Data Node Configuration Requirements 20
Networking and Switching Considerations 22
Hardware Switch Example 24
Data Store Placement Considerations 26
Analytics Deployment Requirements 26
1. Configuring Your Firewall for Communications 27
Open Ports (All Appliances) 27
Additional Open Ports for Data Nodes 27
Communication Ports and Protocols 28
Additional Open Ports for Data Store 30
Optional Communication Ports 31
Secure Network Analytics Deployment Example 32
Secure Network Analytics Deployment with Data Store Example 33
2. Installation Warnings and Guidelines 34
Installation Warnings 34
Installation Guidelines 40
Safety Recommendations 42
Maintain Safety with Electricity 42
Prevent ESD Damage 43
Site Environment 43
Power Supply Considerations 43
Rack Configuration Considerations 44
3. Mounting Your Appliances 45
Hardware Included with the Appliance 45
Additional Required Hardware 45
4. Connecting Your Appliances to the Network 46

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. Reviewing Specifications 46
2. Connecting Your Appliance to the Network 46
5. Connecting to Your Appliance 48
Connecting with a Keyboard and a Monitor 48
Connecting with a Serial Cable or Serial Console 49
Connecting with CIMC (Required for Remote Access) 50
6. Configuring Your Secure Network Analytics System 51
System Configuration Requirements 51
Contacting Support 54
Change History 55

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Introduction

Overview

This guide explains how to install Cisco Secure Network Analytics (formerly Stealthwatch) x2xx Series hardware appliances. This guide also describes the mounting and installation of the Secure Network Analytics hardware.

> ⚠ Read the Regulatory and Compliance Safety Information document before installing the Secure Network Analytics x2xx Series appliances.

Hardware in the x2xx Series includes:

Appliance	Part Number
Manager 2210 (formerly Stealthwatch Management Console)	ST-SMC2210-K9
Data Store 6200 (three Data Nodes)	ST-DS6200-K9 (three ST-DNODE-G1)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210 Engine	ST-FC5210-E
Flow Collector 5210 Database	ST-FC5210-D
UDP Director 2210	ST-UDP2210-K9
Flow Sensor 1210	ST-FS1210-K9
Flow Sensor 3210	ST-FS3210-K9
Flow Sensor 4240	ST-FS4240-K9

Audience

This guide is designed for the person responsible for installing Secure Network Analytics hardware. We assume that you already have some general understanding of installing network equipment.

If you prefer to work with a professional installer, please contact your local Cisco Partner or Cisco Support.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Installing Appliances and Configuring Your System

Please note the overall workflow for installing and configuring Secure Network Analytics.

1. **Install Appliances:** Install your Secure Network Analytics x2xx Series hardware (physical) appliances using this installation guide. To install Virtual Edition appliances, follow the instructions in the Virtual Edition Appliance Installation Guide.
2. **Configure Secure Network Analytics:** After you install hardware and virtual appliances, you are ready to configure Secure Network Analytics into a managed system. Follow the instructions in the System Configuration Guide

Related Information

For more information about Secure Network Analytics, refer to the following online resources:

- **Regulatory and Compliance Safety Information:** Read the Regulatory and Compliance Safety Information document before installing the Secure Network Analytics x2xx Series appliances.
- **Overview:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Data Store Design Guide:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Hardware and Software Version Support Matrix:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Appliance Specifications:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics product.

A "**cluster**" is your group of Secure Network Analytics appliances that are managed by the Manager.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
DMZ	Demilitarized Zone (a perimeter network)
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
NIC	Network Interface Card
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TAP	Test Access Port
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

About Secure Network Analytics Appliances

Secure Network Analytics comprises several hardware appliances that gather, analyze, and present information about your network to improve network performance and security. This section describes each Secure Network Analytics x2xx Series appliance.

Manager 2210

The Manager manages, coordinates, configures, and organizes all of the different components of the system. Secure Network Analytics software allows you to access the console's web UI from any computer with access to a web browser. You can easily access real-time security and network information about critical segments throughout your enterprise. Featuring Java-based platform independence, the Manager enables:

- Centralized management, configuration, and reporting for up to 25 Secure Network Analytics Flow Collectors
- Graphical charts for visualizing traffic
- Drill-down analysis for troubleshooting
- Consolidated and customizable reports
- Trend analysis
- Performance monitoring
- Immediate notification of security breaches

If you are deploying a Data Store, you can configure a Manager 2210 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. If you are not deploying a Data Store, you can only configure the 1 Gbps/10 Gbps interface as eth0.

Data Store 6200

The Data Store provides a central repository to store your network's telemetry, collected by your Flow Collectors. The Data Store is comprised of a cluster of Data Nodes, each containing a portion of your data, and a backup of a separate Data Node's data. Because all of your data is in one centralized database, as opposed to spread across multiple Flow Collectors, your Manager can retrieve query results from the Data Store more quickly than if it queried all of your Flow Collectors separately. The Data Store cluster provides improved fault tolerance, improved query response, and quicker graph and chart population.

Refer to **Secure Network Analytics with Data Store** for details.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Flow Collector 4210 and 5210

The Flow Collector gathers NetFlow, cFlow, J-Flow, Packeteer 2, NetStream, and IPFIX data to provide behavior-based network protection.

The Flow Collector aggregates high-speed network behavior data from multiple networks or network segments to deliver end-to-end protection and improve performance across geographically dispersed networks.

If you are deploying a Data Store, you can configure a Flow Collector 4210 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. If you are not deploying a Data Store, you can only configure the 100Mbps/1Gbps/10Gbps copper interface as eth0.

> As the Flow Collector receives data, it identifies known or unknown attacks, internal misuse, and misconfigured network devices, regardless of packet encryption or fragmentation. Once Secure Network Analytics identifies the behavior, the system can take any action you have configured, if any, for that kind of behavior.

UDP Director 2210

The UDP Director is a high-speed, high-performance UDP packet replicator. The UDP Director is very helpful in redistributing NetFlow, sFlow, syslog, or Simple Network Management Protocol (SNMP) traps to various collectors. It can receive data from any connectionless UDP application and then retransmit it to multiple destinations, duplicating the data if required.

When you use the UDP Director High Availability (HA) configuration, make sure you connect two UDP Director appliances with crossover cables. For instructions, see **2. Connecting Your Appliance to the Network**.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Flow Sensor 1210, 3210, and 4240

The Flow Sensor is a network appliance that operates similarly to a traditional packet capture appliance or IDS in that it plugs into a switch port analyzer (SPAN), mirror port, or Ethernet test access port (TAP). The Flow Sensor augments visibility into the following network areas:

- Where NetFlow is not available.
- Where NetFlow is available, but you want deeper visibility into performance metrics and packet data.

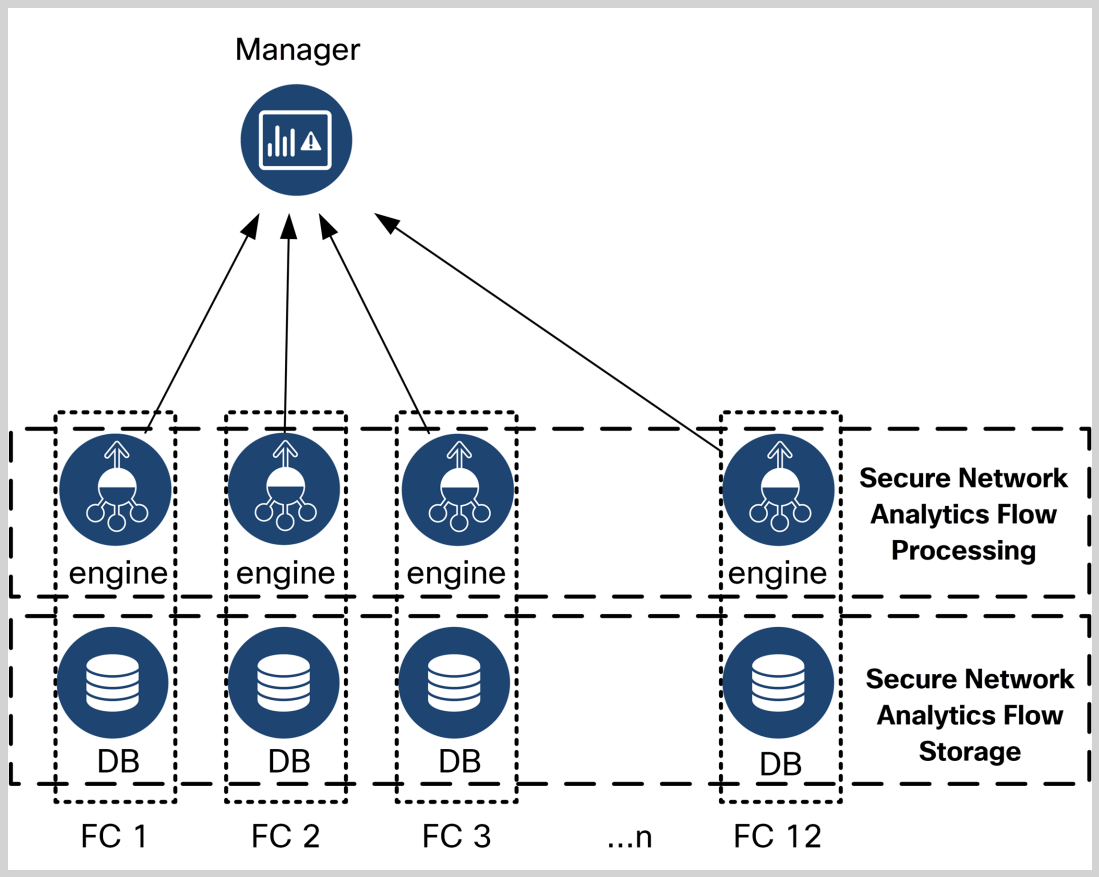
By directing the Flow Sensor toward any NetFlow v9-capable Flow Collector, you can gain valuable detailed traffic statistics from NetFlow. When combined with the Secure Network Analytics Flow Collector, the Flow Sensor also provides deep insight into performance metrics and behavioral indicators. These flow performance indicators provide insight into any round-trip latency introduced by the network or by the server-side application.

Because the Flow Sensor has packet-level visibility, it can calculate round-trip time (RTT), server response time (SRT), and packet loss for TCP sessions. It includes all of these additional fields in the NetFlow records that it sends to the Flow Collector.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics without Data Store

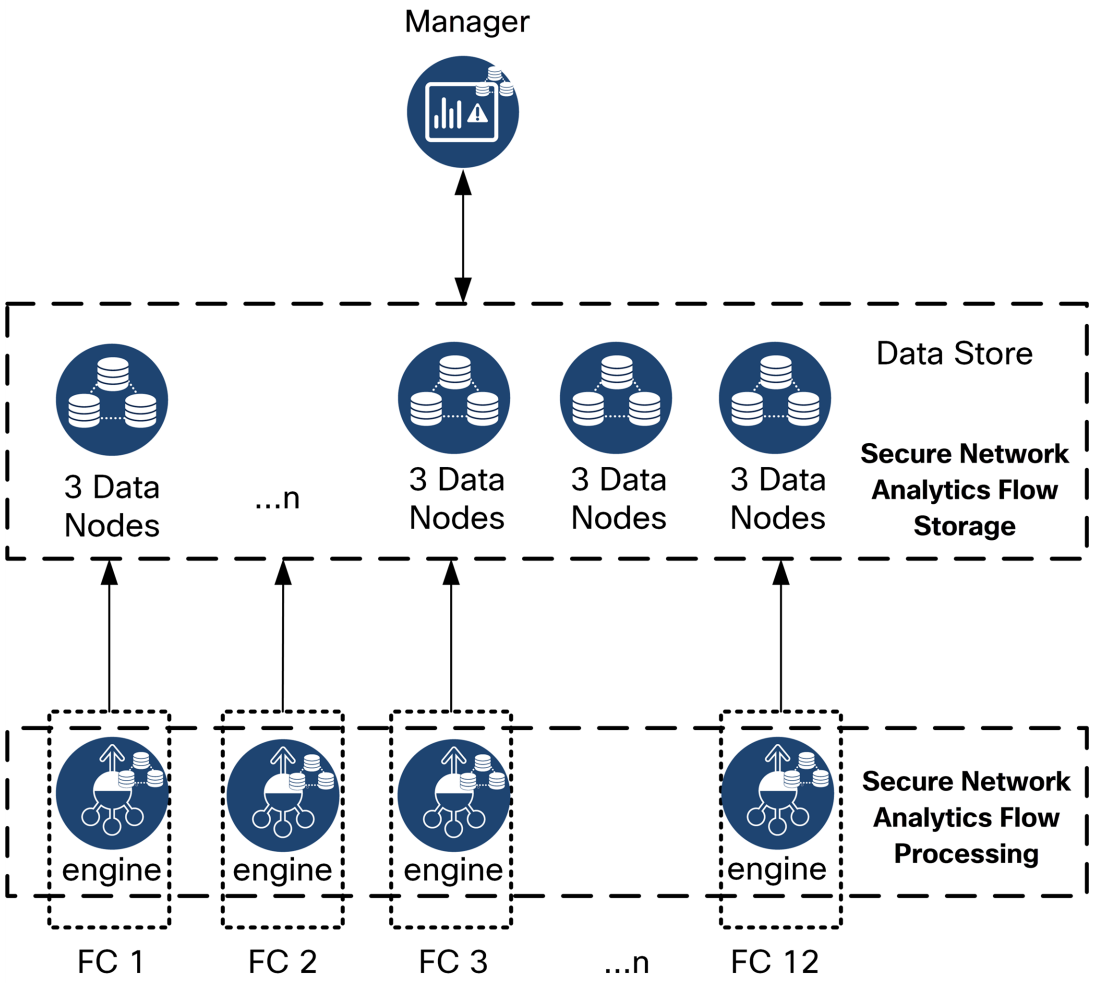
In a Secure Network Analytics deployment without a Data Store, one or more Flow Collectors ingests and deduplicates data, performs analysis, and reports data and results directly to the Manager. To resolve user-submitted queries, including graphs and charts, the Manager queries all of the managed Flow Collectors. Each Flow Collector returns matching results to the Manager. The Manager collates the information from the different result sets, then generates a graph or chart displaying the results. In this deployment, each Flow Collector stores data on a local database. See the following diagram for an example.



© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics with Data Store

In a Secure Network Analytics deployment with a Data Store, the Data Store cluster sits between your Manager and Flow Collectors. One or more Flow Collectors ingests and deduplicates flows, performs analysis, and reports data and results directly to the Data Store, distributing it roughly equally to all of the Data Nodes. The Data Store facilitates data storage, keeps all of your traffic in that centralized location as opposed to spread across multiple Flow Collectors, and it offers greater storage capacity than multiple Flow Collectors. See the following diagram for an example.



The Data Store provides a central repository to store your network's telemetry, collected by your Flow Collectors. The Data Store is comprised of a cluster of Data Nodes, each containing a portion of your data, and a backup of a separate Data Node's data. Because all of your data is in one centralized database, as opposed to spread across multiple Flow Collectors, your Manager can retrieve query results from the Data Store more quickly than if it queried all of your Flow Collectors separately. The Data Store cluster provides

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

improved fault tolerance, improved query response, and quicker graph and chart population.

Queries

To resolve user-submitted queries, including graphs and charts, the Manager queries the Data Store. The Data Store finds matching results in the columns relevant to the query, then retrieves the matching rows and returns the query results to the Manager. The Manager generates the graph or chart without needing to collate multiple result sets from multiple Flow Collectors. This reduces the cost of querying, as compared to querying multiple Flow Collectors, and improves query performance.

Data Store Storage and Fault Tolerance

The Data Store collects data from Flow Collectors and distributes it equally across Data Nodes within the cluster. Each Data Node, in addition to storing a portion of your overall telemetry, also stores a backup of another Data Node's telemetry. Storing data in this fashion:

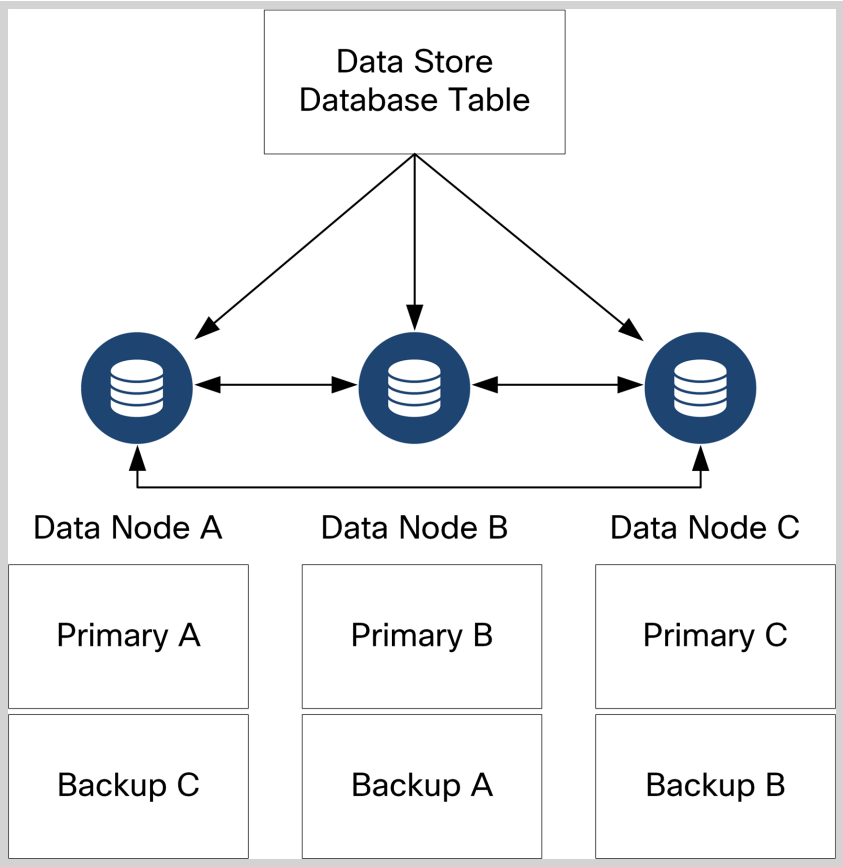
- helps with load balancing
- distributes processing across each node
- ensures all data ingested into the Data Store has a backup for fault tolerance
- allows for increasing the number of Data Nodes to improve overall storage and query performance

If your Data Store has 3 or more Data Nodes, and a Data Node goes down, as long as the Data Node containing its backup is still available, and at least half of your total number of Data Nodes are still up, the overall Data Store remains up. This allows you time to repair the downed connection or faulty hardware. After you replace the faulty Data Node, the Data Store restores that node's data from the existing backup stored on the adjacent Data Node, and creates a backup of data on that Data Node.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Telemetry Storage Example

See the following diagram for an example of how 3 Data Nodes store telemetry:



© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

General Deployment Requirements

Before you begin, review this guide to understand the process as well as the preparation, time, and resources you'll need to plan for the installation.

Hardware and Software Version Release Matrix

Review the Hardware and Software Version Release Matrix for compatibility details. The matrix is available at https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

Specifications

Download the specifications sheet for each appliance you plan to install. The specifications are available at https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

Cisco Integrated Management Controller (CIMC)

After you install your appliances, make sure you configure the Cisco Integrated Management Controller (CIMC) to enable access to the server configuration and a virtual server console. You can also use the CIMC to monitor hardware health.

- **Instructions:** Refer to Technical References page and identify the specification for your UCS Platform in the Specification Sheets section. Then, locate the corresponding installation guide for your UCS Platform on this page and follow the instructions.
- **Default Password:** As part of the initial configuration, you will log in to the CIMC as admin and type **password** in the Password field.
- **Password Requirement:** When you log in, change the default password to protect the security of your network.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Standard Appliance Requirements (without Data Store)

If you are installing Secure Network Analytics without a Data Store, install the following appliances:

Appliance	Requirement
Manager	• Minimum of 1 Manager
Flow Collector	• Minimum of 1 Flow Collector
Flow Sensor	Optional
UDP Director	Optional

To review appliance installation requirements for Secure Network Analytics with a Data Store, refer to **Data Store Deployment Requirements**.

Manager and Flow Collector Deployment Requirements

For each Manager and Flow Collector that you deploy, assign a routable IP address to the `eth0` management port.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store Deployment Requirements

To deploy Secure Network Analytics with a Data Store, review the following requirements and recommendations for your deployment.

Appliance Requirements (with Data Store)

The following table provides an overview for the appliances required to deploy Secure Network Analytics with Data Store.

Appliance	Requirement
Manager	• Minimum of 1 Manager
Data Store	• Minimum of 1 or 3 Data Nodes • Additional sets of 3 Data Nodes to expand the Data Store, maximum of 48 Data Nodes **Note**: Deployments larger than 18 nodes using IPv6 or IPSec configurations may experience performance degradation. • Deploying only 2 Data Nodes in a cluster is not supported.
Flow Collector	• Minimum of 1 Flow Collector
Flow Sensor	Optional

> ⚠ Do not update the appliance BIOS, as it may cause issues with appliance functionality.

Manager and Flow Collector Deployment Requirements

For each Manager and Flow Collector that you deploy, assign a routable IP address to the `eth0` management port.

- **eth0 Port Configuration:** You can configure the use of a **BASE-T** copper 1G/10G port or SFP+ twinax cable 10G port for the Manager and Flow Collector`eth0` management port.
- **Throughput:** We require 10G throughput for the BASE-T copper port for Data Store use. If you're not deploying a Data Store, you can only configure the 100Mbps/1Gbps/10 Gbps copper interface as `eth0` .

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Node Deployment Requirements

Each Data Store is comprised of Data Nodes.

- **Hardware:** Each hardware Data Node is its own chassis. You can deploy 1, 3, or more Data Nodes (in sets of 3).
- **Virtual Edition:** When you download a virtual Data Store, you can deploy 1, 3, or more Data Nodes Virtual Edition (in sets of 3).

> Make sure your Data Nodes are all hardware or all Virtual Edition. Mixing hardware and virtual Data Nodes is not supported and hardware must be from the same hardware generation (all DS 6200 or all DN 6300).

Multi-Data Node Deployment

A multi-Data Node deployment provides maximum performance results. For example, a 3 Data Node 6300 Data Store deployment can retain approximately 1.5 million flows per second for approximately 90 days.

Note the following:

- **Sets of Three:** The Data Nodes can be clustered as part of your Data Store in sets of 3, from a minimum of 3 to a maximum of 48. Deploying only 2 Data Nodes in a cluster is not supported.

  > **Note**: Deployments larger than 18 nodes using IPv6 or IPSec configurations may experience performance degradation.

- **All Hardware or All Virtual:** Make sure your Data Nodes are all hardware (of the same generation) or all Virtual Edition. Mixing hardware and virtual Data Nodes or mixing Data Store 6200 and Data Node 6300 Data Nodes is not supported.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Supported Hardware Metrics (with Analytics enabled)

Number of Nodes	Flows Per Second	Unique Internal Hosts
1	600,000	1.3 million
3 and above	1.5 million	500,000
3 and above	1 million	1 million
3 and above	500,000	2 million

These recommendations consider only telemetry. Your performance may vary depending on additional factors, including host count, Flow Sensor use, traffic profiles, and other network characteristics. Contact Cisco Support for assistance with sizing.

Supported Hardware Metrics (without Analytics enabled)

Number of Nodes	Flows Per Second	Unique Internal Hosts
1	Up to 1 million	Up to 33 million
3 and above	Up to 3 million	Up to 33 million

These numbers are generated in our test environments using average customer data with 1.3 million unique hosts. There are several factors that may affect your specific performance, such as number of hosts, average flow size, and more. Contact Cisco Support for assistance with sizing.

Single Data Node Deployment

If you choose to deploy a single (1) Data Node:

- **Flow Collectors:** A maximum of 4 Flow Collectors are supported.
- **Adding Data Nodes:** If you deploy only one Data Node, you can add Data Nodes to your deployment in the future. Refer to **Multi-Data Node Deployment** for details.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> These recommendations consider only telemetry. Your performance may vary depending on additional factors, including host count, Flow Sensor use, traffic profiles, and other network characteristics. Contact Cisco Support for assistance with sizing.

> Currently, the Data Store does not support deploying spare Data Nodes as automatic replacements if a primary Data Node goes down. Contact Cisco Support for guidance.

Data Node Configuration Requirements

To deploy a Data Store, assign the following to each Data Node. The information you prepare will be configured in First Time Setup using the System Configuration Guide.

- **Routable IP Address (eth0):** For management, ingest, and query communications with your Secure Network Analytics appliances.
- **eth0 Port Configuration:** You can configure the use of a **BASE-T** copper 1G/10G port or SFP+ twinax cable 10G port for the `eth0` management port with any supported transceiver.
- **Throughput:** We require 10G throughput for the BASE-T copper port for Data Store use.
- **Inter-Data Node Communications:** Configure a non-routable IP address from the `169.254.42.0/24` CIDR block within a private LAN or VLAN to be used for inter-Data Node communication.

  For improved throughput performance, connect the Data Node `eth2` port (or port channel containing `eth2` and `eth3`) to the switches for inter-Data Node communication. As part of the Data Store, your Data Nodes communicate between and among each other.
- **Network Connections:** You need two 10G network connections, one for the management, ingest, and query communications, and one for the inter-Data Node communications.
- **Additional Connection and Switch:** Optionally on hardware Data Nodes only, for network redundancy and criticality of the inter-Data Node communications, an additional 10G connection, and an additional switch for establishing a port channel on the Data Node.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Configure your Data Nodes so that adjacent-numbered Data Nodes are powered with separate, redundant power supplies. This configuration improves data redundancy and overall Data Store uptime.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Networking and Switching Considerations

The following table provides an overview for the networking and switching considerations for deploying Secure Network Analytics with a Data Store.

Network Consideration	Description
Inter-Data Node Communications	• Establish a recommended round-trip time (RTT) latency of under 200 microseconds between and among Data Nodes • Keep clock skew at 1 second or lower between and among your Data Nodes. • Establish a recommended throughput of 6.4 Gbps or greater (10 Gbps full duplex switched connection) between and among your Data Nodes. • For hardware Data Nodes, configuring an `eth2` port for 10G throughput is sufficient for normal inter-Data Node communication. Creating an LACP `eth2/eth3` bonded port channel for up to 20G throughput enables faster communication between and among Data Nodes, and quicker Data Node addition or replacement to the Data Store, as each new Data Node receives traffic from adjacent Data Nodes to populate its data. Note that LACP port bonding is the only bonding option available for hardware Data Nodes.
Data Node Hardware Power	• If a hardware Data Node loses power unexpectedly, the data can be corrupted. Use both power supplies on separate circuits from uninterruptible power supplies. • When you initialize the Data Store cluster, alternate Data Node configuration based on the power supplies that each Data Node uses. This can optimize fault tolerance by minimizing the number of Data Nodes that go down if power is lost.
Data Node Switching	• Data Nodes require their own Layer 2 VLAN to allow inter-Data Node communication. Hardware Data Nodes can be connected to a shared or dedicated 10G switch. • We recommend that hardware Data Nodes be connected to 2 switches to help ensure constant connectivity during

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

	switch outages and upgrades. Due to the low latency required for inter-Data Node communication, Cisco recommends a redundant pair of switches, where the 2 switches are interconnected and carry the Layer 2 VLAN across both switches.
Secure Network Analytics Appliance Communications	• Manager and Flow Collectors must be able to reach all Data Nodes • Data Nodes must be able to reach Manager, all Flow Collectors, and each Data Node

Currently, the Data Store does not support deploying spare Data Nodes as automatic replacements if a primary Data Node goes down. Please contact Cisco Support for guidance.

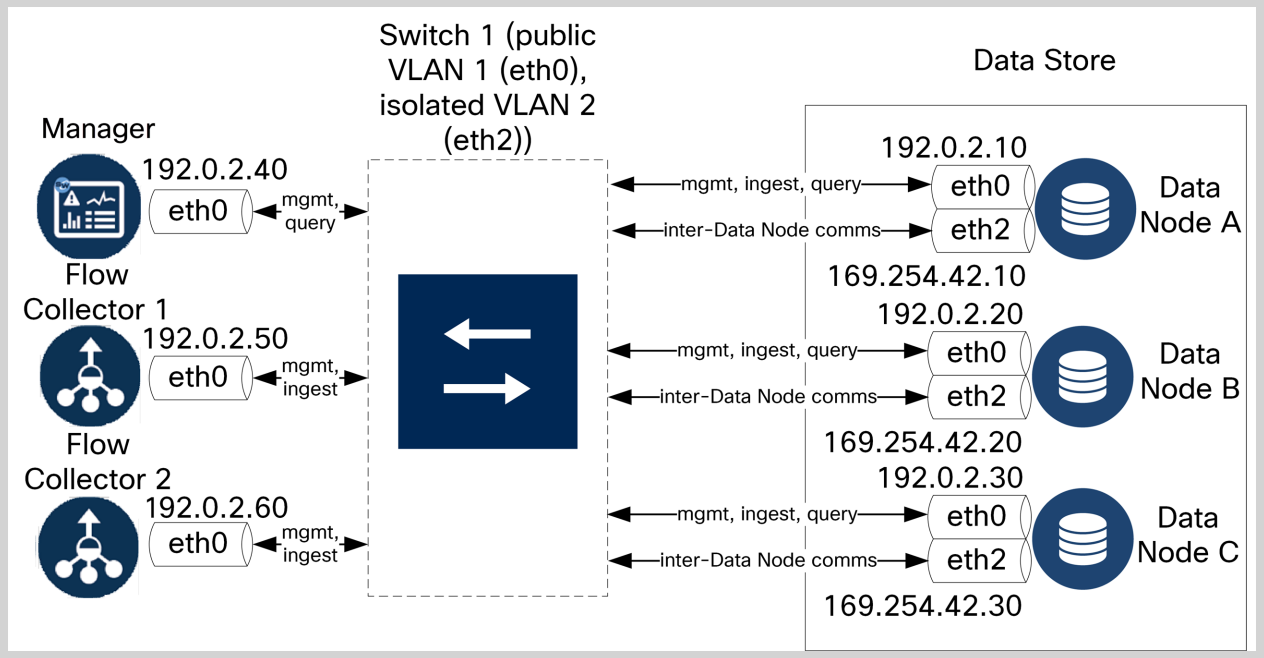
© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Hardware Switch Example

To enable inter-Data Node communications over `eth2` or the `eth2/eth3` port channel, deploy 1 switch that supports 10G speeds.

Configure a LAN or VLAN for Data Nodes `eth0` communications with the Manager and Flow Collectors, and an isolated LAN or VLAN for inter-Data Node communications.

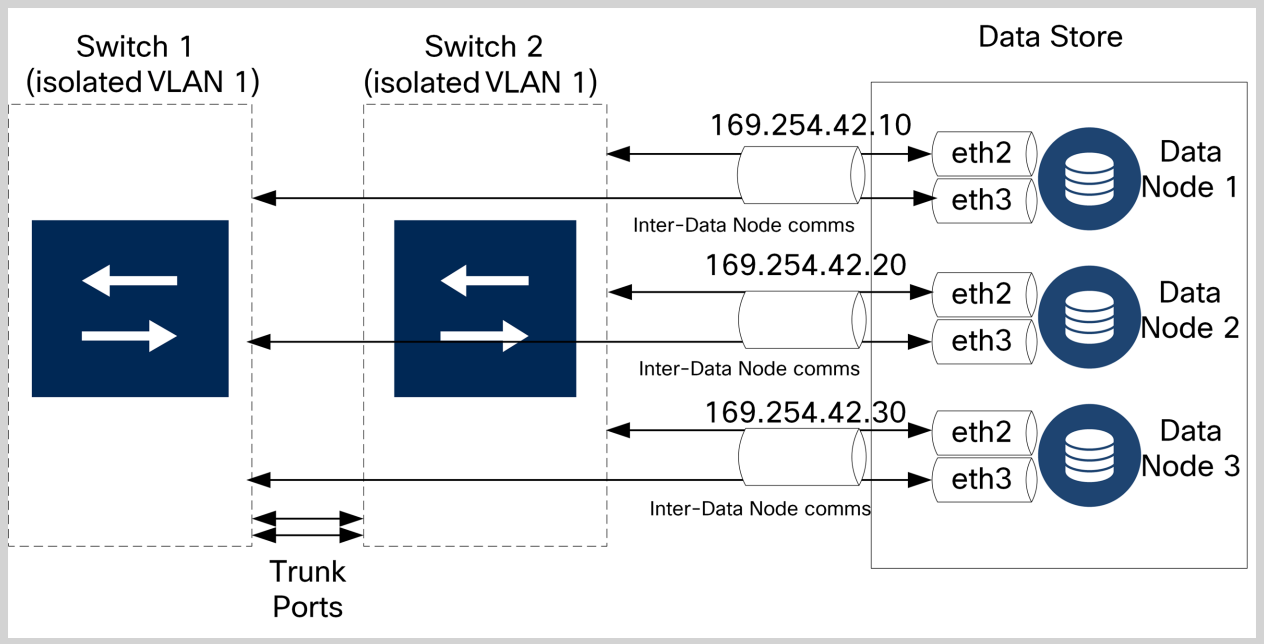
You can share these switches with other appliances, but create separate LANs or VLANs for the additional appliance traffic. See the following diagram for an example:



The Data Store cluster requires a continuous heartbeat between nodes within the isolated VLAN. Without this heartbeat, Data Nodes may potentially go offline, which increases the risk of the Data Store going down.

If you want additional network redundancy, for planning around switch updates and planned outage, make sure you configure your Data Nodes with port channels for dedicated inter-Data Node communication. Connect every Data Node to 2 switches, with each physical port connected to a different switch. See the following diagram for an example:

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



Contact Cisco Professional Services for assistance with planning your deployment.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store Placement Considerations

Place each Data Node so that it can communicate with all of your Flow Collectors, your Manager, and every other Data Node. For best performance, colocate your Data Nodes and Flow Collectors to minimize communication latency, and colocate Data Nodes and Manager for optimum query performance.

- **Firewall:** We highly recommend placing the Data Nodes within your firewall, such as within a NOC.
- **Power:** If the Data Store goes down due to loss of power or hardware failure, you run an increased risk of data corruption and data loss. Install your Data Nodes with constant uptime in mind.

> If a Data Node loses power unexpectedly, and you reboot the appliance, the database instance on that Data Node may not automatically restart. Refer to the System Configuration Guide for troubleshooting and manually restarting the database.

- **Policy:** Check that a hardware Data Node power restore policy is set to **Restore Last State**, which restarts the Data Node automatically after power loss, and attempts to restore running processes. See the UCS C-Series GUI Configuration Guide for more information on configuring the power restore policy in CIMC.

Analytics Deployment Requirements

Secure Network Analytics uses dynamic entity modeling to track the state of your network. In the context of Secure Network Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they perform on your network. For more information, refer to the Analytics: Detections, Alerts, and Observations Guide.

In order to enable Analytics, your deployment must be configured

- on a Virtual or a Hardware Data Store deployment with any number of Flow Collectors.
- with only 1 Secure Network Analytics Data Store domain.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. Configuring Your Firewall for Communications

In order for the appliances to communicate properly, you should configure the network so that firewalls or access control lists do not block the required connections. Use the information provided in this section to configure your network so that the appliances can communicate through the network.

Open Ports (All Appliances)

Consult with your network administrator to ensure that the following ports are open and have unrestricted access on your appliances (Managers, Flow Collectors, Data Nodes, Flow Sensors, and UDP Directors):

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Additional Open Ports for Data Nodes

In addition, if you deploy Data Nodes to your network, ensure that the following ports are open and have unrestricted access:

- TCP 5433
- TCP 5444
- TCP 9450

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Communication Ports and Protocols

The following table shows how the ports are used in Secure Network Analytics:

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	Manager	TCP/389, UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
External log sources	Manager	UDP/514	SYSLOG
Flow Collector	Manager	TCP/443	HTTPS
UDP Director	Manager	TCP/443	HTTPS
UDP Director	Flow Collector (sFlow)	UDP/6343*	sFlow
UDP Director	Flow Collector (NetFlow)	UDP/2055*	NetFlow
UDP Director	3rd Party event management systems	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector (NetFlow)	UDP/2055	NetFlow
NetFlow Exporters	Flow Collector (NetFlow)	UDP/2055*	NetFlow
sFlow Exporters	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS
Manager	Cisco ISE	TCP/443	HTTPS

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

From (Client)	To (Server)	Port	Protocol
Manager	Cisco ISE	TCP/8910	XMPP
Manager	DNS	UDP/53	DNS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Flow Exporters	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	CRL Distribution Points	TCP/80	HTTP
Manager	OCSP responders	TCP/80	OCSP
User PC	Manager	TCP/443	HTTPS

*This is the default port, but any UDP port could be configured on the exporter.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Additional Open Ports for Data Store

The following lists the communication ports to open on your firewall to deploy the Data Store.

#	From (Client)	To (Server)	Port	Protocol or Purpose
1	Manager	Flow Collectors and Data Nodes	22/TCP	SSH, required to initialize Data Store database
1	Data Nodes	All other Data Nodes	22/TCP	SSH, required to initialize Data Store database and for database administration tasks
2	Manager, Flow Collectors, and Data Nodes	NTP server	123/UDP	NTP, required for time synchronization
2	NTP server	Manager, Flow Collectors, and Data Nodes	123/UDP	NTP, required for time synchronization
3	Manager	Flow Collectors and Data Nodes	443/TCP	HTTPS, required for secure communications between appliances
3	Flow Collectors	Manager	443/TCP	HTTPS, required for secure communications between appliances
3	Data Nodes	Manager	443/TCP	HTTPS, required for secure communications between appliances
4	NetFlow Exporters	Flow Collectors - NetFlow	2055/UDP	NetFlow ingestion
5	Data Nodes	All other Data Nodes	4803/TCP	Inter-Data Node messaging service
6	Data Node	All other Data	4803/UDP	Inter-Data Node messaging

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

		Nodes		service
7	Data Nodes	All other Data Nodes	4804/UDP	Inter-Data Node messaging service
8	Manager, Flow Collectors, and Data Nodes	Data Nodes	5433/TCP	Vertica client connections
9	Data Node	All other Data Node	5433/UDP	Vertica messaging service monitoring
10	sFlow Exporters	Flow Collector (sFlow)	6343/UDP	sFlow ingestion
11	Data Nodes	All other Data Nodes	6543/UDP	Inter-Data Node messaging service
12	Data Nodes	All other Data Nodes	9222 /UDP	Inter-Data Node SSH service

Optional Communication Ports

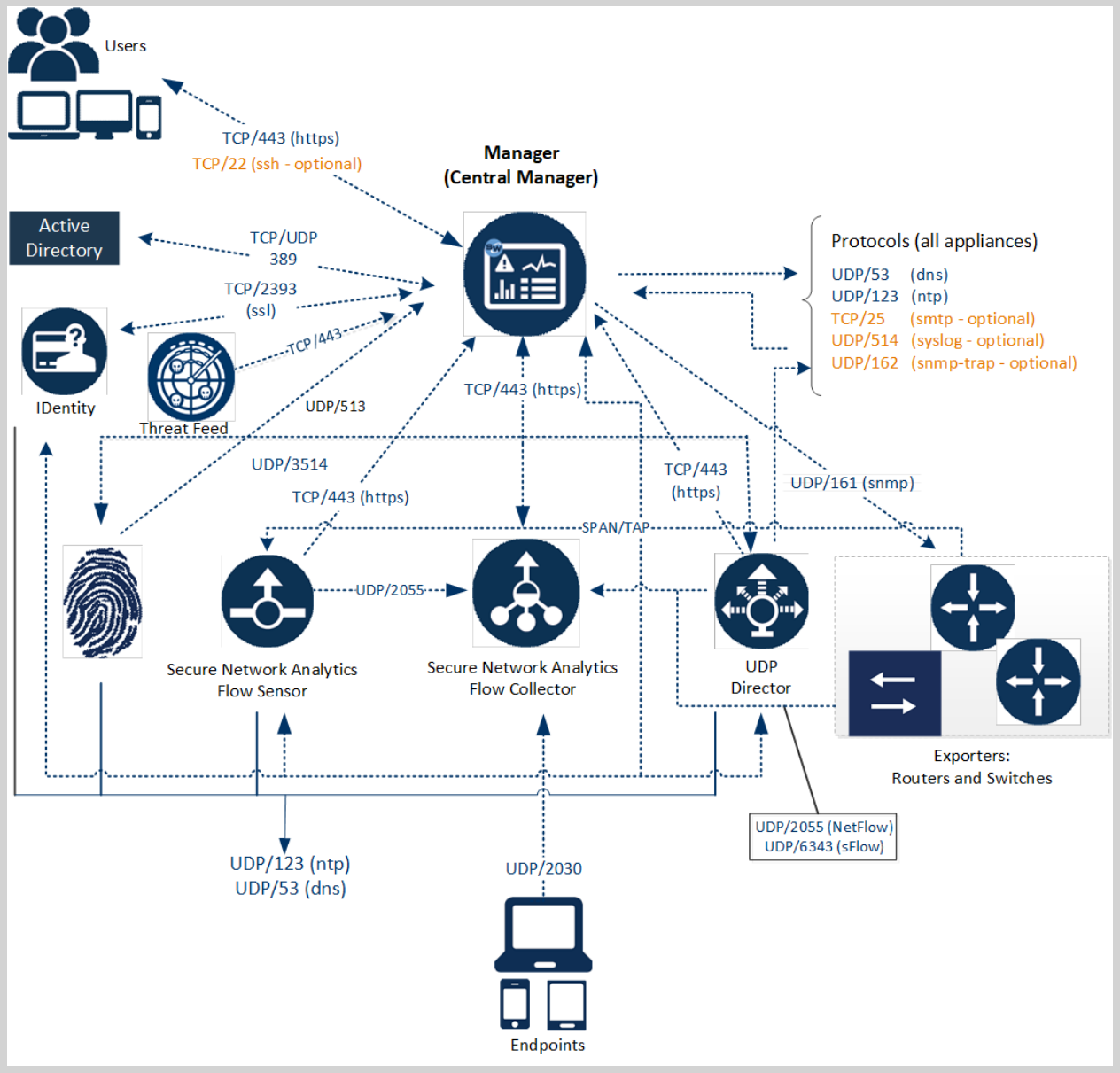
The following table is for optional configurations determined by your network needs:

From (Client)	To (Server)	Port	Protocol
All appliances	User PC	TCP/22	SSH
Manager	3rd Party event management systems	UDP/162	SNMP-trap
Manager	3rd Party event management systems	UDP/514	SYSLOG
Manager	Email gateway	TCP/25	SMTP
Manager	Threat Feed	TCP/443	SSL
User PC	All appliances	TCP/22	SSH

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics Deployment Example

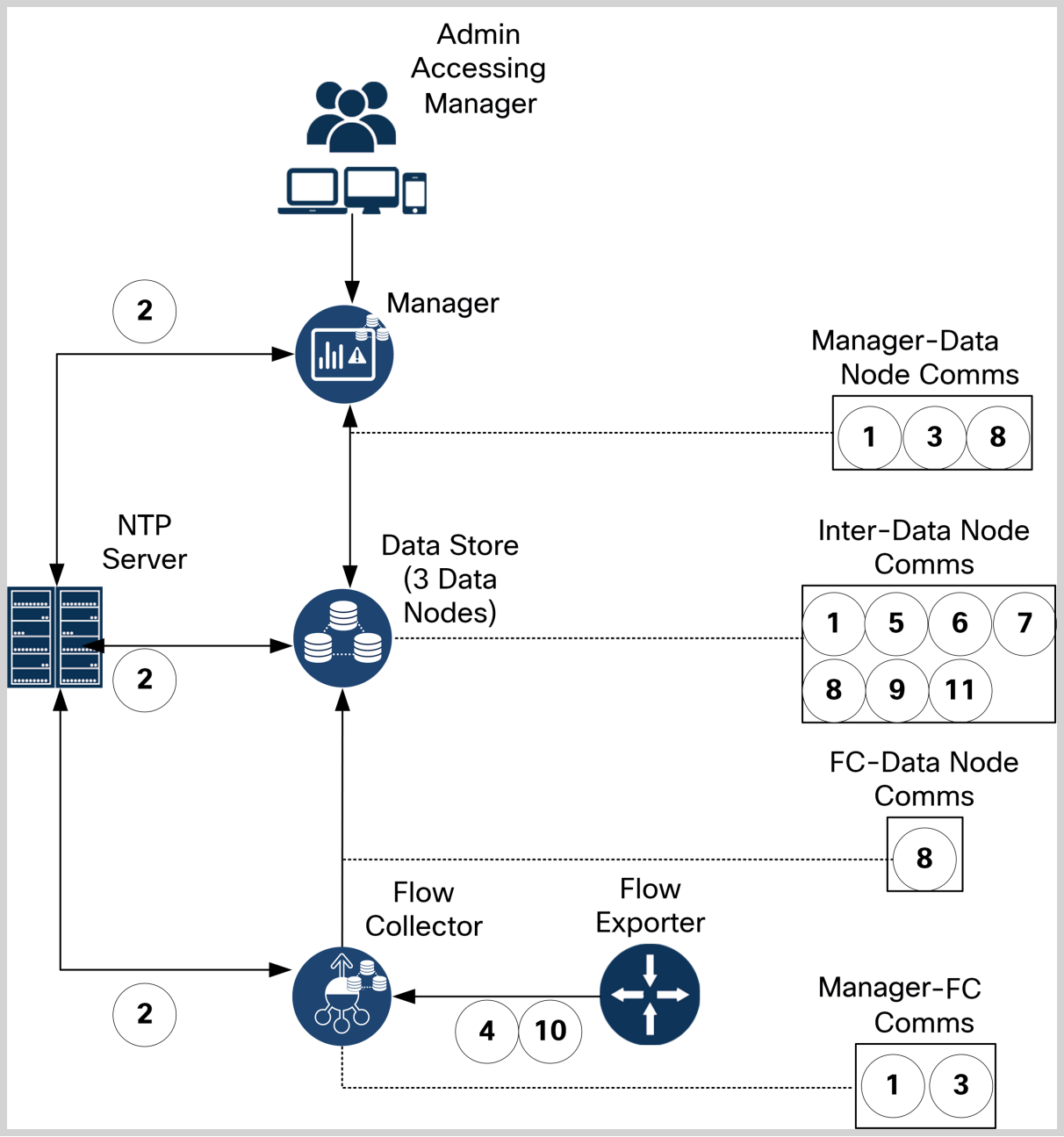
The following diagram shows the various connections used by Secure Network Analytics. Some of these ports are optional.



© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Secure Network Analytics Deployment with Data Store Example

As shown in the figure below, you can strategically deploy Secure Network Analytics appliances to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

2. Installation Warnings and Guidelines

Installation Warnings

Read the Regulatory Compliance and Safety Information document before installing the Secure Network Analytics x2xx Series appliances.

Take note of the following warnings:

Statement 1071—Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Statement 1004—Installation Instructions

Read the installation instructions before using, installing or connecting the system to the power source.

Statement 1005—Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection.

Statement 1006—Chassis Warning for Rack-Mounting and Servicing

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

to the top with the heaviest component at the bottom of the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

Statement 1015—Battery Handling

To reduce risk of fire, explosion, or leakage of flammable liquid or gas:
- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Do not dismantle, crush, puncture, use a sharp tool to remove, short the external contacts, or dispose of the battery in fire.
- Do not use if battery is warped or swollen.
- Do not store or use battery in a temperature > 140° F/60° C.
- Do not store or use battery in low air pressure environment < 69.7 kPa.

Statement 1017—Restricted Area

This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Statement 191—Voluntary Control Council for Interference (VCCI) Class A Warning for Japan

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, you may be required to take corrective actions.

Statement 164—Lifting Requirement

Two people are required to lift the heavy parts of the product. To prevent injury, keep your back straight and lift with your legs, not your back.

Statement 256—Class A Warning for Hungary

This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 294—Class A Warning for Korea

This is a Class A device and is registered for electromagnetic compatibility (EMC) requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.

Statement 340—Class A Warning for CISPR22/EN55022/CISPR32/EN55032

This is a class A product. In a domestic environment this product may cause radio interference in which case you may be required to take adequate measures.

Statement 1021—SELV Circuit

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Statement 1024—Ground Conductor

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 1028—More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.

Statement 1029—Blank Faceplates and Cover Panels

Blank faceplates and cover panels serve three important functions: they reduce the risk of electric shock and fire, they contain electromagnetic interference (EMI) that might disrupt other equipment, and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 1030—Equipment Installation

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Statement 1032—Lifting the Chassis

To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules, such as power supplies, fans, or cards. These types of handles are not designed to support the weight of the unit.

Statement 9001—Product Disposal

Ultimate disposal of this product should be handled according to all national laws and regulations.

Statement 1051—Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Statement 1055—Class 1/1M Laser

Invisible laser radiation is present. Do not expose to users of telescopic optics. This applies to Class 1/1M laser products.

Statement 1008—Class 1 Laser Product

This product is a Class 1 laser product.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 1056—Unterminated Fiber Cable

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments, for example, eye loupes, magnifiers, and microscopes, within a distance of 100 mm, may pose an eye hazard.

Fiber Type and Core Diameter (µm)	Wavelength (nm)	Maximum Power (mW)	Beam Divergence (rad)
SM 11	1200–1400	39–50	0.1–0.11
MM 62.5	1200–1400	150	0.18 NA
MM 50	1200–1400	135	0.17 NA
SM 11	1400–1600	112–145	0.11–0.13

Statement 1089—Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

Statement 1090—Installation by Skilled Person

Only a skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of a skilled person.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 1091—Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

Statement 1074—Comply with Local and National Electrical Codes

Installation of the equipment must comply with local and national electrical codes.

Statement 2017—Class A Notice for FCC

Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users are required to correct the interference at their own expense.

Statement 2021—Class A Notice for Canada

This Class A digital apparatus complies with Canadian ICES-003/NMB-003.

Statement 7001—ESD Mitigation

This equipment may be ESD sensitive. Always use an ESD ankle or wrist strap before handling equipment. Connect the equipment end of the ESD strap to an unfinished surface of the equipment chassis or to the ESD jack on the equipment if provided.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 7003—Shielded Cable Requirements for Intrabuilding Lightning Surge

The intrabuilding port(s) of the equipment or subassembly must use shielded intrabuilding cabling/wiring that is grounded at both ends.
The following port(s) are considered intrabuilding ports on this equipment:

Statement 7005—Intrabuilding Lightning Surge and AC Power Fault

The intrabuilding port(s) of the equipment or subassembly is suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring for more than 6 meters (approximately 20 feet). These interfaces are designed for use as intrabuilding interfaces only (Type 2, 4, or 4a ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection in order to connect these interfaces metallically to an OSP wiring system.
The following ports are considered intrabuilding ports on the equipment:

Installation Guidelines

Take note of the following warnings:

Statement 1047—Overheating Prevention

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of : 41 to 95° F (5 to 35° C)

Statement 1019—Main Disconnecting Device

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Statement 1075—Power Cable and AC Adapter

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors/batteries. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the "UL" or "CSA" shown on the cord), not regulated with the subject law by showing "PSE" on the cord, for any other electrical devices than products designated by CISCO.

Statement 1073—No User-Serviceable Parts

No user-serviceable parts inside. Do not open.

When you are installing a chassis, use the following guidelines:

- Ensure that there is adequate space around the chassis to allow for servicing and for adequate airflow. The airflow in the chassis is from front to back.

To ensure proper airflow it is necessary to rack your chassis using rail kits. Physically placing the units on top of one another or stacking without the use of the rail kits blocks the air vents on top of the chassis, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your chassis on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the chassis. No additional spacing between the chassis is required when you mount them using rail kits.

- Ensure that the air-conditioning can keep the chassis at a temperature of 41 to 95° F (5 to 35° C).
- Ensure that the cabinet or rack meets the rack requirements.
- Ensure that the site power meets the power requirements listed in the specification sheet for your appliance. If available, you can use a UPS to protect against power failures.

Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with these systems, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Safety Recommendations

The following information helps to ensure your safety and to protect the chassis. This information may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

Observe these safety guidelines:

- Keep the area clear and dust free before, during, and after installation.
- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the chassis.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person.

Maintain Safety with Electricity

⚠ Before working on a chassis, be sure the power cord is unplugged.

Follow these guidelines when working on equipment powered by electricity:

- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
    - Use caution; do not become a victim yourself.
    - Disconnect power from the system.
    - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
    - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Prevent ESD Damage

ESD occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, which can result in intermittent or complete failure of your equipment.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the antistatic strap, which should be between one and 10 megohms.

Site Environment

To avoid equipment failures and reduce the possibility of environmentally caused shutdowns, plan the site layout and equipment locations carefully. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

When installing the chassis, consider the following:

- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the appliance; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply.
- Install an uninterruptible power source for your site, if possible.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Rack Configuration Considerations

Consider the following when planning a rack configuration:

- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

3. Mounting Your Appliances

You can mount Secure Network Analytics appliances directly in a standard 19'' rack or cabinet, any other suitable cabinet, or on a flat surface. When mounting an appliance in a rack or cabinet, follow the instructions included in the rail mounting kits. When determining where to place an appliance, make sure that clearance to the front and rear panels is as follows:

- The front-panel indicators can be read easily
- Access to ports on rear panel is sufficient for unrestricted cabling
- The rear panel power inlet is within reach of a conditioned AC power source.
- Airflow around the appliance and through the vents is unrestricted.

Hardware Included with the Appliance

The following hardware is included with Secure Network Analytics appliances:

- AC power cord
- Access keys (for front face plate)
- Rail kit for rack mounting or mounting ears for smaller appliances
- For the Flow Collector 5210, a 10 GB SFP cable

Additional Required Hardware

You must provide the following additional required hardware:

- Mounting screw for a standard 19" rack
- Uninterruptible power supply (UPS) for each appliance you are installing
- To configure locally (optional), use one of the following methods:
    - Laptop with a video cable and a USB cable (for the keyboard)
    - Video monitor with a video cable and keyboard with a USB cable

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

4. Connecting Your Appliances to the Network

Use the same procedure to connect each appliance to the network. The only difference for connection is the type of appliance you have.

1. Reviewing Specifications

Use the same procedure to connect each appliance to the network. The only difference for connection is the type of appliance you have.

- **Specification Sheets:** For detailed specification information about each appliance, refer to Secure Network Analytics Specification Sheets.
- **UCS Platform:** The Cisco x2xx hardware all use the same UCS platform, UCSC-C220-M5SX., except for the Flow Collector 5210 DB, which uses UCSC-C240-M5SX. The variations in appliances are in NIC cards, processor, memory, storage and RAID.
- **Manager 2210 :** If you are deploying a Data Store, you can configure a Manager 2210 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. If you are not deploying a Data Store, you can only configure the 100Mbps/1 Gbps/10 Gbps copper interface as eth0.
- **Flow Collector 4210 :** If you are deploying a Data Store, you can configure a Flow Collector 4210 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. If you are not deploying a Data Store, you can only configure the 100Mbps/1 Gbps/10 Gbps copper interface as eth0.
- **Flow Collector 5210:** The Flow Collector 5210 consists of two connected servers (database and engine) so they function as a single appliance. Because of this, the installation slightly differs from other appliances. First, connect them together directly by a 10G SFP+ DA Cross Connect cable. Then, connect to your network.
- When you configure your system, make sure you configure the database and engine in the order specified in the System Configuration Guide.

> ⚠ Do not update the appliance BIOS, as it may cause issues with appliance functionality.

2. Connecting Your Appliance to the Network

To connect your appliance to your network:

1. Connect an Ethernet cable to the management port, at the rear of the appliance.
2. Connect at least one monitor port for Flow Sensors and UDP Directors.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- **UDP Director High Availability:** Connect the two UDP Directors by crossover cables. Connect the eth2 port of one UDP Director to the eth2 port of the second UDP Director. Similarly, connect the eth3 port of each UDP Director with a second crossover cable. The cable can be fiber or copper.
- **Ethernet Label:** Note the Ethernet label (eth2, eth3, etc.) for each port. These labels correspond to the network interfaces (eth2, eth3, etc.) that are used in the system configuration.

3. Connect the other end of the Ethernet cables to your network's switch.
4. Connect the power cords to the power supply. Some appliances have two power connections: Power Supply 1 and Power Supply 2.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. Connecting to Your Appliance

This section describes how to connect to your appliance for system configuration.

Choose your connection procedure:

- **Connecting with a Keyboard and a Monitor**
- **Connecting with a Serial Cable or Serial Console**
- **Connecting with CIMC (Required for Remote Access)** To connect to the appliance for remote access, use this procedure.

Connecting with a Keyboard and a Monitor

To configure the IP address locally, complete the following steps:

1. Plug in the power cable to the appliance.
2. Push the Power button to turn on the appliance. Wait for it to finish booting up completely. Do not interrupt the boot up process.

> You may need to remove the front panel to apply power.
>
> The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.
>
> Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

3. Connect the keyboard:
    - If you have a standard keyboard, connect it to the standard keyboard connector.
    - If you have a USB keyboard, connect it to a USB connector.
4. Connect the video cable to the video connector. The login prompt appears.
5. Go to **6. Configuring Your Secure Network Analytics System**.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Connecting with a Serial Cable or Serial Console

You can also connect to the appliance with a serial cable or serial console, such as a laptop that has a terminal emulator. We use a laptop as an example in the instructions.

1. Connect your laptop to the appliance using one of the following methods:

   - Connect an RS232 cable from the serial port connector (DB9) on your laptop to the Console Port on the appliance.
   - Connect a crossover cable from the Ethernet port on your laptop to the Management port on the appliance.

2. Plug in the power cable to the appliance.
3. Push the Power button to turn on the appliance. Wait for it to finish booting up completely. Do not interrupt the boot up process.

   > You may need to remove the front panel to apply power.
   >
   > The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on. Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

4. On the laptop, make a connection into the appliance.

   You can use any available terminal emulator to communicate with the appliance.

5. Apply the following the settings:

   - BPS: 115200
   - Data bits: 8
   - Stop bit: 1
   - Parity: None
   - Flow Control: None

   The login screen and login prompt are displayed.

6. Go to **6. Configuring Your Secure Network Analytics System**.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Connecting with CIMC (Required for Remote Access)

The Cisco Integrated Management Controller (CIMC) enables access to the server configuration and a virtual server console, as well as monitors for hardware health. You will also use the CIMC in the Secure Network Analytics system configuration.

1. Follow the instructions in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide.
2. Log in to the CIMC as admin and type **password** in the Password field.
3. Change the default password to protect the security of your network.
4. Go to **6. Configuring Your Secure Network Analytics System**.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

6. Configuring Your Secure Network Analytics System

If you've finished installing your Virtual Edition appliances and/or hardware appliances, you are ready to configure Secure Network Analytics into a managed system.

> ⚠ To configure Secure Network Analytics, follow the instructions in the Secure Network Analytics System Configuration Guide. This step is critical for the successful configuration and communication of your system.
>
> Make sure you configure your appliances in the order specified in the System Configuration Guide.

System Configuration Requirements

Make sure you have access to the appliance console through the **Cisco Integrated Management Controller (CIMC)**.

Use the following table to prepare the required information for each appliance.

Configuration Requirement	Details	Appliance
IP Address	Assign a routable IP address to the `eth0` management port.	
Netmask		
Gateway		
Host Name	A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.	
Domain Name	A fully qualified domain name is required for each appliance. We cannot install an appliance with an empty domain.	

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

DNS Servers	Internal DNS server for name resolution	
NTP Servers	Internal Time server for synchronization between servers. At least 1 NTP server is required for each appliance. Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic and it is no longer supported in our default list of NTP servers.	
Mail Relay Server	SMTP Mail server to send alerts and notifications	
Flow Collector Export Port	Required for Flow Collectors only. NetFlow Default: 2055	
Non-routable IP Address within a private LAN or VLAN (for inter-Data Node communication)	Required for Data Nodes only. • Hardware eth2 or bond of eth2 and eth3. Creating an LACP `eth2/eth3` bonded port channel for up to 20G throughput enables faster communication between and among Data Nodes, and quicker Data Node addition or replacement to the Data Store. Note that LACP port bonding is the only bonding option available for hardware Data Nodes. • Virtual eth1 **IP Address:** You can use the **provided IP address** or **enter a value** that meets the following requirements for inter-Data Node communications. • **Non-routable IP Address** from the	

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

	169.254.42.0/24 CIDR block, between 169.254.42.2 and 169.254.42.254. • **First Three Octets:** 169.254.42 • **Subnet:** /24 • **Sequential:** For ease of maintenance, select sequential IP addresses (such as 169.254.42.10, 169.254.42.11, and 169.254.42.12). **Netmask:** The Netmask is hard coded to 255.255.255.0 and cannot be modified.	
eth0 Hardware Connection Port	Required for Secure Network Analytics with Data Store hardware appliances only: • Manager • Flow Collector • Data Nodes eth0 Hardware Connection Port Options: • **SFP+**:	

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Change History

Document Version	Published Date	Description
1_0	December 15, 2023	Initial version
1_1	June 5, 2024	Removed unnecessary virtual hardware information. Removed version information.
1_2	June 7, 2024	Added General Deployment requirements.
1_3	August 13, 2024	Added requirement to install Data Nodes on the same public/management interface (eth0) Layer 3 subnet.
1_4	July 28, 2025	Added the "9222/UDP" port details to "Additional Open Ports for Data Store" table.
1_5	August 22, 2025	Updated the "Supported Hardware Metrics (with Analytics enabled)" table.
1_6	August 11, 2026	Updated the "Cisco Integrated Management Controller (CIMC)" instructions.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.