Cisco Secure Network Analytics

System Configuration Guide 7.4.2

Table of Contents

Introduction

Overview

Use this guide to configure the following Cisco Secure Network Analytics (formerly Stealthwatch) hardware and Virtual Edition appliances to one managed system in v7.4.2:

- Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console)
- Cisco Secure Network Analytics Data Node
- Cisco Secure Network Analytics Flow Collector
- Cisco Secure Network Analytics Flow Sensor
- Cisco Secure Network Analytics UDP Director

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

- **Overview:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Appliances:** https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html
- **Release Notes:** For details, refer to the Release Notes.

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for installing and configuring Secure Network Analytics products.

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

Installation Requirements

Before you configure Secure Network Analytics into a managed system using this guide, install your hardware and virtual appliances using the following guides:

Hardware

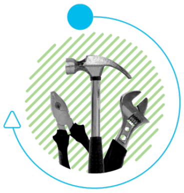
- **Hardware Installation:** Install your appliance hardware (physical appliances) using the Secure Network Analytics x2xx Series Hardware Installation Guide or the Secure Network Analytics x3xx Series Hardware Installation Guide before you start this configuration.
- **Specifications:** Hardware specifications are available on Cisco.com.
- **Supported Platforms:** To view the supported hardware platforms for each system version, refer to the Hardware and Software Version Support Matrix on Cisco.com.

Virtual Edition (VE) Appliances

- **Virtual Edition Installation:** Install your virtual appliances using the Secure Network Analytics Virtual Edition Installation Guide before you start this configuration.

Quick Reference Overview

For a successful installation, follow these procedures in order. For detailed instructions, click the procedure link.

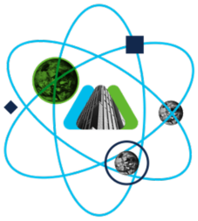


Before You Begin and Planning Your System Configuration

Make sure you have all required information to configure your appliances and deploy Secure Network Analytics with a Data Store or without a Data Store.

1. Configuring Your Environment Using First Time Setup

- **Log In:** Log in to each appliance through the console as sysadmin (password: lan1cope). At the command prompt, type `SystemConfig`.
- **Flow Collector with Data Store:** Log in as root (password: lan1cope).
- **Required Appliances:** Manager and Flow Collector are required for all deployments. For deployments with a Data Store, you also need to configure Data Nodes (with inter-Data Node communications).



2. Configuring the Managed System

Use the Appliance Setup Tool to configure each appliance in order so it is managed by your Manager. You will also create a Data Store domain or Non-Data Store domain for your appliances.

- **Appliance Setup Tool:** In your address field of your browser, type **https://** followed by the IP address of the appliance.
- **Log In:** admin
- **Password:** lan411cope
- **Sysadmin and Root Password Default:** lan1cope

Configure your appliances in order. Check the Central Management inventory and confirm each appliance status is **Connected** (or **Data Store Not Initialized**) before you start configuring the next appliance in your cluster.

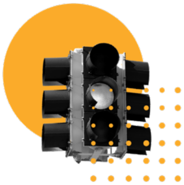
1. Primary Manager (Central Management)
2. Data Nodes
3. Flow Collector 5000 Series Database
4. Flow Collector 5000 Series Engine
5. All Other Flow Collectors
6. UDP Directors
7. Flow Sensors
8. Secondary Manager

3. Defining a Manager Failover Relationship

- This procedure is required if you've configured a primary Manager and a secondary Manager.
- Use Failover to establish a failover pair between two Managers so that one of them serves as a backup console to the other.
- Follow the instructions in the Secure Network Analytics Failover Configuration Guide.

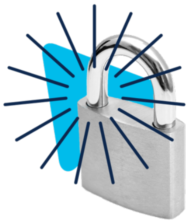
4. Configuring Site Redundancy

- This procedure is optional and requires you to have a Data Store.
- Use site redundancy to establish near-redundancy across clusters in two Cisco Secure Network Analytics sites that contain separate deployments with similar appliances.



5. Installing v7.4.2 Patches

- Download the latest **v7.4.2 patches** from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
- Follow the instructions in the patch readme file to install each patch.



6. Initializing the Data Store

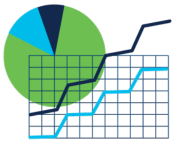
Required for Data Store deployments only.

1. Log in to your Manager appliance console (SystemConfig) as root.
2. Select **Data Store** > **SSH**.
3. Select **Data Store** > **Initialization**.

7. Installing the Desktop Client

Required for Non-Data Store deployments only.

- Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.
- Log in to your Manager. Click the ⤓ (**Download**) icon.



8. Verifying Communications

- Log in to your Manager. Review the Flow Collection Trend.
- Review the Data Store database status to confirm it is Up. (Configure > GLOBAL Central Management > Data Store tab)
- Run reports in Report Builder to confirm flows are received at the Flow Collector and Data Store. (Report > Report Builder > Flow Collection Trend by Flow Collector Report, Flow Database Ingest Trend Report)

9. Finishing Appliance Configurations

- Flow Sensor Application ID and Payload (required for all Flow Sensors)
- UDP Director High Availability
- Other optional appliance configurations

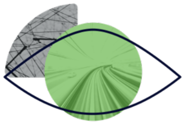
10. Configuring Telemetry

Required for Data Store deployments with additional telemetry types enabled.

- **NVM Flows:** Follow the instructions in the Endpoint License and Network Visibility Module (NVM) Configuration Guide
- **Firewall Logs:** Follow the instructions in the Security Analytics and Logging: Firewall Event Integration Guide and install the app on your Manager.

11. Licensing Secure Network Analytics

- Register your product instance in your Cisco Smart Account at https://software.cisco.com before the 90-day evaluation period expires.
- Follow the instructions in the Secure Network Analytics Smart Software Licensing Guide.



12. Managing Secure Network Analytics

Log in to your Manager and select:

- **Host Groups:** Configure > DETECTION Host Group Management.
- **Policies:** Configure > DETECTION Policy Management.
- **Flow Searches:** Investigate> Flow Search.
- **Reports:** Dashboards > Report Builder.
- **User Management:** Configure > GLOBAL User Management
- **Instructions:** Select the ? (**Help**) icon > **Help** from any page. Also, refer to Managing Your Environment, Investigating Behavior, and Responding to Threats.

Review the guide for additional configurations, maintenance, and troubleshooting, including:

- **Analytics**
- **Apps**
- **Authentication/Authorization**
- **Domains**
- **Passwords**
- **SSL/TLS Appliance Identity and Additional SSL/TLS Client Identities**
- **Threat Feed**
- **Central Management (Managing your Appliances)**
- **Data Store Database**
- **Data Store Maintenance**
- **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors**
- **Troubleshooting**

Before You Begin

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

Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics product, including virtual products such as the Flow Sensor Virtual Edition (VE).

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

Abbreviations

The following abbreviations may appear in this guide:

Abbreviations	Definition
DNS	Domain Name System (Service or Server)
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
GB	Gigabyte
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Standards Organization
IT	Information Technology
KVM	Kernel-based Virtual Machine
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
TB	Terabyte

Abbreviations	Definition
UUID	Universally Unique Identifier
VDS	vNetwork Distributed Switch
VE	Virtual Edition
VLAN	Virtual Local Area Network
VM	Virtual Machine

Configuration Details

The Secure Network Analytics system configuration includes the following:

- **Requirements:** You can configure Secure Network Analytics with a Data Store, without a Data Store, or as a hybrid deployment (both Data store and Non-Data Store domains). Refer to **Planning Your System Configuration** to review the appliance configuration and domain requirements.
- **Configuration Order:** Make sure you configure the appliances following the instructions in this guide and using the specified order for the Appliance Setup Tool.
- **Certificates:** Appliances are installed with a unique, self-signed appliance identity certificate.
- **Central Management:** You can manage your appliances from the primary Manager/Central Manager.

Downloading Software

Use Cisco Software Central to download virtual appliance (VE) installation files, patches, and software update files. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.

Password Requirements

During the system configuration, you will replace the default passwords and create new passwords for the following:

User	Default Password
admin	lan411cope

root	lan1cope
sysadmin	lan1cope
dbadmin	You will assign the password when you initialize the Data Store.
readonlyuser	You will assign the password when you initialize the Data Store.
CIMC admin	For remote access to your hardware appliances, log in to the CIMC. If you haven't already configured the CIMC, follow the instructions in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide. The default password is **password**. Make sure you change it when you first log in.

Licensing

For licensing Secure Network Analytics, you will use your Smart Account to register your product instance, manage licenses, run reports, and configure notifications. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.

When you use Secure Network Analytics in Evaluation mode, you can use selected features for 90 days. To use Secure Network Analytics with maximum default functionality, and to add licenses and features to your account, register your product instance for Smart Software Licensing. Refer to **11. Licensing Secure Network Analytics** for more information.

⚠ Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, flow collection will stop. To start flow collection again, register your product instance.

TLS

Secure Network Analytics requires v1.2.

Third Party Applications

Secure Network Analytics does not support installing third party applications on appliances.

Browsers

Secure Network Analytics supports the latest version of Chrome, Firefox, and Edge.

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.

NTP Server

- **Configuration:** At least 1 NTP server is required for each appliance.
- **Problematic NTP:** 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.

Time Zone

All Secure Network Analytics appliances use Coordinated Universal Time (UTC).

- **Virtual Host Server:** Make sure your virtual host server is set to the correct time.

> ⚠ Make sure the time setting on the virtual host server (where you will be installing the virtual appliances) is set to the correct time. Otherwise, the appliances may not be able to boot up.

Planning Your System Configuration

Before you start the configuration, review the instructions so you understand the planning, time, and requirements for configuring your appliances in First Time Setup and configuring them into one managed system in the Appliance Setup Tool.

System Configuration Requirements

Consult with your network architect and administrator to confirm the details of your v7.4.2 Secure Network Analytics deployment. Refer to each section for configuration requirements:

- **Secure Network Analytics with Data Store**
- **Secure Network Analytics without Data Store**
- **Secure Network Analytics Hybrid Deployment**
- **Planning Your System Configuration**

Secure Network Analytics with Data Store

In Secure Network Analytics with a Data Store, the Flow Collector sends its telemetry to the Data Store Data Nodes for storage.

- **Number of Data Nodes:** The Data Store can include 1 Data Node (Single Data Node deployment) or 3 or more Data Nodes (Multi-Data Node deployment). A Data Store with only 2 Data Nodes is not supported.
- **Hardware or Virtual:** Make sure your Data Nodes are the same type: all hardware or all Virtual Edition.
- **Size:** Make sure your Data Nodes Virtual Edition use the same profile size so they have the same RAM, CPU, and disk space. Refer to the Virtual Appliance Installation Guide for details.
- **Telemetry Ingest:** In addition to NetFlow, you can configure telemetry ingest for NVM flows (Network Visibility Module) and firewall logs.

For a successful configuration, note the following:

1. In First Time Setup, configure your appliances for a Data Store configuration. Make sure you configure the following appliances:

    - **Manager:** Refer to **Configuring a Manager**
    - **Flow Collector:** Refer to **Configuring a Flow Collector with Data Store**

- **Data Nodes:** Refer to **Configuring a Data Node**

2. In the Manager Appliance Setup Tool, make sure you create a Data Store domain for your Secure Network Analytics appliances.
3. To enable telemetry ingest for NVM flows and firewall logs, make sure you complete the additional configuration instructions in **10. Configuring Telemetry**.

Secure Network Analytics without Data Store

In Secure Network Analytics without a Data Store, the Flow Collector stores its telemetry locally on the Flow Collector or on the Flow Collector database (5000 Series only).

For a successful configuration, note the following:

1. In First Time Setup, make sure you configure the following appliances:

   - **Manager:** Refer to **Configuring a Manager**
   - **Flow Collector:** Refer to **Configuring a Flow Collector without Data Store**

2. In the Manager Appliance Setup Tool, make sure you create a Non-Data Store domain for your Secure Network Analytics appliances.

After you finish configuring your managed system, you can add a Data Store to your deployment in the future (for instructions, refer to **Adding Data Store to a Non-Data Store Deployment**).

You can also transition your existing Flow Collectors to use the Data Store database without losing pre-transition data or visibility. Doing so allows you to take advantage of features only available in Data Store. For more information, refer to **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors**

Secure Network Analytics Hybrid Deployment

In Secure Network Analytics with a hybrid configuration, you can configure specific Flow Collectors to send telemetry to the Data Store Data Nodes for storage, and you can configure other Flow Collectors to store telemetry locally on the Flow Collector or the Flow Collector database (5000 Series only).

For a successful configuration, configure your appliances and domains in the following order:

1. In First Time Setup, configure your appliances without Data Store. Make sure you configure the following appliances:

- **Manager:** Refer to **Configuring a Manager**
- **Flow Collector:** Refer to **Configuring a Flow Collector without Data Store**

2. In the Manager Appliance Setup Tool, make sure you create a Non-Data Store domain for your Secure Network Analytics appliances.
3. Complete all procedures through **9. Finishing Appliance Configurations** to finish your initial system configuration with a Non-Data Store domain.
4. Follow the instructions in **Adding Data Store to a Non-Data Store Deployment**. You will create a Data Store domain and add Flow Collectors and Data Nodes to it.

Appliance Configuration Requirements

You need the following information to configure each appliance in First Time Setup. You will also use this information to configure your appliances into a managed system with the Appliance Setup Tool.

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.	
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	Required for Flow Collectors only.	

Export Port	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 **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 2210 • Flow Collector 4210 • Data Nodes eth0 Hardware Connection Port Options: • **SFP+**: SFP+: 10G SFP+/DAC fiber port for eth0. • **BASE-T**: 100Mbs/1GbE/10GbE BASE-T copper port for eth0. BASE-T is the default.	

Connecting to Your Hardware (Physical) Appliances

Connect to your appliance with Cisco Integrated Management Controller (CIMC), a keyboard and monitor, or serial cable or serial console. For instructions, refer to the x2xx Series Hardware Installation Guide or the Secure Network Analytics x3xx Series Hardware Installation Guide.

CIMC Access

For remote access, log in to the CIMC. If you haven't already configured the CIMC, follow the instructions in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide.

The default password is **password**. Make sure you change it when you first log in.

Connecting to Your Virtual Edition Appliances

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

   If the virtual machine does not power on, and you receive an error message about insufficient available memory, do one of the following:

- **Resources:** Increase the available resources on the system where the appliance is installed. Refer to **Resource Requirements** in the Virtual Edition Appliance Installation Guide for details.
- **VMware Environment:** Increase the memory reservation limit for the appliance and its resource pool.

> Review Resource Requirements to allocate sufficient resources. This step is critical for system performance.
>
> ⚠ If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

4. Access the virtual machine console. Allow the virtual appliance to finish booting up.

> ℹ Depending on the speed of your VM host, it may take approximately 30 minutes for all services to boot up.

1. Configuring Your Environment Using First Time Setup

Use the following instructions to configure the basic environment for each appliance. Whether hardware (physical) appliances or Virtual Edition (VE) appliances, you can configure your appliances in any order in First Time Setup.

Review **Planning Your System Configuration** before you start these configuration procedures.

Appliance Configuration Overview

Appliance Instructions	Required for Data Store	Notes
Configuring a Manager	yes	A Manager is required for deployments with Data Store and without Data Store.
Configuring a Data Node	yes	You can deploy 1 Data Node (Single Data Node deployment) or 3 or more Data Nodes (Multi-Data Node deployment). Deploying only 2 Data Nodes is not supported. Make sure your Data Nodes are all hardware or all Virtual Edition. Also, make sure your Data Nodes Virtual Edition use the same profile size so they have the same RAM, CPU, and disk space. Refer to the Virtual Appliance Installation Guide for details.
Configuring a Flow Collector with Data Store	yes	The Flow Collector sends its telemetry to the Data Store Data Nodes for storage. You will also confirm telemetry types to ingest.

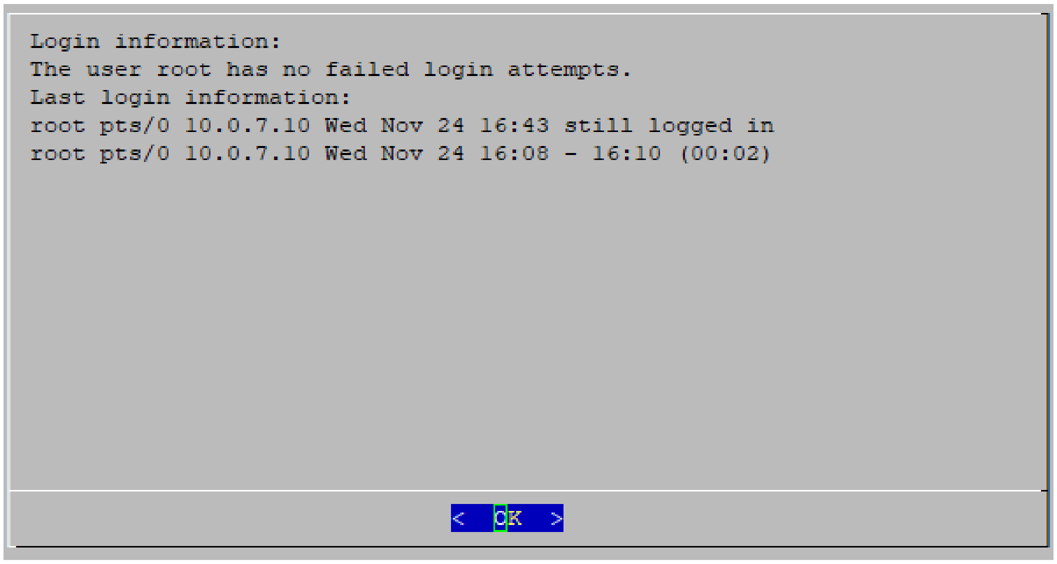
Configuring a Flow Collector without Data Store		The Flow Collector stores its telemetry locally on the Flow Collector or on the Flow Collector database (5000 Series only).
Configuring a Flow Sensor or UDP Director		Flow Sensors and UDP Directors are optional. To install Cisco Telemetry Broker instead of the UDP Director, finish the instructions in this guide to finish your system configuration. Then, follow the instructions in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.

Configuring a Manager

1. Log in to the Manager through the console.

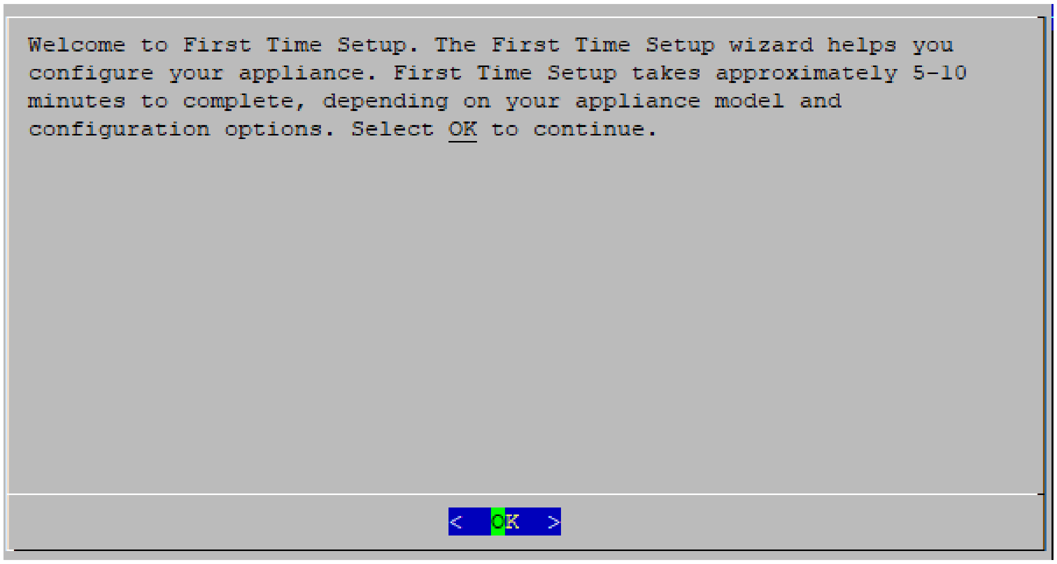
    - **Login:** sysadmin
    - **Default Password:** lan1cope
    - You will change the default password when you configure the system.

2. System Configuration (`SystemConfig`) opens.
3. Review the failed login attempts information. Select **OK** to continue.



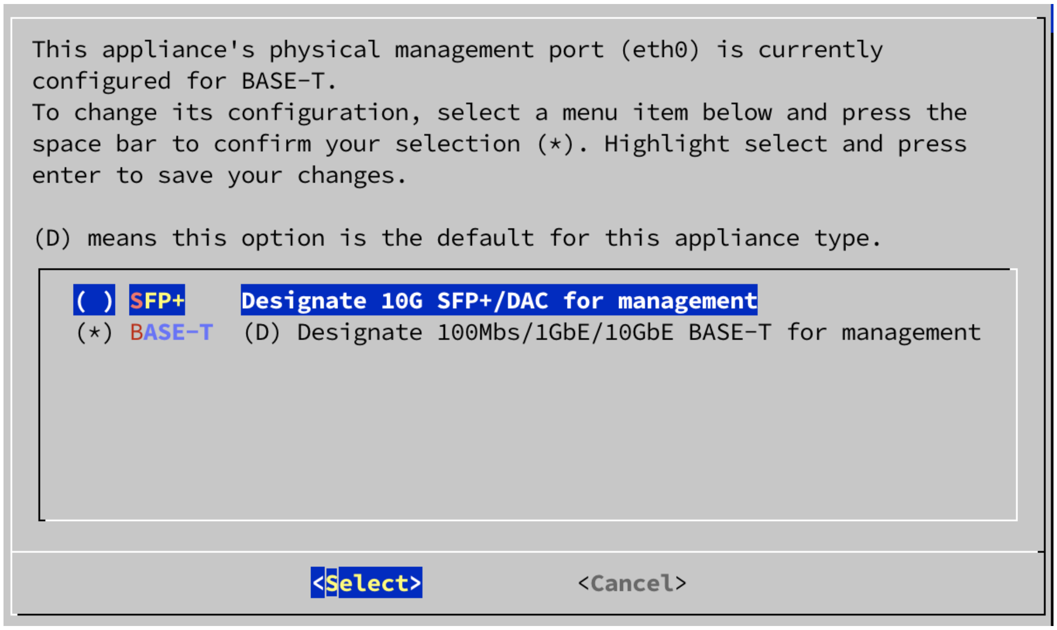
```
Login information:
The user root has no failed login attempts.
Last login information:
root pts/0 10.0.7.10 Wed Nov 24 16:43 still logged in
root pts/0 10.0.7.10 Wed Nov 24 16:08 - 16:10 (00:02)
```

4. Review the First Time Setup introduction. Select **OK** to continue.



```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

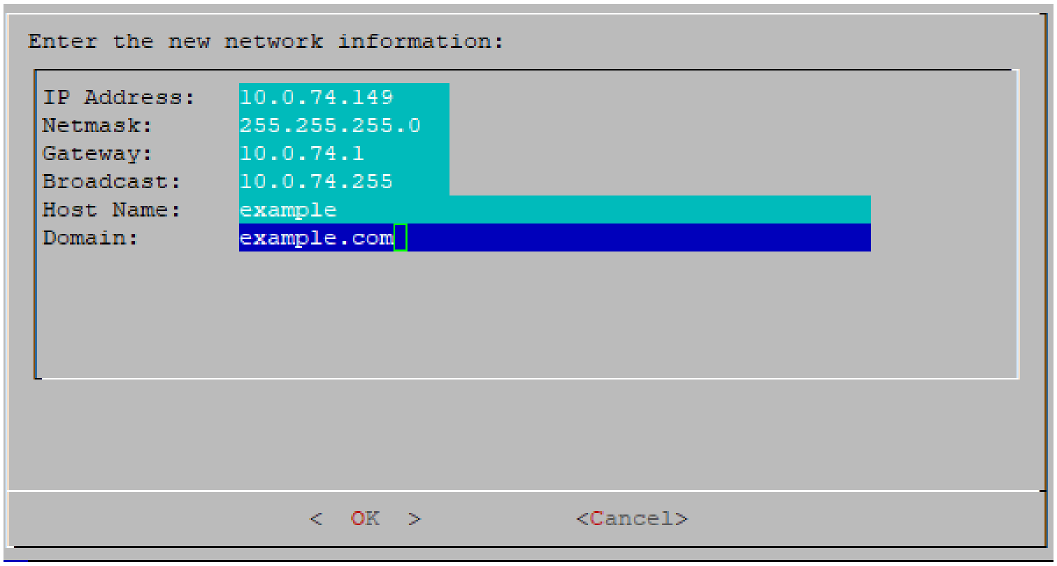
5. **Port Order Configuration for eth0 (Manager 2210 Hardware Only):** Choose one of the following:
   - **SFP+**: Configure your appliance to use a 10G SFP+/DAC fiber port for eth0.
   - **BASE-T**: Configure your appliance to use a 100Mbs/1GbE/10GbE BASE-T copper port for eth0. BASE-T is the default.



```
This appliance's physical management port (eth0) is currently
configured for BASE-T.
To change its configuration, select a menu item below and press the
space bar to confirm your selection (*). Highlight select and press
enter to save your changes.

(D) means this option is the default for this appliance type.

  ( ) SFP+     Designate 10G SFP+/DAC for management
  (*) BASE-T   (D) Designate 100Mbs/1GbE/10GbE BASE-T for management
```

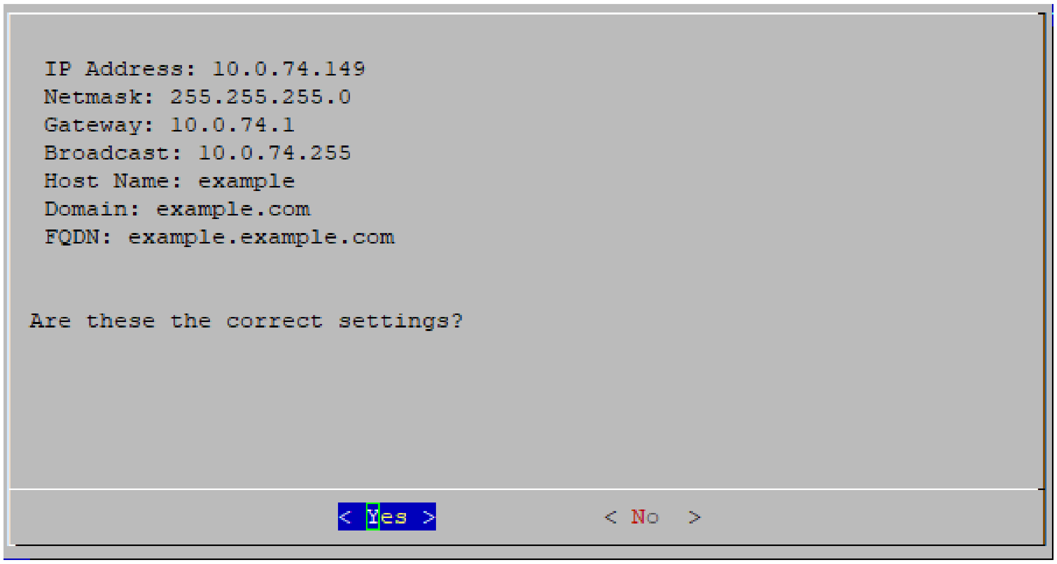
6. Enter the management interface **IP Address** (eth0), **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.

⚠ 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.



```
Enter the new network information:

IP Address:    10.0.74.149
Netmask:       255.255.255.0
Gateway:       10.0.74.1
Broadcast:     10.0.74.255
Host Name:     example
Domain:        example.com
```

7. Confirm your settings. Select **Yes** to continue.



```
 IP Address: 10.0.74.149
 Netmask: 255.255.255.0
 Gateway: 10.0.74.1
 Broadcast: 10.0.74.255
 Host Name: example
 Domain: example.com
 FQDN: example.example.com


Are these the correct settings?
```

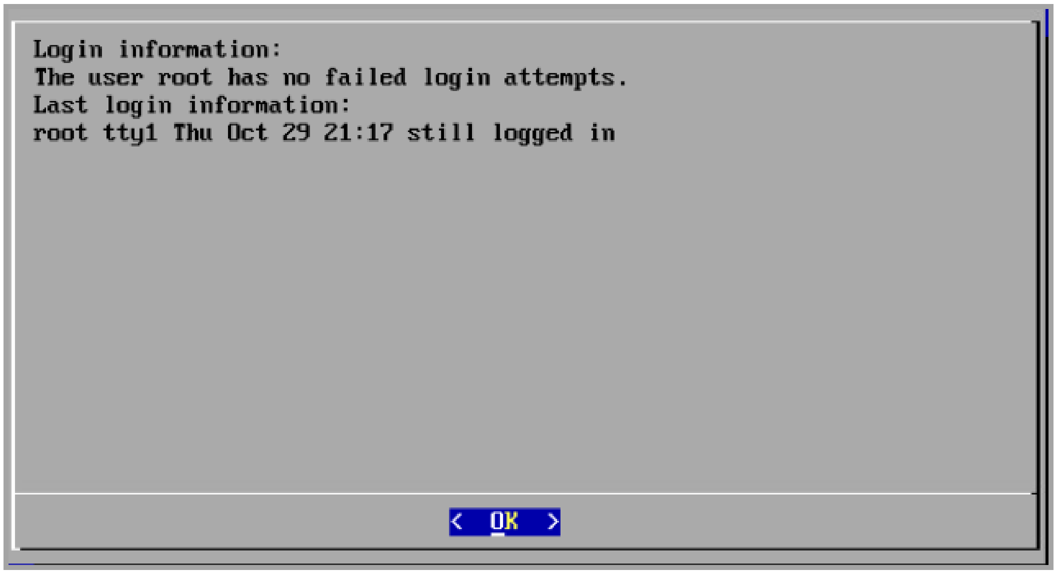
8. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.
9. Press **Ctrl + Alt** to exit the console.
10. Repeat all the steps in **Configuring a Manager** for the next Manager in your system.

    If you've configured all Managers in First Time Setup, return to **Appliance Configuration Overview** and configure your Flow Collectors and other appliances.

Configuring a Data Node

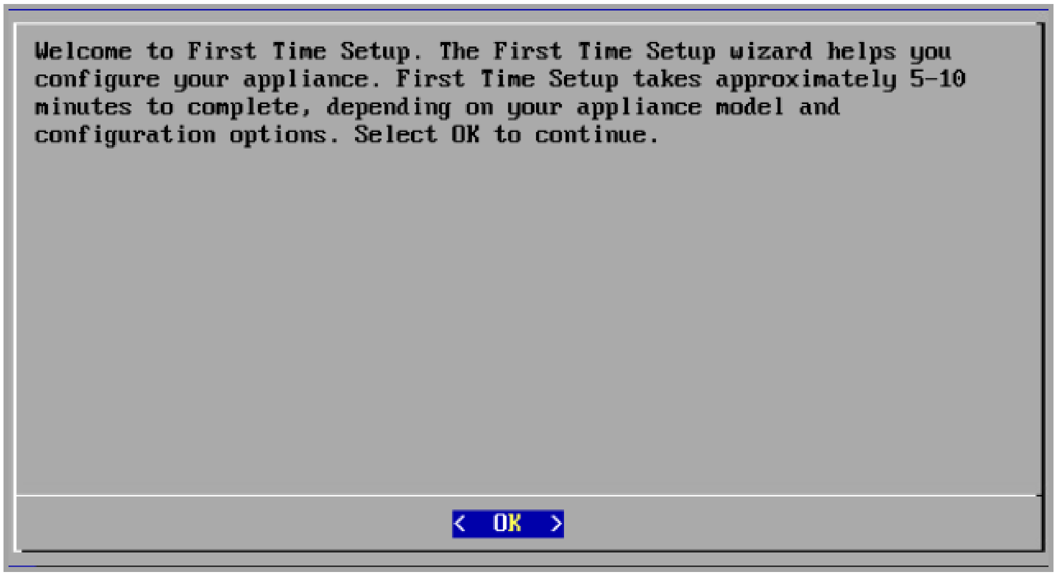
You can deploy 1 Data Node (Single Data Node deployment) or 3 or more Data Nodes (Multi-Data Node deployment). Deploying only 2 Data Nodes is not supported.

1. Log in to a Data Node through the console.
   - **Login:** sysadmin
   - **Default Password:** lan1cope
   - You will change the default password when you configure the system.
2. System Configuration (`SystemConfig`) opens.
3. Review the failed login attempts information. Select **OK** to continue.



```
Login information:
The user root has no failed login attempts.
Last login information:
root tty1 Thu Oct 29 21:17 still logged in
```

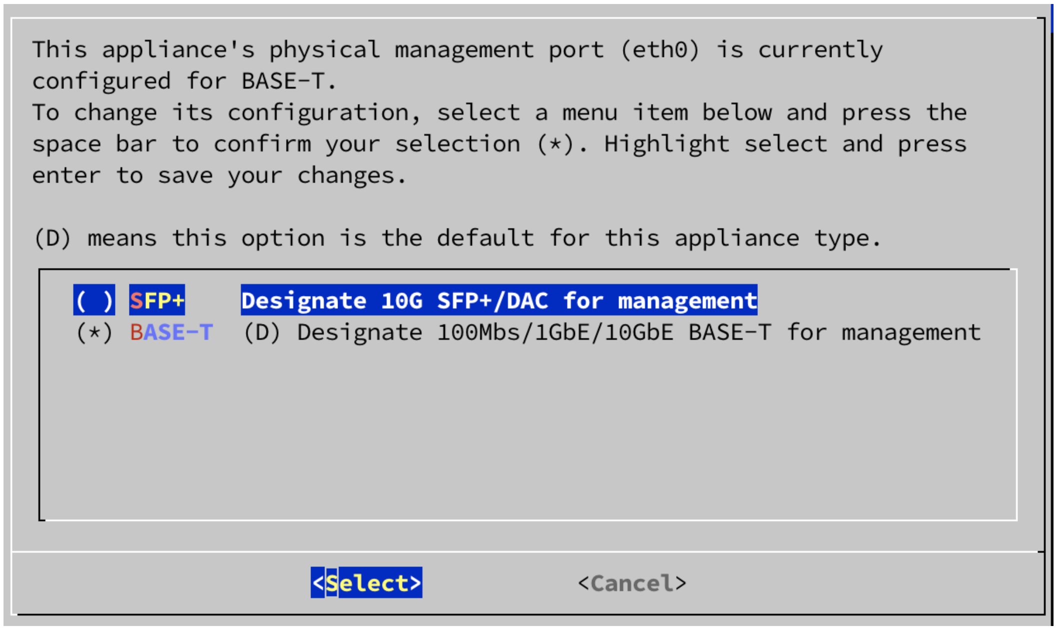
4. Review the First Time Setup introduction. Select **OK** to continue.



```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

5. **Port Order Configuration for eth0 (Data Store 6200 Hardware Only):** Choose one of the following:

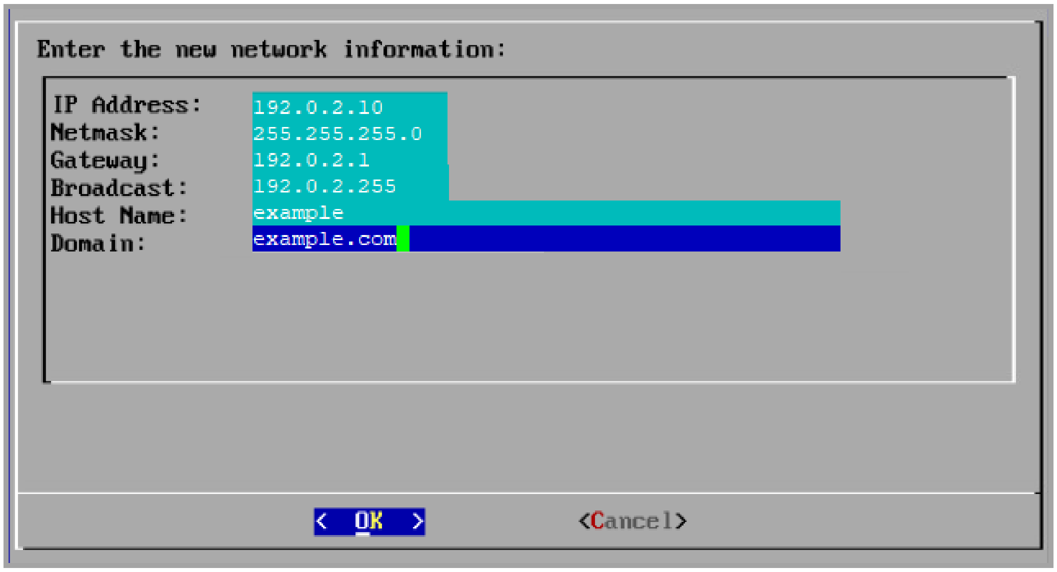
    - **SFP+**: Configure your appliance to use a 10G SFP+/DAC fiber port for eth0.
    - **BASE-T**: Configure your appliance to use a 100Mbs/1GbE/10GbE BASE-T copper port for eth0. BASE-T is the default.



```
This appliance's physical management port (eth0) is currently
configured for BASE-T.
To change its configuration, select a menu item below and press the
space bar to confirm your selection (*). Highlight select and press
enter to save your changes.

(D) means this option is the default for this appliance type.

  ( ) SFP+     Designate 10G SFP+/DAC for management
  (*) BASE-T   (D) Designate 100Mbs/1GbE/10GbE BASE-T for management
```

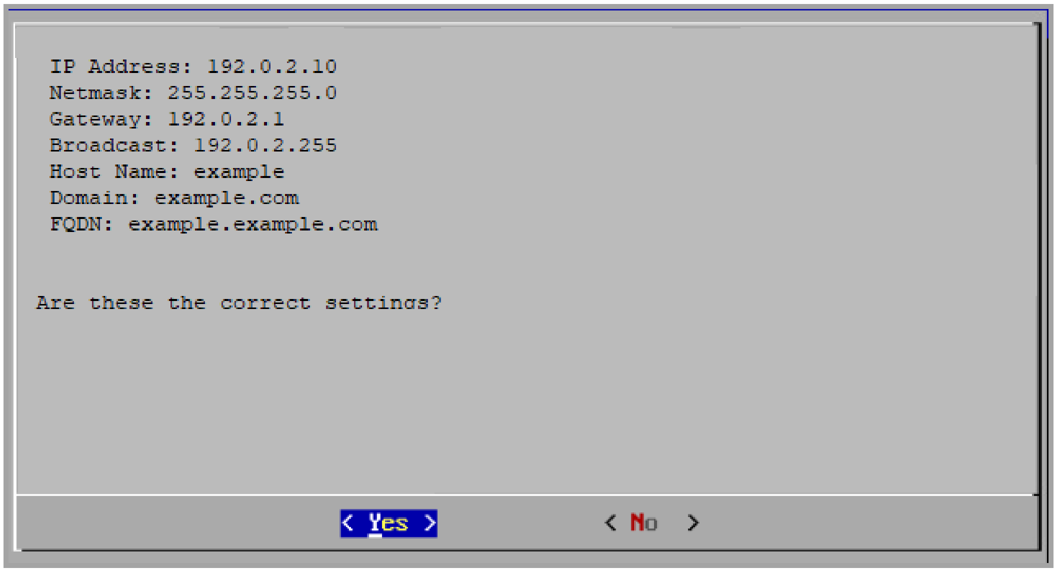
6. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.

> ⚠ 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.



```
Enter the new network information:

IP Address:     192.0.2.10
Netmask:        255.255.255.0
Gateway:        192.0.2.1
Broadcast:      192.0.2.255
Host Name:      example
Domain:         example.com
```

7. Confirm your settings. Select **Yes** to continue.



```
 IP Address: 192.0.2.10
 Netmask: 255.255.255.0
 Gateway: 192.0.2.1
 Broadcast: 192.0.2.255
 Host Name: example
 Domain: example.com
 FQDN: example.example.com


Are these the correct settings?
```

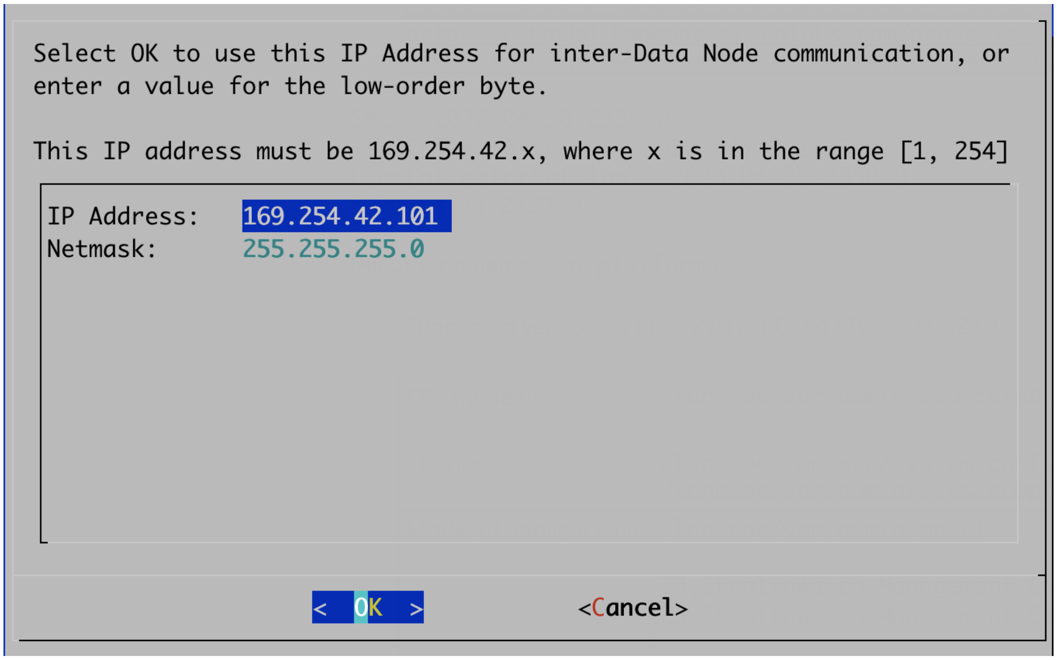
8. Select **OK** to confirm your selection. Follow the on-screen prompts.

9. **Configure the physical port (eth2) or port channel (eth2 and eth3) for inter-Data Node communications.**

> ⓘ 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.

Enter the following:

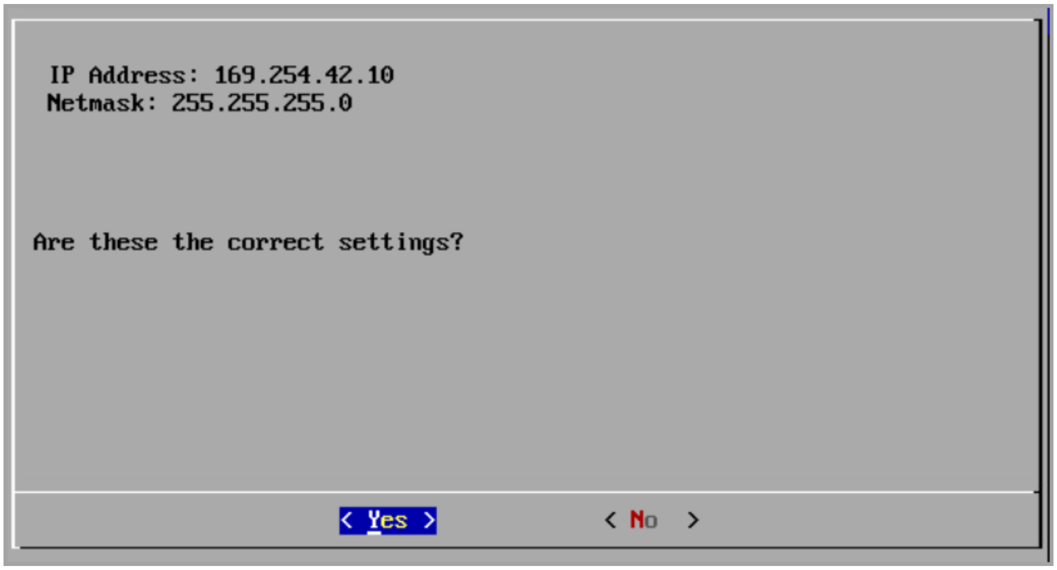
Field	Requirements
IP Address	Use the **provided IP address** or **enter a value** that meets the following requirements for the eth2 and eth3 interface for inter-Data Node communications. • **Non-routable IP Address** from the **169.254.42.0/24 CIDR block**, between 169.254.42.2 and 169.254.42.254. • **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	255.255.255.0



```
Select OK to use this IP Address for inter-Data Node communication, or
enter a value for the low-order byte.

This IP address must be 169.254.42.x, where x is in the range [1, 254]

IP Address:    169.254.42.101
Netmask:       255.255.255.0
```

10. Select **OK** to continue.

11. Confirm your settings. Select **Yes** to continue.



```
  IP Address: 169.254.42.10
  Netmask: 255.255.255.0



Are these the correct settings?
```

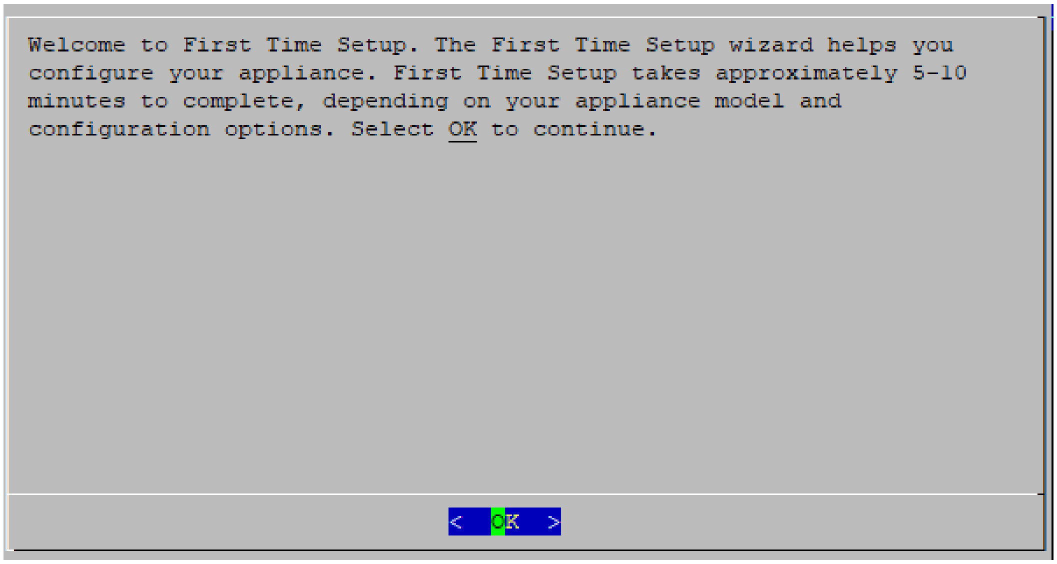
12. Follow the on-screen prompts to finish the environment and restart the appliance.
13. Press **Ctrl + Alt** to exit the console.
14. Repeat all the steps in **Configuring a Data Node** for the next Data Node in your system.
    - If you've configured all Data Nodes in First Time Setup, go to the next section and configure your Flow Collectors with Data Store or return to **Appliance Configuration Overview** and configure your other appliances.
    - If you've configured all appliances in First Time Setup, go to **2. Configuring the Managed System**.

Configuring a Flow Collector with Data Store

If you configure your Flow Collector for use with the Data Store, the Flow Collector sends its telemetry to the Data Store Data Nodes for storage. You will also confirm telemetry types to ingest.

> Starting in v7.4.2, you can transition Non-Data Store Flow Collectors to Data Store Flow Collectors. Refer to **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors** for more information.

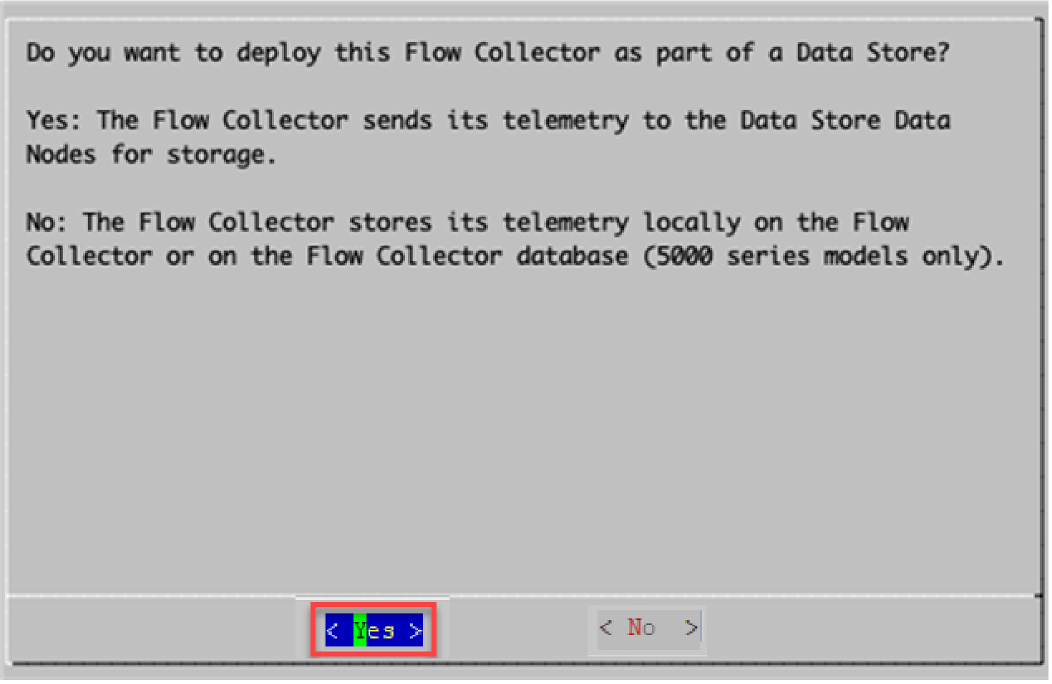
1. Log in to the Flow Collector through the console.
   - **Login:** root
   - **Default Password:** lan1cope
   - You will change the default password when you configure the system.
2. At the command prompt, type `SystemConfig`. Press Enter.
3. Review the failed login attempts information. Select **OK** to continue.
4. Review the First Time Setup Introduction. Select OK to continue.



```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

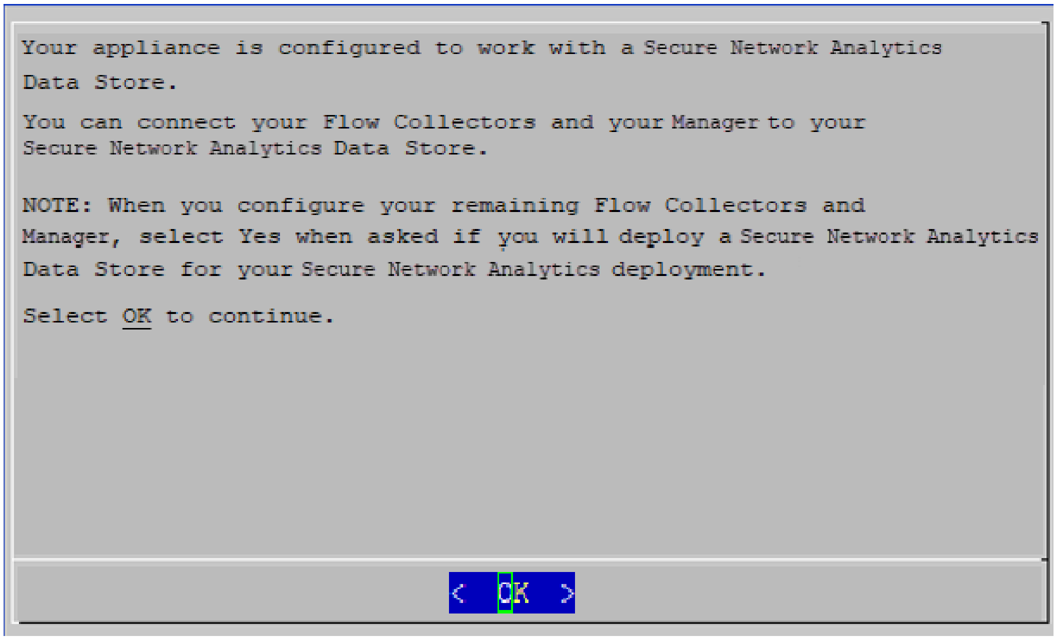
5. Do you want to deploy this Flow Collector as part of a Data Store? Select **Yes**.

> ⚠ After you choose to configure your Flow Collector for use with Data Store, you cannot change this configuration. Select Yes only if you plan to deploy a Data Store to your network.
>
> If you need to deploy Secure Network Analytics without a Data Store, do not follow the instructions in this section. Follow the instructions in **Configuring a Flow Collector without Data Store**.
>
> If you select the wrong choice, deploy a new virtual appliance or RFD your appliance.



```
Do you want to deploy this Flow Collector as part of a Data Store?

Yes: The Flow Collector sends its telemetry to the Data Store Data
Nodes for storage.

No: The Flow Collector stores its telemetry locally on the Flow
Collector or on the Flow Collector database (5000 series models only).
```

6. Select **OK** to continue.



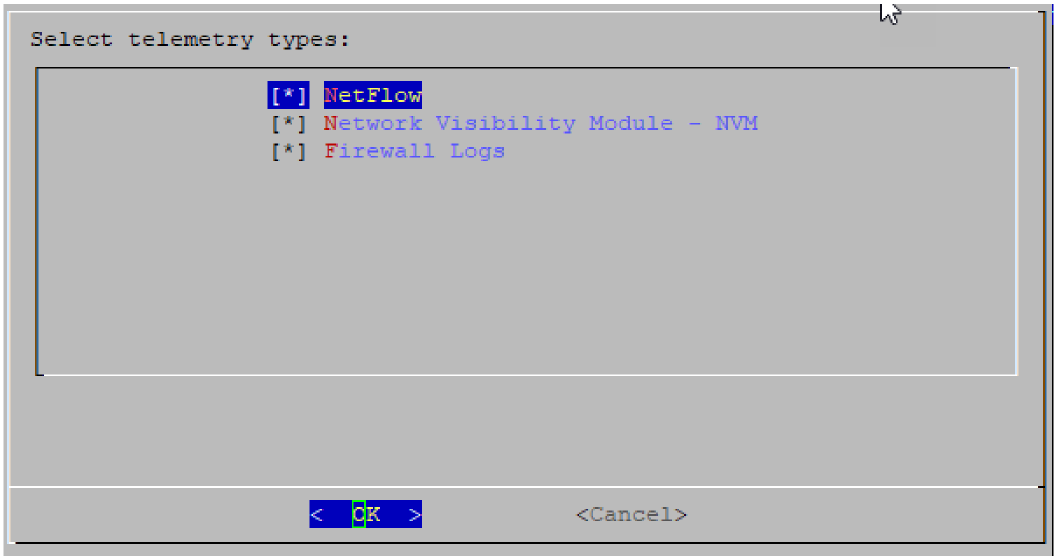
```
Your appliance is configured to work with a Secure Network Analytics
Data Store.
You can connect your Flow Collectors and your Manager to your
Secure Network Analytics Data Store.

NOTE: When you configure your remaining Flow Collectors and
Manager, select Yes when asked if you will deploy a Secure Network Analytics
Data Store for your Secure Network Analytics deployment.

Select OK to continue.
```

7. Select which telemetry types to ingest.
   - **Default:** All telemetry types are selected by default. The asterisk (*) indicates the selected telemetries.
   - **Deselecting:** To deselect a telemetry, select the telemetry type and click it (or press the space key on your keyboard).

More Information:

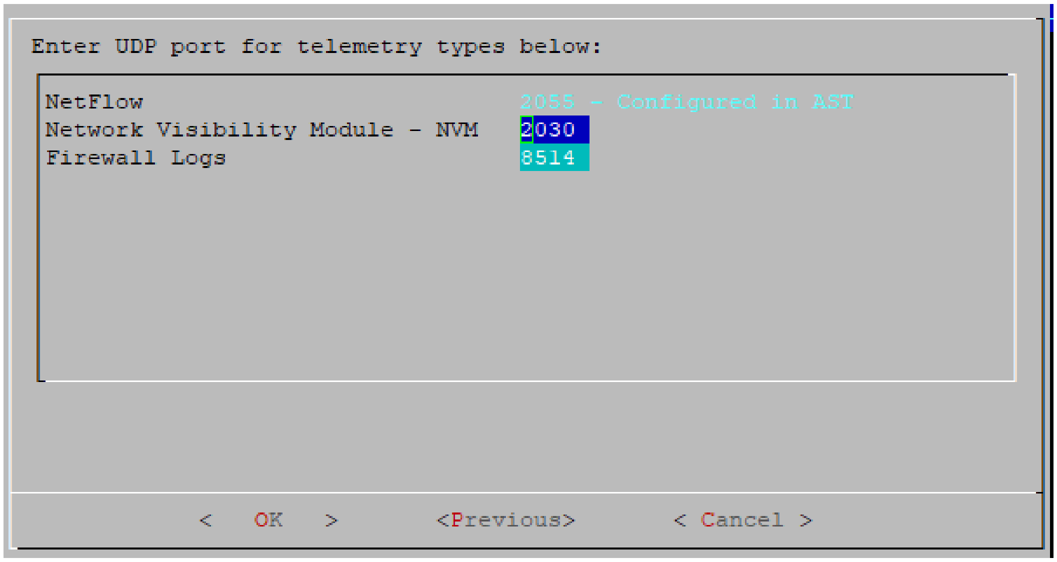
- **Network Visibility Module - NVM:** If you select Network Visibility Module - NVM, the Flow Collector will ingest and store NVM flows. Refer to the Cisco Secure Network Analytics Endpoint License and Network Visibility Module (NVM) Configuration Guide for more information.
- **Firewall Logs:** If you select Firewall Logs, the Flow Collector will ingest and store firewall event logs for Cisco Security Analytics and Logging (On Premises). Refer to the Security Analytics and Logging: Firewall Event Integration Guide for more information.

> If you configure the Flow Collector to have NetFlow disabled, updating configuration options, such as altering Exporters, Host Groups, Security Events, Host Reports, etc., will have no effect.



```
Select telemetry types:

                    [*] NetFlow
                    [*] Network Visibility Module - NVM
                    [*] Firewall Logs
```

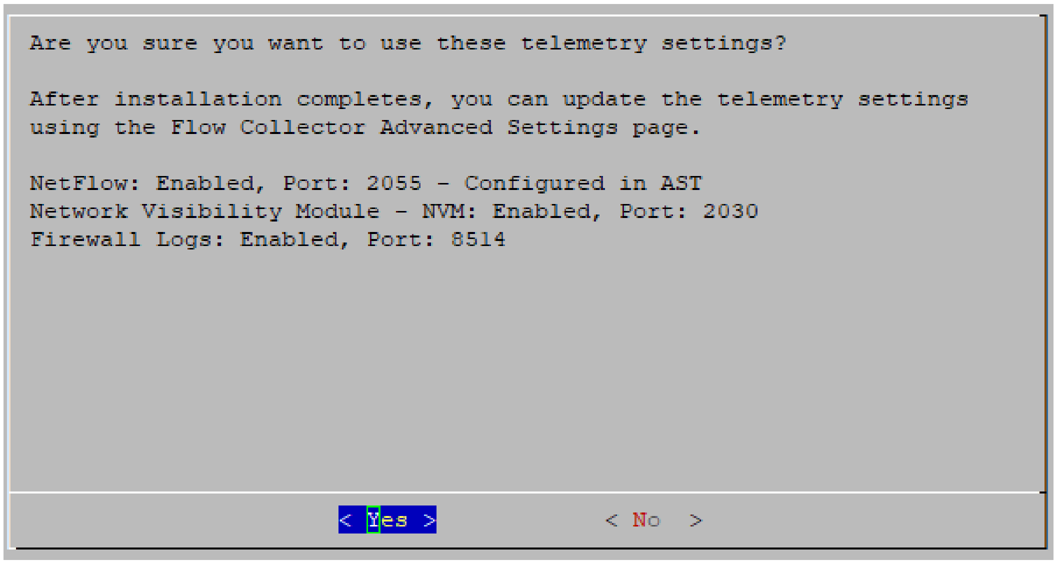
8. Enter the UDP port for the selected telemetry types. Select **OK**.



```
Enter UDP port for telemetry types below:

NetFlow                            2055 - Configured in AST
Network Visibility Module - NVM    2030
Firewall Logs                      8514
```

Make sure your telemetry ports are unique. If you configure duplicate telemetry ports, the ports will be reset to their internal defaults to avoid loss of flow data. For example, if NetFlow and NVM are exported to the same telemetry port, each device exporting NVM data will create an exporter on the Flow Collector and exhaust the exporter resources in the Flow Collector engine, resulting in loss of flow data.

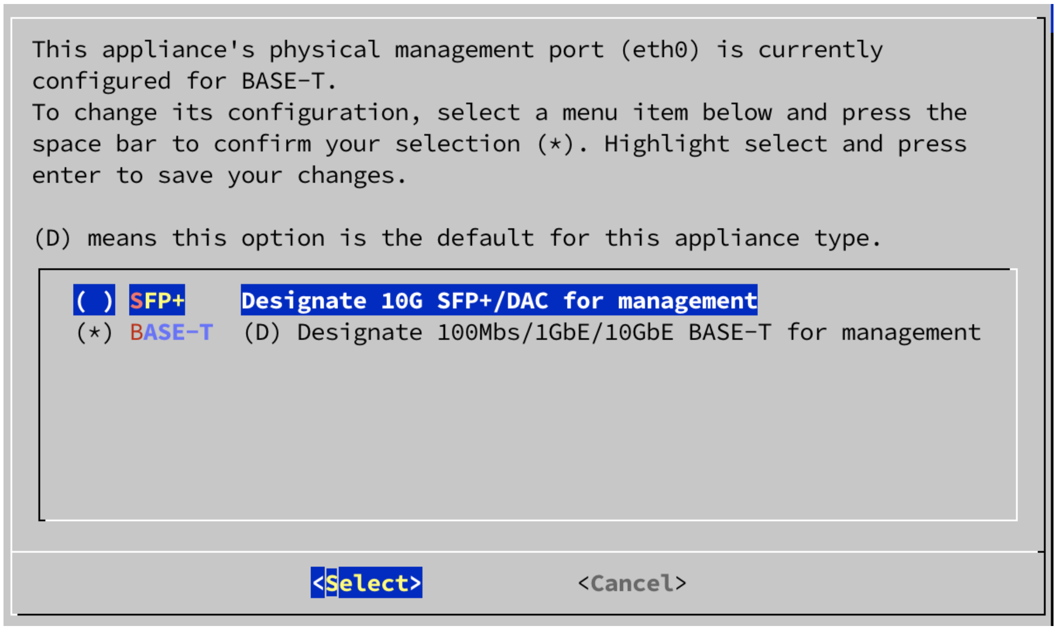
9. Confirm your settings. Select **Yes** to continue.



```
Are you sure you want to use these telemetry settings?

After installation completes, you can update the telemetry settings
using the Flow Collector Advanced Settings page.

NetFlow: Enabled, Port: 2055 - Configured in AST
Network Visibility Module - NVM: Enabled, Port: 2030
Firewall Logs: Enabled, Port: 8514
```

10. **Port Order Configuration for eth0 (Flow Collector 4210 Hardware Only):** Choose one of the following:

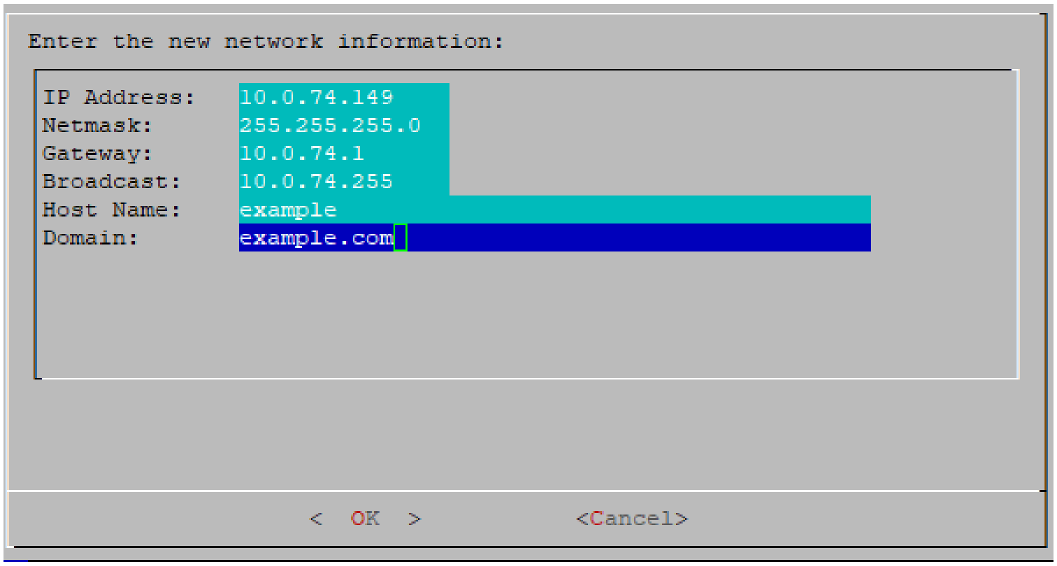
    - **SFP+**: Configure your appliance to use a 10G SFP+/DAC fiber port for eth0.
    - **BASE-T**: Configure your appliance to use a 100Mbs/1GbE/10GbE BASE-T copper port for eth0. BASE-T is the default.



```
This appliance's physical management port (eth0) is currently
configured for BASE-T.
To change its configuration, select a menu item below and press the
space bar to confirm your selection (*). Highlight select and press
enter to save your changes.

(D) means this option is the default for this appliance type.

  ( ) SFP+    Designate 10G SFP+/DAC for management
  (*) BASE-T  (D) Designate 100Mbs/1GbE/10GbE BASE-T for management
```

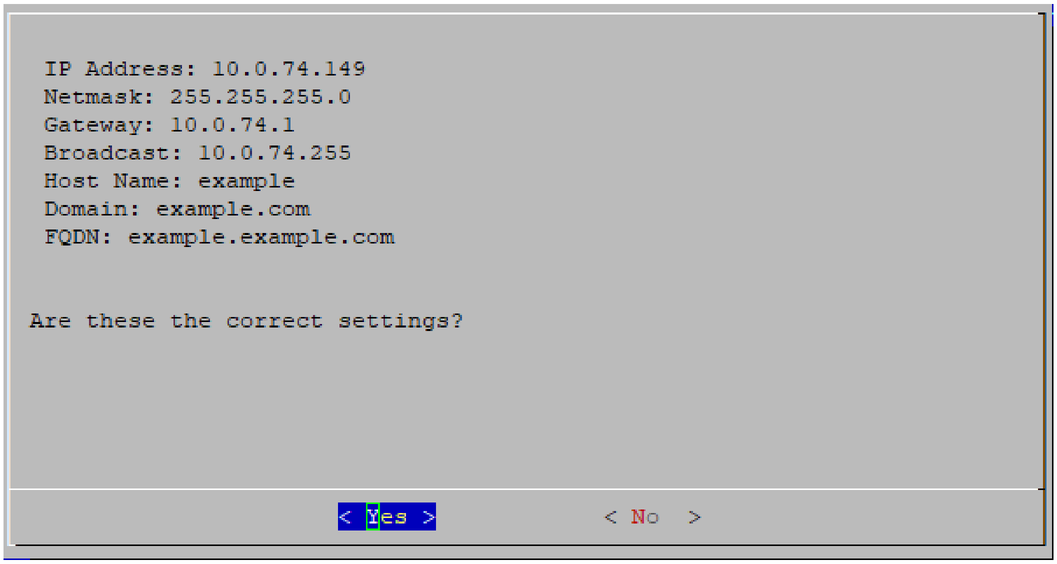
11. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.

> ⚠ 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.



```
Enter the new network information:

 IP Address:    10.0.74.149
 Netmask:       255.255.255.0
 Gateway:       10.0.74.1
 Broadcast:     10.0.74.255
 Host Name:     example
 Domain:        example.com
```

12. Confirm your settings. Select **Yes** to continue.



```
  IP Address: 10.0.74.149
  Netmask: 255.255.255.0
  Gateway: 10.0.74.1
  Broadcast: 10.0.74.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

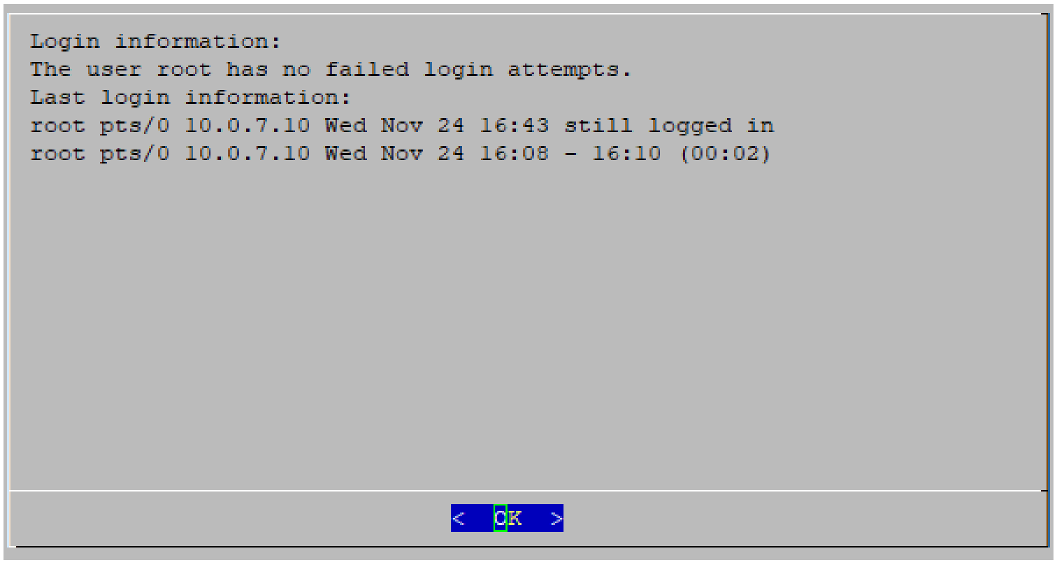
13. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.
14. Press **Ctrl + Alt** to exit the console.
15. Repeat all the steps in **Configuring a Flow Collector with Data Store** for the next Flow Collector in your system.

    If you've configured all Flow Collectors for Data Store in First Time Setup, return to **Appliance Configuration Overview** to configure your other appliances.

Configuring a Flow Collector without Data Store

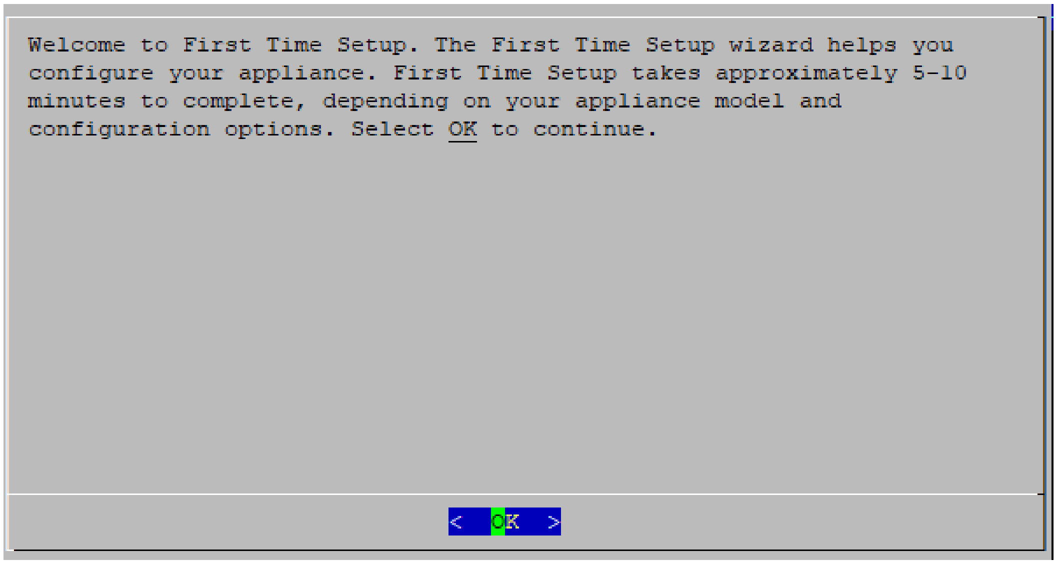
If you configure your Flow Collector for use without a Data Store, the Flow Collector stores its telemetry locally on the Flow Collector or on the Flow Collector database (5000 Series only).

1. Log in to the Flow Collector through the console.
    - **Login:** sysadmin
    - **Default Password:** lan1cope
    - You will change the default password when you configure the system.
2. System Configuration (`SystemConfig`) opens.
3. Review the failed login attempts information. Select **OK** to continue.



```
Login information:
The user root has no failed login attempts.
Last login information:
root pts/0 10.0.7.10 Wed Nov 24 16:43 still logged in
root pts/0 10.0.7.10 Wed Nov 24 16:08 - 16:10 (00:02)
```

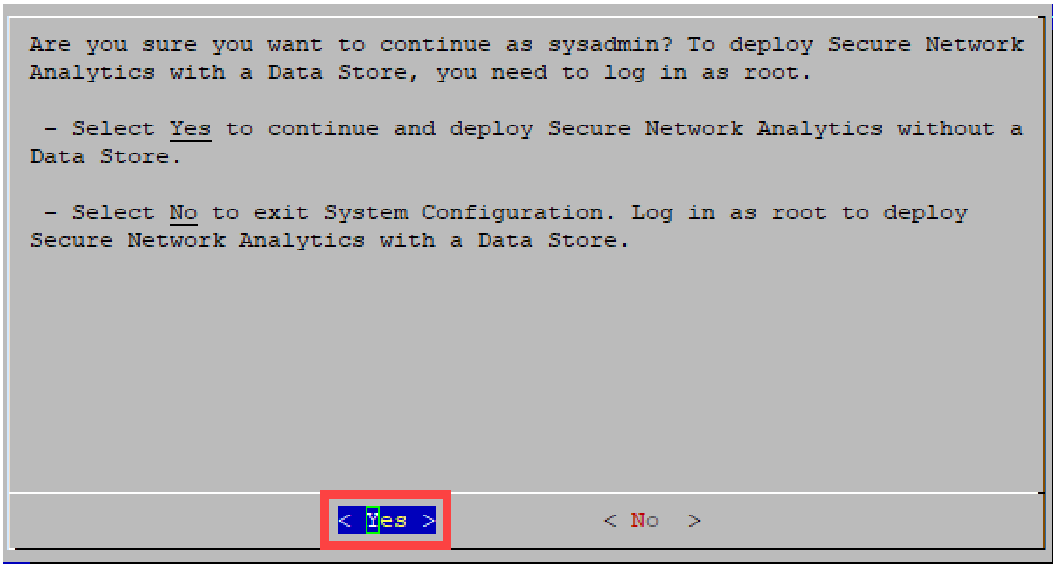
4. Review the First Time Setup introduction. Select **OK** to continue.



```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

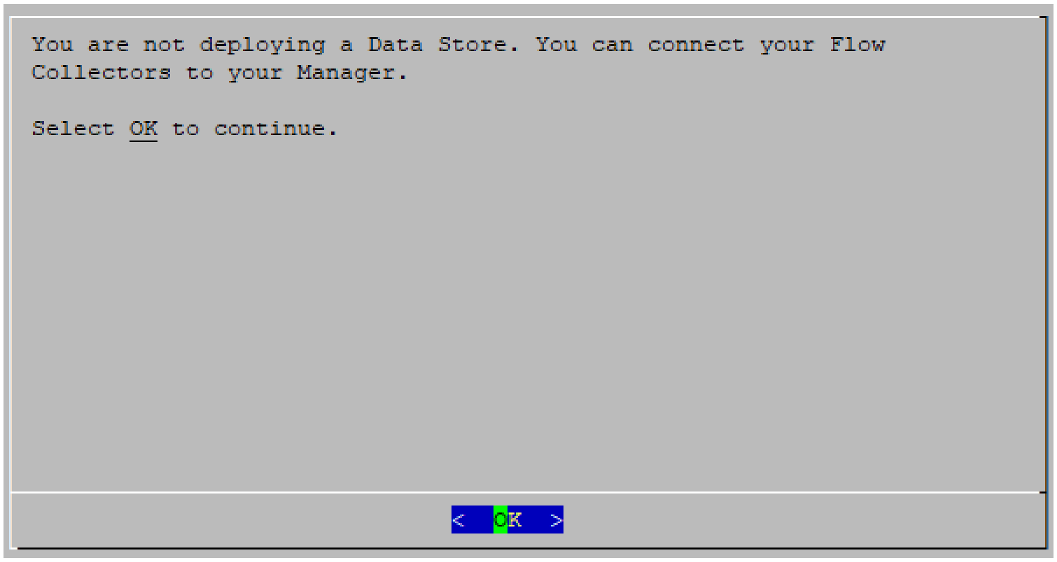
5. Are you sure you want to continue as sysadmin? Select **Yes** to continue the configuration without a Data Store.

> ⚠ Make sure you select **Yes**. If you need to deploy Secure Network Analytics with a Data Store, do not follow the instructions in this section. Follow the instructions in **Configuring a Flow Collector with Data Store**.
> If you select the wrong choice, deploy a new virtual appliance or RFD your virtual appliance.



```
Are you sure you want to continue as sysadmin? To deploy Secure Network
Analytics with a Data Store, you need to log in as root.

 - Select Yes to continue and deploy Secure Network Analytics without a
Data Store.

 - Select No to exit System Configuration. Log in as root to deploy
Secure Network Analytics with a Data Store.
```

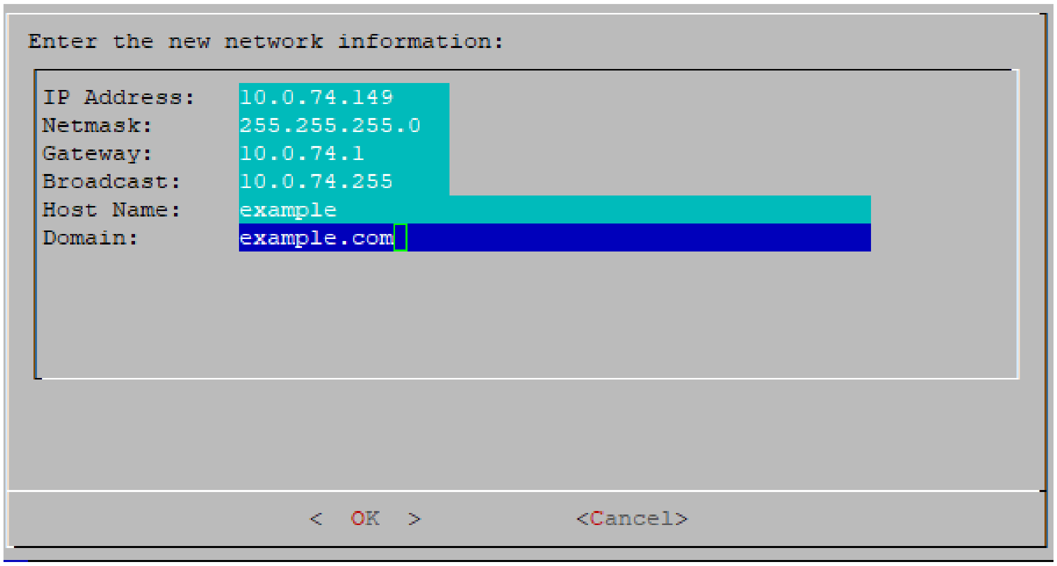
6. Confirm that you are deploying Secure Network Analytics without a Data Store. Select **OK** to continue.



```
You are not deploying a Data Store. You can connect your Flow
Collectors to your Manager.

Select OK to continue.
```

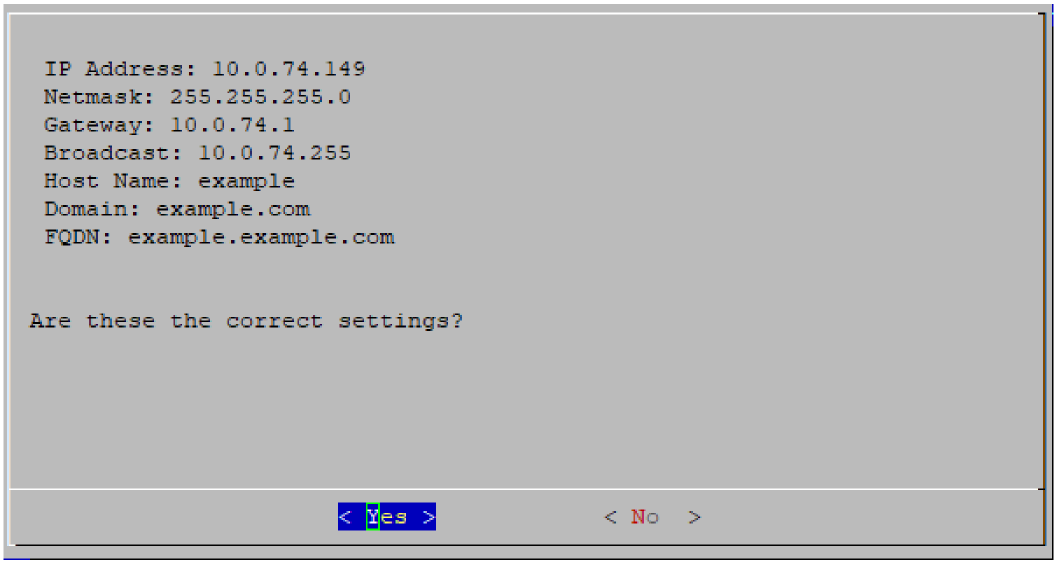
7. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**. Select **OK** to continue.

> 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.



```
Enter the new network information:

IP Address:    10.0.74.149
Netmask:       255.255.255.0
Gateway:       10.0.74.1
Broadcast:     10.0.74.255
Host Name:     example
Domain:        example.com
```

8. Confirm your settings. Select **Yes** to continue.



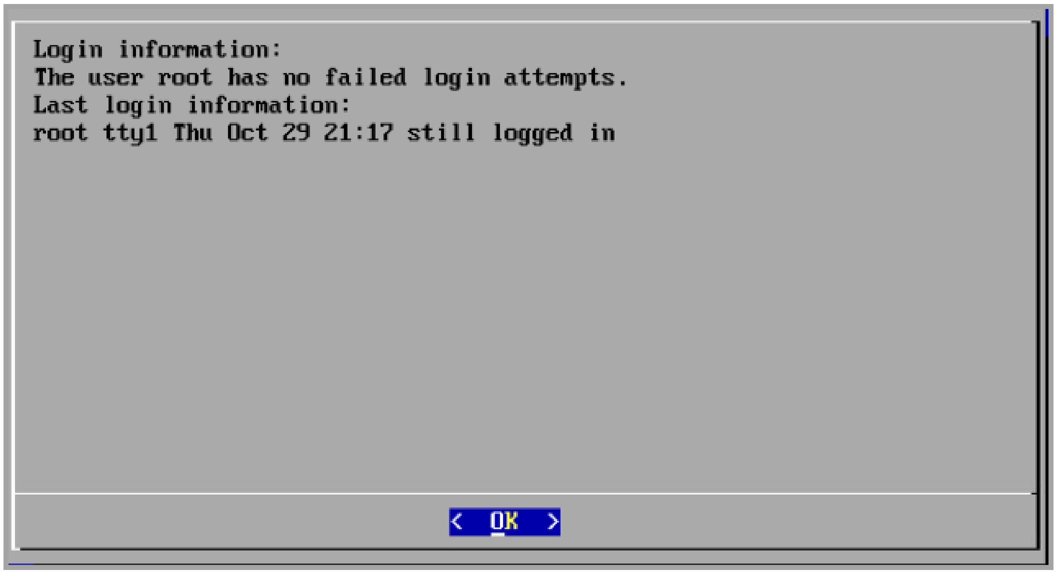
```
  IP Address: 10.0.74.149
  Netmask: 255.255.255.0
  Gateway: 10.0.74.1
  Broadcast: 10.0.74.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

9. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.
10. Press **Ctrl + Alt** to exit the console.
11. Repeat all steps in **Configuring a Flow Collector without Data Store** for the next Flow Collector in your system.

    - If you've configured all Flow Collectors without Data Store in First Time Setup, go to the next section (**Configuring a Flow Sensor or UDP Director**) or return to **Appliance Configuration Overview** to configure other appliances.
    - If you've configured all appliances in First Time Setup, go to **2. Configuring the Managed System**.

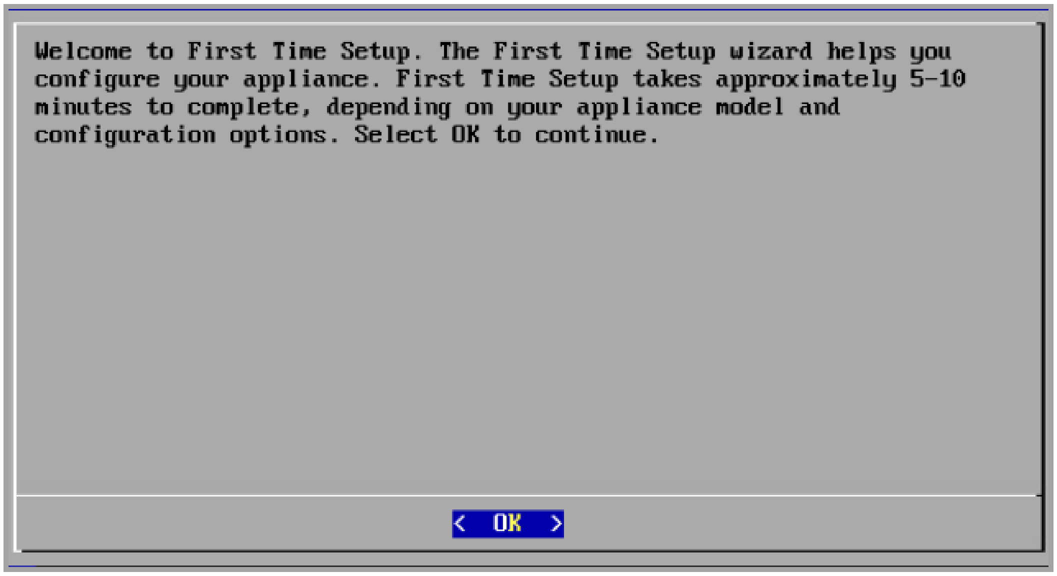
Configuring a Flow Sensor or UDP Director

1. Log in to a Flow Sensor or UDP Director through the console.
    - **Login:** sysadmin
    - **Default Password:** lan1cope
    - You will change the default password when you configure the system.
2. System Configuration (`SystemConfig`) opens.
3. Review the failed login attempts information. Select **OK** to continue.



```
Login information:
The user root has no failed login attempts.
Last login information:
root tty1 Thu Oct 29 21:17 still logged in
```

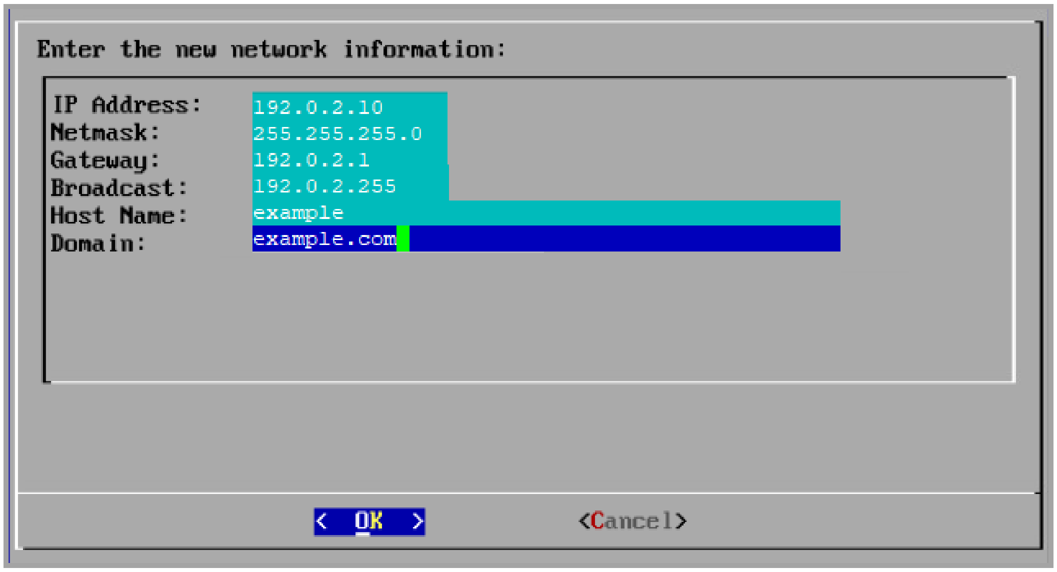
4. Review the First Time Setup introduction. Select **OK** to continue.



```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

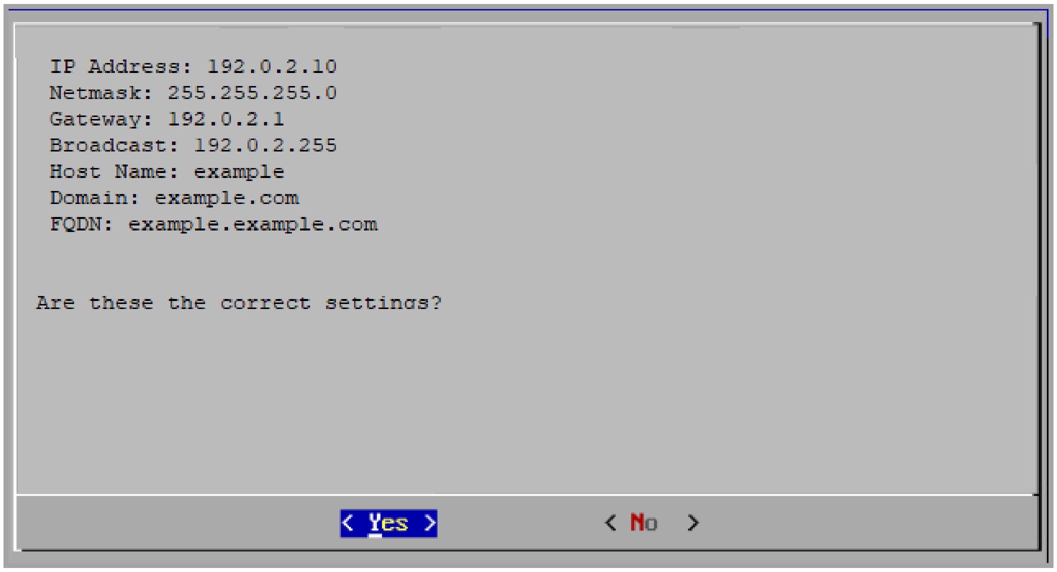
5. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.

> ⚠ 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.



```
Enter the new network information:

 IP Address:     192.0.2.10
 Netmask:        255.255.255.0
 Gateway:        192.0.2.1
 Broadcast:      192.0.2.255
 Host Name:      example
 Domain:         example.com
```

6. Confirm your settings. Select **Yes** to continue.



```
  IP Address: 192.0.2.10
  Netmask: 255.255.255.0
  Gateway: 192.0.2.1
  Broadcast: 192.0.2.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

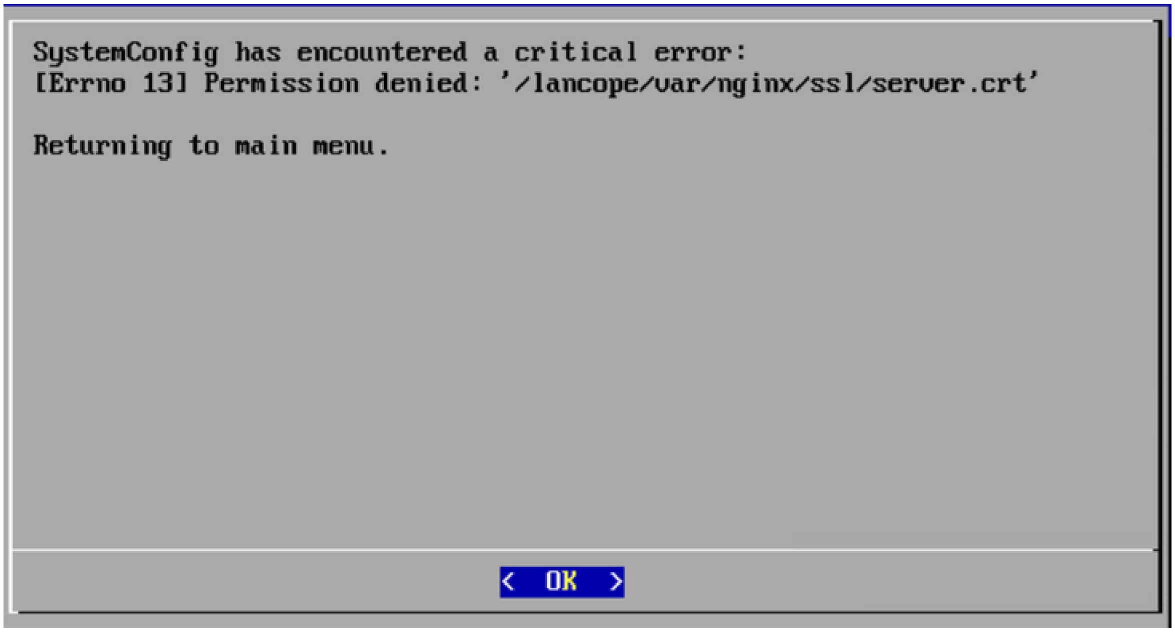
7. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.
8. Press **Ctrl + Alt** to exit the console.
9. Repeat all steps in **Configuring a Flow Sensor or UDP Director** to configure the next Flow Sensor or UDP Director in your system.

   If you've configured all appliances in First Time Setup, go to **2. Configuring the Managed System**.

Troubleshooting

Certificate Error

If your VM environment usage is high, there may be a timing error and some events occur out of order. If you receive the following error that permission is denied due to a certificate error **(.crt)**, do the following:



```
SystemConfig has encountered a critical error:
[Errno 13] Permission denied: '/lancope/var/nginx/ssl/server.crt'

Returning to main menu.
```

1. Log in to the appliance console as **sysadmin**. The default password is lan1cope.
2. Select **Advanced** > **Root Shell**.
3. Run the following command:

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

4. Run `SystemConfig`.
5. Exit System Configuration.
6. Return to **Appliance Configuration Overview** and complete all steps in the section. If you cannot access the appliance, please contact Cisco Support.

Accessing the Appliance

If you cannot access the appliance after it restarts, do the following:

1. Log in as root.
2. Run the following commands and confirm the docker containers and services are up and running:
   - `docker ps`
   - `systemctl list-units --failed`
   - `systemd-analyze critical-chain`
3. Once all docker containers and services are up and running, try the login again. If you cannot access the appliance, please contact Cisco Support.

2. Configuring the Managed System

When you log in to the appliance for the first time, you will use the Appliance Setup Tool to configure each appliance so it is managed by your Manager.

Preparation

Before you start the configuration, review the instructions so you understand the appliance configuration order, best practices, and additional requirements.

Appliance Setup Tool Requirements

- Confirm your firewalls and ACLs (Access Control List) will allow access.
- Gather the host name for the appliance and IP addresses for the following:
    - appliance
    - subnet mask
    - default and broadcast gateways
    - NTP and DNS servers
    - Manager IP address for Central Management

For details, refer to **Appliance Configuration Requirements**.

Managed Appliances

As part of the Appliance Setup Tool, you will configure your appliance to be managed by your primary Manager.

When your appliances are managed by your Manager, you can use Central Management to edit appliance configurations, update software, reboot, shut down, and more.

Manager Failover

If you have more than one Manager, you can set up a Manager failover pair so that one of them serves as backup console to the other.

- Use the Appliance Setup Tool to configure each individual Manager.
- Plan which Manager will be primary and secondary.
- Define the Manager failover relationship after you configure both Managers and all other appliances with the Appliance Setup Tool. Refer to **3. Defining a Manager Failover Relationship** for details.

Secure Network Analytics Domain

When you configure your Manager, you will create a Data Store domain or Non-Data Store domain for your Secure Network Analytics appliances. When you configure your other appliances in the Appliance Setup Tool, you will add them to the domain you created. Refer to **Planning Your System Configuration** for details.

After you finish your system configuration with your first domain, you can add domains to your configuration (refer to **Domains**). If you configure Secure Network Analytics with a Non-Data Store domain, you can add a Data Store to your deployment after you finish the system configuration. Follow the instructions in **Adding Data Store to a Non-Data Store Deployment**).

Best Practices

To configure your system successfully, make sure you follow the instructions in this guide. Make sure you review the following:

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** (or **Data Store Not Initialized**) before you start configuring the next appliance in your cluster.
- **Order:** Follow the appliance configuration order.
- **Multiple Central Managers:** You can configure more than one Central Manager in your system. However, each appliance can be managed by only one primary Manager/Central Manager.
- **Access:** You need administrator privileges to access Central Management.

Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

Order	Appliance	Details
1.	Primary Manager	Your primary Manager is your Central Manager. Make sure the Manager is shown as **Connected** before you start configuring the next appliance in the system. When you configure your Manager, you will create a Secure Network Analytics domain with a Data Store (Data Store domain) or without a Data Store (Non-Data Store domain).
2.	All Data Nodes	Required for Data Store deployments. Make sure the Data Node appliance status is **Data Store Not Initialized** before you configure the next appliance in your cluster.
3.	Flow Collector 5000 Series Database	Make sure the database appliance status is **Connected** before you start the engine configuration. **Database and Engine Pair:** If you have more than one database and engine pair, configure each pair one at a time. For example, configure pair1 (database1 and engine1) before you configure pair2 (database2 and engine2). In each pair, confirm the database is shown as **Connected** before you start the engine configuration. Also, when you configure unique host names, name each database and engine pair so you can identify them in Central

		Management. After you've completed the system configuration, you can review the appliance identity certificates in the trust stores for each pair. Refer to **Reviewing Trust Store Certificates** for details.
4.	Flow Collector 5000 Series Engine	Make sure the Flow Collector 5000 series database is shown **Connected** before you start the engine configuration.
5.	All Other Flow Collectors	**Flow Collectors with Data Store:** Make sure the appliance status is **Data Store Not Initialized** before you configure the next appliance in your cluster. **Flow Collectors without Data Store:** Make sure the appliance status is **Connected** before you configure the next appliance in your cluster.
6.	UDP Directors (also known as FlowReplicators)	Make sure the UDP Director appliance status is **Connected** before you configure the next appliance in your cluster. If you are installing Cisco Telemetry Broker instead of the UDP Director, finish the Secure Network Analytics system configuration. Then, follow the instructions in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.
7.	Flow Sensors	Make sure your Flow Sensor appliance status is **Connected** before you start the Flow Sensor configuration.
8.	Secondary Manager (if used)	Make sure the primary Manager appliance status is shown as **Connected**

		before you start the secondary Manager configuration. The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured using the Appliance Setup Tool. Refer to **3. Defining a Manager Failover Relationship** for details.

ℹ Your system might not have all the appliances shown here.

1. Log In to the Appliance Setup Tool

Use the following instructions to configure each appliance using the Appliance Setup Tool.

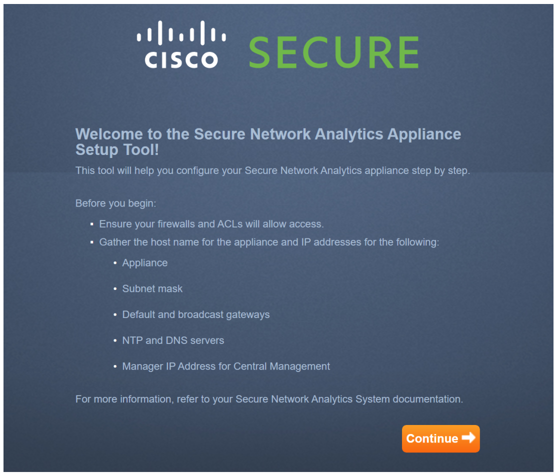
1. In the address field of your browser, type **https://** followed by the IP address of the appliance.

   - **Primary Manager:** Configure the primary Manager first.
   - **Connected:** Confirm each appliance is Connected or Data Store Not Initialized before you start configuring the next appliance in your cluster.
   - **Order:** Make sure you configure your appliances in order so they communicate correctly.

> If you cannot access the appliance, refer to **Troubleshooting** in 1. Configuring Your Environment Using First Time Setup for instructions.

2. Enter the following credentials to log in:

   - **User Name:** admin
   - **Password:** lan411cope



Welcome to the Secure Network Analytics Appliance Setup Tool!

This tool will help you configure your Secure Network Analytics appliance step by step.

Before you begin:

- Ensure your firewalls and ACLs will allow access.
- Gather the host name for the appliance and IP addresses for the following:
  - Appliance
  - Subnet mask
  - Default and broadcast gateways
  - NTP and DNS servers
  - Manager IP Address for Central Management

For more information, refer to your Secure Network Analytics System documentation.

> If this is not a first-time installation, go to **Troubleshooting** (at the end of this guide) to change appliance network settings such as host name, network domain name, or IP address.

2. Configure the Appliance

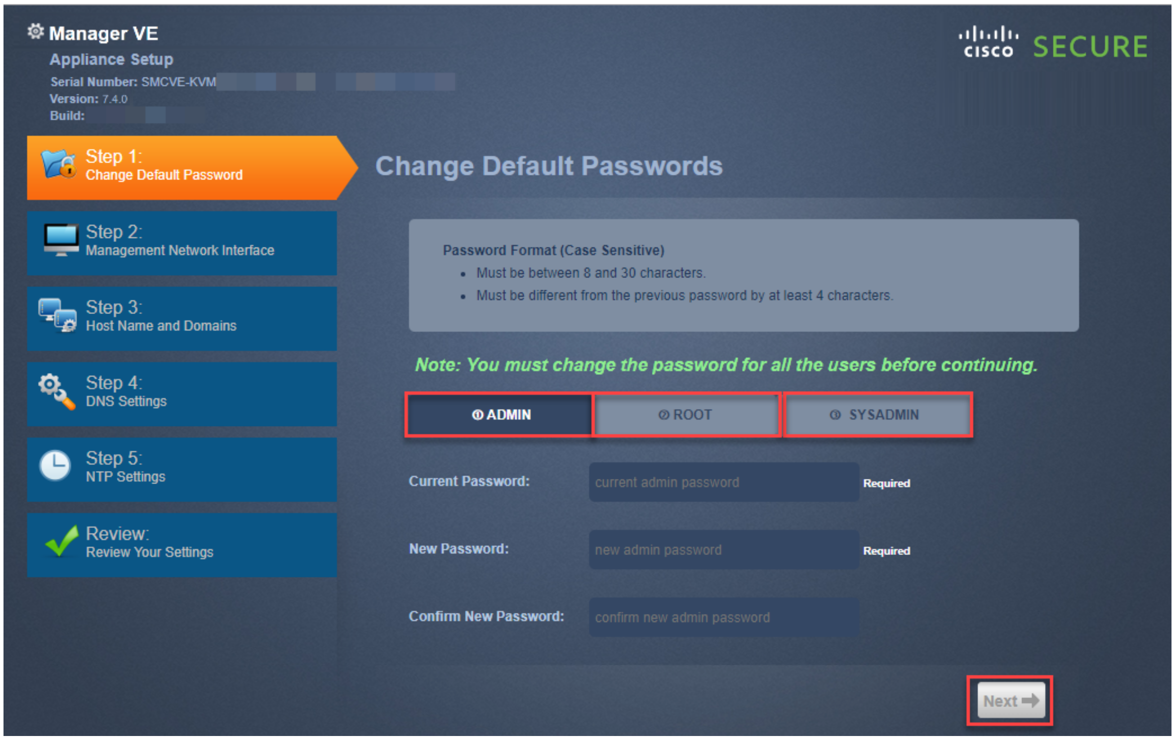
When you log in to the appliance for the first time, the Appliance Setup Tool guides you through each configuration step.

1. **Change Default Password:** Enter new passwords for admin, root, and sysadmin. Click **Next** to scroll to each user.

   Use the following criteria:

   - **Length:** 8 to 256 characters
   - **Change:** Make sure the new password is different from the default password by at least 4 characters.

User	Default Password
admin	lan411cope
root	lan1cope
sysadmin	lan1cope



Manager VE
Appliance Setup
Serial Number: SMCVE-KVM[redacted]
Version: 7.4.0
Build: [redacted]

cisco SECURE
Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Review: Review Your Settings

Change Default Passwords

Password Format (Case Sensitive)

- Must be between 8 and 30 characters.
- Must be different from the previous password by at least 4 characters.

Note: You must change the password for all the users before continuing.

Current Password: current admin password Required

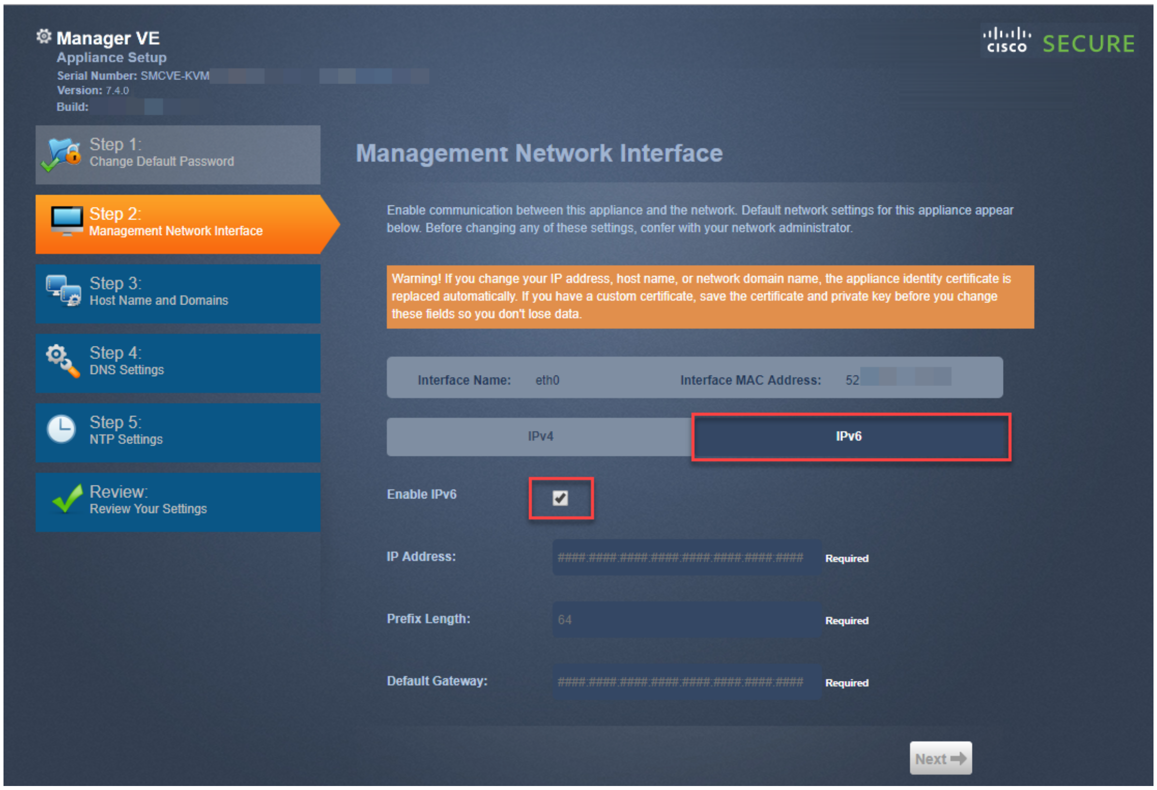
New Password: new admin password Required

Confirm New Password: confirm new admin password

> The sysadmin and root menus are unavailable if you've already changed the default passwords during the hardware installation.

2. **Management Network Interface:** Review the IP address and network interface fields. Confirm the default settings are correct. Click **Next**.

    - **Changes:** To change this information, confer with your network administrator and refer to **Troubleshooting**.
    - **IPv6 (optional):** To enable IPv6, click **IPv6**. Check the **Enable IPv6** check box and complete the fields.



Manager VE
Appliance Setup
Serial Number: SMCVE-KVM[redacted]
Version: 7.4.0
Build: [redacted]

SECURE
Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Review: Review Your Settings

Management Network Interface

Enable communication between this appliance and the network. Default network settings for this appliance appear below. Before changing any of these settings, confer with your network administrator.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Interface Name: eth0   Interface MAC Address: 52[redacted]

Enable IPv6 ☑

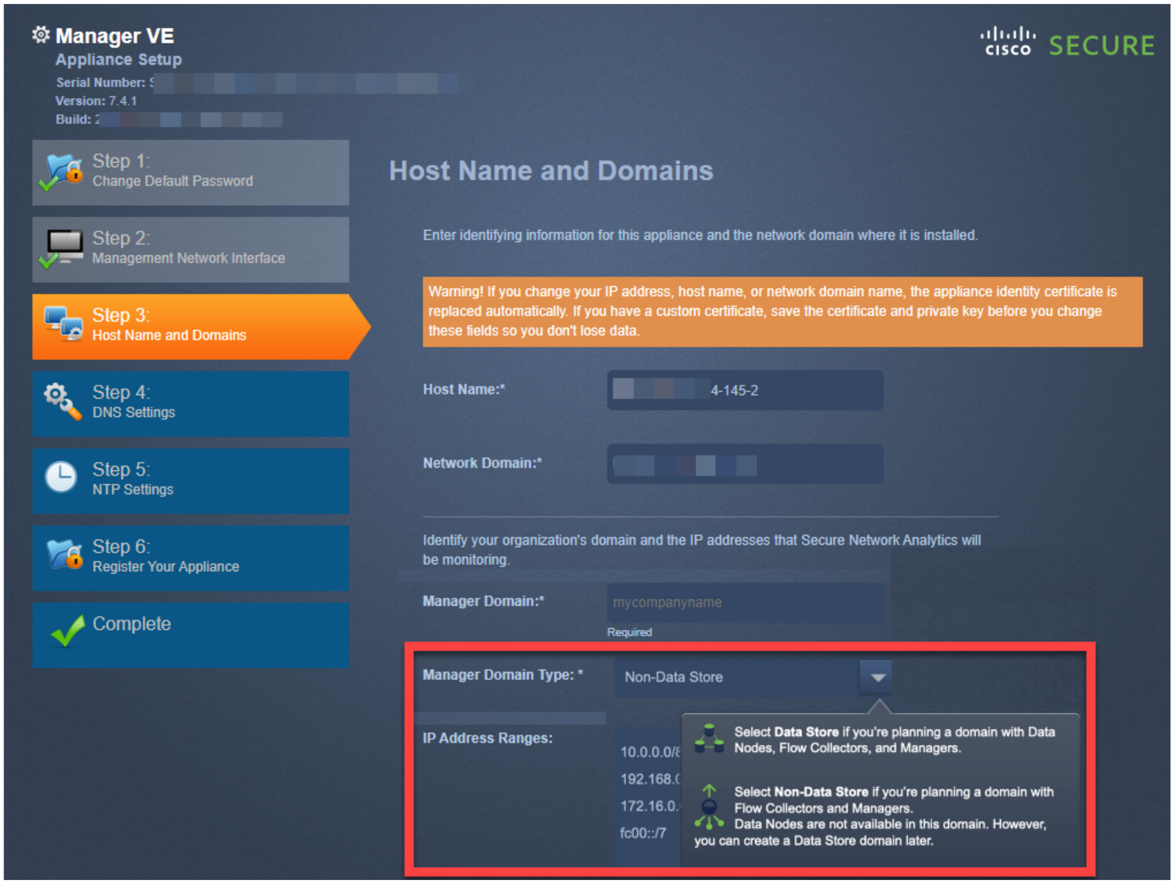
IP Address: ####:####:####:####:####:####:####:#### Required

Prefix Length: 64 Required

Default Gateway: ####:####:####:####:####:####:####:#### Required

3. **Host Name and Domains:** Enter the following information. Click **Next**.

Field Name	**Notes**
Host Name	A unique host name is required for each appliance. If you assign the same host names to your appliances, they will not install successfully. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts. **Flow Collector 5000 Series Database and Engine Pair:** Name each database and engine pair with unique host names that will help you identify the pair in Central Management. For example, database1 and engine1, database2 and engine2.
Network Domain	A fully qualified domain name is required for each appliance.
Manager Domain (Manager only)	Enter a domain name for your Secure Network Analytics deployment.
Manager Domain Type (Managers only)	**Data Store Domain:** If you configured your appliances with Data Store in First Time Setup, select Data Store Domain. **Non-Data Store Domain:** If you configured your appliances without Data Store in First Time Setup, select Non-Data Store Domain. After you finish your system configuration in this guide, you can add domains to your deployment. Refer to **Domains**.
IP Address Ranges (Manager only)	Select the IP address range for your Secure Network Analytics network.


Manager VE
Appliance Setup
cisco SECURE
Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Step 6: Register Your Appliance
Complete

Serial Number: [redacted]
Version: 7.4.1
Build: [redacted]

Host Name and Domains

Enter identifying information for this appliance and the network domain where it is installed.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Host Name:* [redacted]4-145-2

Network Domain:* [redacted]

Identify your organization's domain and the IP addresses that Secure Network Analytics will be monitoring.

Manager Domain:* mycompanyname
Required

Manager Domain Type: * Non-Data Store

IP Address Ranges: 10.0.0.0/8 192.168.(172.16.0. fc00::/7

Select **Data Store** if you're planning a domain with Data Nodes, Flow Collectors, and Managers.

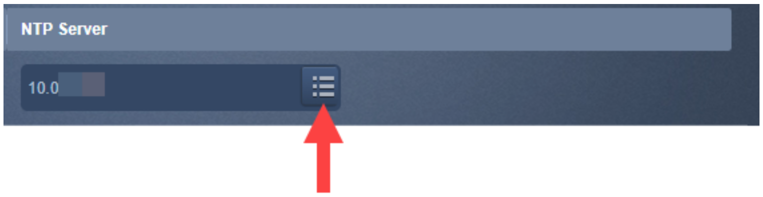
Select **Non-Data Store** if you're planning a domain with Flow Collectors and Managers.
Data Nodes are not available in this domain. However, you can create a Data Store domain later.

4. **DNS Settings**: Confirm the default is correct, or enter your domain server IP address. Click **Next**.

   Add or Delete DNS Servers (optional):

   - **Add:** Click the + icon.
   - **Delete:** Click the check box to select the DNS server. Click the - icon.

5. **NTP Settings:** Confirm the default is correct, or click the **Menu** icon to select your network time protocol (NTP) server. Click **Next**.



NTP Server

10.0[redacted]

- **Multiple NTP Servers:** We recommend setting up multiple NTP servers for redundancy and accuracy.
- **Public Source:** pool.ntp.org is a good, public source for NTP.

Add or Delete NTP Servers (optional):

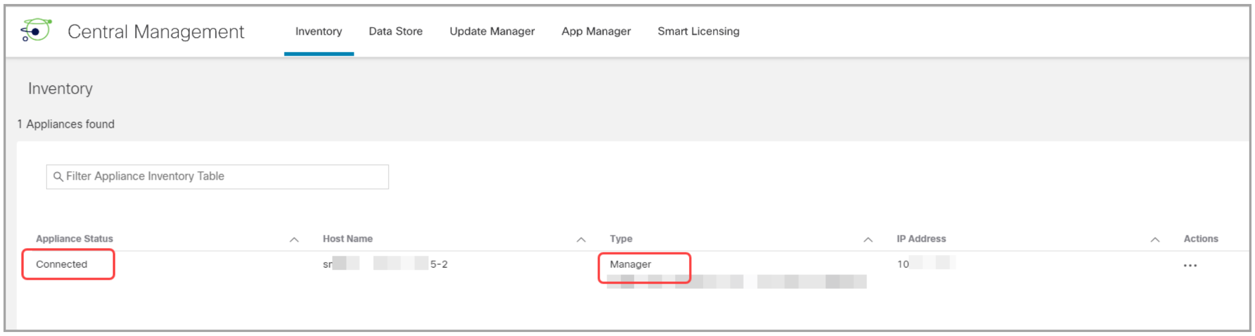
- **Add:** Click the + icon.
- **Delete:** Click the check box to select the NTP server. Click the - icon.

6. Your primary Manager is your Central Manager. Add your appliances to Central Management as follows:

    - **Managers:** If the appliance is a Manager, go to **3. Register the Manager**.
    - **All Other Appliances:** If the appliance is not a Manager, go to **4. Add Appliances to Central Management**.

3. Register the Manager

1. **Review Your Settings**: Confirm the appliance information is accurate.
2. Click **Apply** or **Restart and Proceed.**
    - Follow the on-screen prompts while the appliance restarts.
    - Wait a few minutes for your new system settings to take effect. You may need to refresh the page.
3. Log in to the Manager.
4. The Appliance Setup Tool opens again. Click **Continue.**
5. On the Register Your Appliance tab, review the IP address and click **Save.**
    - The Manager IP address is detected automatically and cannot be changed.
    - This step installs Central Management on the Manager.
6. When the appliance setup is completed, click **Go to Dashboard.**
7. Select **Configure > GLOBAL Central Management.**
8. Review the inventory. Confirm the Manager appliance status is shown as **Connected.**



Inventory

1 Appliances found

Filter Appliance Inventory Table

Appliance Status	Host Name	Type	IP Address	Actions
Connected	sr[redacted]5-2	Manager [redacted]	10[redacted]	...

Make sure the primary Manager appliance status is shown as Connected before you start configuring the next appliance in your cluster using the configuration order and details.

9. To configure the next appliance in your system, return to **1. Log In to the Appliance Setup Tool** and configure the next appliance in your cluster.

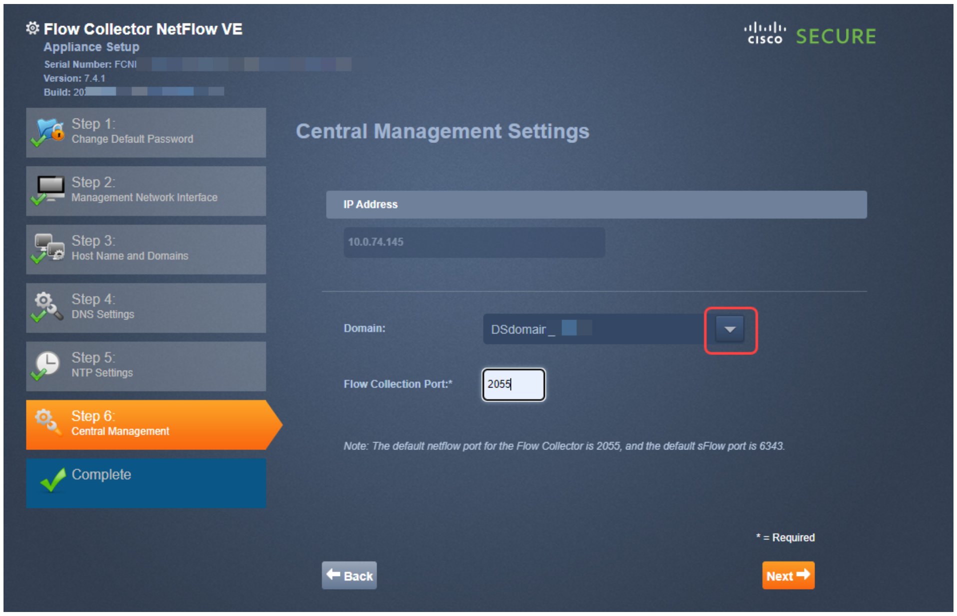
4. Add Appliances to Central Management

The Appliance Setup Tool continues to guide you through the appliance configuration with Central Management. Some of the steps may vary depending on the appliance. Follow the on-screen prompts.

1. On the Central Management tab, enter the IP address of your primary Manager.
2. Click **Save**.
3. Follow the on-screen prompts to trust the primary Manager appliance identity certificate. Click **Yes** to trust the certificate and allow the appliance to communicate with the Manager
4. Enter the login credentials for your primary Manager.
5. **Domain:** Select your Secure Network Analytics Domain. This the domain you configured as a Data Store domain or Non-Data Store domain when you registered the Manager.

    - **Flow Collectors:** Enter the Flow Collection port number. Netflow Default: 2055
    - **Flow Sensors:** Select a Flow Collector.

Selecting your Secure Network Analytics Domain



Flow Collector NetFlow VE
Appliance Setup
Serial Number: FCNI[redacted]
Version: 7.4.1
Build: 20[redacted]

cisco SECURE
Step 1: Change Default Password
Step 2: Management Network Interface
Step 3: Host Name and Domains
Step 4: DNS Settings
Step 5: NTP Settings
Step 6: Central Management
Complete

Central Management Settings

IP Address: 10.0.74.145

Domain: DSdomair_[redacted]

Flow Collection Port:* 2055

Note: The default netflow port for the Flow Collector is 2055, and the default sFlow port is 6343.

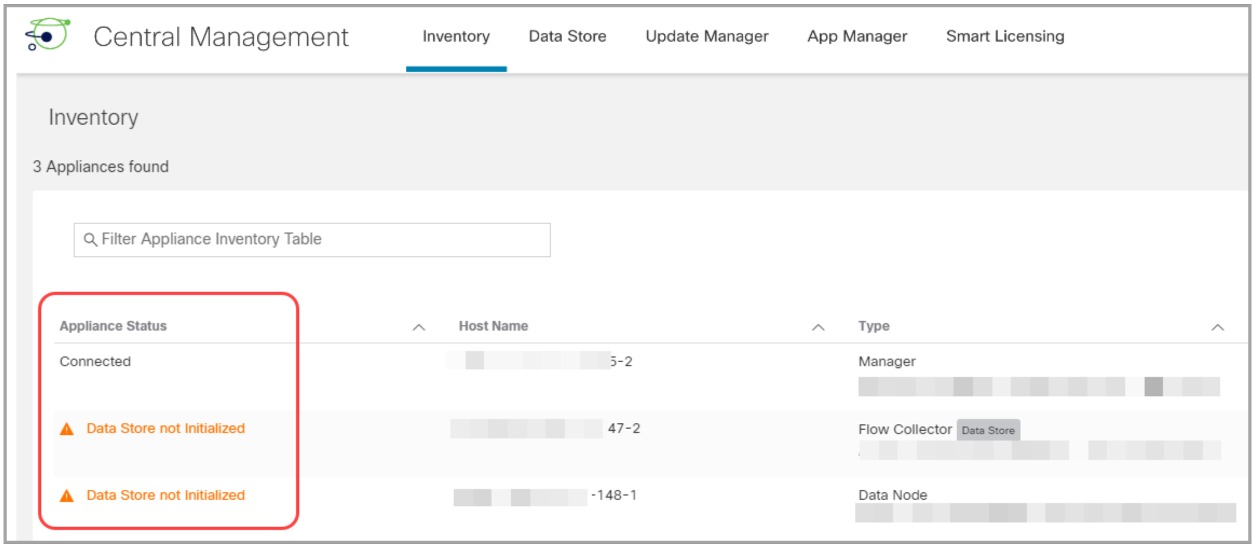
* = Required

6. Click **Go to Central Management.** Go to **5. Confirm Appliance Status**.

5. Confirm Appliance Status

After you configure an appliance in the Appliance Setup Tool, confirm the appliance status in Central Management.

1. The Appliance Setup Tool opens to the Central Management inventory, or you can open it as follows:
   - Log in to your primary Manager.
   - Select **Configure > GLOBAL Central Management**.
2. Review the appliances on the Inventory tab.
   - Confirm the appliance is shown in the inventory.
   - **Appliance Status:** Make sure the primary Manager and each appliance is shown as **Connected** before you start configuring the next appliance in your cluster.
   - **Data Store Not Initialized:** For Flow Collectors and Data Nodes in a Data Store domain, confirm the appliance status is **Data Store Not Initialized.** They will be shown as Connected after you complete the initialization in a later procedure.
   - **Type:** If a Flow Collector has a Data Store tag, it is configured to send flows to your Data Store database.



3 Appliances found

Appliance Status	Host Name	Type
Connected	[redacted]5-2	Manager [redacted]
⚠ Data Store not Initialized	[redacted]47-2	Flow Collector Data Store [redacted]
⚠ Data Store not Initialized	[redacted]-148-1	Data Node [redacted]

⚠ Make sure the primary Manager and each appliance is shown as Connected (or Data Store Not Initialized) before you start configuring the next appliance in your cluster using the configuration order and details.

3. To configure the next appliance in your system, go to **1. Log In to the Appliance Setup Tool**, and complete the all procedures through **5. Confirm Appliance Status**.

3. Defining a Manager Failover Relationship

Use Failover Configuration to establish a failover pair between two Managers so that one of them serves as a backup console to the other. If you have Secure Network Analytics with a Data Store deployment, it is important to configure Failover before you initialize the Data Store.

If you do not have a secondary Manager, go to **5. Installing v7.4.2 Patches**.

For a successful Failover configuration and operation, review the requirements and follow the instructions in the Secure Network Analytics Failover Configuration Guide.

⚠ If your primary Manager goes offline, please note that the Managers do not swap roles automatically. Make sure you change the Manager roles in the order shown in the Secure Network Analytics Failover Configuration Guide.

Data Store

If you've deployed Secure Network Analytics with a Data Store, make sure you configure Failover before you initialize the Data Store. If you configure Failover after you've initialized the Data Store, follow the instructions in the Secure Network Analytics Failover Configuration Guide to configure the secondary Manager for secure communication with the Data Store.

Configuring Failover

To configure your Managers as a failover pair, follow the instructions in the Secure Network Analytics Failover Configuration Guide.

The guide includes details that are critical for a successful configuration, including:

- **Certificates:** To set up trust between appliances so they can communicate, make sure you save the correct certificates to the required appliance Trust Stores.
- **Backup Files:** Back up the appliances before you start the failover configuration.
- **Configuration Order:** You will configure the secondary Manager for failover before you configure the primary Manager.
- **Changing Roles:** If your primary Manager goes offline, make sure you change the Manager roles in the order shown in the guide. The order is critical, and they do not swap roles automatically.
- **Troubleshooting:** Refer to the Secure Network Analytics Failover Configuration Guide for solutions.

⚠ For a successful configuration and operation, follow the instructions in the Secure Network Analytics Failover Configuration Guide.

Primary and Secondary Roles

As part of the configuration, you will assign a primary Manager and a secondary Manager. When you save the configuration, the following occurs:

- **Primary Manager**: The primary Manager pushes its domain configuration, user settings, and policies to the secondary Manager. Use the primary Manager to manage your appliances, change appliance configurations, change passwords, define alarms, apply policies, and more.
- **Secondary Manager**: The secondary Manager deletes its configuration, so it can synchronize with the primary Manager configuration and settings. Also, the secondary Manager changes to read-only for all users, which means that you will not have access to sections of the secondary Manager and you cannot retrieve files from the secondary Manager.

4. Configuring Site Redundancy

> ⓘ If you do not have a Data Store configured or you do not want to create a redundant site, go to **6. Initializing the Data Store**.

Site Redundancy allows you to establish near-redundancy across clusters in two Cisco Secure Network Analytics sites that contain separate deployments with similar appliances. Site Redundancy enables you to maintain your domain and Analytics configuration in your primary site and manually synchronize it with the redundant site. It also provides high availability protection in the event a data center loses power. With site redundancy, you will be able to log into either of the redundant clusters and see nearly the same data.

> ⓘ This feature is only available to Admin and Configuration Manager roles.

Site Redundancy configuration synchronization includes the following:

Data Store domain specific configuration as well as alert configuration (if enabled). Domain configuration includes:

- Host Group Management
- Policy Management
- Applications
- Exporter SNMP profiles (not including passwords)
- Alarm Severity
- Services
- Domain AS Numbers

Analytics configuration includes the following:

- Priorities
- Country Watchlist
- Alert Expiration

Redundant Site Requirements

Review the following requirements before you begin your redundant site configuration.

- Create redundant Data Store domains in both your primary and redundant site using identical names. Make sure that both sites have the same number of Data Store domains and that the Data Store domain names are identical in both sites. For more information on domains, refer to **Domains**.

> Only Data Store domains are synchronized for site redundancy. Non-Data Store domains are not synchronized.

- Ensure that the Secure Network Analytics software version is the same at both sites.
- Add your redundant Manager certificates to the primary Manager Trust Store. See Adding Certificates to Trust Stores for more information.
- Add your primary Manager certificates to the redundant Manager Trust Store. See Adding Certificates to Trust Stores for more information.

Once you have completed the requirements, you can proceed to the Configuring a Redundant Site procedure.

Adding Certificates to Trust Stores

Use the following instructions to save the required appliance identity certificates and chains to the Trust Stores.

Trust Store Requirements

The instructions will guide you through the following requirements:

- Adding the redundant Manager certificates to the primary Manager Trust Store.
- Adding the primary Manager certificates to the redundant Manager Trust Store.

Certificate Chain

If your appliance identity certificate includes a certificate chain, make sure you add the certificate chain (root and intermediate) to the Trust Stores.

Uploading Certificates to the Trust Store

Upload each file individually.

1. Download the Appliance Identity Certificates

Use the following instructions to download and save your appliance identity certificates. The steps vary based on the browser you are using.

If your certificates are already saved, you can skip this procedure. Go to **2. Add Certificates to the Manager Trust Stores**.

> You can also click the lock/security icon in your browser. Follow the on-screen prompts to download your certificates. The steps vary based on the browser you are using.

1. In the browser address bar, replace the path after the IP address with the following: **/secrets/v1/server-identity**

   For example: https://<IPaddress>/secrets/v1/server-identity

2. Follow the on-screen prompts to save the certificate.

   Open: To view the file, select a text file format.

   Troubleshooting: If you do not see the prompt to download the certificate, check your Downloads folder in case it was downloaded automatically, or try a different browser.

3. Repeat steps 1 and 2 on each Manager.

2. Add Certificates to the Manager Trust Stores

Use the following instructions to save your redundant Manager appliance identity certificate and chain (if applicable) to the primary Manager Trust Store.

1. Log in to your Manager.
2. Select **Configure > GLOBAL Central Management**.
3. Confirm the Appliance Status is shown as Connected.
4. Click the **Actions** menu for the Manager.
5. Select **Edit Appliance Configuration**.
6. On the **Central Management Inventory** > **General** tab, locate the **Trust Store** section.
7. Click **Add New**.

⚠ Make sure you upload each appliance identity certificate and chain (root and intermediate) certificate individually.

8. In the **Friendly Name** field, enter a name for the certificate.
9. Click **Choose File**. Select the certificate.
10. Click **Add Certificate**. Confirm the certificate is shown in the Trust Store list.
11. Repeat steps 6 through 9 to add any other required certificates to the Trust Store.

    - If you are logged in to the redundant Manager, add the primary Manager certificates.

- If you are logged in to the primary Manager, add the redundant Manager certificates.

12. Click **Apply Settings**. Follow the on-screen prompts.
13. **Connected:** On the Central Management Inventory page, confirm the Appliance Status returns to Connected.
14. Repeat steps 1 through 13 on the other Manager.

Open Site Redundancy Configuration

Use the following instructions to open Site Redundancy Configuration.

1. Log in to your Manager as admin or configuration manager.
2. From the main menu, choose **Configure > GLOBAL Manager**.
3. Click the **Site Redundancy Configuration** tab.

Configuring a Redundant Site

Follow these steps to configure a redundant site.

1. Select the **Enable Configuration** check box.
2. Enter the Fully Qualified Domain Name (FQDN) or IP address for the Manager at your redundant site in the **Name of Manager at Redundant Site** field. Note that the Manager name must match the Common Name or Subject Alternative Name in the Manager identity certificate.
3. Click the **Save** button to save your changes.
4. Click the **Synchronize** button to synchronize your primary site with your remote site. This will synchronize your domain configuration and analytics configuration between the two sites.
5. Follow the on-screen prompts to confirm that you want to synchronize your changes. Click **Synchronize** to continue.

   You will see the "in progress" ellipsis icon indicating the synchronization is in progress. When it is complete you will see a success or failure banner.

   > ⓘ When you perform a synchronization, the Redundant Site Flow Collector Engine configuration is overwritten in the process. It is not recommended to synchronize more than once per hour.

Disabling a Redundant Site

Perform the following steps to disable your redundant site.

1. To disable a redundant site, de-select the **Enable Configuration** check box.
2. Click the **Save** button to save your changes. This will disable the redundant site as well as the Synchronize button.
3. (optional) Removing the site certificates of a disabled redundant site can add an additional layer of protection to your Secure Network Analytics system. If you want to remove the site certificates that you added during the Configuring a Redundant Site procedure, you can do so by performing the following steps.
    1. Log in to your Manager.
    2. Select **Configure > GLOBAL Central Management**.
    3. Confirm the Appliance Status is shown as Connected.
    4. Click the **Actions** menu for the Manager.
    5. Select **Edit Appliance Configuration**.
    6. On the **Central Management Inventory** > **General** tab, locate the **Trust Store** section.
    7. Under the **Actions** column, click **Delete** for each of the certificates you want to remove.

Troubleshooting

In the event that you encounter an issue with your site redundancy configuration, ensure the following:

- Verify your certificates are in the correct Trust Stores. Refer to Adding Certificates to Trust Stores for more information.
- The Secure Network Analytics software version needs to be the same at both sites.
- The number and names of your Data Store domains at both sites needs to match.

To review the log file for errors, navigate to /lancope/var/smc/log/smc-configuration.log

5. Installing v7.4.2 Patches

Install the latest v7.4.2 patches on your appliances.

1. Download the latest **v7.4.2 patches** from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
2. Follow the instructions in the patch readme file to install each patch.
3. After you have updated your appliances with the latest patches, go to the next procedure in this guide:

    - **Data Store Domains:** Follow the instructions in **6. Initializing the Data Store**.
    - **Non-Data Store Domains:** Follow the instructions in **7. Installing the Desktop Client**.

6. Initializing the Data Store

Use System Configuration to initialize your Data Store. You will enable SSH temporarily as part of this procedure.

> ℹ Before you start this procedure, add all appliances to your Central Management inventory. Flow Collectors are not required to initialize a Data Store, however you will need to have at least one Data Node and one Manager in your Central Management inventory before you begin the initialization process.

1. Log in to your Manager appliance console (SystemConfig) as root.
2. From the main menu, select **Data Store**.
3. Select **SSH**. Follow the on-screen prompts to enable SSH.
4. Select **Initialization** from the Data Store menu.
5. Follow the on-screen prompts to initialize the Data Store.

   When you exit the Data Store menu, the system restores your previous SSH settings.

6. Go to the next procedure: **8. Verifying Communications**.

7. Installing the Desktop Client

Starting with v7.4.0, the SMC has been renamed to Manager. The SMC is referred to as Manager within this section.

⚠ If your Secure Network Analytics system is deployed with only Data Store Flow Collectors, you will not use the Desktop Client. For a hybrid Data Store/Non-Data Store system, the Desktop Client will only work with Non-Data Store domains.

The following information applies to installing and using the Desktop Client:

- You can locally install different versions of Desktop Client.
- The Desktop Client includes Stealthwatch terminology such as Stealthwatch Management Console and SMC (Manager).
- If you want to access multiple versions of Desktop Client, you will need a different executable file for each Manager.
- If you are using both a primary and a secondary Manager, you will need to log off one Manager before you can log in to the other Manager.
- You can have different versions of Desktop Client open simultaneously.
- When you update to a later version of Secure Network Analytics, you will need to install the new version of Desktop Client.
- Use the Web App to monitor and configure your Secure Network Analytics installation if you deploy a Data Store. The Desktop Client is incompatible with a Data Store.

Instructions for installing the Desktop Client vary depending on whether you're using Windows or macOS:

- **Install the Desktop Client Using Windows**
- **Install the Desktop Client Using macOS**

You will also change memory size differently, depending on whether you're using Windows or macOS:

- **Change the Memory Size From Windows Explorer**
- **Change the Memory Size From Finder**

Install the Desktop Client Using Windows

- You must have sufficient rights to install Desktop Client.
- Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.

Use the following instructions to install the Desktop Client using Windows:

1. Log in to your Manager.
2. Click the ⤓ (**Download**) icon.
3. Click the .exe file to begin the installation process.
4. Follow the steps in the wizard to install the Desktop Client.
5. On your desktop, click the Desktop Client icon .
6. In the **SMC Server Name** field, enter the Manager server name or IP address (IPv4 or IPv6).
7. Enter the Manager user name and password.
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

Change the Memory Size From Windows Explorer

ⓘ You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Desktop Client interface.

Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

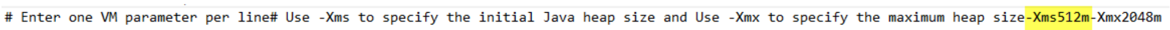
1. In Windows Explorer, go to your home directory.
2. Open these folders: AppData > Roaming > Stealthwatch.

   You may need to search "Stealthwatch" if the folder is hidden.

3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.
4. Open the **application.vmoptions** file using an appropriate editing application to begin editing. (This file is created after you open the Desktop Client for the first time.)

   Minimum Memory Size (Xms): We recommend that you allocate no less than 512 MB. This number is listed in the third line of the file.

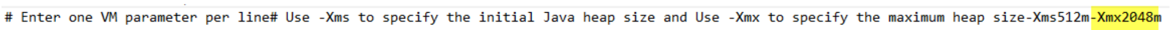
For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the minimum memory size.



```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

Maximum Memory (Xmx): You can allocate up to half the size of your computer's RAM for the maximum memory size. This number is listed in the fourth line of the file.

For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the maximum memory size.



```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

Use whole numbers. For example, enter Xmx512m, not Xmx0.5m.

- If you notice that the Desktop Client appears to "hang" frequently, try increasing the memory size.
- If you receive an error message involving Java, try selecting a lower memory allocation.

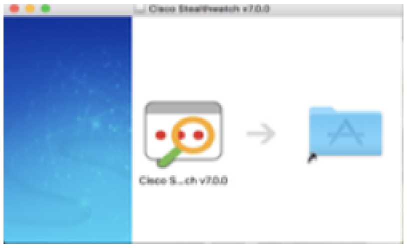
Install the Desktop Client Using macOS

- You must have sufficient rights to install Desktop Client.
- Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.

Use the following instructions to install the Desktop Client using macOS:

1. Log in to your Manager.
2. Click the ⭳ (**Download**) icon.
3. Click the .dmg file to begin the installation process.

   An icon and folder are displayed on your monitor, as shown below.

4. Drag the Desktop Client icon () into the Application folder.

   The icon is added to the Launchpad.

5. On your desktop, click the Desktop Client icon .
6. In the **SMC Server Name** field, enter the Manager server name or IP address (IPv4 or IPv6).
7. Enter the Manager user name and password.
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

Change the Memory Size From Finder

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Desktop Client interface.

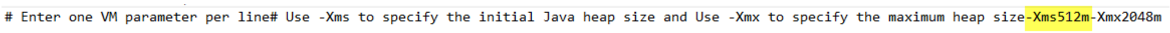
Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. In Finder, go to your home directory.
2. Open the Stealthwatch folder.

3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.
4. Open the application.vmoptions file using an appropriate editing application to begin editing. (This file is created after you open the Desktop Client for the first time.)

   Minimum Memory Size (Xms): We recommend that you allocate no less than 512 MB. This number is listed in the third line of the file.

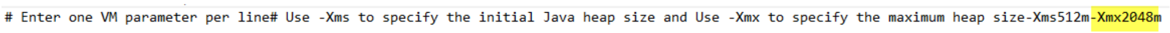
   For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the minimum memory size.

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   Maximum Memory Size (Xmx): You can allocate up to half the size of your computer's RAM for the maximum memory size. This number is listed in the fourth line of the file.

   For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the maximum memory size.

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   Use whole numbers. For example, enter Xmx512m, not Xmx0.5m.

- If you notice that the Desktop Client appears to "hang" frequently, try increasing the memory size.
- If you receive an error message involving Java, try selecting a lower memory allocation.

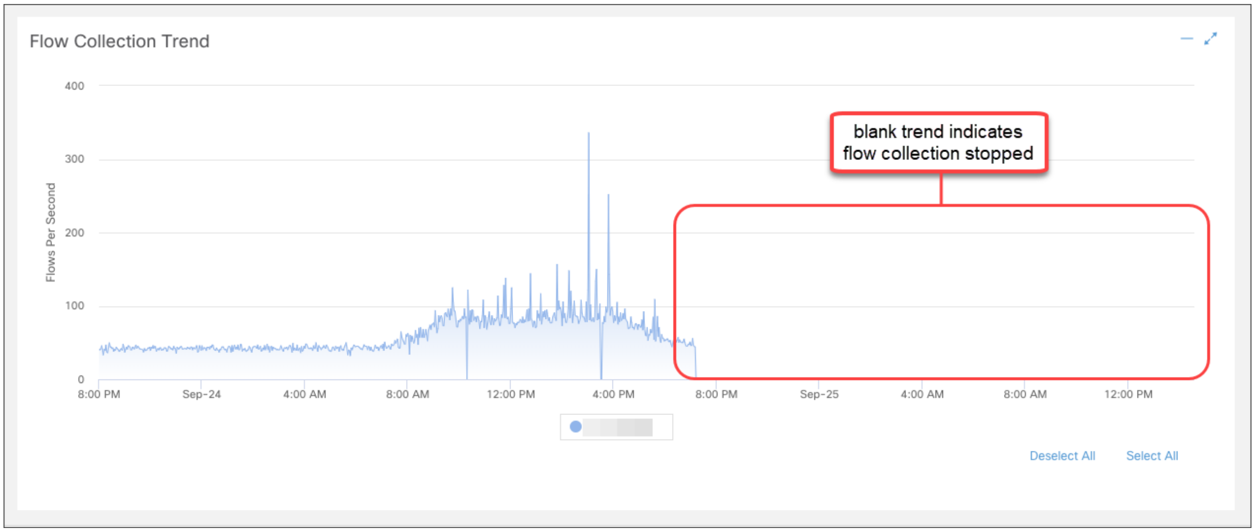
8. Verifying Communications

1. Review the Flow Collection Trend

1. Log in to your primary Manager.

   Failover Configuration: Log in to your primary Manager and secondary Manager.

2. Review the Flow Collection Trend.



2. Verify the Data Store Database Status

> If you did not deploy Secure Network Analytics with a Data Store, go to **3. Run Reports in Report Builder**.

1. In your primary Manager dashboard, select **Configure > GLOBAL Central Management**.
2. Click the **Data Store** tab.
3. Confirm the Data Store database status is shown as Up.

   If the database status is Down, click the ••• (**Ellipsis**) icon in the Actions column for the database. Select **Start**.

4. Confirm the status for all Data Nodes is shown as Up.

If a Data Node status is Down, click the ••• (**Ellipsis**) icon in the Actions column for the Data Node. Select **Start**.

> For more information about the Data Store tab, refer to **Data Store Database**.

3. Run Reports in Report Builder

1. Return to your Security Insight Dashboard.
2. Select the **Report** menu.
3. Select **Report Builder**.
4. Click **Create New Report**.
5. Click the **Flow Collection Trend by Flow Collector** template.
6. Select the parameters as needed. Click **Run**.
7. Review the report to confirm your Flow Collectors are receiving flows.
8. If you have a Flow Collector database (5000 Series only) or a Data Store, return to the Report Builder dashboard and repeat steps 4 through 7 to run the **Flow Database Ingest Trend Report.** Confirm the database or Data Store are receiving flows.

> For more information about Report Builder, refer to the information in the Help.

9. Finishing Appliance Configurations

Make sure you finish any required configurations for your appliances.

Appliance	Required Configurations	Optional Configurations
Data Node	none	Data Compression Flow Interface Statistics
Flow Collectors	none	Change NetFlow to sFlow
UDP Directors	none	High Availability (available on hardware only)
Flow Sensors	Application ID and Payload	Identifying Applications

Changing the Flow Settings in a Flow Collector

The following steps require a reboot of your Flow Collector to apply these changes.

Follow the steps below to change the flow settings in a Flow Collector.

1. Log in to the Flow Collector.
2. Click **Support** > **Advanced Settings**.
3. In the **engine_startup_mode field**, enter one of the following values:

   - Default value from the model file - 0
   - NetFlow -1
   - sFlow - 2

If the engine_startup_mode field does not appear in the Advanced Settings list, you can add it at the bottom of the page by using the Add New Option and Option Value fields.

4. Click **Apply** and then click **OK**.
5. Reboot your Flow Collector to apply your changes.
6. Log in to your Manager.
7. Select **Configure** > **SYSTEM Flow Collectors**.
8. Enter one of the following numeric values in the Monitor Port field (these are industry standard default port numbers for NetFlow and sFlow. If your exporters are configured to use a non-standard port, you must use that port number instead).

   - 2055 - NetFlow
   - 6343 - sFlow

9. Click **Save** to save your changes.

   Once the mode switch (NetFlow to sFlow or sFlow to NetFlow) completes, the following items that are based on flows from the previous mode are cleared:

   - Caches: host cache, flow cache, security event cache
   - Saved baseline files

You can confirm the mode switch by checking the flow trend graph on the dashboard to see if flows are being processed under the new mode.

Configuring UDP Directors for High Availability (Hardware Only)

Use the following instructions to configure your UDP Directors as a High Availability pair.

> High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

- **Forwarding Rules:** Configure at least one forwarding rule if you're planning to set up High Availability. Refer to **Configuring Forwarding Rules**
- **High Availability:** If you have more than one UDP Director, you can set up a High Availability pair. Configure at least one forwarding rule if you're planning to set up High Availability (refer to **Configuring High Availability**).

Configuring Forwarding Rules

SSL is used to send messages from the UDP Director to the Manager.

1. Log in to the Manager.
2. Select **Configure> GLOBAL UDP Director**.
3. Click the **Actions** menu for the appliance. Select **Configure Forwarding Rules**.
4. Click **Add New Rule**.
5. **Description:** Enter a brief description that identifies the rule.
6. **Source IP Address:Port:** Type the IP address of the device that sends data to the UDP Director and the input port number (where the data will be sent).
    - **Format:** Use the syntax [IP address]:[Port Number].
    - **Range:** You can use Classless Inter-Domain Routing (CIDR) notation to enter a range of IP addresses.
    - **All:** You can type "All" to accept data from any source IP address on this port.
    - **Combinations:** You can add Source IP Address:Port combinations within a rule by adding them to a new line.

Examples:

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **Destination IP Address:** Enter the IP address of the device receiving data from the UDP Director.
8. **Destination Port Number:** Enter the port number for the receiving device.
9. Click **Save**.
10. **Optional:** To sync your changes, click Sync.
11. Repeat the procedure to add forwarding rules as needed.
12. To set up a High Availability pair, go to **Configuring High Availability**.

> ⓘ High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

Configuring High Availability

If you have more than one UDP Director, use the Appliance Admin interface to configure high availability.

> ⓘ High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

The UDP Director High Availability (HA) allows a user to configure settings for redundant UDP Directors. Both nodes are fully redundant, however only one node is online at a time.

> ⓘ If you have high availability configured on your UDP Directors and update Secure Network Analytics to version 7.4.0 or later, reconfigure high availability after the update using the instructions below.
> For more information about updating Secure Network Analytics, refer to the Update Guide.

Primary Node and Secondary Node

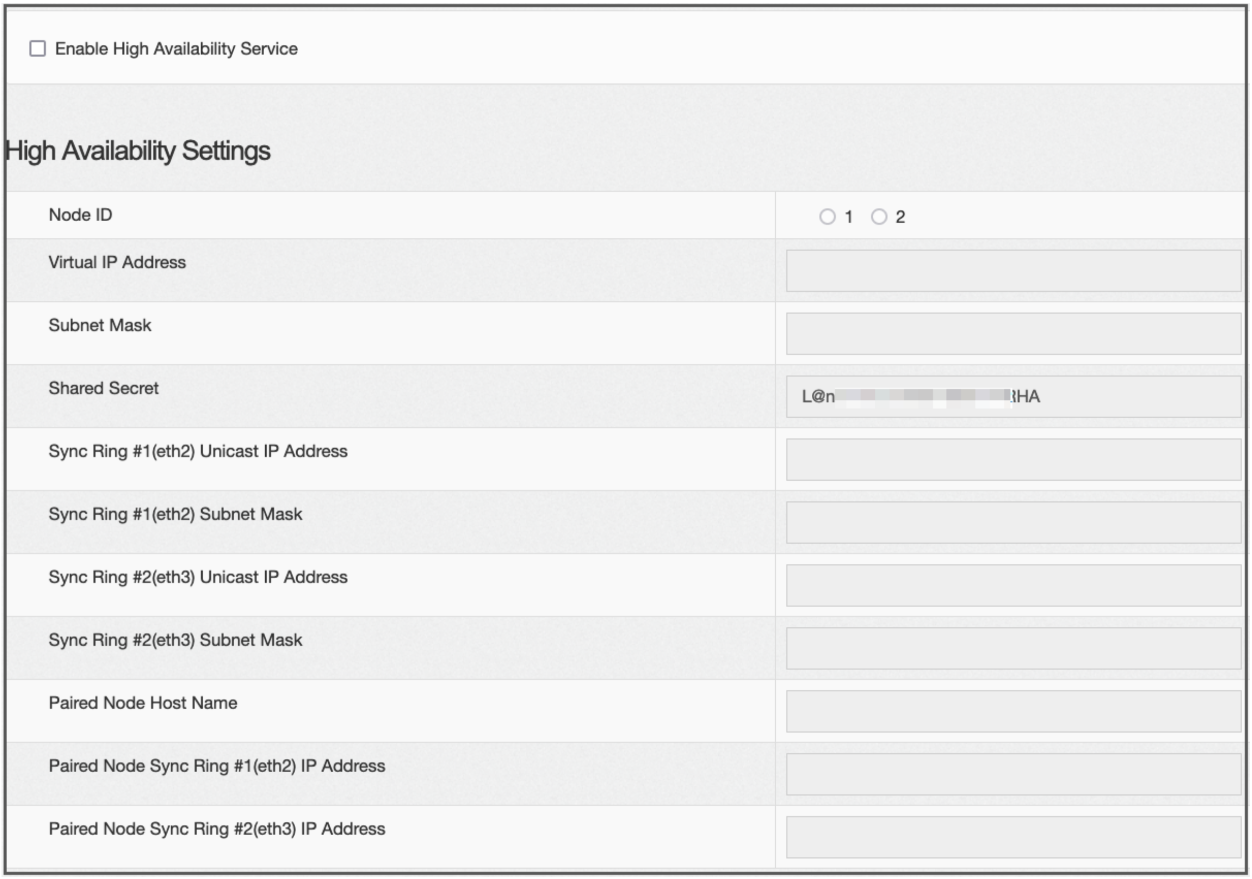
The online node is known as the Primary in the pair, while the offline node is the Secondary. If the Primary node in the pair should fail, the Secondary node takes over and becomes the Primary.

Requirements

- **Forwarding Rules:** Configure at least one forwarding rule for the UDP Director in the High Availability system.
- **Save the Rules Configuration File:** If the UDP Director has already been configured with rules, export (save the rules configuration file) the UDP Director rules. Then, import the file to the second UDP Director to ensure that the rules for each match.
- **Order:** Configure the Primary UDP Director and then repeat the configuration on the Secondary one.
- **New or Established:** If the both UDP Directors are new, make sure you follow the procedures for each in this guide. However, if the secondary is already configured as an appliance on the Secure Network Analytics system, log in to the secondary UDP Director and configure its High Availability components as described here.

1. Configure the Primary UDP Director High Availability

1. Log in to the primary UDP Director.
2. Click **Configuration** > **High Availability**.
3. Check the **Enable High Availability Service** check box for the High Availability Settings.



☐ Enable High Availability Service

High Availability Settings

Node ID	○ 1 ○ 2
Virtual IP Address	
Subnet Mask	
Shared Secret	L@n[redacted]HA
Sync Ring #1(eth2) Unicast IP Address	
Sync Ring #1(eth2) Subnet Mask	
Sync Ring #2(eth3) Unicast IP Address	
Sync Ring #2(eth3) Subnet Mask	
Paired Node Host Name	
Paired Node Sync Ring #1(eth2) IP Address	
Paired Node Sync Ring #2(eth3) IP Address	

4. Select your **Node ID**. If this is a primary UDP Director, select 1. If this a secondary UDP Director, select 2.
5. In the **Virtual IP Address** field, enter an unused IP adddress that is on the same subnet as the eth0 interface. Set the **Subnet Mask** value to the value of the subnet mask used on the eth0 interface.

> Make sure the Virtual IP Address is the same on both nodes.

6. In the **Shared Secret** field, type a string for both UDP Directors. (This will be encrypted for secure transfer.)
7. In the fields for **Sync Ring #1 (eth2) Unicast IP Address**, enter the IP address and the subnet mask. (A Unicast IP Address identifies a single network destination.)
8. In the fields for **Sync Ring #2 (eth3) Unicast IP Address**, enter the IP address and the subnet mask.

   Each of the IP addresses--eth0, eth02, eth03--must be on its own separate unicast subnet.

9. In the **Paired Node Host Name** field, enter the host name for the secondary UDP Director.
10. In the **Paired Node Sync Ring #1(eth2) IP Address** field, enter the Eth2 IP address for the secondary UDP Director.
11. In the **Paired Node Sync Ring #1(eth3) IP Address** field, enter the Eth3 IP address for the secondary UDP Director.
12. After reviewing the setting, click **Apply** to set the configuration.
13. Continue to the next section to configure the second UDP Director of the cluster.

2. Configure the Secondary UDP Director High Availability

> ⓘ If you selected Node ID 2 in step 4 above, complete the steps below for the primary UDP Director.

To configure the secondary UDP Director complete the following steps:

1. Log in to the secondary UDP Director.
2. Click **Configuration** > **High Availability**.
3. Enter the host name for the secondary UDP Director into the **Paired Node Host Name** field.
4. Configure all of the parameters on this screen (including any Advanced Parameters that you may have changed on the first appliance) exactly as you did on the first appliance with exactly same values for every field except for the following:

    - **Sync Ring #1(eth2) Unicast IP Address**: Enter a different IP address from what you configured in this field on the primary, but it must be in the same subnet as the Sync Ring 1 Unicast address given on the primary.
    - **Sync Ring #2(eth3) Unicast IP Address**: Enter a different IP address from what you configured in this field on the primary, but it must be in the same subnet as the Sync Ring 2 Unicast address given on the primary.
    - **Paired Node Host Name**: Enter the host name for the primary UDP Director in this field.
    - **Paired Node Sync Ring #1(eth2) IP Address**: Enter the Eth2 IP address for the primary UDP Director in this field.
    - **Paired Node Sync Ring #1(eth3) IP Address**: Enter the Eth3 IP address for the primary UDP Director in this field.

5. Click **Apply** to save your changes and to start the clustering services on this appliance.
6. Click **Promote** to designate the primary appliance.

Configuring the Flow Sensor

1. Configure the Application ID and Payload

The configuration of a Flow Sensor requires an additional step of configuring the application ID and payload.

1. Log in to the Flow Sensor Appliance Admin interface.
2. Click **Configuration** > **Advanced Settings**.

The Advanced Settings page opens.

3. Select the proper settings for your network:

Item	Description
Export Packet Payload	Allows you to specify whether the Flow Sensor includes the first 26 bytes of binary payload data in the data that it sends to the collector.
Export Applications Identification	Allows you to specify whether the Flow Sensor attempts to identify applications before sending data to the collector. In addition, this setting must be enabled for the following settings to take affect: Include IPv6 – Allows you to specify whether or not the Flow Sensor analyzes both IPv4 and IPv6 packets. When this setting is disabled, the Flow Sensor analyzes only IPv4 packets. Export HTTPS Header Data – Allows you to specify whether the Flow Sensor includes header data from HTTPS flows in the data that it sends to the collector. The data includes the SSL common name and SSL organization name. This setting requires that the Flow Type is set to IPFIX. The maximum is 256 bytes. Export HTTP Header Data – Allows you to specify whether or not the Flow Sensor includes header data from HTTP flows in the data

Item	Description
	that it sends to the collector. When this setting is selected, a secondary field allows you to specify the maximum length of the HTTP path (in bytes) that the Flow Sensor includes as part of the flow data. This setting requires that the Flow Type is set to IPFIX.
Enable VXLAN Decapsulation	Allows you to specify whether the Flow Sensor uses Virtual Extensible Local Area Network (VXLAN) decapsulation capabilities. Without VXLAN decapsulation, the Flow Sensor simply detects VXLAN encapsulated traffic as flows between two Virtual Tunnel Endpoints (VTEPs). Decapsulation allows for much richer content by being able to analyze the tunneled traffic and thus gain greater insight into the traffic patterns in the network. ⓘ The Flow Sensor will only decapsulate VXLAN traffic which was originally sent to the standard VXLAN port (4789).
Enable GENEVE Decapsulation	Allows you to specify whether the Flow Sensor uses Generic Network Virtualization Encapsulation (GENEVE) decapsulation for traffic received on its monitoring ports.
Enable ERSPAN Decapsulation	Allows you to specify whether to Flow Sensor uses Encapsulated Remote Switching Port Analyzer (ERSPAN) decapsulation capabilities to detect the ERSPAN header in packets, and then decapsulate the header and process the inner packet contents. You are required to assign the monitoring interface an IP address to allow termination of the ERSPAN tunnel on the Flow Sensor. ERSPAN decapsulation is not supported on the FS 4210.
Enable X-Forwarded-For Processing	Allows you to specify whether the Flow Sensor uses X-Forwarded-For (XFF) processing to identify the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer. ⓘ ETA and X-Forwarded-For Processing cannot be configured together.

Item	Description
Enable ETA Processing	Allows you to specify whether the Flow Sensor uses ETA processing to generate and transmit IDP and SPLT fields to your Manager. ⓘ Enabling ETA increases NetFlow bandwidth usage, especially when using v9. We recommend using IPFIX for the Flow Export Format. ⓘ ETA and X-Forwarded-For Processing cannot be configured together. ⓘ ETA cannot be enabled on Dell or PowerEdge Flow Sensor models.
Enable Load Balancing	Allows you to specify whether the Flow Sensor 4000 series can distribute flow data to more than one Flow Collector. Use this option if the flow data from the Flow Sensor exceeds the capacity of one Flow Collector.
Monitoring Interface Selection	Allows you to specify the following: • Flow Sensor 4240 - 2 x 40G or 4 x 10G (SFP) interfaces • Flow Sensor 4300 - 2 x 40G/100G or 4 x 10G (SFP) interfaces You must be using multiple Flow Collectors and have Load Balancing enabled for this setting to work properly. Go to the Flow Sensor and Load Balancer Integration Guide for more information. This option is only available on the Flow Sensor 4240 and Flow Sensor 4300. The default setting is 2 x 40G.
Cache Mode	Allows you to select one of the following settings: Use single, shared, cache for all monitoring ports –

Item	Description
	• Use when asymmetric routing is present. • Single state table for application and latency calculations. • Uses less memory. • Lower overall pps processing rates. • Results in one NetFlow event created across multiple interfaces. • Use only when the Flow Sensor has only two ports and is connected by a TAP Use independent caches for each monitoring port – • Allows deduplication of packets across each Flow Sensor interface. • Uses more memory. • Higher overall pps processing rates. • Each interface maintains its own latency and application database. • Results in a unique NetFlow record for each interface that sees a given packet.

4. Click **Apply** to save your settings.

2. Configure the Flow Sensor to Identify Applications (optional)

If you want the Flow Sensor to identify applications, configure the following settings:

1. Log in to the Flow Sensor Appliance Admin interface.
2. Click **Configuration** > **Advanced Settings**
3. Check the **Export Application Identification** check box. By default, this option is not selected.
4. If you have more than 1 monitoring NIC, select one of the following options in the **Cache Mode** section:

- **Use single, shared, cache for all monitoring ports:** typically used for systems that monitor flows using the TAP method.

- **Use independent caches for each monitoring port:** typically used to experience better performance and for systems that monitor flows using the SPAN method.

3. Restart the Appliance

1. Select **Operations** > **Restart Appliance**.
2. Confirm the appliance status is Connected in Central Management.

10. Configuring Telemetry

If you've deployed Secure Network Analytics with a Data Store, your Flow Collectors can ingest multiple types of telemetry simultaneously. You can configure your Flow Collectors during First Time Setup or, if it is an existing Flow Collector, you can update the telemetry ingest settings using Flow Collector Advanced Settings.

⚠ Make sure your telemetry ports are unique. If you configure duplicate telemetry ports, the ports will be reset to their internal defaults to avoid loss of flow data. For example, if NetFlow and NVM are exported to the same telemetry port, each device exporting NVM data will create an exporter on the Flow Collector and exhaust the exporter resources in the Flow Collector engine, resulting in loss of flow data.

Network Visibility Module

If you select and configure Network Visibility Module - NVM, the Flow Collector will ingest and store NVM flows. Follow the instructions in the Cisco Secure Network Analytics Endpoint License and Network Visibility Module (NVM) Configuration Guide to complete the configuration requirements.

Firewall Logs

If you select and configure Firewall Logs, the Flow Collector will ingest and store firewall event logs for Cisco Security Analytics and Logging (On Premises). Follow the instructions in the Security Analytics and Logging: Firewall Event Integration Guide to complete the configuration requirements.

App Requirement: If you select and configure Firewall Logs, install the Security Analytics and Logging (OnPrem) app on your Manager.

Updating Telemetry Settings

If you have an existing Flow Collector ingesting NetFlow or any other telemetry, you can update your telemetry ingest settings using Flow Collector Advanced Settings. To access Advanced Settings:

1. Log in to your Flow Collector (formerly known as Appliance Administration (Admin) interface).
2. Select **Support > Advanced Settings**.

ⓘ Each telemetry type has two settings. For more information on configuring telemetry using Advanced Settings, follow the instructions in the Help. Select ? **(Help) icon > Help**.

Cisco Telemetry Broker

Instead of using the UDP Director to send NetFlow to your Flow Collector, you now have the option to use Cisco Telemetry Broker to ingest network telemetry from many inputs, transform the telemetry format, and forward that telemetry to one or multiple destinations. To install Cisco Telemetry Broker, follow the instructions in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.

11. Licensing Secure Network Analytics

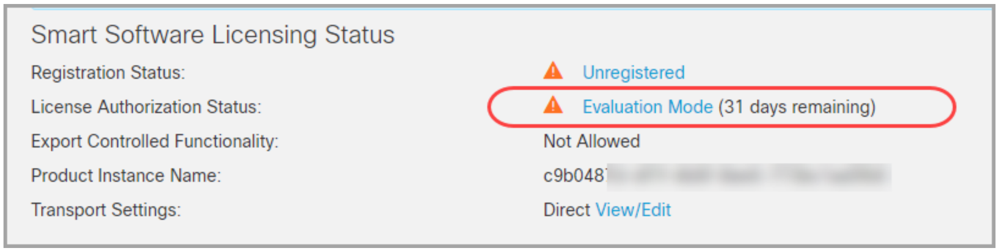
Use Cisco Smart Software Licensing to license your Secure Network Analytics appliances and features. For more information, refer to Smart Licensing on cisco.com.

- **Online:** To use Smart Licensing and Secure Network Analytics online, please refer to the Secure Network Analytics Smart Software Licensing Guide. You need Internet access for this configuration.
- **Offline:** To discuss your licensing options for closed/airgap networks, contact Cisco Support.
- **Cisco Smart Account:** To set up a Cisco Smart Account, register at https://software.cisco.com or contact your administrator.

Evaluation Mode

When you use Secure Network Analytics in Evaluation mode, you can use selected features for 90 days. To use Secure Network Analytics with maximum default functionality, and to add licenses and features to your account, register your product instance for Smart Software Licensing.

> ⚠ Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, flow collection will stop. To start flow collection again, register your product instance.



Smart Software Licensing Status

Registration Status:	⚠ Unregistered
License Authorization Status:	⚠ Evaluation Mode (31 days remaining)
Export Controlled Functionality:	Not Allowed
Product Instance Name:	c9b048[redacted]
Transport Settings:	Direct View/Edit

- **Admin User:** To review Smart Licensing status and usage details in your Manager, log in as the admin user.
- **Days Remaining:** To review the days remaining in Evaluation Mode, log in to the Manager as the admin user. Go to **Central Management** > **Smart Licensing**. Review the **License Authorization Status**.
- **Product Instance:** The Product Instance Name is the identifier we use for your Secure Network Analytics product instance, which includes your Manager and managed appliances.

12. Managing Secure Network Analytics

After you have finished configuring your appliances, the Help provides instructions for managing your environment, investigating behavior, responding to threats, and more.

> ℹ To review the instructions, select the ? (**Help**) icon > **Help** from any page.

Configuring Host Groups

1. Log in to your Manager.
2. Select **Configure** > **DETECTION Host Group Management**.

Creating and Managing Policies

1. Log in to your Manager.
2. Select **Configure** > **DETECTION Policy Management**.

Building Flow Searches

1. Log in to your Manager.
2. Select **Investigate** > **Flow Search**.

Running Reports in Report Builder

1. Log in to your Manager.
2. Select **Report** > **Report Builder**.

Managing User Permissions

1. Log in to your Manager.
2. Select **Configure > GLOBAL User Management**.

Investigating Behavior (Alarms, Security Events, etc.)

For information about investigating alarms, events, hosts, and more, review the information in Help.

1. Log in to your Manager.
2. Click the ? (**Help**) icon.
3. Select **Help**.

4. At the top of the page, select the **Help** menu.
5. Select **Investigating Behavior**.

Responding to Threats

For policy information, review the information in Help.

1. Log in to your Manager.
2. Click the ? (**Help**) icon.
3. Select **Help**.
4. At the top of the page, select the **Help** menu.
5. Select **Responding to Threats**.

Analytics

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.

To install appliances, follow the instructions in the Virtual Edition Appliance Installation Guide, the x2xx Series Hardware Appliance Installation Guide, or the x3xx Series Hardware Appliance Installation Guide.

Apps

Secure Network Analytics apps are optional independently releasable features that enhance and extend the capabilities of Secure Network Analytics.

The release schedule for Secure Network Analytics apps is independent from the normal Secure Network Analytics upgrade process. Consequently, we can update Secure Network Analytics apps as needed without having to link them with a core Secure Network Analytics release. Occasionally, an app that is designed to correspond with a new release of Secure Network Analytics may not be immediately available for installation. You may need to wait a few weeks for the newest version of the app.

For the latest Secure Network Analytics apps information, availability, and compatibility, refer to the following:

- Secure Network Analytics Apps Version Compatibility Matrix
- Secure Network Analytics Apps Release Notes

Authentication/Authorization

For details about each authentication or authorization configuration with Secure Network Analytics, refer to the following instructions.

Name	Instructions
LDAP	Follow the instructions in the Help. 1. Log in to your Manager. 2. Select **Configure > GLOBAL User Management**. 3. Click the **Authentication and Authorization** tab. 4. Select the ? (**Help**) icon > **Help**.
Security Assertion Markup Language Single Sign-On (SAML SSO)	Refer to the **Configuring SAML SSO** section in this guide.
TACACS+ Configuration Guide	Refer to the TACACS+ Configuration Guide.

Configuring SAML SSO

Use the following instructions to configure Security Assertion Markup Language Single Sign-On (SAML SSO). SSO is an authentication process that allows a user to access multiple applications with one set of credentials.

Support Details

Please note the following configurations are supported or not supported.

Supported	Not Supported
Microsoft Active Directory Federation Services (ADFS) for SAML/SSO	Cloud Services of Microsoft ADFS
On-Premise solutions of Microsoft ADFS	Integrated Windows Authentication (IWA)
Additional Proxies	External Services
	SAML request signing

ⓘ The Desktop Client is not supported in Data Store deployments.

1. Prepare for Configuration

You need the following information to configure SSO:

Requirement	Details
Identity Provider URL	The URL must use the fully qualified domain name or IPv4 address.
Identity Provider Certificate	If the IDP URL starts with HTTPS, download the CA certificate.

2. Upload Certificates to the Trust Store

If the Identity Service Provider (IDP) URL starts with HTTPS, add the **root CA certificate** to the Manager Trust Store.

> ⓘ If the IDP URL does not start with HTTPS, you can skip this step and go to the next section, **3. Configure the Service Provider**.

Use the following instructions to add the root CA certificate to the Manager Trust Store.

1. On the Central Management Inventory page, click the **Actions** menu for the Manager.
2. Select **Edit Appliance Configuration**.
3. On the **Appliance Manager** > **General** tab, locate the Trust Store section.
4. Click **Add New**.
5. In the **Friendly Name** field, enter a name for the certificate.
6. Click **Choose File**. Select the new certificate.
7. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.
8. Click **Apply Settings**. Follow the on-screen prompts.
9. **Connected:** On the Inventory page, make sure the Manager finishes the configuration changes and the Appliance Status returns to **Connected**.

> ⚠ Do not force the appliance to reboot while configuration changes are pending.

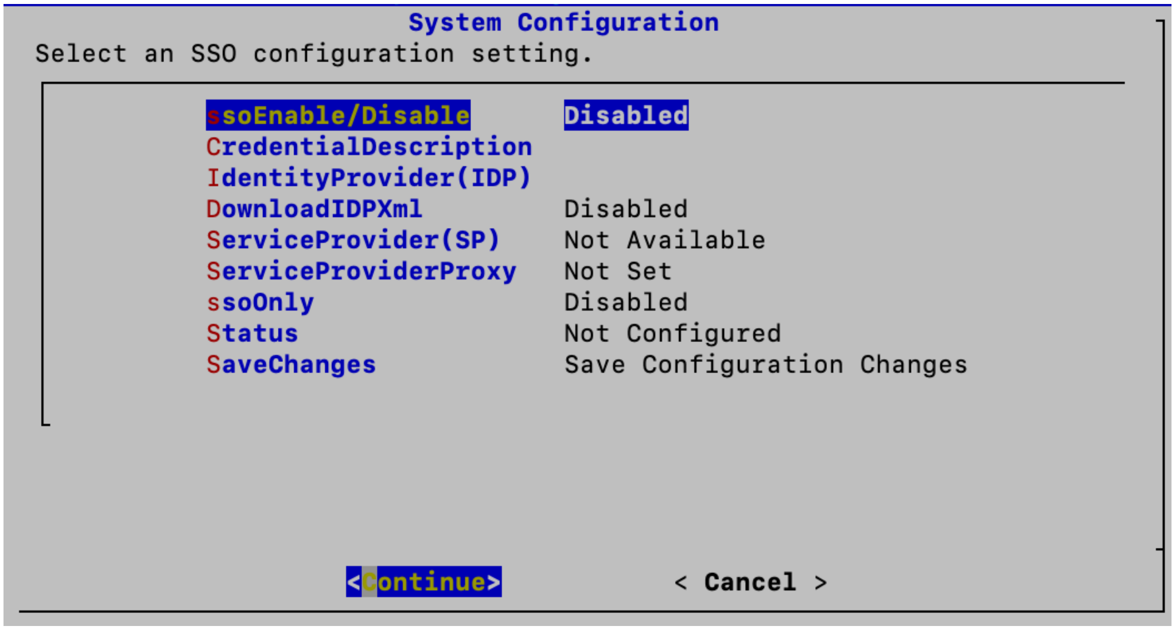
10. If you have a secondary Manager, repeat this procedure to add the root CA certificate to the secondary Manager Trust Store.
11. If you have added the root CA certificate to the Manager Trust Stores, go to the next section.

> ⓘ If you update any meta data on your LDP, you may notice that SSO does not connect. The meta data needs to be updated. The easiest way to do this is to simply reboot after updating your new SSO information in the System Configuration tool.

3. Configure the Service Provider

1. Log in to the Manager console as root.
2. Type `SystemConfig`. Press Enter.
3. Select **Advanced**

4. Select **SSO.**
5. Confirm **ssoEnable/Disable** is shown as **Disabled.**



```
                         System Configuration
 Select an SSO configuration setting.

           ssoEnable/Disable       Disabled
           CredentialDescription
           IdentityProvider(IDP)
           DownloadIDPXml          Disabled
           ServiceProvider(SP)     Not Available
           ServiceProviderProxy    Not Set
           ssoOnly                 Disabled
           Status                  Not Configured
           SaveChanges             Save Configuration Changes



                 <Continue>              < Cancel >
```

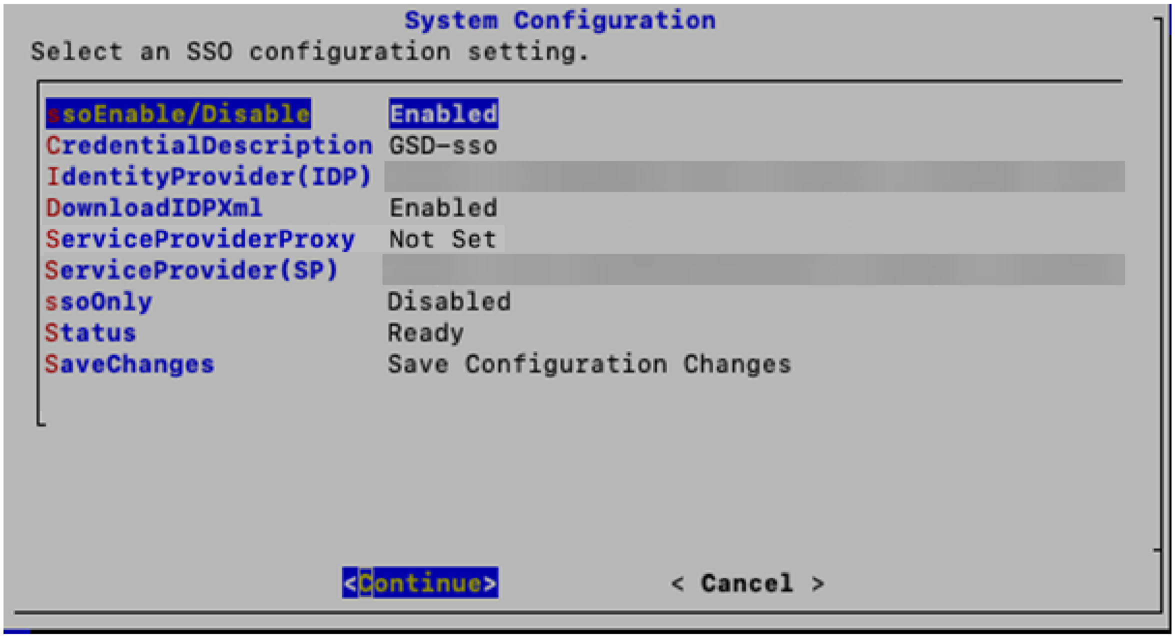
6. Select **IdentityProvider (IDP).** Click **Continue.**
7. Enter the URL where the Identity Provider's configuration file can be downloaded.

   Requirements: Enter the fully qualified domain name or IPv4 address.

8. Select **DownloadIDP.** Follow the on-screen prompts to enable it.
9. Select **SaveChanges**. Click **Continue.**

   Follow the on-screen prompts to download the IDP configuration file.

10. Select **SSO.**
11. Review **ServiceProvider(SP).** Copy the URL. You will use it to configure the identity provider.
12. Review **Status.** Confirm it is shown as **Ready.**



```
                         System Configuration
 Select an SSO configuration setting.

 ssoEnable/Disable          Enabled
 CredentialDescription      GSD-sso
 IdentityProvider(IDP)      [redacted]
 DownloadIDPXml             Enabled
 ServiceProviderProxy       Not Set
 ServiceProvider(SP)        [redacted]
 ssoOnly                    Disabled
 Status                     Ready
 SaveChanges                Save Configuration Changes

                  <Continue>          < Cancel >
```

4. Enable SSO

1. Select **ssoEnable/Disable**.
2. Follow the on-screen prompts to enable SSO.
3. Select **CredentialDescription.** Click **Continue.**
4. Enter a description of the SSO service credentials users need to log in.
5. Click **OK.**
6. Select **DownloadIDP.** Disable DownloadIDP until you need to save a new SSO configuration.

    - Click **Continue**.
    - Follow the on-screen prompts to disable DownloadIDP.

7. Select **SaveChanges**. Click **Continue**.
8. Exit System Configuration.

5. Configure a Service Provider Proxy (optional)

1. Confirm **ssoEnable/Disable** is shown as **Enabled.**
2. Select **ServiceProviderProxy**.
3. Enter the Fully Qualified Domain Name (FQDN) of the Service Provider Proxy you want to use.

4. Click **OK**.
5. Reboot your Manager to complete the proxy configuration process.

6. Configure the Identity Provider

1. In the address field of your browser, type the Service Provider URL.
2. Download the Service Provider metadata file **sp.xml**.
3. Configure the Identity Provider with **sp.xml**.
4. Make sure the outgoing claim type includes the user email address.

    - **For example:** If the Attribute store is the Active Directory, set the outgoing claim type to the email address for the LDAP Attribute type user ID.
    - **Microsoft Active Directory Federation Services (ADFS):** If the IDP type is ADFS, confirm the following custom rule is shown:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue
(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

7. Add an SSO User

Use the following instructions to add an SSO user. Users are authenticated through/by the Identity Provider.

1. Log in to the Manager (Web App).
2. Select **Configure > GLOBAL User Management**.
3. Select **Create** > **User**.

   For instructions, click the ? (**Help**) icon. Select **Help**. For details about adding users, refer to "Configuring Users."

4. Complete the fields to create a new user. Configure the user as follows:
    - **Authentication Service:** Select SSO.
    - **User Name:** Enter the first part of the email address for the IDP account. Make sure the ID is identical to the one that will be used for SSO at login. For example, for name@cisco.com, enter "name" in this field.

5. Click **Save**.
6. Confirm the SSO User is shown in User Management.

8. Test SAML Login

1. On the Web UI login page, select **Log in with SSO**.
2. Click the credentials button.
3. Enter the login credentials. The Manager opens to the Security Insight Dashboard.

Troubleshooting

Scenario	Notes
Account Lockout	Disable SSO Only from System Configuration through emergency account access.
Cannot download IDP XML	Make sure the IDP certificate is uploaded to the Manager Trust Store.
Cannot save IDP configuration	Review the IDP configuration and make sure the data you entered is accurate and doesn't include any extra spaces. Also, review the IDP event logs.
Additional Issues	Download a SAML tracer for your browser. Repeat the SSO login to review the exchanges between the IDP and SP.

Domains

A domain is a grouping of hosts and other devices that you want to monitor and manage. Flow Collectors exist within domains, and you can have multiple domains within one Secure Network Analytics system. Domains are completely independent of other domains, and every domain contains the Host Group tree. For information about which host groups exist in the Host Group tree, see Managing and Configuring Host Groups in the Help.

This section includes the following topics:

- **Data Store Domains and Non-Data Store Domains**
- **Adding and Configuring Domains**
- **Synchronizing Data Store and Non-Data Store Domains**
- **Deleting a Domain**

Data Store Domains and Non-Data Store Domains

When you configure your Manager in the Appliance Setup Tool and set up your system, you will create a Secure Network Analytics domain with a Data Store (Data Store domain) or without a Data Store (Non-Data Store domain).

- **Data Store Domain:** The Flow Collector sends its telemetry to the Data Store Data Nodes for storage.
- **Non-Data Store Domain:** The Flow Collector stores its telemetry locally on the Flow Collector or on the Flow Collector database (5000 Series only).
- **Hybrid Configuration:** In Secure Network Analytics with a hybrid configuration, you can configure a Data Store domain and Non-Data Store domain. When you configure your Flow Collectors, you can choose which domain they will use, which determines where they send data.

> ℹ If you are adding a Data Store domain to a Non-Data Store deployment, review the instructions in **Adding Data Store to a Non-Data Store Deployment**.

Adding and Configuring Domains

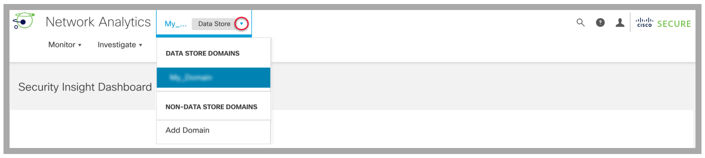
Use the following instructions to add a domain and define the domain settings. You can also import a Non-Data Store configuration into a new Data Store domain.

- **Role Permissions:** You need Admin or Configuration Manager roles to configure domains. Power Analysts can only view the domains.

- **Data Store Domains:** If you are adding a Data Store domain to a Non-Data Store deployment, review the instructions in **Adding Data Store to a Non-Data Store Deployment** before you start this procedure.

1. Add a Domain

1. From the menu bar, choose **[Current domain name] > Add Domain**.



2. Configure the following fields:

   - **Domain Name**: The name to be assigned to the domain. This name is shown on the Host Group tree.
   - **Select Method**: Select one of the methods described in the table below to designate which host group structure you want to use for the domain you are adding.

If you select this method...	Then...
Default	Secure Network Analytics creates the domain with the default host group structure but without any Flow Collectors.
Import from File	Secure Network Analytics creates the domain and uses the appropriate configuration, based on the specific domain content you exported (host group, domain, or both). For information on exporting XML files containing the domain configuration, refer to the Export Settings section. • XML files containing the domain configuration are not backwards compatible. These files are only compatible within the same system version number (for example, from Flow Collector v7.0 to Manager v7.0). • You can also import the entire host group configuration using the Host Group Management page. • If you need to import interface groups in the Network Devices branch of the Host Group tree from another domain, use this option. You must first export the groupings as an XML file to

If you select this method...	Then...
	your local drive. - None of the Flow Collectors contained in the XML file is imported.

ⓘ If you add a Flow Collector to an existing domain, that domain's specific configuration (policy, alarm severity, services, exporter SNMP, etc.) is applied to this Flow Collector.

3. Select **Add a Domain** to select your domain type. A Data Store domain is for Secure Network Analytics systems that are using a Data Store, and a Non-Data Store domain is for Secure Network Analytics systems that are not using a Data Store. For details, refer to **Data Store Domains and Non-Data Store Domains**.

   Check the **Configure as a Data Store Domain** check box if you are adding a Data Store domain.

⚠ Do not turn on Analytics if you have created more than one Data Store domain as this will cause Analytics to have sub-optimal performance.

4. To save your configuration, click **Add**.

Creating a Data Store Domain by Importing an Existing Non-Data Store Domain Configuration (Optional)

If you are currently on a Non-Data Store domain and you want to add a Data Store domain to your Secure Network Analytics system for a future expansion into Data Store, you can do so by importing a Non-Data Store configuration into a new Data Store domain.

When you import a existing domain, you won’t have to re-configure items such as alarms, host groups, and so on. Importing from an existing domain is like creating a new domain but with an existing configuration.

If the domain is newly created, then you will have to re-configure your Secure Network Analytics settings.

Follow the steps below to add a new Data Store domain and import all of its configuration from your Non-Data Store domain.

1. Use the **Add a Domain** drop-down menu to select your Non-Data Store domain.
2. Select **Configure > SYSTEM Domain Properties** from the top menu.

3. Make sure the **Export All configuration** radio button is selected. Refer to the Configuring Domain Settings section below to view a list of the data that is exported.
4. Click the **Export** button to download the XML file.
5. In the upper left corner of any page, at the left end of the main menu, choose **[Current domain name] > Add Domain**.
6. Enter a name for your new domain in the **Domain Name** field.
7. Click the Select Method drop-down menu and select the **Import from File** option.
8. Select the XML file you downloaded in step 4.
9. Click the **Configure as a Data Store** domain check box to select it.
10. Click the **Add** button to add your new domain.

2. Configure Domain Settings

1. Complete the following settings for the domain you are adding.

Setting	Description
Domain Name	Name for the domain you are currently in.
Archive Hour	Allows you to set the time at which each Flow Collector in the domain clears all counts. You can enter whole numbers between 0 and 23, where 0 is midnight in your local time zone. The local time zone is indicated to the right of the Archive hour field. At the defined time, the Flow Collector resets all index counts to 0. In addition, the Flow Collector saves the log files and Web files that it has gathered during the preceding 24 hours and then begins a new day of data collection.
Internal Autonomous System (AS) Number	Click inside the Internal AS Numbers field and type your AS numbers. Separate multiple entries with commas or by pressing **Enter** after each entry to place each one on a separate line. You can assign internal autonomous system (AS) numbers only to domains that contain Flow Collectors When Secure Network Analytics encounters traffic containing these numbers in flow data, it categorizes the traffic as "origin" traffic on the Autonomous System Traffic document. Origin traffic signifies traffic from or within your network as opposed to traffic from an external network that is passing through your network (transit traffic).

	For information about the Autonomous System Traffic document, see the "Autonomous System Traffic" topic in the Desktop Client help.

2. Configure your Export Settings

   The Export page on the Domain Properties dialog allows you to export specific domain content. You may want to use the content as a template for any additional domains you add in the future.

   Refer to the following table for information about the available settings.

If you select this check box...	**Secure Network Analytics exports this data...**
Export All configurations*	All of the data listed in "Export the Domain configuration" below. In addition, a list of your flow collectors as well as your exporters and their interfaces are also exported.
Export the Host Group configuration*	The entire host group definition structure, including the host group names and IP address ranges. This output does not include policies.
Export the Domain configuration*	• Archive hour setting from the Domain Properties dialog. • All Service definitions. For information about services, see the "Services" topic in the Desktop Client help. • All Alarm Configuration settings. For information about configuring alarms, see the "About Alarm Severities" topic in the Desktop Client help. • The entire host group structure, including the host group names and IP address ranges. Refer to the Managing and Configuring Host Groups topic in the Secure Network Analytics Help for more information. • All policies. Refer to the Managing Core Policies topic in the Secure Network Analytics Help for more information. Mitigation alarm actions are only exported when they have been manually changed from the defaults (set to *Not inherited*).
* You can use any of the XML files resulting from these commands to replace the host group configuration. For more information, see the "How to Replace the Host Group Configuration" topic in the Desktop Client help.	

3. Click **Export**.

   Secure Network Analytics saves the corresponding settings in an XML file that is downloaded to your Downloads folder.

> ⓘ Exporting a domain is not the same thing as backing up a configuration. To back up an appliance configuration, refer to **Creating an Appliance Configuration Backup**

Synchronizing Data Store and Non-Data Store Domains

If you are in the process of transitioning a Non-Data StoreFlow Collector to a Data StoreFlow Collector, you may want to keep your configurations and tuning synchronized between your Non-Data Store domain and your Data Store domain. This section describes the process for synchronizing your Non-Data Store domain with its associated Data Store domain.

Before You Begin

Ensure that you have already created a Data Store domain that you will be synchronizing with your Non-Data Store domain. If you have already followed the process outlined in **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors**, your Data Store domain should already be created. Refer to **Adding and Configuring Domains** for instructions on adding a domain.

> ⓘ You need administrator access for this procedure.

Synchronized Properties

The following properties will be synchronized between domains:

- Data Store domain specific configuration as well as alert configuration (if enabled). Domain configuration includes:
  - Host Group Management
  - Alarm Severity
  - Policy Management
  - Services, Applications
  - Exporter SNMP profiles (not including passwords)
  - Domain AS Numbers.

Recommended Synchronization Frequency

While you can synchronize your domains as often as you like, we recommend that you limit your synchronizations to only after you perform a group of changes or once a day or week.

This is because the synchronization process requires the use of resources that take away from daily processing.

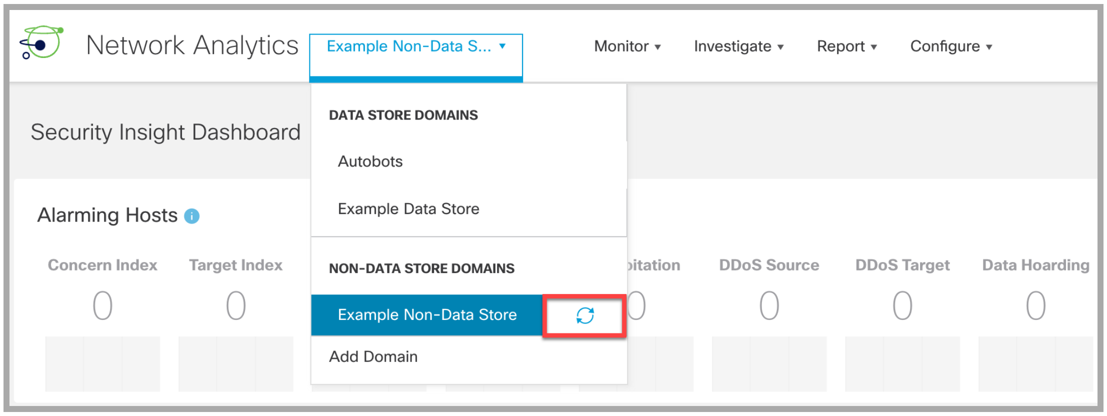
Synchronizing Domains Procedure

Follow these steps to synchronize your Non-Data Store domain (Source) with your Data Store domain (Target).

1. From the menu bar, choose the Non-Data Store domain that you want to synchronize with your Data Store domain.
2. From the main menu, choose **Configure > SYSTEM Domain Properties**.
3. Select the **Edit** button.
4. Choose the Data Store domain that you want to synchronize this domain with in the **Target Domain to Synchronize** drop-down menu.

> You can only synchronize your target Data Store domain with one source Non-Data Store domain. If you attempt to synchronize your target Data Store domain with more then one source Non-Data Store domain, you will receive an error.

5. Click the **Save** button to save your changes. A synchronize button appears next to the Non-Data Store domain that you selected to synchronize with your Data Store domain.



Removing a Domain Synchronization Target Domain

Follow the steps below to remove a target domain.

1. From the menu bar, choose the Non-Data Store domain that you want to synchronize with your Data Store domain.
2. From the main menu, choose **Configure > Domain Properties**.
3. Select the **Edit** button.

4. Click the **Clear Target Domain** button.
5. Click the **Save** button to save your changes.

Deleting a Domain

Before you delete a domain, review these instructions to make sure you understand the requirements.

> ⚠ When you delete a domain, you will lose access to all data that has been collected for that domain. Make sure you only delete a domain if you no longer need access to the collected data in it.

1. Remove Flow Collectors from Central Management

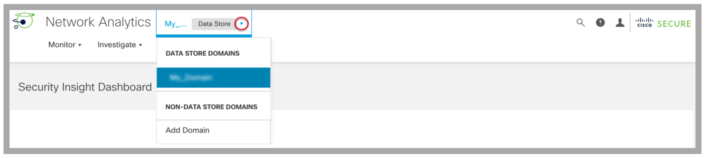
If your domain includes Flow Collectors, remove them from Central Management before you delete the domain. You can add the Flow Collectors to another domain, but the procedure includes resetting them to their factory defaults (RFD). For instructions, refer to the following:

1. **Removing an Appliance from Central Management**
2. **Resetting Factory Defaults**
3. **Adding an Appliance to Central Management**

> ⚠ If you remove Flow Collectors from Central Management and delete the domain, you will lose the associated Flow Collector data.

2. Delete a Domain

1. If you first need to access the domain, choose the **[Current domain name]** from the drop-down menu.



2. From the main menu, choose **Configure > SYSTEM Domain Properties**.
3. Click **Delete Domain**.

> ⚠ When you delete a domain, you will lose access to all data that has been collected for that domain. Make sure you only delete a domain if you no longer need access to the collected data in it.

Deleting a Desktop Client Domain

If you are using the Desktop Client in Secure Network Analytics without a Data Store, you can also delete domains from the Desktop Client.

⚠ Use caution when deciding which Desktop Client domains you want to delete as you will lose access to all data which has been collected for the domain you are deleting. **Workaround**: If you accidentally delete all of your domains in the Desktop Client and lock yourself out of the Manager Web App, create a new Non-Data Store domain in the Desktop Client. This will allow you to regain access into the Manager Web App. For information on creating a domain refer to the Add a Domain topic in the Desktop Client help.

Integrations and Additional Configurations

We have the following additional integrations and configurations available at

https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html. There may be more integrations than the list shown here.

- Configuring Cisco's ASA for NSEL Export to Stealthwatch
- Customer Success Metrics Configuration Guide
- Enabling Multiple NetFlow Exporters
- Endpoint License and Network Visibility Module (NVM) Configuration Guide
- Flow Sensor and Load Balancer Configuration Guide
- Global Threat Alerts Configuration Guide
- ISE and ISE-PIC Configuration Guide
- Secure Network Analytics and SecureX Integration Guide
- SSL/TLS Certificates Guide for Managed Appliances
- TACACS+ Configuration Guide
- Cisco Security Analytics and Logging (On Premises)

Passwords

You can change passwords as follows:

- **Enabling or Disabling Password Reset**
- **Resetting Passwords to Default Settings**
- **Changing Passwords**
- **Changing the Data Store Database Passwords**
- **Changing the Flow Collector Database Password (Non-Data Store Domains)**

Enabling or Disabling Password Reset

Use the following instructions to enable or disable the password reset function. If you select Enable, passwords can be reset to the default settings using the GRUB command line interface.

> ⚠ If you disable the password reset, and you lose your passwords, you will lose access to the data saved to your appliance. To access the appliance again, reset factory defaults and reconfigure it.

1. Log in to the appliance console as root.
2. Type **SystemConfig**. Press Enter.
3. Select **Security**.
4. Select **Password Reset**.
5. Follow the on-screen prompts to enable or disable password reset.

Resetting Passwords to Default Settings

There are a two ways to reset your passwords to their default settings.

- **Admin Password:** Use **Resetting the Admin Password on the Manager**
- **Admin, Root, Sysadmin Passwords:** Use **Resetting Admin, Root, Sysadmin Passwords to Default**.

> ⚠ After you reset your appliance passwords to the default, make sure you change them. This step is critical for security. Refer to **Changing Passwords** for instructions.

Resetting the Admin Password on the Manager

Use the following instructions to reset your **admin** password to the default setting on the Manager. Then, change the appliance password for maximum security.

- **Requirements:** You need the appliance root password to complete these instructions.
- **Other Users:** These instructions reset the admin user to the default password. The individual user passwords will not be changed.
- **Other Appliances:** These instructions do not reset the admin password on other Secure Network Analytics appliances (Flow Collector, Flow Sensor, or UDP Director).

1. Log in to the appliance console as root.
2. Type `rm /lancope/var/smc/config/users/admin/user.xml`. Press Enter.
3. Type `docker restart smc`. Press Enter.
4. Type `docker restart nginx`. Press Enter.

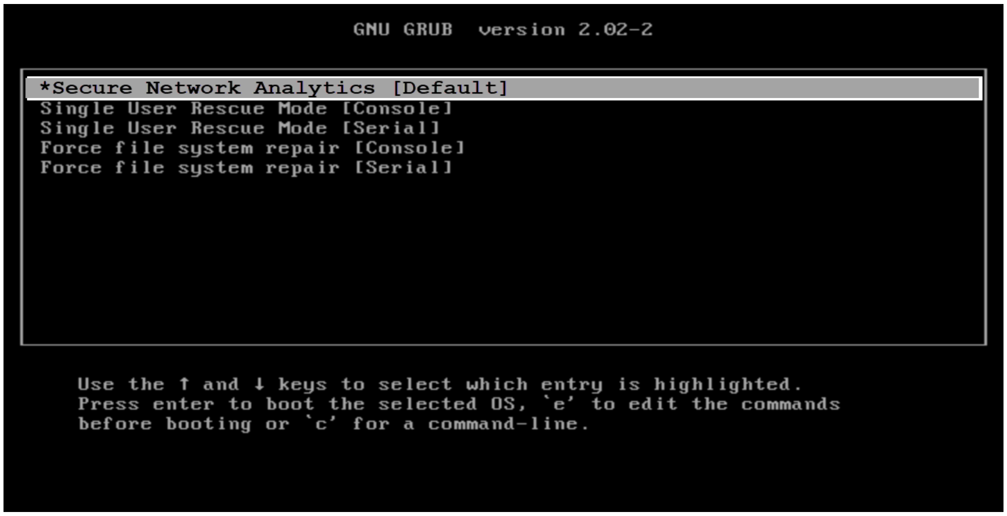
   This will reset admin password to the default value.

5. Exit the appliance console.
6. Go to **Changing Passwords** to change the admin password from the default. This step is critical for security.

Resetting Admin, Root, Sysadmin Passwords to Default

Use console access to reset your appliance **admin**, **root**, and **sysadmin** passwords to the default settings. Then, change the appliance passwords for maximum security.

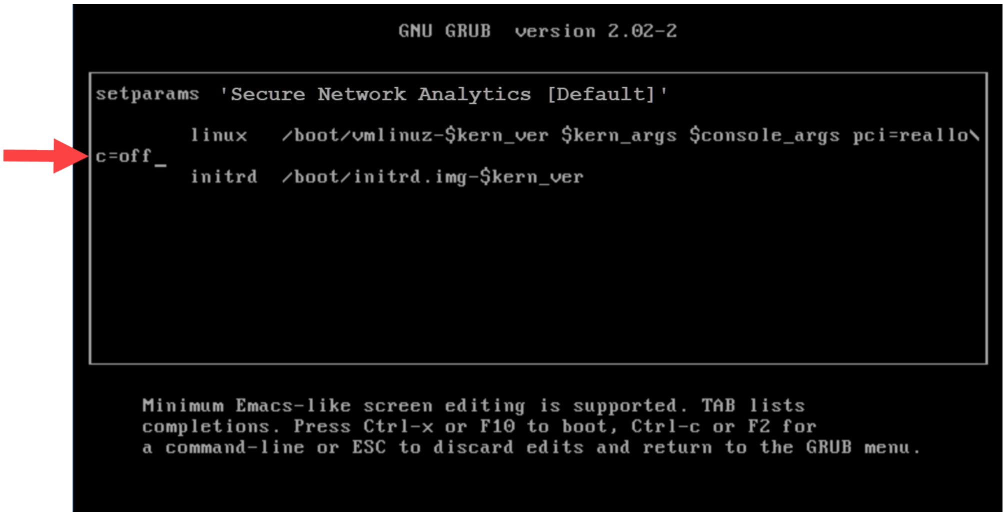
1. Log in to the appliance console (CIMC or hypervisor).
2. Reboot the appliance.
3. When the console screen reaches the GRUB menu, type "e" to enter edit mode.



```
                    GNU GRUB  version 2.02-2

 *Secure Network Analytics [Default]
  Single User Rescue Mode [Console]
  Single User Rescue Mode [Serial]
  Force file system repair [Console]
  Force file system repair [Serial]

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

4. Advance the cursor to the second line.

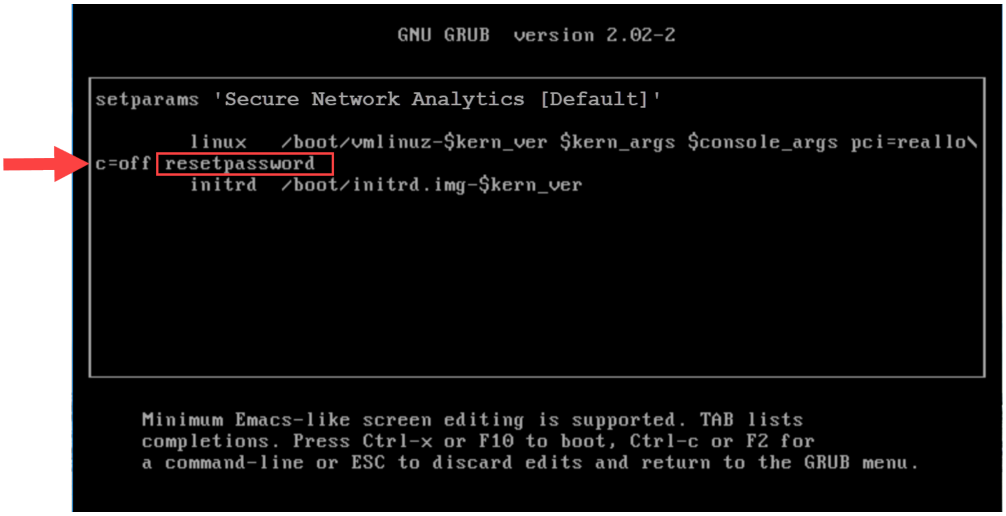
   The command line might look slightly different depending on your appliance version.



```
                    GNU GRUB  version 2.02-2

setparams 'Secure Network Analytics [Default]'

        linux   /boot/vmlinuz-$kern_ver $kern_args $console_args pci=reallo\
c=off_
        initrd  /boot/initrd.img-$kern_ver

     Minimum Emacs-like screen editing is supported. TAB lists
     completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
     a command-line or ESC to discard edits and return to the GRUB menu.
```

5. Type `resetpassword` after `c=off` to make the command line look like the following example:

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
c=off resetpassword
```



```
                      GNU GRUB  version 2.02-2

setparams 'Secure Network Analytics [Default]'

        linux   /boot/vmlinuz-$kern_ver $kern_args $console_args pci=reallo\
c=off resetpassword
        initrd  /boot/initrd.img-$kern_ver




    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
    a command-line or ESC to discard edits and return to the GRUB menu.
```

6. Type CTRL-X to resume booting.

   This will reset your admin, root, and sysadmin passwords to their default values.

7. Go to **Changing Passwords** to change the passwords from the default. This step is critical for security.

Changing Passwords

Use the following instructions to change your passwords from the default password or a previous password. Make sure you use the following criteria:

- **Length:** 8 to 256 characters
- **Change:** Make sure the new password is different from the previous password by at least 4 characters.

User	Default Password
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

Changing the Sysadmin Password

1. Log in to the appliance console as sysadmin.
2. Select **Security**.

3. Select **Password.**
4. Follow the on-screen prompts to change the sysadmin password.
5. Exit System Configuration.

Changing the Root Password

1. Log in to the appliance console as root.
2. Type **SystemConfig.** Press Enter.
3. Select **Security**.
4. Select **Password.**
5. Follow the on-screen prompts to change the root password.
6. Exit System Configuration.

Changing the Admin Password on the Manager

1. Log in to the Manager as admin.

    - **URL:** https://<IPAddress>
    - **Login:** admin
    - **Default Password:** lan411cope

2. Select **Configure > GLOBAL User Management**.
3. Locate the **admin** user in the list.
4. Click the **Actions** menu. Select **Change Password**.
5. Follow the on-screen prompts to change the admin password. Use the following criteria:

    - **Length:** 8 to 256 characters
    - **Change:** Make sure the new password is different from the default password by at least 4 characters.

Changing the Admin Password on All Other Appliances

Use the following instructions to change the admin user password on a Data Node, Flow Collector, Flow Sensor, or UDP Director.

1. Log in to the Appliance Administration interface as admin.

- **URL:** https://<IPAddress>
- **Login:** admin
- **Default Password:** lan411cope

2. Select **Manage Users** > **Change Password**.
3. Enter the current password and new password.
4. Click **Apply**. Follow the on-screen prompts to change the password.
5. To change the admin password on another appliance, repeat steps 1 through 4.

Changing the Data Store Database Passwords

Use System Configuration to change your Data Store database passwords (dbadmin and readonlyuser). You need to enable SSH temporarily as part of this procedure.

1. Log in to your Manager appliance console (SystemConfig) as root.
2. From the main menu, select **Data Store**.
3. Select **SSH**. Follow the on-screen prompts to enable SSH.
4. Select **Passwords** from the Data Store menu.
5. Follow the on-screen prompts to change the passwords.

   Your previous SSH settings are restored when you exit the Data Store menu.

Changing the Flow Collector Database Password (Non-Data Store Domains)

Use the Database tab on the Central Management page to update your Flow Collector database password for all Flow Collector databases in a Non-Data Store domain.

> ⓘ Make sure you change the default password. When a new Flow Collector is added to Central Management, the database password automatically updates to match the current password.

1. Open Central Management.
2. Click the Database tab.
3. To generate a random password, click the **Generate Password** button, otherwise enter your password in the Password and Confirm Password fields.
4. Check the **Show Password** check box to view your chosen password.
5. Click the **Apply Settings** button to save your changes.

ⓘ When you change a database password, only Non-Data Store Flow Collectors and Transition Flow Collectors will receive the new password.

SSL/TLS Appliance Identity and Additional SSL/TLS Client Identities

Use SSL/TLS Appliance Identity and Additional SSL/TLS Client Identities to manage your Secure Socket Layer (SSL) and Transport Layer Security (TLS) Certificates for the selected appliance. Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide for all certificate-related changes.

> ⚠ Your certificates are critical for your system's security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss. Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide for all certificate-related changes.

Appliance Identity

Each Secure Network Analytics version 7.x appliance is installed with a unique, self-signed appliance identity certificate. To replace the appliance identity certificate, follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

The appliance uses the SSL certificate to verify its identity to other appliances. For example, when a Manager generates a flow query and communicates to a Flow Collector, the Manager is authenticated by presenting its server identity certificate. The Flow Collector checks if this presented server identity certificate is a trusted certificate.

Client Identity

The client identity is used for communication between external services. For details, follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

Reviewing Certificates

Use the following instructions to review the appliance identity certificate or client certificates for the selected appliance.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Select **Edit Appliance Configuration**.
4. Select the **Appliance** tab.
5. **To review the appliance identity certificate,** go to the SSL/TLS Appliance Identity section.

To review the client identity certificates, go to the Additional SSL/TLS Client Identities section.

⚠ Your certificates are critical for your system's security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss. Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide for all certificate-related changes.

Adding Appliances to Central Management with Custom Certificates

Refer to **Adding an Appliance to Central Management** for more information. If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.

⚠ If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.

Changing the Host Name, Network Domain Name, or IP Address

To change the appliance host name, network domain name, or IP address after you've installed and configured your appliances, follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

As part of the procedure, you will remove the appliance from Central Management temporarily, and the appliance identity certificate is replaced automatically.

⚠ The appliance identity certificate is replaced automatically as part of this procedure.

If your appliance uses a custom certificate, please contact Cisco Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.

Reviewing Trust Store Certificates

When you add a certificate to an appliance trust store, you are allowing communication with that identity, whether it is another Secure Network Analytics appliance or an external service.

- **Instructions:** Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide for all trust store changes.
- **Upload Individual Files:** If your file includes more than one certificate, upload each certificate individually to the trust store.

⚠ When you add a certificate to your appliance Trust Store, your appliance trusts that identity and allows communication with it. Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide for all trust store changes.

Use the following instructions to review the certificates saved to the selected appliance Trust Store.

1. Open Central Management.
2. Click the **Actions** menu for the appliance.
3. Select **Edit Appliance Configuration**.
4. Select the **General** tab.
5. Review the **Trust Store** list.

Threat Feed

The Cisco Secure Network Analytics Threat Feed (formerly Stealthwatch Threat Intelligence Feed) provides data from the global Threat Feed about threats to your network. The feed updates frequently and includes IP addresses, port number, protocols, host names, and URLs known to be used for malicious activity. The following host groups are included in the feed: command-and-control servers, bogons, and Tors.

Licensing

Add the Threat Feed License to your Cisco Smart Account. For instructions, refer to the Secure Network Analytics Smart Software Licensing Guide.

Enabling

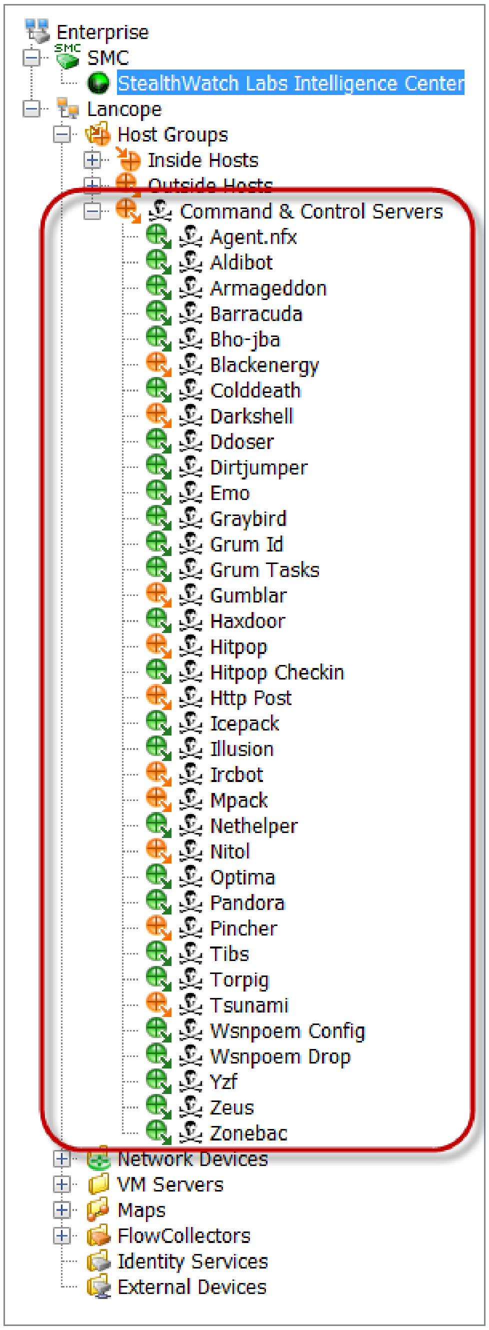
To enable the feed in Central Management, follow the instructions in the help. Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

1. Log in to your primary Manager.
2. Select **Configure > GLOBAL Central Management**.
3. Click the ? **(Help) icon**. Select **Help**.
4. Select **Appliance Configuration** > **Threat Feed**.

Reviewing Alarms and Security Events

When the Threat Feed is enabled, the Stealthwatch Labs Intelligence Center icon is shown in the Desktop Client Enterprise tree with an alarms status, and threats are displayed in their respective host group branches. For more information, refer to the Desktop Client User Guide or the help.

> **Help:** To access the Help, right-click the Stealthwatch **Labs Intelligence Center** branch and select **Configuration > SLIC Threat Feed Configuration**. Click **Help**.



- Enterprise
  - SMC
    - StealthWatch Labs Intelligence Center
  - Lancope
    - Host Groups
      - Inside Hosts
      - Outside Hosts
      - Command & Control Servers
        - Agent.nfx
        - Aldibot
        - Armageddon
        - Barracuda
        - Bho-jba
        - Blackenergy
        - Colddeath
        - Darkshell
        - Ddoser
        - Dirtjumper
        - Emo
        - Graybird
        - Grum Id
        - Grum Tasks
        - Gumblar
        - Haxdoor
        - Hitpop
        - Hitpop Checkin
        - Http Post
        - Icepack
        - Illusion
        - Ircbot
        - Mpack
        - Nethelper
        - Nitol
        - Optima
        - Pandora
        - Pincher
        - Tibs
        - Torpig
        - Tsunami
        - Wsnpoem Config
        - Wsnpoem Drop
        - Yzf
        - Zeus
        - Zonebac
    - Network Devices
    - VM Servers
    - Maps
    - FlowCollectors
    - Identity Services
    - External Devices

Central Management (Managing your Appliances)

Use Central Management to manage your appliances from your primary Manager. We've included an overview of Central Management here, and details for each section are available in Help.

- **About Central Management:** When your appliances are managed by Central Management, you can review their status and manage the following: edit appliance configuration, update software, reboot, shut down, and more.
- **Help:** To open the Help, click the ? (**Help**) icon. Select **Help**.

This section covers the following topics:

- **Central Management and Appliance Administration Interface**
- **Opening Central Management**
- **Opening Appliance Admin**
- **Editing the Appliance Configuration**
- **Viewing Appliance Statistics**
- **Removing an Appliance from Central Management**
- **Adding an Appliance to Central Management**
- **Creating an Appliance Configuration Backup**
- **Enabling/Disabling SSH**

Central Management and Appliance Administration Interface

When an appliance is managed by Central Management, you will access functions for your appliance in Central Management and the Appliance Administration interface (Appliance Admin) as follows:

Central Management	Appliance Admin Interface
Edit appliance configuration	View system statistics
Review license status (overview)	

Back up configuration files	Back up database files
View audit logs	Create diagnostics packs
Reboot	Network Host and IP Lookup
Shut down	Packet Capture
Update software	Clearing the DNS Cache
	Appliance-specific configurations

> If you configure a Flow Collector for Data Store compatibility, the Appliance Administration interface (Appliance Admin) hides certain functionality. Use Central Management to configure the Flow Collector and other related tasks.

Opening Central Management

1. Log in to your primary Manager.
2. Select **Configure > GLOBAL Central Management**.

Opening Appliance Admin

You can access the Appliance Admin interface through Central Management or by logging in to the appliance directly.

Opening Appliance Admin through Central Management

1. On the Central Management Inventory page, click the **Actions** menu for the appliance.
2. Select **View Appliance Statistics**.
3. Log in to the Appliance Administration interface.

Opening Appliance Admin through Direct Login

1. In your browser address bar, type the appliance IP address as follows:

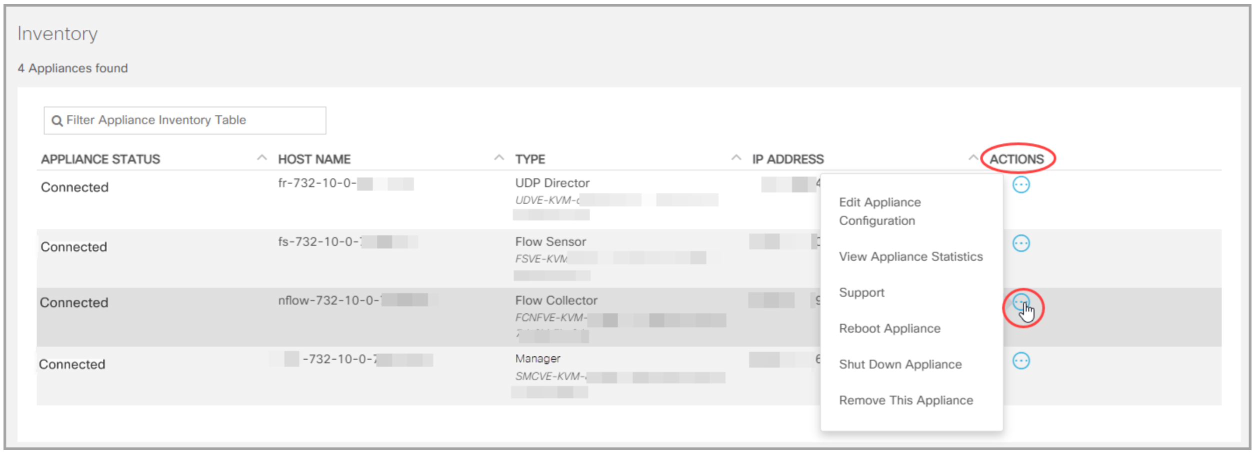
   https://<IPAddress>

- **Manager:** add **/Manager/index.html** after the IP address.
- **For example:** https://1.1.1.1/Manager/index.html

2. Press Enter.

Editing the Appliance Configuration

1. On the Central Management Inventory page, click the **Actions** menu for the appliance.
2. Select **Edit Appliance Configuration**.



Inventory

4 Appliances found

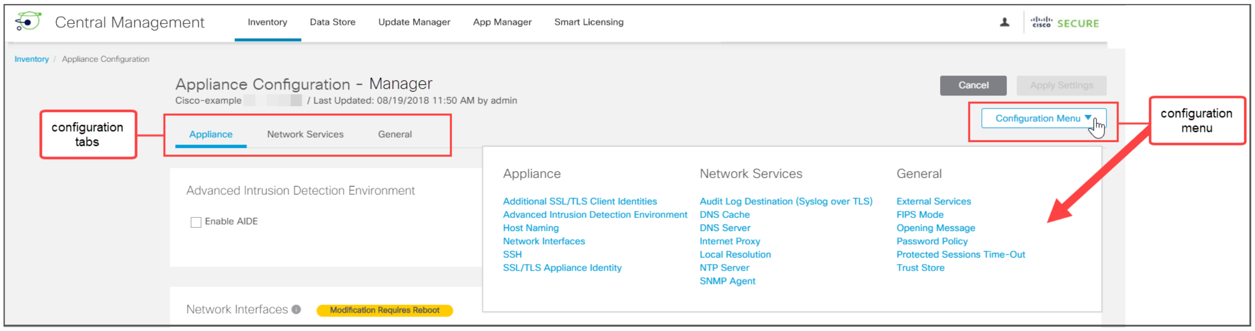
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected	fr-732-10-0-[redacted]	UDP Director UDVE-KVM-[redacted]	[redacted]	⋯
Connected	fs-732-10-0-[redacted]	Flow Sensor FSVE-KVM[redacted]	[redacted]	⋯
Connected	nflow-732-10-0-[redacted]	Flow Collector FCNFVE-KVM-[redacted]	[redacted]	⋯
Connected	[redacted]-732-10-0-[redacted]	Manager SMCVE-KVM-[redacted]	[redacted]	⋯

Filter Appliance Inventory Table
Edit Appliance Configuration
View Appliance Statistics
Support
Reboot Appliance
Shut Down Appliance
Remove This Appliance

3. Click the **Configuration** menu. Select an item from the list.

   or

   Click each tab to review each configuration category.



Appliance Configuration - Manager

Cisco-example [redacted] / Last Updated: 08/19/2018 11:50 AM by admin

Advanced Intrusion Detection Environment

□ Enable AIDE

4. Make changes to each configuration section as needed. You can edit more than one configuration category on each configuration tab.

> ⓘ For instructions, click the **User** icon.

5. Click **Apply Settings**. Follow the on-screen prompts to save your configuration changes.

   Some changes require a system reboot. If you prefer to wait, you can revert your changes and edit your configuration settings and reboot later.

> ⚠ The appliance reboots automatically. Do not force the appliance to reboot while configuration changes are pending. To confirm the appliance status is Connected, review Central Management > Inventory.

6. **Connected:** On the Inventory page, make sure the appliance finishes the configuration changes and the Appliance Status returns to **Connected**.

Viewing Appliance Statistics

Hover: For more information about each appliance status, hover your pointer over the status.

To see system statistics, services, disk usage, and docker services, log in to the Appliance Admin interface:

1. On the Central Management Inventory page, click the **Actions** menu for the appliance.
2. Select **View Appliance Statistics**.
3. Log in to the Appliance Administration interface.

Removing an Appliance from Central Management

Use the following instructions to remove an appliance from your Central Manager.

1. On the Central Management Inventory page, click the **Actions** menu for the appliance.
2. Select **Remove This Appliance**.

   - **Data Store Appliances:** Go to **Removing Data Store Appliances from Central Manager** for additional requirements.
   - **Flow Collectors:** If you removed a Flow Collector from Central Management, it is also removed from the domain. You need to reset the factory defaults (RFD) if you plan to add it to a different domain. Go to **Adding an Appliance to Central Management** and **Removing an Appliance from Central Management** for instructions.

- **Config Channel Down:** If you're removing the appliance because the configuration channel is down, go to the Config Channel Down procedure in Troubleshooting for additional instructions.
- **Troubleshooting:** If you log in to the Appliance Admin interface and the appliance is not removed from Central Management, go to the Config Channel Down procedure in Troubleshooting to remove it using System Configuration.
- **Central Management:** To add the appliance to a different Central Manager, use the Appliance Setup Tool.

⚠ If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.

Removing Data Store Appliances from Central Manager

If you remove Data Store appliances from Central Manager (Manager, Flow Collector, Data Node), it does not remove them from the Data Store itself. This needs to be manually cleaned up.

- **Managers and Flow Collectors:** For Managers and Flow Collectors, you can remove them from the **/lancope/var/services/data-store/config-datastore-inventory-snapshot** directory.
- **Data Nodes:** Contact Cisco Support for assistance with the removal Data Nodes as that process is more complicated.

Adding an Appliance to Central Management

Use the Appliance Setup Tool to add an appliance to Central Management. It is important to review the following:

- **Custom Certificates:** If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to its own Trust Store and the Manager Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.
- **Manager Administration Credentials:** You need the Manager, user ID and password to add an appliance to Central Management.
- **RFD:** If you reset the factory defaults on an appliance, configure the appliance IP address, host name, and domain before you add it to Central Management (even if you preserve network settings when you RFD).

Log in to the appliance console as **sysadmin** and follow the on-screen prompts to configure the IP address, host name, and domain. For instructions, refer to your Secure Network Analytics hardware or Virtual Edition installation guide.

- **New Installations:** If this is a new installation, make sure you complete the installation and configure the IP address, host name, and domain before you add it to Central Management. For instructions, refer to **1. Configuring Your Environment Using First Time Setup**.

> ⚠ If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management. Refer to the SSL/TLS Certificates for Managed Appliances Guide.

1. Log in to the appliance.

   In your browser address bar, type the appliance IP address as follows: **https://<IPAddress>**

2. Replace the end of the URL with /lc-ast:

   https://<IPAddress>/lc-ast

3. Press Enter.
4. Click **Next** to scroll to the Central Management tab.
5. **IP Address:** Enter the Manager/Central Manager IP address.
6. Click **Save**.
7. Follow the on-screen prompts to enter the Manager administration credentials and finish the configuration. Depending on the type of appliance, you may need to enter additional information.
8. For more information about the Appliance Setup Tool, refer to **2. Configuring the Managed System**

Creating an Appliance Configuration Backup

Use Central Management to back up an appliance configuration.

> ⓘ Before you back up an appliance, make sure you follow the instructions in the Help. To back up a Data Store, refer to **Creating a Data Store Backup**. To back up a Flow Collector database, refer to **Creating a Database Backup (Non-Data Store Domains)**.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Select **Support**.
4. Select the **Configuration Files** tab.
5. Select the ? (**Help**) icon. Follow the instructions in the Help.

   To restore an appliance configuration backup, follow the instructions in the Help.

Enabling/Disabling SSH

Use this section to control the ability to access the appliance using SSH (secure shell).

Default: disabled

> ⚠ When SSH is enabled, the system's risk of compromise increases. It is important to enable SSH only when you need it. When you are finished using SSH, disable it.

Open SSH

Use the following instructions to open SSH for a selected appliance.

1. Open Central Management.
2. Click the **Actions** menu for the appliance.
3. Select **Edit Appliance Configuration**.
4. Select the **Appliance** tab.

Enable SSH

1. Locate the SSH section.
2. To allow SSH access on the appliance, check the **Enable SSH** check box.

3. To allow root access on the appliance, check the **Enable Root SSH Access** check box.
4. Click **Apply Settings**.
5. Follow the on-screen prompts.

Disable SSH

1. To remove SSH access on the appliance, click the **Enable SSH** check box to clear it.
2. To remove root access on the appliance, click the **Enable Root SSH Access** check box to clear it.
3. Click **Apply Settings**.
4. Follow the on-screen prompts.

Creating a Database Backup (Non-Data Store Domains)

Use the following instructions to back up your Manager and Flow Collector databases. To back up the Data Store, refer to **Creating a Data Store Backup**.

> ⚠ Without a backup, you will not be able to recover your files if a problem occurs during the update process. Make sure you follow the instructions and complete all procedures for the database backup. Also note that this procedure only applies to Non-Data Store Flow Collectors. For assistance, contact Cisco Support.

This process involves completing the following procedures:

1. Trim the Flow Collector Database

2. Delete the Database Snapshots

3. Back Up to Remote File System

4. Delete the Database Snapshots

1. Trim the Flow Collector Database

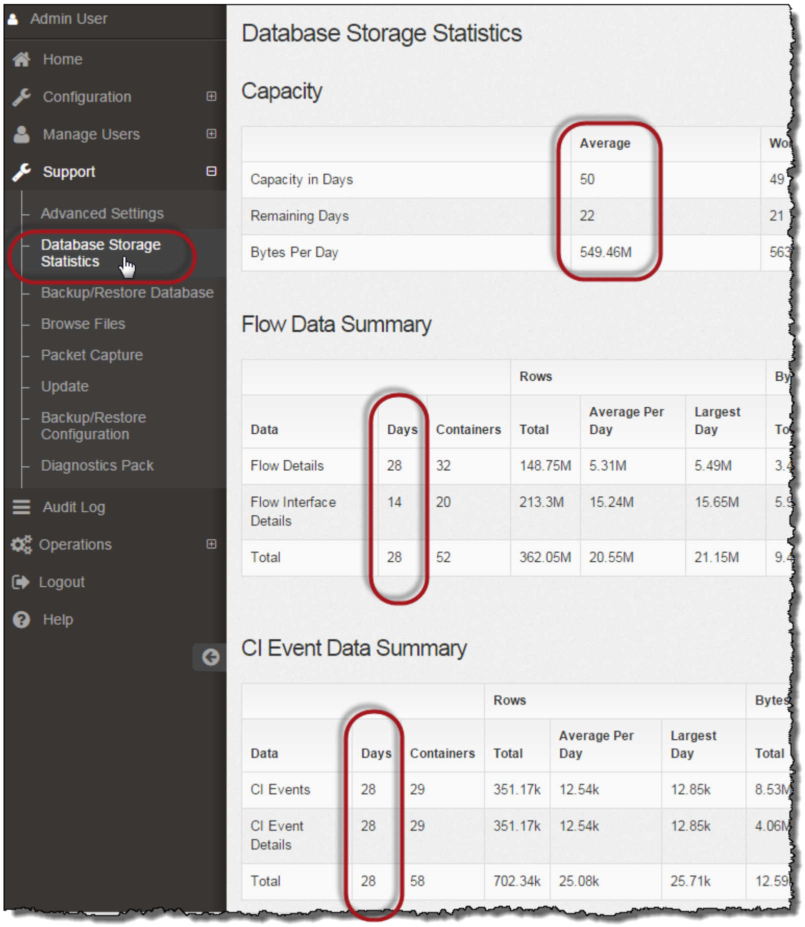
The Flow Collector database backup can take multiple days to finish and will slow your network speed if the database is large. Before you back up your databases, we recommend trimming the Flow Collector database. This will free the available disk space for storing flows and reduce the amount of time it takes to back up the database.

The Flow Collector stores the maximum number of days based on the disk space and the amount of data collected per day. When the maximum (75% of the /lancope/var partition) is hit, the database will start to delete the oldest data first to allow new data to come in.

1. Review your Database Storage Statistics

Use the following instructions to check your database storage.

1. Log in to the Flow Collector Appliance Admin interface.
2. Select **Support** > **Database Storage Statistics**.
3. Review the days stored in Capacity, Flow Data Summary, and CI Event Data Summary (or Security Event Data Summary).



Database Storage Statistics

Capacity

	Average	Wo
Capacity in Days	50	49
Remaining Days	22	21
Bytes Per Day	549.46M	563

Flow Data Summary

			Rows			By
Data	Days	Containers	Total	Average Per Day	Largest Day	To
Flow Details	28	32	148.75M	5.31M	5.49M	3.4
Flow Interface Details	14	20	213.3M	15.24M	15.65M	5.5
Total	28	52	362.05M	20.55M	21.15M	9.4

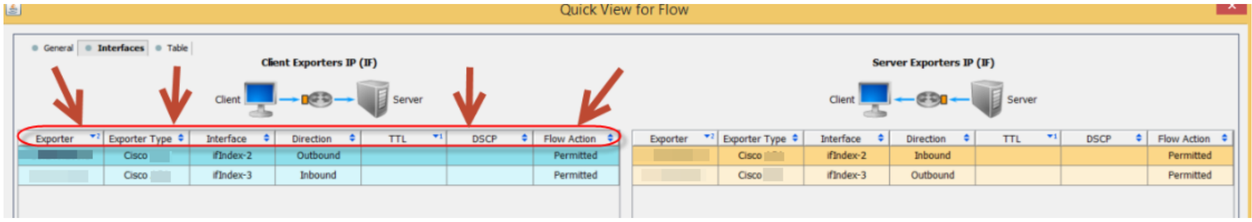
CI Event Data Summary

			Rows			Bytes
Data	Days	Containers	Total	Average Per Day	Largest Day	Total
CI Events	28	29	351.17k	12.54k	12.85k	8.53M
CI Event Details	28	29	351.17k	12.54k	12.85k	4.06M
Total	28	58	702.34k	25.08k	25.71k	12.59

2. Trim the Interface Details

The Flow Interface Data is the data related to the interfaces of exporters. Secure Network Analytics saves flow interface data and flow data.

The Flow Interface default setting causes the system to push out the flow data, so it can keep all the interface statistics it can. This function uses the Desktop Client as a main tool which does not apply to Data Store systems. A node may be needed to indicate that the trimming procedure only applies to Non-Data Store systems.



Client Exporters IP (IF)

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
[redacted]	Cisco [redacted]	ifIndex-2	Outbound			Permitted
[redacted]	Cisco [redacted]	ifIndex-3	Inbound			Permitted

Server Exporters IP (IF)

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
[redacted]	Cisco [redacted]	ifIndex-2	Inbound			Permitted
[redacted]	Cisco [redacted]	ifIndex-3	Outbound			Permitted

Backing up this data takes time. If you don't need all of it, shorten the storage limit (for example: 7 days). Any data older than the limit will be lost.

Use the following instructions to purge the database of the interface statistics data older than the limit you set, so you can free up the available disk space for storing flows.

1. Log in to Desktop Client as the admin user.
2. Locate the Flow Collector in the Enterprise Tree. Click the plus (**+**) sign to expand the container.
3. Right-click the Flow Collector. Select **Configuration** > **Properties**.
4. In the Flow Collector Properties dialog box, click **Advanced**.
5. Select the **Store flow interface data**.
6. Shorten the storage limit. For example, if you set the limit to **Up to 7 days**, anything older than 7 days will be lost.
7. Click **OK**.
8. Wait 5 minutes to proceed to the next steps.

3. Trim Flow Details and CI Event Data

To reduce the size of the Flow Details and CI Event/Details in the Flow Collector database, contact Cisco Support. This step is optional, and the trimming process takes only a few minutes to complete, but the process requires guidance.

When you trim the NetFlow, you will specify the number of days to keep Flow Details & CI Event/Details in the Flow Collector database. Two things will occur with this configuration:

- The database is trimmed down to the number of days you enter.
- The database starts rolling the older data out based on the oldest day but without trying to save as much as possible.

2. Delete the Database Snapshots

Before you create backup files, make sure you delete any saved snapshots on the Manager and Flow Collector databases using the following instructions.

> ⚠ Make sure you delete the Manager and Flow Collector database snapshots. This step is critical for a successful backup.

1. Log in to the Manager and Flow Collector appliance database console as **admin.**
2. **Check for Snapshots:** Type:

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from
database_snapshots;"
```

3. **Delete Snapshots (if they exist):** Type:

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. **Wait until the snapshot folder is removed:** Check:

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   If the results are not empty, continue to wait. You may need to wait several minutes until the folder is removed, depending on the size of the database.

5. Repeat steps 1 through 4 to delete all saved Manager and Flow Collector database snapshots.

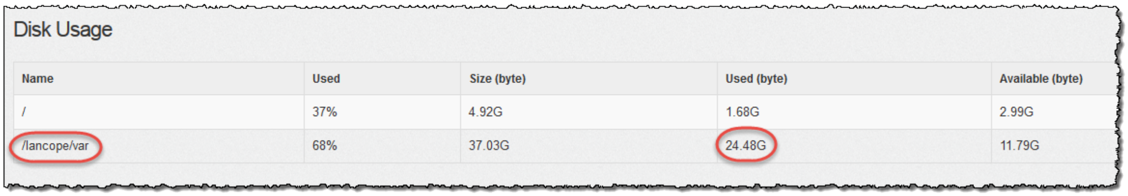
3. Back Up to Remote File System

To back up a database to a remote file system, complete the following steps:

- **Space:** Make sure the remote file system has enough space to store the database backup.
- **Time:** After you back up the database once, subsequent backups will be quicker because the process backs up only what has changed since the last backup. This process backs up approximately 0.5 GB to 2 GB of data per minute.

1. Return to the Appliance Admin interface (but do not close the Desktop Client).
2. Determine how much space you will need on the remote file system to store the database backup as follows:

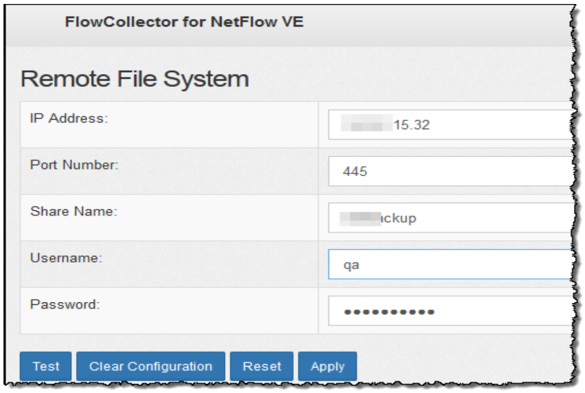
   - Click **Home**.
   - Locate the **Disk Usage** section.
   - Review the **Used (byte)** column for the **/lancope/var** file system. You will need at least this much space plus 15% more on the remote file system to store the database backup.



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G

3. Click **Configuration** > **Remote File System.**


FlowCollector for NetFlow VE

Remote File System

IP Address:	[redacted]15.32
Port Number:	445
Share Name:	[redacted]ckup
Username:	qa
Password:	●●●●●●●●●●●

4. Complete the fields using the settings for the remote file system where you want to store the backup files.

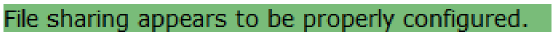
   The file share uses the CIFS (Common Internet File System) protocol, also known as SMB (Server Message Block).

5. Click **Apply** to place the settings in the configuration file.

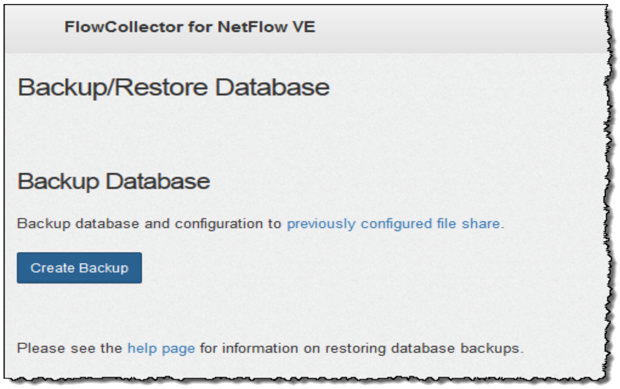
   If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

6. Click **Test** to verify that the appliance and the remote file system can communicate with each other.

   You should see the following message at the bottom of the Remote File System page when the test is complete.


File sharing appears to be properly configured.

7. Click **Support** > **Backup/Restore Database**. The Backup Database page opens as shown in the following example.



FlowCollector for NetFlow VE

Backup/Restore Database

Backup Database

Backup database and configuration to previously configured file share.

Please see the help page for information on restoring database backups.

8. Click **Create Backup**. This process may take a long time.

    - After the backup process starts, you can mouse away from the page without interrupting the process. However, if you click **Cancel** while the backup is in progress, you may not be able to resume the backup without restarting the appliance.
    - Follow the on-screen prompts until the backup is completed.
    - To view details of the backup process, click **View Log**.

9. Click **Close** to close the progress window.

> If you cancel the backup before it finishes, make sure you delete the database snapshots again. See **4. Delete the Database Snapshots** for detailed instructions.

4. Delete the Database Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots on the Manager and Flow Collector databases.

> ⚠ Make sure you delete the Manager and Flow Collector database snapshots. This step is critical for a successful update.

1. Log in to the Manager or Flow Collector appliance database console as **admin**.
2. **Check for Snapshots:** Type:

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from
database_snapshots;"
```

3. **Delete Snapshots (if they exist):** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_
   database_snapshot('StealthWatchSnap1');"
   ```

4. **Wait until the snapshot folder is removed:** Check:

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   If the results are not empty, continue to wait. You may need to wait several minutes until the folder is removed, depending on the size of the database.

5. Repeat steps 1 through 4 to delete all saved Manager and Flow Collector database snapshots.

Restoring a Database Backup (Non-Data Store Domains)

Use the following instructions to restore your Manager and Flow Collector databases. To restore the Data Store, refer to **Restoring a Data Store Backup**.

Overview

⚠ We recommend that you contact Cisco Support before restoring a database.

The Restore Database operation will **overwrite** your current database and configuration with the contents of the previous backup. Existing network settings are not overwritten.

- **Same Version:** You cannot use a backup file from a previous version of the Secure Network Analytics appliance to restore an appliance database. Make sure the backup file version matches the appliance version.
- **Restore Previous Backup:** You can use a command line interface to restore a previous backup of the database. The database that is backed up is the database that exists in the previously configured remote file system (the file share).
- **Default:** If you do not specify the name of the database to be restored, the default name (your system's serial number) will be used.

Restore a Database

⚠ The Restore Database operation will overwrite your current database and configuration with the contents of the previous backup. Existing network settings are not overwritten.

Do not interrupt the restoration process after it has begun.

After the operation has started, you can leave the page ("mouse away"), and the process will continue without interruption. When you return, the status will be updated.

1. Log into the appliance console as sysadmin to access the root shell.
2. Type **sysadmin** and then press **Enter**.
3. When the password prompt appears, type **lan1cope** and then press **Enter**.
4. On the System Configuration menu, select **Advanced** and the press **Enter**.
5. Select **Root Shell** and then press **Enter**.

6. Type the root shell password and then press **Enter**.
7. Run the following command:

   ```
   cd /var/tmp
   nohup doDbRestore -c -q &
   ```

   To see the switches that are available with this tool, enter this command:

   ```
   doDbRestore -h
   ```

> ⚠ If you do not specify the name of the database to be restored, the default name (your system's serial number) will be used.

8. To check the status of a restore operation that is in progress, you can display two files:

   /lancope/var/logs/VerticaRestore.log

   /lancope/var/logs/DatabaseRestore.log

   After the system completes the restore operation, it will reboot and then begin collecting data.

Data Store Database

If you've configured Secure Network Analytics with a Data Store, you can access the Data Store tab in Central Management.

> ⓘ To add Data Store to your configuration, refer to **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors** and **Adding Data Store to a Non-Data Store Deployment**.

Data Store Tab

Use the Data Store tab in Central Management to:

- **Status:** View the status of your database or any Data Node. For details, refer to **Viewing the Data Store Database Status**.
- **Start or Stop:** You can also start or stop the database or any Data Node. For details, refer to **Viewing the Data Store Database Status**.
- **Storage Usage:** View the current storage usage statistics for your database. You can also modify retention status for flow interface data. For details, refer to **Viewing Database Retention**.
- **Update Status:** View the status of all Data Nodes during updates. For details, refer to **Monitoring the Data Node Update Status**.

> ⓘ Be sure to enable SSH on all Data Nodes. If SSH is not enabled on all Data Nodes, some database actions will not be able to complete successfully.

Opening the Data Store Tab

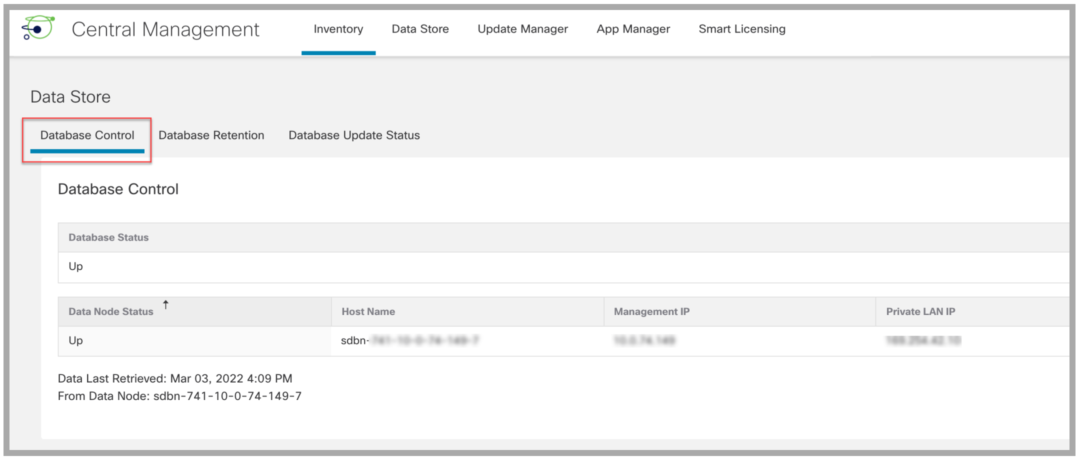
1. Log in to your Manager.
2. Select **Configure > GLOBAL Central Management**.
3. Click the **Data Store** tab.

Viewing the Data Store Database Status

The Database Control page opens when you click the Data Store tab in Central Management. This tab displays the status of the database and each Data Node.

- **Sorting:** The Data Nodes on this tab are sorted by their Private LAN IPs by default. You can re-sort the Data Nodes nodes by clicking the column header by which you want to sort.

- **Status:** Under normal conditions, your database and all Data Nodes will show a status of **Up**. Your database may be Up but the status of one of your Data Nodes could be Down. After recovering a failed Data Node, you may see your database showing as Up but your newly recovered Data Node will be in a "recovering” state.
- **Actions Menu:** Make sure you use the Actions menu to start or stop your database (or a Data Node).



Database Control

Database Status
Up

Data Node Status ↑	Host Name	Management IP	Private LAN IP
Up	sdbn-[redacted]	[redacted]	[redacted]

Data Last Retrieved: Mar 03, 2022 4:09 PM
From Data Node: sdbn-741-10-0-74-149-7

> Make sure you use the Actions menu to start or stop your database (or a Data Node).

Starting the Database

1. Ensure that the Database Control tab is selected.
2. Click the ••• (**Ellipsis**) icon in the Actions column for the database.
3. Select **Start**.
4. Confirm the database status is shown as Up.

Stopping the Database

1. Ensure that the Database Control tab is selected.
2. Click the ••• (**Ellipsis**) icon in the Actions column for the database.
3. Select **Stop**.
4. Confirm the database status is shown as Down.

Starting a Data Node

Follow the steps below to start a Data Node.

1. Ensure that the Database Control tab is selected.
2. Find the Data Node you want to start. Click the ••• (**Ellipsis**) icon in the Actions column.
3. Select **Start** to start the Data Node.
4. Confirm the Data Node status is shown as Up.

Stopping a Data Node

Follow the steps below to stop a Data Node.

1. Ensure that the Database Control tab is selected.
2. Find the Data Node you want to stop. Click the ••• (**Ellipsis**) icon in the Actions column.
3. Select **Stop** to stop the Data Node.
4. Confirm the Data Node status is shown as Down.

Reviewing Last Action Results

Only one action may be in progress at any time regardless of the number of users. When an action is in progress, no other actions can be taken. Once an action has completed, the completion status will be displayed for all users in a banner at the top of the screen. Follow the steps below to review last action results.

1. Ensure that the Database Control tab is selected.
2. Click the **Last Action Results** link at the bottom of the screen. The Action Results banner will remain on screen until you dismiss it.

Viewing Database Retention

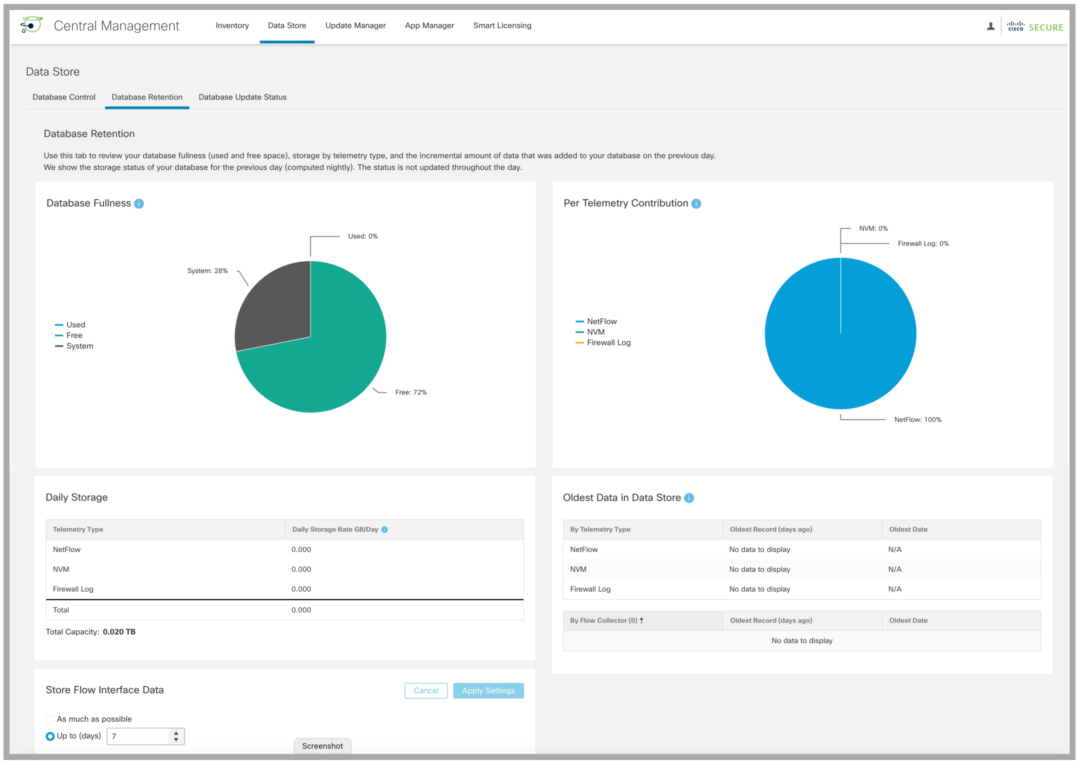
The Database Retention tab answers questions such as:

- How full is my database?
- How much is each telemetry type (NetFlow, NVM, firewall log) contributing to this fullness?
- How much data was newly stored in my database yesterday?
- What is the total capacity of my database?

> ⓘ All of the charts as well as the Data Storage Statistics section on this page are updated once per day.

Opening the Data Store - Database Retention Tab

1. Select **Configure > GLOBAL Central Management**.
2. Click the **Data Store** tab.
3. Click the **Database Retention** tab.



Database Retention

Use this tab to review your database fullness (used and free space), storage by telemetry type, and the incremental amount of data that was added to your database on the previous day.
We show the storage status of your database for the previous day (computed nightly). The status is not updated throughout the day.

Daily Storage

Telemetry Type	Daily Storage Rate GB/Day
NetFlow	0.000
NVM	0.000
Firewall Log	0.000
Total	0.000

Total Capacity: **0.020 TB**

Oldest Data in Data Store

By Telemetry Type	Oldest Record (days ago)	Oldest Date
NetFlow	No data to display	N/A
NVM	No data to display	N/A
Firewall Log	No data to display	N/A

By Flow Collector (0) ↑	Oldest Record (days ago)	Oldest Date
	No data to display	

Store Flow Interface Data

○ As much as possible
● Up to (days) 7

Database Fullness Chart

The Database Fullness chart displays the amount of used and free space that exists in your Data Store database.

Per Telemetry Contribution Chart

The Per Telemetry Contribution chart displays a breakdown of the data that exists in your Data Store database.

Daily Storage

The Daily Storage section displays the incremental amount of data that was added to your database on the previous day. By monitoring your daily storage rate, you can evaluate how quickly your database is filling as well as how much each telemetry type is contributing to your daily storage accumulation.

Oldest Data in Data Store

This table shows the date and number of days since the oldest record was written to the Data Store. This data is updated once per day.

Data stored locally in a Flow Collector (or Flow Collector database) is not included in this table. If you are transitioning a Non-Data Store Flow Collector to a Data Store Flow Collector and have a data retention policy, you can use this table to understand how much new data is in your Data Store and to know when it is an ideal time to complete your transition.

Changing the Flow Interface Data Storage

Flow interface statistics provide a more detailed view of flow statistics. They are useful for troubleshooting and investigating recent flow data by providing multiple vantage points in the network for a given flow. For example, if a flow is observed on multiple exporters or multiple interfaces of the same exporter, the details are stored in flow interface statistics.

The Data Store retains data for as long as possible, and the amount of retention time is determined by your system's ingest rate. Once the Data Store reaches full capacity, it starts deleting the oldest data automatically.

Flow interface statistics consume storage at a higher rate, potentially reducing the time you can retain other important data (such as flow statistics).

> ⓘ Changing the flow interface data storage period here only impacts the NetFlow portion of the data that is occupying space in your system. The default is 7 days. You can increase or decrease the retention days as needed.

1. In the Store Flow Interface Data section, choose **As much as possible** or **Up to days** (click the up or down arrows to change the number of days).
2. Click **Apply Settings**.

    - When you change the retention to a longer period, wait for the difference of time to expire before the data being stored corresponds exactly to the retention settings. Until that time, the data is displayed using the most reduced (coarsest) resolution available. For example, if you change the retention from 3 days to 10 days, then you need to wait 7 days before the data being stored corresponds exactly to the retention settings.
    - Your data may be deleted sooner than the retention period you select, due to critical trimming of data according to disk usage. If you choose to store data as long as possible, when the Data Store reaches full capacity, the system starts deleting the oldest data.

Monitoring the Data Node Update Status

After initiating an update of your Data Nodes from your Central Management Update Manager, use the Database Update Status tab to monitor the progress of the database services update on each Data Node.

Opening the Data Store - Database Update Status Tab

1. Select **Configure > GLOBAL Central Management**.
2. Click the **Data Store** tab.
3. Click the **Database Update Status** tab.

Monitoring the Database Update Status

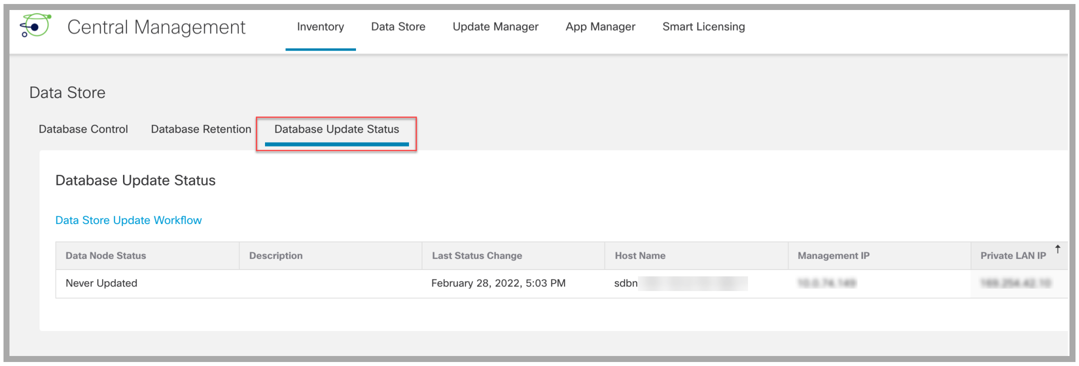
Each Data Node progresses through a series of states during an update. Click the Data Store Update Workflow link to see a visual representation of the update process (shown below).

> For a successful update, follow the update order and instructions in the Cisco Secure Network Analytics System Update Guide.

> Some of the state transitions shown in the image below happen very quickly during the update process so you may not see them occur during a screen refresh.

The Database Update Status tab shows the current update status for your Data Nodes. After you start a software update (upgrade or patch) in Update Manager, use this Database Update tab to monitor the status of each Data Node to confirm it completes the update. To see visual representation of the update workflow, click **View Diagram**.

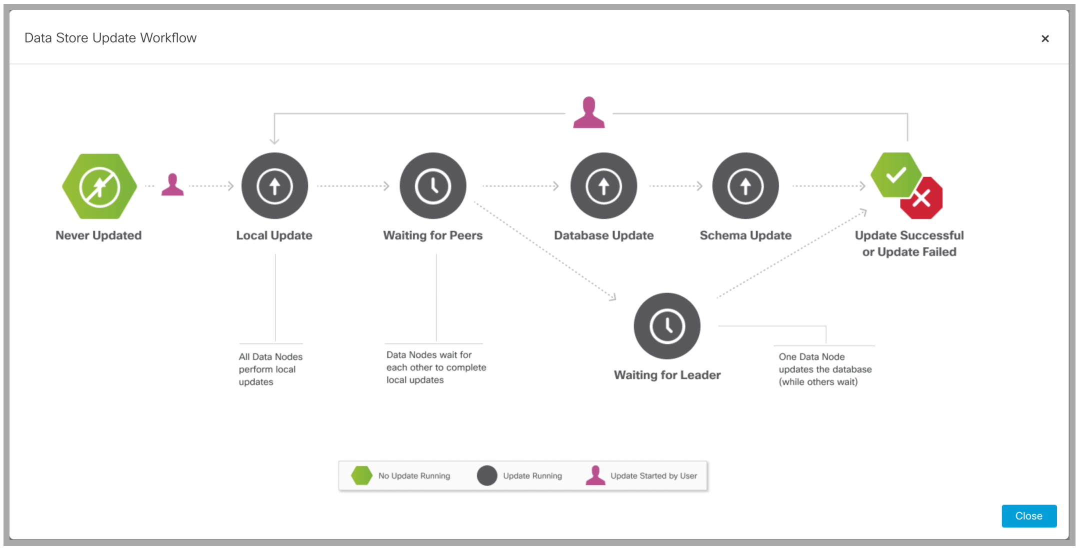
After the update is completed, go to the **Data Store Database** to confirm your database status is Up. For more information, refer to the Update Guide.



Database Update Status

Data Node Status	Description	Last Status Change	Host Name	Management IP	Private LAN IP
Never Updated		February 28, 2022, 5:03 PM	sdbn[redacted]	[redacted]	[redacted]

The following image shows the Data Store update workflow.



Data Store Update Workflow

All Data Nodes perform local updates

Data Nodes wait for each other to complete local updates

One Data Node updates the database (while others wait)

Creating a Data Store Backup

> ⓘ Contact Cisco Professional Services for assistance with planning and implementing these tasks.

> ⓘ Be sure to read and follow the instructions for installing the *update-dnode-ROLLUP20231018-7.4.2- v2-01.swu* Data Store Update Patch on your Data Node before you begin the backup procedures.

To backup your Data Store, complete the following procedures:

1. Estimate Backup Host Storage Requirements

2. Prepare a Backup Host with twice the storage capacity of the backup size. Install Python v3.7 and rsync v3.0.5 on the backup host.

> ⓘ Use a Linux-based host separate from your Secure Network Analytics appliances.

3. Enable Passwordless SSH Access for dbadmin. Make sure all Data Nodes can reach the backup host using passwordless SSH access.

4. Initialize the Backup Directory on the Backup Host

5. Back Up the Data Store Database

1. Estimate Backup Host Storage Requirements

1. Log in to your Data Node console as `root`.
2. Copy the following command, paste it into the command line, and press Enter to connect to the database using vsql and execute the query. Enter your password when prompted. Note the results.

```
/opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_bytes)
FROM storage_containers;"
```

3. Multiply the sum by 2 to estimate how much storage space your backup host needs.

2. Prepare a Backup Host

1. Based on the storage requirements you estimated in **1. Estimate Backup Host Storage Requirements**, identify a host running Linux on your network to store the backup, or deploy a host running Linux with the necessary storage requirements.

> ⓘ Use a Linux-based host separate from your Secure Network Analytics appliances.

2. Log into the backup host console as `root`.
3. From the command prompt, enter `python3 --version` and press Enter to see what version of Python you have installed. You have the following options:
    - If Python 3.7 or later is installed, go to step 6.
    - Otherwise, install Python 3.7, beginning with step 4.
4. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including Python. Enter your password when prompted.
5. Enter `sudo apt-get install python 3.7` and press Enter to install Python 3.7 (modify the command to install a different version).
6. From the command prompt, enter `rsync --version` and press Enter to see what version of rsync you have installed. You have the following options:
    - If rsync 3.0.5 or later is installed, continue to step 9.
    - Otherwise, install rsync 3.0.5. Continue to step 7.
7. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including rsync. Enter your password when prompted.
8. Enter `sudo apt-get install rsync` and press Enter to install rsync.
9. From the command prompt, enter `getent passwd | grep dbadmin` and press Enter to determine if a `dbadmin` user account exists on this host. You have the following options:
    - If a `dbadmin` user account exists, the backup host is ready. Continue to **3. Enable Passwordless SSH Access for dbadmin**.
    - Otherwise, create a `dbadmin` user account on this host. Continue to step 10.
10. From the command prompt, enter `adduser dbadmin` and press Enter to create a `dbadmin` user account.
11. Enter `passwd dbadmin` and press Enter to assign a password to `dbadmin`.
12. Enter a **New password** and press Enter to set the `dbadmin` password. Confirm the password when prompted.

3. Enable Passwordless SSH Access for dbadmin

1. Open port 22/TCP between the backup host and each Data Node for SSH, and port 50000/TCP between the backup host and each Data Node for rsync.
2. Review the OpenSSH documentation on `ssh-copy-id dbadmin@<hostname>` for more information.
3. Log into the first Data Node as `dbadmin` by typing the following:

   ```
   su dbadmin
   ```

4. Copy the following command and paste it into a plaintext editor:

   `ssh-copy-id dbadmin@[hostname]` where `[hostname]` is the backup host's hostname or IP address.

5. Copy the updated command, paste it into the command prompt, and press Enter to copy the `dbadmin` SSH authorized key to the backup host.
6. Copy the following command and paste it into a plaintext editor:

   `ssh 'dbadmin@[hostname]'` where `[hostname]` is the backup host's hostname or IP address.

7. Copy the updated command, paste it into the command prompt, and press Enter to verify that you can log into the remote host's console over SSH without needing a password from this Data Node.

4. Initialize the Backup Directory on the Backup Host

1. Log in to the first Data Node console as `root`.

> ⓘ Note the Data Node you use to initialize the backup directory. You will use the same Data Node to back up the Data Store database in a later procedure (**5. Back Up the Data Store Database**).

2. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
3. Enter `ssh [backup-host]` where [backup host] is the hostname or ip address of your backup server. You should be able to log into the backup host's interface as `dbadmin` without being prompted for a password. If the backup host prompts you for a password, check your settings.
4. Enter `cd /home/dbadmin` and press Enter to change directories.
5. Enter `mkdir backups` and press Enter to create the `backups` directory.
6. Enter `exit` and press Enter to return to the Data Node's command line prompt.

7. Enter `vi pw.ini` and press Enter to create the `pw.ini` backup password file, and edit it.

> If you updated the dbadmin password using the setup-sw-datastore-secure-connectivity script, you must also update the password stored in the pw.ini backup password file, or your backup fails.

8. Copy the following lines to a plaintext editor:

   ```
   [Passwords]
   dbPassword = [dbadmin-password]
   ```

9. Update `[dbadmin-password]` to the Data Store `dbadmin` password.
10. Copy the updated lines and paste them into the `pw.ini` backup password file.
11. Press Esc, then enter `:wq`, then press Enter to exit and save your changes.
12. Enter `chmod 640 pw.ini` and press Enter to change the `pw.ini` file permissions to allow the `dbadmin` user to read and edit the file.
13. Copy the following lines and paste them into a plaintext editor:

    ```
    [Mapping]
    v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
    v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
    v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

    [Misc]
    snapshotName = data_store_backup
    passwordFile = /home/dbadmin/pw.ini
    enableFreeSpaceCheck = True
    retryCount = 2
    retryDelay = 1

    [Transmission]
    encrypt = true
    checksum = true
    concurrency_backup = 2
    concurrency_restore = 2
    ```

14. Enter `vi config.ini` and press Enter to create the `config.ini` backup configuration file and edit it.
15. Copy the text you pasted into a plaintext editor in step 15 and paste it into your `config.ini` file.
16. Replace *`backup-host-ip`* with the backup host's IP address.

17. If the host names under `[Mapping]` do not match your Data Nodes, update these host names. To determine your Data Node node names, do the following:

    - Connect to any Data Node console as `root`
        - Enter `su dbadmin`
        - Enter `admintools -t node_map`
    - Use the node names in the “NODENAME” column for the `[Mapping]` entries

    Example:

    ```
    dbadmin@sdbn-742-10-0-56-133-5:/root$ admintools -t node_map
    DATABASE   | NODENAME               | HOSTNAME
    --------------------------------------------------------
    sw         | v_sw_node0001          | 169.254.42.10
    sw         | v_sw_node0002          | 169.254.42.12
    sw         | v_sw_node0003          | 169.254.42.15
    ```

18. Ensure that you have an entry for each Data Node if you deployed more than three to your environment. If you have only a single Data Node, remove the extra `[Mapping]` lines leaving only the one line for your single Data Node.
19. Press Esc, then enter `:wq`, then press Enter to exit and save your changes.
20. Enter `vbr -t init -c config.ini` and press Enter to initialize the `/home/dbadmin/backups` directory on the backup host to receive Data Store backups.

5. Back Up the Data Store Database

> ⓘ You will only need to issue the backup command on one Data Node in order to back up your entire multi-node database.

1. As `root`, log into the console of the Data Node where you initialized the backup host directory in **4. Initialize the Backup Directory on the Backup Host**.
2. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
3. Enter `vbr -t backup -c config.ini --debug 3 --dry-run` and press Enter to perform a test of the backup without creating the backup. You have these options:

   - If the backup test resolves successfully, back up the Data Store and continue to step 4.
   - If the backup test fails, a snapshot file may have been created and must be removed. See Data Store Backup Failure for removal instructions. If the backup test fails to resolve, review the debug log files in the `/tmp/vbr` directory, resolve the root cause, then test the backup again. Contact Cisco Support for more assistance.

4. Enter `vbr -t backup -c config.ini` and press Enter to backup the Data Store to the `/home/dbadmin/backups` directory on the backup host.

Data Store Backup Failure

If your Data Store backup fails, make sure to remove the database snapshot before attempting another backup. Follow these steps to remove the Data Store database snapshot.

1. Connect to your Data Store database cluster using **`vsql`**.
2. Execute the following command to retrieve a list of your snapshots:

   ```
   select * from database_snapshots;
   ```

3. Replace ‘snapshot_name’ with the name of the snapshot that you want to remove, then execute the following command:

   ```
   select remove_database_snapshot('snapshot_name');
   ```

4. Execute the following command to exit.

   ```
   \q
   ```

Restoring a Data Store Backup

> ⓘ Contact Cisco Professional Services for assistance with planning and implementing these tasks.

To backup your Data Store, complete the following procedures:

1. Review the Backup Names and Software Versions

2. Stop the Data Store Database

3. Restore the Data Store from a Backup

4. Start the Data Store

5. Remove the Catalog Snapshot

6. Review the Restored Database

> ⓘ You can only restore a Data Store backup to the same Data Store that you took the backup from. You cannot take a backup from one Data Store and restore it to another Data Store. When creating a Data Store backup, use any Data Node to issue the backup command. When restoring a Data Store backup, use any Data Node to issue the restore command (it does not need to be the same Data Node you used to create the backup).

1. Review the Backup Names and Software Versions

1. Confirm the Data Store database backup and the Data Store have identical Data Node names and the same number of Data Nodes.
2. Confirm the Data Store database backup and the Data Store have the same version of Secure Network Analytics installed.

> ⓘ We do not support restoring a database to a version that is different from the backup version.

2. Stop the Data Store Database

1. Log in to your Manager.
2. Select **Configure > GLOBAL Central Management**.
3. Click the **Data Store** tab.
4. Locate the Database.

5. Click the ••• (**Ellipsis**) icon in the Actions column.
6. Select **Stop**.
7. Keep the Data Store Database Control tab open. You will use it in a later procedure.

3. Restore the Data Store from a Backup

> Make sure you run the following commands before and after the database is restored, for comparison:
>
> ```
> /opt/vertica/bin/vsql -U dbadmin -w <'password'> -c "select*
> from partitions;" >/lancope/var/tcpdump/partitions-full-
> DBbackup
> ```

1. If you updated the `dbadmin` password using the `setup-sw-datastore-secure-connectivity` script, you must also update the password stored in the `pw.ini` backup password file, or your restore fails.
2. Identify the Data Node on which you stored the `config.ini` backup configuration file, and log into its console as `root`. Refer to **4. Initialize the Backup Directory on the Backup Host** for details.
3. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
4. From the command prompt, enter `vbr --task restore --config-file config.ini` and press Enter to restore the Data Store from the backup host.

> You will only need to issue the restore command on one Data Node in order to restore your entire multi-node database.

4. Start the Data Store

1. Return to the Data Store Database Control Tab in Central Management.
2. Locate the Database.
3. Click the ••• (**Ellipsis**) icon in the Actions column.
4. Select **Start**.

5. Remove the Catalog Snapshot

After you restart the Data Store, remove the snapshot named `catalog`. This snapshot is not required after the restore resolves, and it prevents Vertica from running retention management.

1. Log in to your Data Node console as `root`.
2. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
3. Type the following command, replacing `[password]` with your `dbadmin` password, and then press Enter. This will remove the `catalog` snapshot.

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select
   remove_database_snapshot('catalog');"
   ```

6. Review the Restored Database

Make sure you run the following commands before and after the database is restored, for comparison:

```
/opt/vertica/bin/vsql -U dbadmin -w <password> -c "select*
from partitions;" >/lancope/var/tcpdump/partitions-full-
DBbackup
```

Data Store Maintenance

This section includes the following Data Store topics:

- **Enabling Data Compression in the Data Store**
- **Adding a Data Store Domain**
- **Adding a Secondary Manager or Flow Collectors after the Data Store is Initialized**
- **Adding Data Nodes to the Data Store**
- **Replacing a Data Node (Hardware Only)**

> ⓘ Make sure you review the procedure before you start. Some of the procedures include contacting Cisco Support for assistance.

Enabling Data Compression in the Data Store

Data compression is enabled by default on new installations for Flow Collectors that are configured with Data Store. You can use it to reduce bandwidth usage between a Flow Collector and the Data Store. It is especially helpful in scenarios where the network bandwidth from a Flow Collector to the Data Store is limited.

By enabling compression, you may reduce this bandwidth by up to 90%. If Data Compression is disabled, it can be enabled on a per Flow Collector basis. Make the following configuration changes in the Flow Collector interface to enable compression of data sent to the Data Store.

1. Log in to the Flow Collector Appliance Admin interface.
2. Click **Support > Advanced Settings**.
3. In the ingest_enable_compression field, enter one of the following
    - 1 - Enable data compression
    - 0 - Disable data compression
4. Click **Apply** and then click **OK** in the information window.

While many of the settings on this page could negatively impact performance if set incorrectly, enabling data compression can only improve system performance in regards to data transfer between a Flow Collector and the Data Store.

Adding a Data Store Domain

You can add Managers, Flow Collectors, and Data Nodes to an existing Data Store domain as shown in this section. If you do not have a Data Store domain in your deployment, follow the instructions in **Adding Data Store to a Non-Data Store Deployment**.

Adding a Secondary Manager or Flow Collectors after the Data Store is Initialized

Use the following instructions to add a secondary Manager or Flow Collector to your Data Store if you've already initialized the Data Store.

For detailed information about the secondary Manager and failover configuration, refer to **3. Defining a Manager Failover Relationship**.

If you have existing Flow Collectors that you configured for use without a Data Store, you can transition them to a Data Store Flow Collector without loss of pre-transition data or visibility by following the instructions in **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors**.

Adding Data Nodes to the Data Store

> ℹ Contact Cisco Professional Services for assistance with planning and implementing these tasks.

Requirements

Before you add Data Nodes to your Data Store, review the following requirements:

- The Data Store supports 1 or 3 or more Data Nodes. You can add Data Nodes in sets of 3.
- If you have a Single-Data Node (1) deployment, you can add 2 Data Nodes to expand your deployment to a set of 3 Data Nodes (and additional sets of 3).
- A Data Store with only 2 Data Nodes is not supported.

Before you Begin

You may want to consider using a maintenance window when expanding your Data Store.

Before expanding your Data Store, all data is distributed evenly across your Data Nodes. For example, in a three node Data Store, one third of your data resides on each Data Node. Upon expansion of a Data Store, all data is redistributed evenly across the newly added nodes. For example, if a 3 node Data Store is expanded to 6 nodes total, redistribution results in one sixth of the data on each Data Node. When expanding a single node Data Store to three nodes, data is redistributed one third to each node.

During the operation of redistributing data, the query performance of your Data Store may be temporarily reduced. The size and duration of the impact is related to the amount of data which needs to be moved and the bandwidth of your private LAN between Data Nodes. For example, a hardware Data Store with port bonding could use 20GB of private LAN bandwidth to move the data. The database will remain operational during the redistributing of data but we suggest using a maintenance window if you want to minimize impact to your users.

Procedures

To add Data Nodes to your deployment, complete the following procedures:

1. Create a Data Store Backup

Before you add a Data Node, back up the Data Store. For instructions, refer to **Creating a Data Store Backup** for more information.

2. Configure the Data Node and Add it to Central Management

1. Deploy the Data Nodes to your network. For instructions, refer to the x2xx Series Hardware Appliance Installation Guide, the Secure Network Analytics x3xx Series Hardware Installation Guide, or the Virtual Edition Appliance Installation Guide.

> Make sure you assign your Data Node Virtual Edition with two network adapters during the installation. When you start First Time Setup, it will fail to resolve if it cannot detect a second network adapter, which will prevent you from assigning a non-routable IP address for inter-Data Node communications.

2. Configure the Data Node in First Time Setup. You will assign a routable (eth0) management IP address and configure inter-Data Node communications in this procedure.
3. Add the Data Node to Central Management using the Appliance Setup Tool.

3. Add Data Nodes to the Data Store

1. Log in to the Manager appliance console as root.
2. Type `SystemConfig` and press Enter.
3. Select **Data Store**.
4. Select **SSH**. Wait while SSH is enabled across your appliances.

5. From the **Data Store** menu, select **New Data Nodes**. Follow the on-screen prompts.

    - After the process completes, check Central Management to ensure that the appliance status is Connected.
    - When you exit the Data Store menu, the system restores your previous SSH settings.

4. Rebalance Data in the Data Store

> ⚠ A rebalance is required after adding additional Data Nodes to the Data Store. Contact Cisco Support for assistance with this process.

Replacing a Data Node (Hardware Only)

Use the following instructions to prepare a new (spare) Data Node for the following scenarios:

- Replacing a Data Node with a spare Data Node with different IP addresses
- Replacing an unresponsive Data Node
- Adding a spare Data Node after an existing Data Node goes down

In all scenarios, you will prepare the new (spare) Data Node and work with Cisco Support to complete the replacement.

> ℹ Contact Cisco Professional Services for assistance with planning and implementing these tasks.

1. Prepare the New (Spare) Data Node

1. Install the new (spare) Data Node appliance in the same rack setup as the existing Data Node appliances. For installation instructions, refer to the x2xx Series Hardware Appliance Installation Guide or the Secure Network Analytics x3xx Series Hardware Installation Guide.

    Check the following:

    - Ensure that the new Data Node is connected to the same switches/ports.
    - Ensure that the new Data Node is in the same VLANs as the private and public interfaces on the existing Data Nodes.

2. Connect the Data Node to power and power on.
3. Upgrade the image on the new Data Node to match the image already running on the existing Data Nodes. Please contact Cisco Support for assistance.
4. Configure the Data Node in First Time Setup. Assign it the appropriate eth0 management IP and private IP addresses, and confirm it is in the same VLANs as the existing Data Node eth0 and private IPs.
5. Verify full connectivity by performing the following steps:
    - Ping from the Manager and all Flow Collectors to the eth0 IP address of the new Data Node.
    - Ping from all existing Data Nodes to the private IP of the new Data Node.
    - Ping from the new Data Node to the eth0 management IPs of the Manager and all Flow Collectors.
    - Ping from the new Data Node to the private IP of all existing Data Nodes.

2. Create a Data Store Backup

For instructions, refer to **Creating a Data Store Backup** for more information.

3. Contact Cisco Support

Contact Cisco Support to complete the replacement.

Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors

Use the following instructions to transition your Non-Data Store Flow Collectors to Data Store Flow Collectors. This process allows you to transition your existing Flow Collectors to use the Data Store database without loss of pre-transition data or visibility. Once you have completed the steps below, you can preserve your pre-existing data until you no longer need it. Transitioning Non-Data Store Flow Collectors to Data Store Flow Collectors also allows you to take advantage of features only available in Data Store such as:

- **Increased Ingest Capacity:** Data Store deployments are scalable up to 3 million flows per second and may alleviate some of your current ingest capacity limitations. Flow Collectors in Data Store mode may exhibit up to a 200% increase in performance.
- **Multi-Telemetry Support:** Data Store deployments are capable of handling NetFlow, Remote worker/Endpoint (NVM), and Firewall connection and security event telemetry.
- **Long-term Data Retention:** Data Store deployments provide scalable storage, enabling long-term data retention (up to 2 years) without adding Flow Collectors.
- **Enterprise-class Data Resiliency:** Telemetry data is stored redundantly across Data Nodes. This ensures no service interruption during single node failures.
- **Greatly Improved Query and Reporting Response Times:** The Data Store provides drastically improved query performance and reporting response times, in some cases 10x faster or more compared with a Non-Data Store deployment model.
- **Analytics:** Analytics provides additional detection and modeling capabilities as well as new interface features that enable you to review, prioritize, and address any security concerns. Analytics provides:
  - Automated role detection
  - Additional alerting capabilities
  - Experimental alert dashboard
  - Supporting device report

- **SAL Telemetry:** Security Analytics and Logging (SAL) streamlines decision making by aggregating logs from firewalls (FTD and ASA) and providing an intuitive view of network activity. SAL can be expanded at your discretion, allowing for longer retention and analysis, and even alerts on potential threats found in your firewall.

Preparation

Before you start the transition, review the instructions so you understand the preparation and steps that are required to transition your Flow Collector.

Note the following:

- **One at a Time:** You can only initiate the transition for one Flow Collector at a time. However, you can have many Flow Collectors in the transitioning state simultaneously.
- **Query Options:** Once your Flow Collector has entered the transitioning state, you can query both the historical Non-Data Store data, collected prior to initiating the transition via the Non-Data Store Domain as well as the new data collected in the Data Store after the transition via the Data Store Domain.

Backing up Configuration Files

> ⚠ Make sure you back up your Central Management configuration files after you change the Flow Collector state (Non-Data Store, Transitioning, or Data Store). You can only restore to a system when the Flow Collectors are in the same state as when the backup was taken.

Flow Collector Transition Requirements

Before you transition a Flow Collector, confirm that you have deployed at least one Data Node and that you have completed the Data Store initialization process as described in **6. Initializing the Data Store**. If you have not already deployed at least one Data Node, refer to the x2xx Series Hardware Appliance Installation Guide, the x3xx Series Hardware Appliance Installation Guide, or the Virtual Edition Appliance Installation Guide for instructions. Once you have deployed your Data Node, you can follow the **Initiating a Flow Collector Transition to Data Store** procedure.

Initiating a Flow Collector Transition to Data Store

Follow these steps to transition a Non-Data Store Flow Collector to a Data Store Flow Collector.

⚠ Once you begin this process, you will not be able to return your Flow Collector to its previous state. You will need to finish the transition by following the steps below.

1. Review Your Data Store Domains

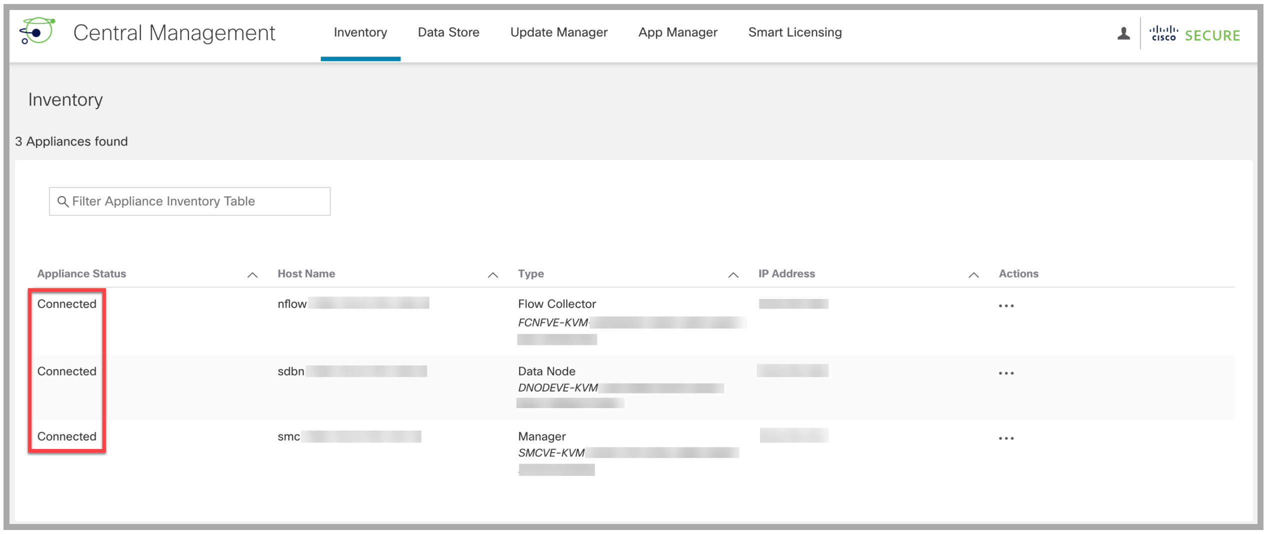
Identify the Data Store domain that corresponds to the Flow Collector you will be transitioning. Your Flow Collector will transition to this domain.

- **Adding a Data Store Domain:** If you need to add a Data Store domain, you can create one by following the instructions in the **Adding and Configuring Domains** section of this guide.
- **Importing Existing Domains:** If you want to import the settings from an existing Non-Data Store domain, make sure you follow the instructions in the **Creating a Data Store Domain by Importing an Existing Non-Data Store Domain Configuration (Optional)** section in this guide.
- **Synchronizing Domains:** During your Flow Collector transition, you can keep your configurations and tuning synchronized between your pre-transition Non-Data Store domain and your Data Store domain. Refer to **Synchronizing Data Store and Non-Data Store Domains** for more information.

2. Check Your Appliance Status

Review your Central Management inventory

1. Select **Configure > GLOBAL Central Management**.
2. Confirm that all appliances are shown as **Connected**. If the appliances are not in these states, attempt to get them into these states before proceeding to the next step. If you are unable to get your appliances into these states, contact Cisco Support.



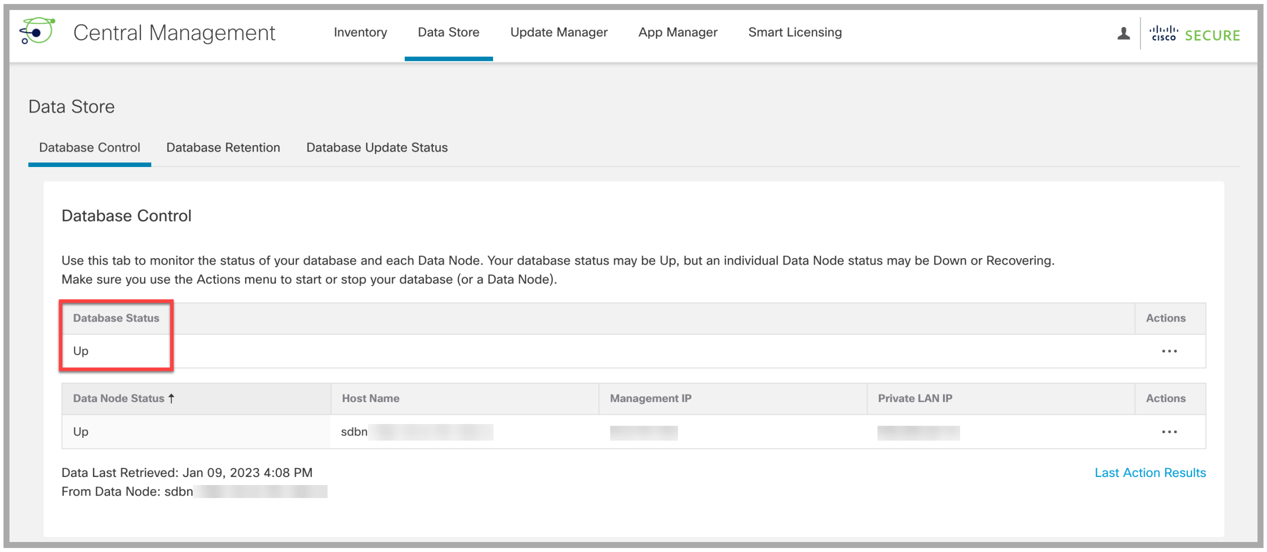
Inventory

3 Appliances found

Filter Appliance Inventory Table

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow[redacted]	Flow Collector *FCNFVE-KVM*[redacted]	[redacted]	...
Connected	sdbn[redacted]	Data Node *DNODEVE-KVM*[redacted]	[redacted]	...
Connected	smc[redacted]	Manager *SMCVE-KVM*[redacted]	[redacted]	...

3. Select the **Data Store Database Control** tab. Confirm that your Database Status is shown as **Up**.



Data Store

Database Control | Database Retention | Database Update Status

Database Control

Use this tab to monitor the status of your database and each Data Node. Your database status may be Up, but an individual Data Node status may be Down or Recovering. Make sure you use the Actions menu to start or stop your database (or a Data Node).

Database Status	Actions
Up	...

Data Node Status ↑	Host Name	Management IP	Private LAN IP	Actions
Up	sdbn[redacted]	[redacted]	[redacted]	...

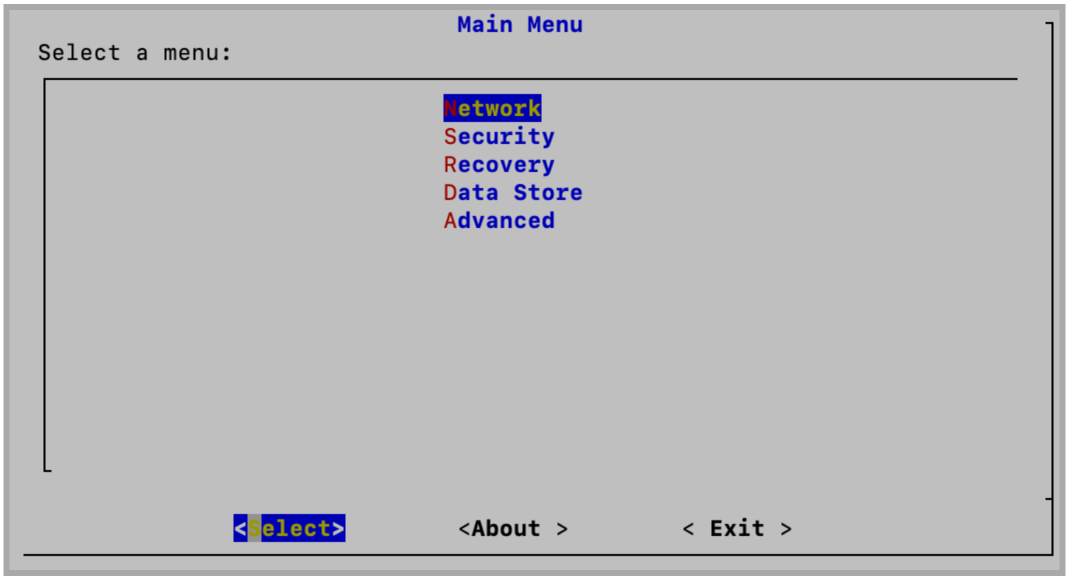
Data Last Retrieved: Jan 09, 2023 4:08 PM
From Data Node: sdbn[redacted]

Last Action Results

3. Transition Your Flow Collector

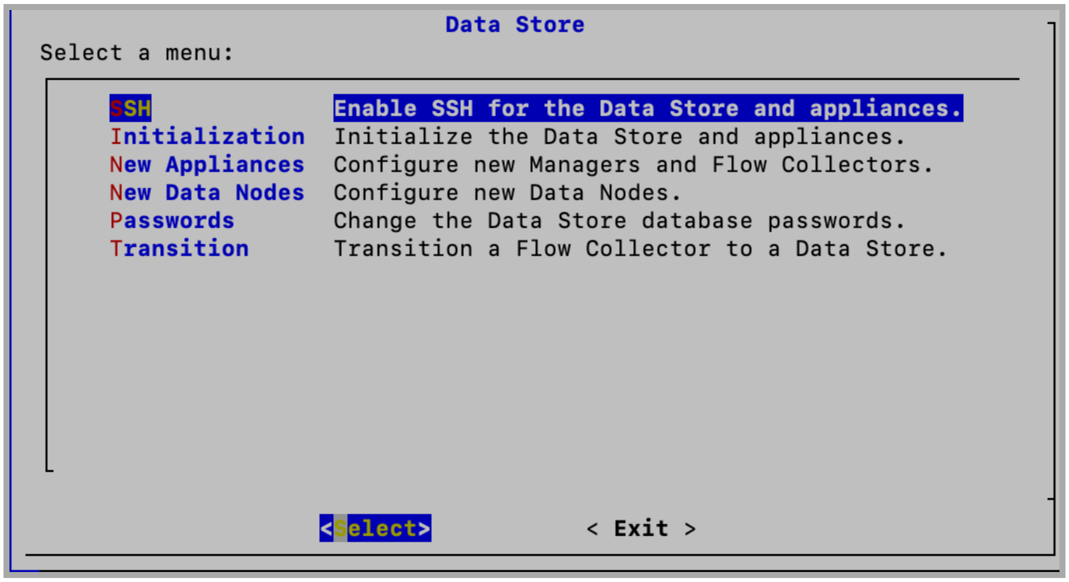
> The Flow Collector will reboot during the transition operation. When the reboot is complete, the Flow Collector will begin to store new data in the Data Store database rather than the local Vertica database on the Flow Collector.

1. Log in to your Manager appliance console (SystemConfig) as root.



```
                              Main Menu
Select a menu:

                             Network
                             Security
                             Recovery
                             Data Store
                             Advanced

         <Select>          <About >          < Exit >
```

2. Select **Data Store > SSH**. This will enable SSH.



```
                              Data Store
Select a menu:

     SSH               Enable SSH for the Data Store and appliances.
     Initialization    Initialize the Data Store and appliances.
     New Appliances    Configure new Managers and Flow Collectors.
     New Data Nodes    Configure new Data Nodes.
     Passwords         Change the Data Store database passwords.
     Transition        Transition a Flow Collector to a Data Store.

                  <Select>             < Exit >
```

> If you don't see the Data Store menu, ensure that you have a Data Store domain. For more information, refer to **1. Review Your Data Store Domains**.

3. From the Data Store menu, select **Transition > Initiate Transition**.
4. Select a Flow Collector to transition.
5. On the Data Store Domains screen, select the Data Store domain that you identified (or created) in 1. Review Your Data Store Domains. Your transitioned Data Store Flow Collector data will be routed to the Data Store database and will be accessible

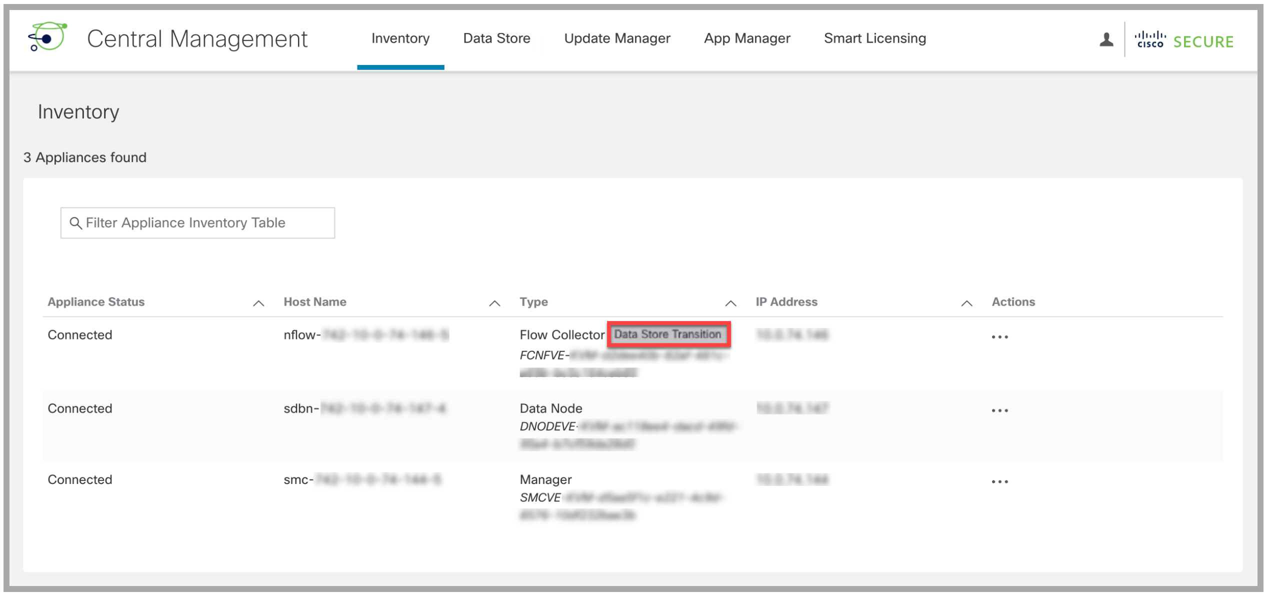
via this new domain instead of the prior Non-Data Store domain.

6. Follow the on-screen prompts to confirm the transition.

> ⚠ Once you are finished with the Initiate Transition procedure, do not complete your Flow Collector transition until you have confirmed you no longer need your historical data stored locally on the Flow Collector, as it will be deleted during this process. For more information, refer to **Completing your Data Store Flow Collector Transition**.

7. Review the Central Management inventory (**Configure > GLOBAL Central Management**).

   Confirm the Flow Collector you transitioned shows the **Data Store Transition** tag.



Inventory

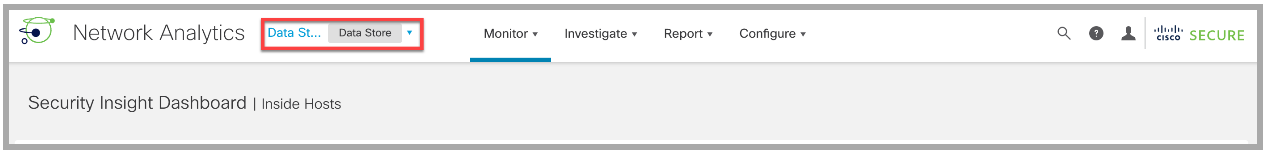
3 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-[redacted]	Flow Collector Data Store Transition FCNFVE-[redacted]	[redacted]	...
Connected	sdbn-[redacted]	Data Node DNODEVE-[redacted]	[redacted]	...
Connected	smc-[redacted]	Manager SMCVE-[redacted]	[redacted]	...

4. Verify Communications

Confirm that your Data Store is receiving flows.

1. Return to your Security Insight Dashboard.
2. Ensure the Data Store domain is selected from the Domains menu at the top of your screen.



Security Insight Dashboard | Inside Hosts

3. Select the **Report** menu.
4. Select **Report Builder**.
5. Click **Create New Report**.
6. Click the **Flow Database Ingest Trend Report** template.
7. Select the parameters as needed. Click **Run**.
8. Review the report to confirm the database or Data Store are receiving flows.

In addition to running the Flow Database Ingest Trend Report, you can also confirm that your Data Store is receiving flows by doing the following:

- **Flow Collector Trend Table:** Navigate to your Security Insight Dashboard to review the Flow Collector Trend table. If your Data Store is receiving flows, you will see them here.
- **Database Retention:** Open Central Management (Configure > GLOBAL Central Management) and review the information on the Data Store > Database Retention tab. The Oldest Data in Data Store table on this page will help you to track the date and number of days since the oldest record was written to Data Store. Note that the data in this table is updated only once per day so you will not see any data in this table on the day of your transition. Refer to the **Viewing Database Retention** section of this guide for more information.

Running Flow Searches

Select Investigate > Flow Search to run a flow query by domain. Use custom date ranges to customize your results.

- **Pre-transition Queries:** To query for pre-transition historical data in the Non-Data Store domain, be sure to select an end date that precedes your Flow Collector transition date.
- **Post-transition Queries:** To query on all post-transition Data Store data, be sure to select a start date that begins on or after the date that you transitioned your Flow Collector.

Removing a Transitioning Flow Collector From your Central Manager Inventory

⚠ Do not remove a transitioning Flow Collector from your Central Manager inventory. If you do, you will be required to complete the transition process with the assistance of Cisco Support.

Transitioning Flow Collectors Behavior

Transitioning Flow Collectors will exhibit the following behavior.

- **New Data:** After you have completed the **Initiating a Flow Collector Transition to Data Store** procedure, your transitioning Flow Collectors will send all new telemetry to the Data Store database on the Data Node(s). Your new data will be accessible in the Data Store domain you identified (or created) in **1. Review Your Data Store Domains** and your local pre-transition data will continue to exist in your Non-Data Store domain.
- **Pre-transition Data:** Flow Collectors will continue to store the pre-transition data locally for as long as you want to maintain access to that data. See **Completing your Data Store Flow Collector Transition** for instructions on how to remove the pre-transition data when you no longer need it.
- **System Performance:** System performance during the Flow Collector transition will be similar to pre-transition performance. Once the transition is completed, you will see performance improvements aligned with Data Store Flow Collectors.

Synchronizing Data Store and Non-Data Store Domains

During your Flow Collector transition, you may want to keep your configurations and tuning synchronized between your pre-transition Non-Data Store domain and your Data Store domain. This section describes the process for synchronizing your Non-Data Store domain with its associated Data Store domain.

> ⓘ You need administrator access for this procedure.

Synchronized Properties

The following properties will be synchronized between domains:

- Data Store domain specific configuration as well as alert configuration (if enabled). Domain configuration includes:
  - Host Group Management
  - Alarm Severity
  - Policy Management
  - Services, Applications
  - Exporter SNMP profiles (not including passwords)
  - Domain AS Numbers.

Recommended Synchronization Frequency

While you can synchronize your domains as often as you like, we recommend that you limit your synchronizations to only after you perform a group of changes or once a day or week. This is because the synchronization process requires the use of resources that take away from daily processing.

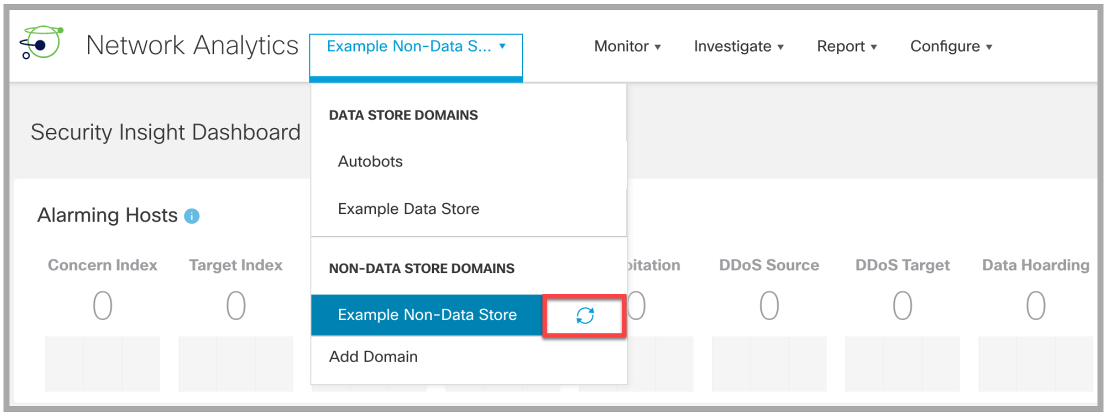
Synchronizing Domains Procedure

Follow these steps to synchronize your Non-Data Store domain (Source) with your Data Store domain (Target).

1. From the menu bar, choose the Non-Data Store domain that you want to synchronize with your Data Store domain.
2. From the main menu, choose **Configure > SYSTEM Domain Properties**.
3. Select the **Edit** button.
4. Choose the Data Store domain that you want to synchronize this domain with in the **Target Domain to Synchronize** drop-down menu.

> ⓘ You can only synchronize your target Data Store domain with one source Non-Data Store domain. If you attempt to synchronize your target Data Store domain with more then one source Non-Data Store domain, you will receive an error.

5. Click the **Save** button to save your changes. A synchronize button appears next to the Non-Data Store domain that you selected to synchronize with your Data Store domain.



Completing your Flow Collector Transition

Once you no longer need your pre-transition data, you can complete the Flow Collector transition by following the steps in **Completing your Data Store Flow Collector Transition**.

> ⚠ Do not complete your Flow Collector transition until you have confirmed you no longer need your historical data stored locally on the Flow Collector, as it will be deleted during this process.

Completing your Data Store Flow Collector Transition

If you have followed the process for transitioning your Non-Data Store Flow Collector to a Data Store Flow Collector and no longer need to keep your locally-stored Non-Data Store data, you can finalize your Data Store Flow Collector transition.

There are two major procedures involved in transitioning your Non-Data Store Flow Collectors to Data Store Flow Collectors.

1. Initiate the transition process by following the steps in the **Initiating a Flow Collector Transition to Data Store** procedure. This transitions your Flow Collectors to the Data Store Transition state described in **Transitioning Flow Collectors Behavior**.

2. Complete the transition process. This causes your Flow Collector to solely become a Data Store Flow Collector. All of the pre-existing Non-Data Store data that this Flow Collector is storing will be deleted and resources will be recovered, thereby improving the performance of your Flow Collector.

Requirements

Before you complete your Data Store Flow Collector transition, review the following:

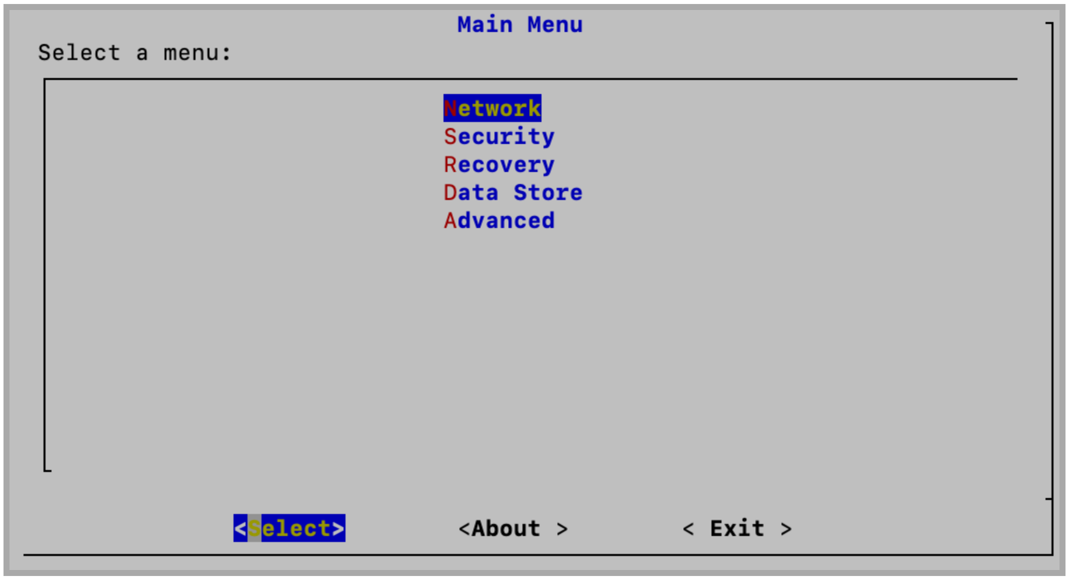
- **Initiate Transition:** Confirm you have completed the **Initiating a Flow Collector Transition to Data Store** procedure.

- **Historical Data:** Confirm that you no longer need your historical data stored locally on the Flow Collector, as it will be deleted during this process. If you have a data retention policy for your Non-Data Store data and want to understand how much new data is in your Data Store before completing your Data Store transition, review the Oldest Data in Data Store table. For more information, refer to **Viewing Database Retention**.

Completing a Flow Collector Transition to Data Store

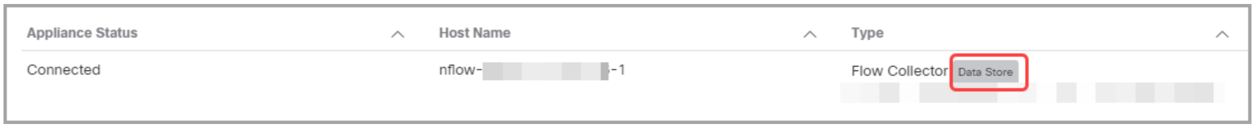
Follow these steps to complete your Data Store Flow Collector transition.

1. Log in to your Manager appliance console (SystemConfig) as root.



2. Select **Data Store > Transition > Complete Transition**.
3. Select a Flow Collector to complete the transition to Data Store.
4. Follow the on-screen prompts to complete the transition.
5. Review the Central Management inventory (**Configure > GLOBAL Central Management**).

   Confirm the Flow Collector you transitioned shows the **Data Store** tag.



Appliance Status	Host Name	Type
Connected	nflow-[redacted]-1	Flow Collector Data Store [redacted]

Post Completion Notes

Once you have finished the **Completing a Flow Collector Transition to Data Store** procedure:

- You will no longer see any NetFlow records in a Flow Query for this Flow Collector in the Non-Data Store domain.
- If there are no Flow Collectors in your old Non-Data Store domain, you can delete that domain. Refer to **Deleting a Domain** for details.
- All of the pre-existing Non-Data Store data that this Flow Collector was storing has been deleted and resources have been recovered, thereby improving the performance of your Flow Collector.

- You will see a significant reduction in disk space usage on your transitioned Flow Collector. To see system statistics, services, disk usage, and docker services, log in to the Appliance Admin interface:

    1. On the Central Management Inventory page, click the ••• (**Ellipsis**) icon for the appliance.
    2. Select **View Appliance Statistics**.
    3. Select **Home** to review the statistics.

Adding Data Store to a Non-Data Store Deployment

Before you use these instructions, make sure you are already working in a Secure Network Analytics system with a Non-Data Store domain. For instructions, refer to **Planning Your System Configuration**.

Use the appropriate instructions to add a Data Store to your Non-Data Store deployment.

- **Adding Data Store with an Existing Flow Collector**
- **Adding Data Store with a New Flow Collector**

> For Data Store compatibility information, refer to the Secure Network Analytics Hardware and Software Version Support Matrix.

Adding Data Store with an Existing Flow Collector

To add a Data Store with an existing Flow Collector, refer to **Adding a Data Store to a Non-Data Store Deployment and Transitioning Your Flow Collectors**. This process allows you to transition your existing Flow Collectors to use the Data Store database without loss of pre-transition data or visibility.

Adding Data Store with a New Flow Collector

Follow the steps below to add a new Flow Collector to your Data Store.

1. Ensure your Flow Collector and appliances are all running on the same software version. Follow the instructions in the Secure Network Analytics Update Guide.
2. Confirm that you have created the Data Store Domain in Secure Network Analytics that you will be associating your Flow Collector with. Refer to the Creating a Data Store Domain section in this guide for details.
3. Deploy and install your hardware or virtual Flow Collector. Refer to the x2xx Series Hardware Appliance Installation Guide,the Secure Network Analytics x3xx Series Hardware Installation Guide, or the Virtual Edition Appliance Installation Guide for more information.
4. Run First Time Setup on the Flow Collector, making sure to deploy the Flow Collector as part of a Data Store.
5. Add the Flow Collector to Central Manager. If you have a 52xx Flow Collector, be sure to add the Flow Collector database and Flow Collector engine (in that order). Select the Data Store domain that you want your Flow Collector to be a part of.
6. Repeat the above steps for all of the Flow Collectors that you want to add to your Data Store.
7. Add your Flow Collector(s) to your Data Store by logging into your Manager appliance console (SystemConfig) and selecting **Data Store>New Appliances**.

Troubleshooting

Analytics jobs are lagging

In both of the following instances, the "Analytics performance has degraded" system alarm will be triggered.

The secondary Manager has been promoted to primary Manager

When you change the role of the primary Manager to that of the secondary Manager, and more than 5 hours has passed before the original primary Manager has been recovered and re-assigned to the primary role, the "Analytics performance has degraded" system alarm will be triggered. Analytics will recover and run the jobs that occurred during the last 6 hours, while the original primary Manager was down. Job performance will continue to lag until your system has processed all jobs from the last 6 hours and begins to process jobs in real time.

An appliance went down due to degradation

If your system is experiencing degradation (which is usually due to insufficient resources such as CPU or memory), jobs will begin to lag. If this lag exceeds 5 hours, then the "Analytics performance has degraded" system alarm will be triggered. At this point, results will be incomplete and unreliable.

A possible cause for this failure is that you have increased the flows per second beyond what is supported in your setup. To resolve this, either reduce the flows per second or increase the resources on the Manager, the Data Store, or both. If you cannot resolve the issue, contact Cisco Support.

Appliance Status: Config Channel Down

If your Inventory page shows **Config Channel Down** for the appliance status, check the following:

- **Communication Settings:** Confirm your network communication settings.
- **Trust Stores:** Make sure your appliance identity certificates are saved to the correct Trust Stores. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.
- **Certificates:** If you've changed the appliance identity certificate, check the procedure and confirm your certificates are saved to the correct Trust Stores. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.
- **Removing an Appliance:** If you remove an appliance from Central Management while the configuration channel is down, make sure you also remove the appliance

from System Configuration:

- Log in to the appliance console as sysadmin.
- Type **SystemConfig**. Press Enter.
- Select **Recovery** > **RemoveAppliance**.

Appliance Status: Data Store Not Initialized

You need to finish your Secure Network Analytics system configuration.

After you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory, you need to initialize the Data Store. For instructions, refer to **6. Initializing the Data Store**.

Appliance Status: Data Store Not Configured

If you've added a new Manager, Flow Collector, or Data Node to your Data Store, you need to finish your system configuration. For instructions, refer to **Data Store Maintenance**.

Opening the Appliance Administration Interface

You can access the Appliance Admin interface through Central Management or by logging in to the appliance directly.

You may need to log in to Appliance Admin if you've removed your Manager from Central Manager for troubleshooting.

1. In your browser address bar, type the appliance IP address as follows:

   https://<IPAddress>

   - **Manager:** add **/Manager/Index.html** after the IP address.
   - **Example:** https://xx.xxx.xx.xxx/Manager/index.html

Replacing the Appliance Identity

Each Secure Network Analytics version 7.x appliance is installed with a unique, self-signed appliance identity certificate. To replace the appliance identity certificate with a certificate from a Certificate Authority, refer to the SSL/TLS Certificates for Managed Appliances Guide for instructions.

> ⚠ Your certificates are critical for your system’s security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss.

Removing Data Store Appliances from Central Manager

If you remove Data Store appliances from Central Manager (Manager, Flow Collector, Data Node), it does not remove them from the Data Store itself. This needs to be manually cleaned up.

- **Managers and Flow Collectors:** For Managers and Flow Collectors, you can remove them from the **/lancope/var/services/data-store/config-datastore-inventory-snapshot** directory.
- **Data Nodes:** Contact Cisco Support for assistance with the removal Data Nodes as that process is more complicated.

Changing the Host Name, Network Domain Name, or IP Address

To change the appliance host name, network domain name, or IP address after you've installed and configured your appliances, follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

As part of the procedure, you will remove the appliance from Central Management temporarily, and the appliance identity certificate is replaced automatically.

> ⚠ The appliance identity certificate is replaced automatically as part of this procedure.
>
> **If your appliance uses a custom certificate,** please contact Cisco Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.

Opening Domain Properties

From the main menu, choose **Configure > SYSTEM Domain Properties**.

For more information, refer to **Domains**.

Deleting a Desktop Client Domain

> ⚠ Use caution when deciding which Desktop Client domains you want to delete as you will lose access to all data which has been collected for the domain you are deleting.
> **Workaround**: If you accidentally delete all of your domains in the Desktop Client and lock yourself out of the Manager Web App, create a new Non-Data Store domain in the Desktop Client. This will allow you to regain access into the

> ⚠ Manager Web App. For information on creating a domain refer to the Add a Domain topic in the Desktop Client help.

Opening the Appliance Setup Tool

Use the following instructions to open the Appliance Setup Tool after you've configured an appliance.

> ⚠ If you change the host name, network domain name, or IP address using the Appliance Setup Tool, the appliance identity certificate is replaced automatically.
>
> **If your appliance uses a custom certificate,** please contact Cisco Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.

1. In the appliance browser address bar, after the IP address, replace the end of the URL with /lc-ast:

   https://<IPAddress>/lc-ast

2. Press Enter.
3. For more information, refer to**1. Configuring Your Environment Using First Time Setup**

System Configuration Overview

We've updated System Configuration with a new menu structure. System Configuration often involves troubleshooting. For assistance, please contact Cisco Support.

- **Users:** The available menus are determined by whether you log in as root, sysadmin, or admin.
- **SSH:** You may need to enable SSH to access a menu.

1. Log in to the appliance console.
2. Type **SystemConfig**. Press Enter.
3. From the main menu, select a menu:

- **Network:** To change appliance management port network, trusted hosts, and network interfaces (eth0 configuration , MTU, etc.), select Network.
- **Security:** To change or reset passwords (refer to **Passwords**) and manage Syslog Compliance, select Security.

- **Recovery:** To remove an appliance from Central Management, reset factory defaults, create a diag pack, or refresh the image, select Recovery.
- **Advanced:** To open the root shell, manage the admin user account, configure Single Sign-On, reboot, or shut down, select Advanced.
- **Data Store:** This menu is available in Managers configured for use with a Data Store. Use this menu for enabling SSH, initialization, adding new Managers and Flow Collectors to the Data Store, adding Data Nodes to the Data Store, changing the Data Store database passwords, and transitioning your Flow Collectors to Data Store.

Changing the Trusted Hosts

You can use System Configuration to change the trusted hosts list from the appliance defaults. However, please contact Cisco Support before you change your trusted hosts.

> ⚠ Please contact Cisco Support before you change your trusted hosts.

If you change the trusted hosts list from the defaults, make sure each Secure Network Analytics appliance is included in the trusted host list for every other Secure Network Analytics appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.

1. Log in to the appliance console as sysadmin.
2. Select **Network** > **Trusted Hosts**.
3. Follow the on-screen prompts to change the Trusted Hosts.

Configuring the Maximum Transmission Unit (MTU)

Use the following instructions to configure the maximum transmission unit (MTU) for the appliance eth0 network interface. The number sets the maximum packet size the eth0 interface can transmit per transaction.

> ⚠ The MTU impacts your network processing. If you change this number, make sure it is configured consistently in your network.

1. Log in to the appliance console as sysadmin.
2. Select **Network** > **Interface**.
3. Select **eth0**.
4. Enter **1500** (default), **9000**, or a number that meets your network configuration requirements.

> ⓘ We support a maximum MTU setting of 8,192 bytes for Firewall Logs and 9,216 bytes for NetFlow, sFlow, and NVM flows. If you are ingesting Firewall Logs using Security Analytics and Logging (OnPrem) and another telemetry type, do not configure the MTU setting greater than 8,192 bytes.

5. Select **Confirm**.
6. Follow the on-screen prompts to confirm your changes.

Creating a Diagnostic Pack

Having a diagnostics pack can be invaluable if you need to work with Cisco Support to troubleshoot an issue. Use the following instructions to create a diagnostics pack for an individual appliance.

1. Log in to the appliance console as root.
2. Select **Recovery**.
3. Select **Diagnostics Pack**.
4. To customize your diagnostics pack, select a menu and click **Edit**.

Menu	Description
File Name Prefix	Add a file name prefix for your diagnostics pack (maximum of 127 characters).
Password	Create a file password for your diagnostics pack. If you do not create a file password, we will encrypt the diagnostics pack with the default method (Cisco key).
Configuration Backup	Select this option and follow the on-screen prompts to include a configuration backup in your diagnostics pack. For more information about backups, refer to Backup Configuration Files in the Help.

Modules	Edit the diagnostic pack contents by selecting the specific modules you want to include.

5. Click **Finish**. Follow the on-screen prompts to create the diagnostics pack.

Resetting Factory Defaults

Use the following instructions to reset an appliance to its factory defaults (RFD). To completely erase data, make sure you reset factory defaults twice.

- **RFD twice:** To completely erase data, make sure you reset factory defaults twice.
- **Back up Configuration:** If you plan to restore the appliance configuration, make sure you save the backup configuration and database backup files. Refer to **Backup Configuration Files** (in Central Management) and **Backup/Restore Database (Appliance Admin interface)** topics in the Help for details. To restore the backup after RFD, contact Cisco Support.

⚠ If you reset factory defaults (RFD) on an appliance, all existing data and configuration information will be deleted and can only be restored if you've made a backup.

⚠ If you reset an appliance to factory defaults, you cannot restore the configuration using Central Management. For assistance, please contact Cisco Support.

1. Log in to the appliance console as sysadmin.
2. Select **Recovery** > **Factory Defaults.**
3. Follow the on-screen prompts to reset factory defaults and restart the appliance.

⚠ Make sure you RFD each appliance twice to completely erase data.

4. Log in to the appliance console as **sysadmin** and follow the on-screen prompts to configure the appliance IP address, host name, and domain. For instructions, refer to the Configuring Your Environment Using First Time Setup section of this guide. This step is required even if you preserve network settings when you RFD.
5. Log in to the Appliance Setup Tool and add the appliance to Central Management. For details, refer to **Central Management (Managing your Appliances)**.

Enabling/Disabling Admin Users

Use the following instructions to enable or disable the default admin account.

1. Log in to the appliance console as sysadmin.
2. Select **Advanced**.
3. Select **Admin User**.
4. Follow the on-screen prompts to enable or disable the Admin User account.
5. Repeat these instructions to enable or disable the Admin User account on all appliances in your Secure Network Analytics cluster.

Data Store Deployment Troubleshooting

Hardware Deployment Troubleshooting

For issues with deploying or configuring your appliances, refer to the x2xx Series Hardware Appliance Installation Guide or the Secure Network Analytics x3xx Series Hardware Installation Guide for more information.

Virtual Appliance Deployment Troubleshooting

For issues with deploying or configuring your Virtual Edition appliances, refer to the Virtual Edition Appliance Installation Guide for more information.

First Time Setup and Data Nodes Virtual Edition

If you do not assign two network adapters to your Data Nodes Virtual Edition during the installation, First Time Setup will fail to resolve because it cannot detect a second network adapter. This will prevent you from assigning a non-routable IP address for inter-Data Node communications. Refer to the Virtual Edition Appliance Installation Guide for more information.

Data Store Troubleshooting

Note that the Data Store reserves up to 40% of the available storage space to maintain the Data Store. At a maximum, 60% of the total space is available for telemetry storage.

Vertica Analytics Platform does not automatically restart after a Data Node loses power and reboots

If a Data Node loses power unexpectedly, and you reboot the appliance, the Vertica Analytics Platform (Vertica) instance on that Data Node may not automatically restart, due to possible corrupted data. If there are still enough running Data Nodes to allow the Data Store to continue running, the Data Store continues ingesting data from the Flow Collectors. However, you need to restart the Data Node as soon as possible, to allow it to rejoin the Data Store, retrieve missed data from adjacent Data Nodes, and catch up with the rest of the Data Nodes.

To restart the Data Node, try each of the following methods:

- Start the Data Node on the Central Management > Data Store tab. Refer to **Starting a Data Node** for details.

- If the Data Node does not start from the Data Store tab, log into the Data Node and force a manual Vertica restart, which deletes corrupted data and allows Vertica to properly restart.

For Data Node hardware appliances, you may need to update the Data Node's power restore policy before it restarts. If the power restore policy is set to Power Off, you must manually restart the Data Node after power loss. See the UCS C-Series GUI Configuration Guide for more information on configuring the power restore policy in CIMC.

1. Log in to your Data Node appliance console as root.
2. Copy the following command and paste it into a text editor:

   ```
   tail /lancope/var/database/dbs/sw/v_sw_[node_name]_cata-
   log/ErrorReport.txt
   ```

3. Replace *[node_name]* with your Data Node name (for example, `node0001`).
4. Copy the updated command and paste it into the command line interface, then press Enter to review the most recent entries in the `ErrorReport.txt` error file. If the error message notes possible data consistency or data corruption issues, proceed to the next step to force a Vertica restart.
5. Copy the following command and paste it into a text editor:

   ```
   admintools -t restart_node --hosts=[data-node-ip-address] --
   database='sw-datastore' --password="[dbadmin-password]" --force
   ```

6. Replace *[data-node-ip-address]* with your affected Data Node's IP address. Make sure you use the private IP address shown in the **Data Store Tab**. Do not use the eth0 management IP address.
7. Replace *[dbadmin-password]* with your Data Store `dbadmin` password.
8. Copy the updated command and paste it into the CLI, then press Enter to force a restart of Vertica on your affected Data Node. Vertica deletes any corrupted data, and recovers that data from adjacent Data Nodes.
9. If the system prompts you with `Do you want to continue waiting? (yes/no) [yes]`, enter `yes` and press Enter to continue waiting.

   Because Vertica restores the affected Data Node's information from adjacent Data Nodes, if these Data Nodes ingested a large amount of flow traffic while the affected Data Node was down, it may take a period of time for the affected Data Node to recover.

10. Review Cisco's recommendations for supplying power to your Data Nodes. Refer to the x2xx Series Hardware Appliance Installation Guide, the Secure Network

Analytics x3xx Series Hardware Installation Guide, or the Virtual Edition Appliance Installation Guide for more information.

Data Store Does Not Start After Power Failure

Review the database status on the Data Store tab in Central Management. You can start the database or Data Node from there. Refer to **Viewing the Data Store Database Status** for details.

Installing Patches and Updating Software

Make sure you keep Secure Network Analytics up-to-date by installing the latest patches for your software version. For details and instructions, visit Cisco Software Central.

Software updates are also posted to your Cisco Smart Account at Cisco Software Central. For a successful update, make sure you follow the instructions in the Secure Network Analytics Update Guide.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	February 27, 2023	Initial version.
1_1	April 5, 2023	Minor updates
1_2	April, 6, 2023	Minor updates
1_3	August 10, 2023	Minor updates
1_4	February 27, 2023	Updated Data Store Backup initialization procedure Fixed broken link
1_5	December 19, 2023	Added Data Store Backup patch information.

Copyright Information