Cisco Secure Network Analytics

Release Notes 7.4.1

Table of Contents

Introduction

Overview

This document provides information about the new features and improvements, bug fixes, and known issues for the v7.4.1 release of Cisco Secure Network Analytics (formerly Stealthwatch).

For additional information about Secure Network Analytics, go to cisco.com.

Rebranding

We've rebranded our Cisco Stealthwatch Enterprise products to Cisco Secure Network Analytics. The other main change to note is Stealthwatch Management Console is now Cisco Secure Network Analytics Manager.

For the complete list, refer to the following table.

Former Branding	**New Branding First Use**	**New Branding Subsequent Use**
Cisco Stealthwatch Cloud	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud Private Network Monitoring	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud Public Cloud Monitoring	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Cisco Stealthwatch Enterprise or Cisco Stealthwatch	Cisco Secure Network Analytics	Secure Network Analytics
Cisco Stealthwatch Data Node	Cisco Secure Network Analytics Data Node	Data Node
Cisco Stealthwatch Data Store	Cisco Secure Network Analytics Data Store	Data Store
Encrypted Traffic Analytics (ETA)	encrypted traffic analytics	encrypted traffic analytics

Former Branding	New Branding First Use	New Branding Subsequent Use
Stealthwatch Endpoint License	Cisco Secure Network Analytics Endpoint license	Endpoint license
Stealthwatch Flow Collector	Cisco Secure Network Analytics Flow Collector	Flow Collector
Stealthwatch Flow Collector Database (FCDB)	Cisco Secure Network Analytics Flow Collector Database	Flow Collector database
Stealthwatch Flow Collector NetFlow (FCNF)	Cisco Secure Network Analytics Flow Collector NetFlow	Flow Collector (NetFlow)
Stealthwatch Flow Collector sFlow (FCSF)	Cisco Secure Network Analytics Flow Collector sFlow	Flow Collector (sFlow)
Stealthwatch Flow Sensor (FS)	Cisco Secure Network Analytics Flow Sensor	Flow Sensor
Stealthwatch Management Console (SMC)	Cisco Secure Network Analytics Manager	Manager
Stealthwatch Cloud Sensor	Cisco Secure Cloud Analytics sensor	sensor
Stealthwatch Threat Intelligence Feed or threat intelligence license	Cisco Secure Network Analytics Threat Feed	Threat Feed
UDP Director	Cisco Secure Network Analytics UDP Director	UDP Director

Terminology

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

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

Before You Update

Before you begin the update process, review the Update Guide.

⚠ Compliance Customers: If choosing to upgrade to v7.4.1, be advised this version includes a compliance violation. For FIPS and CC modes specifically, Secure Network Analytics TLS clients advertise non-compliant curves in the Supported Groups Extension of Client Hello messages, violating FCS_TLSC_EXT.1.4.

For more information, contact Cisco Support.

Software Version

To update the appliance software to v7.4.1, the appliance must have v7.3.x or v7.4.0 installed. It is also important to note the following:

- **Patches:** Make sure you install the latest rollup patch on your appliances before you upgrade. You can download the files from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
- **Downloading Files:** Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator. In the Download and Upgrade section, select **Software Download**. Select **Security** > **Network Visibility and Segmentation** > **Secure Network Analytics**.
- **Update your appliance software versions incrementally:** For example, if you have Secure Network Analytics v7.1.x, make sure you update each appliance from v7.1.x to v7.2.x., then update from v7.2.x to v7.3.2, etc. Each update guide is available on cisco.com.
- **Downgrades:** Version downgrades are not supported because of update changes in data structures and configurations that are required to support new features installed during the update.
- **TLS:** Secure Network Analytics requires TLS v1.2.
- **Third-Party Applications:** Secure Network Analytics does not support installing third-party applications on appliances.

Supported Hardware Platforms

To view the supported hardware platforms for each system version, refer to the Hardware and Version Support Matrix.

CIMC Firmware Version

Make sure to update the CIMC firmware version using the common update process or common update patch specific to your hardware.

The M4 common update process applies to UCS C-Series M4 hardware, and the common update patch applies to M5 hardware, for the appliances shown in the following table.

M4 Hardware	**M5 Hardware**
Manager 2220	Manager 2210
FC 4200	FC 4210
FC 5020 Engine	--
FC 5020 Database	--
FC 5200 Engine	FC 5210 Engine
FC 5200 Database	FC 5210 Database
FS 1200	FS 1210
FS 2200	--
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

Certificate Check

Updating to v7.4.1 includes a certificate check to verify the Cisco Bundles common update will not cause issues with your environment. If you are using certificates, make sure the full chain of certificates (as separate files) is in the Central Management Trust Store. If only the end-entity certificate is present in the Trust Store, the upgrade will fail.

Cisco Bundles

Make sure you have the latest Cisco Bundles common update patch installed. For more information, refer to the readme for the Cisco Bundles Common Update Patch. The patch:

- provides pre-validated digital certificates of a select number of root certificate authorities (CAs), and it
- includes a core certificate bundle and an external certificate bundle, which are used for connecting to Cisco services and to non-Cisco services.

High Availability

If you have high availability configured on your UDP Directors and plan to update Secure Network Analytics to v7.4.0 or later, be sure to make note of your high availability settings on your UDP Director before you begin the update. You will need to reconfigure high availability once the update is complete. For more information about updating Secure Network Analytics, refer to the Update Guide.

Third-Party Applications

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

Browsers

- **Compatible Browsers:** Secure Network Analytics supports the latest version of Chrome, Firefox, and Edge.
- **Microsoft Edge:** There may be a file size limitation with Microsoft Edge. We do not recommend using Microsoft Edge to upload the software update files (SWU).
- **Shortcuts:** If you use browser shortcuts to access the Appliance Admin interface for any of your Secure Network Analytics appliances, the shortcuts may not work after the update process is complete. In this case, delete the shortcuts and recreate them.
- **Certificates:** Some browsers have changed their expiration date requirements for appliance identity certificates. If you cannot access your appliance, refer to the SSL/TLS Certificates for Managed Appliances Guide to replace the certificate or contact Cisco Support.

Alternative Access

> ⚠ It is important to enable an alternative way to access your Secure Network Analytics appliances for any future service needs.

Make sure you can access your Secure Network Analytics appliances using one of the following options:

Virtual Appliances - Console (serial connection to console port)

To access an appliance through **KVM**, refer to Virtual Manager documentation; or to connect to an appliance through **VMware**, refer to the vCenter Server Appliance Management Interface documentation for vSphere.

Hardware - Console (serial connection to console port)

To connect to an appliance using a laptop, or a keyboard with a monitor, refer to the latest Secure Network Analytics Hardware Installation Guide listed on the Install and Upgrade Guides page.

Hardware - CIMC (UCS appliance)

To access an appliance through CIMC, refer to the latest guide for your platform listed on the Cisco Integrated Management Controller (CIMC) Configuration Guides page.

Alternative Method

Use the following instructions to enable an alternative method to access your Secure Network Analytics appliances for any future service needs.

If you cannot log in to the appliance using the virtual or hardware methods, you can enable SSH on the appliance network interface temporarily.

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

1. Log in to the Manager.
2. Click the **Global Settings** icon.
3. Select **Central Management**.
4. Click **Actions** menu for the appliance.
5. Select **Edit Appliance Configuration**.
6. Select the **Appliance** tab.

7. Locate the **SSH** section.
8. Select whether to enable SSH access only or to also enable root access.

    - **Enable SSH:** To allow SSH access on the appliance, check the check box.
    - **Enable Root SSH Access:** To allow root access on the appliance, check the check box.

9. Click **Apply Settings**.
10. Follow the on-screen prompts to save your changes.

⚠ Make sure to disable SSH when you have finished using it.

Data Store Private LAN Settings and Data Node Expansion

Starting with v7.4.1, Secure Network Analytics will be enforcing specific requirements for private LAN IP addresses. Make sure any Data Nodes configured using private LAN IP addresses meet these requirements:

- First three octets must be **169.254.42**
- Subnet must be **/24**

ⓘ Here's an example: 169.254.42.**x**/24 with the **x** representing a number (2 to 255) assigned by your site.

For more information, contact Cisco Support.

Data Node Patch SWU

In the update to 7.4.0, we required installing a patch SWU on each Data Node. The Data Node patch SWU is **not** required for updating Secure Network Analytics to v7.4.1.

What's New

These are the new features and improvements for the Secure Network Analytics v7.4.1 release.

Report Builder

We moved Report Builder from a separate app to the core Secure Network Analytics in v7.4.0. The app is removed automatically as part of the update from to v7.4.1.

> ⚠ Do not uninstall your existing Report Builder app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted.

You do not need to uninstall your existing app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted. Do not delete the Report Builder existing app. Make sure you follow the instructions in the Update Guide. After you've updated Secure Network Analytics to v7.4.1, you can access the Report Builder dashboard in the same location as previous versions:

1. Log in to the Manager.
2. Select the **Dashboards** menu.
3. Select **Report Builder**.

Data Retention Report

We've removed the Data Retention report from Report Builder, and you can view Data Store data in the Data Store tab. Refer to **Data Store Tab** for more information.

New Reports

We've added new reports to Report Builder so you can review the telemetry type received by the Flow Collector (**Collection Trend Reports**) or by the Data Store or Flow Collector database (**Database Ingest Trend Reports**). The reports are available for the following telemetry types:

- NetFlow
- Firewall Logs for Security Analytics and Logging (OnPrem)
- Network Visibility and Logging (NVM)

For more information about Secure Network Analytics with multi-telemetry, refer to **Multi-Telemetry Support**.

Collection Trend Reports

Run a Collection Trend report for a telemetry type to evaluate:

- Are all Flow Collectors receiving flows?
- What is the quantity of flows received?
- Were there any interruptions?

Use these reports for troubleshooting and capacity planning as follows:

- **Initial Deployments:** As you deploy new Flow Collectors, verify they are ingesting the expected amount of telemetry.
- **Troubleshooting:** Confirm your Flow Collectors are receiving telemetry, review the collection rate, and find anomalies in telemetry ingest. Also, compare the current collection rates with historical rates to identify trends in your data.
- **Capacity Planning:** Review the report results to evaluate the telemetry ingest trends over time. Use the growth trends you observe to plan for future expansion and ensure your Flow Collectors are not overloaded based on their specifications.

Name	Description	Data Store Domain Required
Firewall Log Collection Trend Report	View the collection trend for Security Analytics and Logging (OnPrem) firewall events received by your Flow Collectors.	yes
Flow Collection Trend by Exporter Report	View the collection trend for flows received by selected Flow Collectors and exporters. The results are shown by exporter.	
Flow Collection Trend by Flow Collector Report	View the collection trend for flows received by your Flow Collectors.	
NVM Collection Trend Report	View the collection trend for Network Visibility Module (NVM) flows received by your Flow Collectors.	yes

For more information about Data Store domains, refer to **Configure Domains as a Data Store Domain** .

Database Ingest Trend Reports

Run a Database Ingest Trend report for a telemetry type to evaluate:

Data Store (Data Store domain required)

- Is the Data Store receiving flows?
- What is the quantity of flows received?
- Were there any interruptions?

Flow Collector Database (Non-Data Store domain required)

- Is the Flow Collector database receiving flows?
- What is the quantity of flows received?
- Were there any interruptions?

Use these reports for troubleshooting and capacity planning as follows:

- **Initial Deployments:** As you deploy a new Data Store or Flow Collector database, run this report to verify it is ingesting the expected amount of telemetry.
- **Troubleshooting:** Confirm your Data Store or Flow Collector database is receiving flows and find anomalies in telemetry ingest. Also, compare the current collection rates with historical rates to identify trends in your data.
- **Capacity Planning:** Review the report results to evaluate the telemetry ingest trends over time. Use the growth trends you observe to plan for future expansion and ensure your Data Store or Flow Collector database is not overloaded based on the specifications.

Name	Description	Data Store Domain Required
Firewall Log Database Ingest Trend Report	View the Security Analytics and Logging (OnPrem) firewall records written to your Data Store.	yes
Flow Database Ingest Trend Report	View the flow records written to your Flow Collector databases or Data Store.	
NVM Database Ingest Trend Report	View the Network Visibility Module (NVM) records written to your Data Store.	yes

Server Identity Verification

We've added more stringent security checks for TLS connections in v7.4.x that may include additional certificate requirements. For all new configurations, make sure you follow the instructions.

- **Audit Log Destination:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "Audit Log Destination." In v7.4.1, you can configure Audit Log Destination using the server name or IPv4 address of the remote syslog server.
- **Cisco ISE or Cisco ISE-Pic:** Follow the instructions in the ISE and ISE-PIC Configuration Guide. Also, refer to **Strict ISE Server Identity Verification** for related information.
- **SMTP Configuration for Response Management:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "SMTP Configuration."

Server Identity Verification: Preparing for the Update (7.3.x to 7.4.1 only)

As part of the update from 7.3.x to 7.4.1, we will review the following configurations to confirm they meet the requirements for server identity verification:

- Audit Log Destination (Syslog over TLS)
- SMTP Configuration (email notifications for Response Management)

Review your configurations before you start the update. If your configurations do not meet the requirements, the update will fail. For more details, refer to the Update Guide.

Audit Log Destination Requirements

Before the update, make sure your Audit Log Destination configuration meets **both of the following requirements:**

- Confirm the root Certificate Authority (CA) SSL certificate from the syslog server that supports Syslog over TLS is included in your appliance trust store. Check each appliance trust store where you have Audit Log Destination configured.
- Also, if your syslog server identity certificate does not include the syslog server IP address in the Subject or Subject Alternative Name, add it to each appliance trust store where you have Audit Log Destination configured.

To access the trust stores, log in to the Manager. Select the **Global Settings** icon > **Central Management**. Click the ⋯ (**Ellipsis**) icon for the appliance. Choose **Edit Appliance Configuration**. Select the **General** tab and scroll to the **Trust Store** section. For more information, refer to the SSL/TLS Certificates for Managed Appliances Guide.

SMTP Configuration Requirements

Before the update, make sure your SMTP Configuration meets **one of the following requirements**:

- Confirm your SMTP server identity certificate from your Certificate Authority (CA) has a Subject or Subject Alternative Name that matches the IP address or host name you have configured in Secure Network Analytics, **or,**
- Add the SMTP server identity certificate to the Manager trust store.

To access the Manager trust store, log in to the Manager. Select the **Global Settings** icon > **Central Management.** Click the ⋯ (**Ellipsis**) icon for the Manager. Choose **Edit Appliance Configuration.** Select the **General** tab and scroll to the **Trust Store** section. For more information, refer to the SSL/TLS Certificates for Managed Appliances Guide.

Strict ISE Server Identity Verification

Enable Strict ISE Server Identity Verification to require server identity verification when your Manager communicates with your Cisco Identity Services Engine (ISE) or Cisco Identity Services Engine Passive Identity Connector (ISE-PIC) cluster nodes.

In addition to our other security checks, we allow communication if the ISE server identity certificate meets one of the following:

- It includes the pxGrid node name or identification information (such as FQDN) listed as a Common Name or Subject Alternative Name, or,
- It matches a certificate in your Manager trust store.

If you update Secure Network Analytics from a previous version (7.3.x or earlier), you can choose to enable this setting. If you install a new version of Secure Network Analytics at v7.4.0 or later, this setting is enabled by default.

To enable or disable this setting, select **Deploy** > **Cisco ISE Configuration**. For details, refer to the ISE and ISE-PIC Configuration Guide.

Secure Network Analytics 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 and availability, refer to the following:

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

Analytics

As of v7.4.1, on the Alerts Dashboard, you can click an alert to see its details and supporting observations, and you can also pivot to Flow Analysis and the Device Report.

For more information, refer to the Secure Network Analytics Analytics Beta Guide.

NetFlow and sFlow Support for a Single Flow Collector Image

You can now configure a single Flow Collector image for netFlow and sFlow. This enables you to switch modes from NetFlow to sFlow or sFlow to NetFlow. For instructions, refer to the System Configuration Guide.

Data Compression in the Data Store

Data compression to reduce bandwidth usage between a Flow Collector and the Data Store is enabled by default in newly installed v7.4.1 systems. It is especially helpful in scenarios where the network bandwidth from a Flow Collector to the Data Store is limited. Data compression can reduce bandwidth usage by up to 90%. For instructions, refer to the System Configuration Guide.

Data Store Appliance Support

> ⓘ If you plan to purchase a Data Store, contact Cisco Professional Services for assistance with placement, deployment, and configuration, within and as part of, your overall Secure Network Analytics deployment.

The following table describes Data Store appliance support:

Appliance	Required?	Supported Models
Data Store	yes	• DS 6200 multi node (v7.4 or greater) or single node (v7.4.1 or greater), Virtual Edition
Manager	yes	• Manager 2200, Virtual Edition • Manager 2210 or Manager Virtual Edition (v7.4 or greater). Three models available for virtual edition

Appliance	Required?	Supported Models
Flow Collector	yes	• Flow Collector 4200s, 5200s, Virtual Edition • Flow Collector 4210s or Flow Collector Virtual Edition (v7.4 or greater)* • Flow Collector 5210s or Flow Collector Virtual Edition (v7.4 or greater)* * Three models available for Virtual Edition
Flow Sensor	no	• any model at v7.3 or greater
UDP Director	no	• any model at v7.3 or greater
Endpoint Concentrator	not supported	Endpoint Concentrators are not supported for use with the Data Store.

Mix and match of Data Nodes is not supported. Data Nodes must be either all virtual or all hardware.

Single Node Data Store Support

Single Node Data Store is supported in v7.4.1 under certain conditions. For more information, refer to the Secure Network Analytics installation and configuration guides.

General Requirements

- A maximum of 4 Flow Collectors are supported.
- Customers have the option to expand Single Node Data Store systems to Multi-Node systems.

Analytics Requirements

Make sure you have sufficient resources to meet the system requirements. Refer to the Virtual Edition Appliance Installation Guide.

If you have enabled Analytics within a single node deployment, Internal IP Scanner and Worm Propagation jobs may not be trustworthy.

Data Store Enhancements

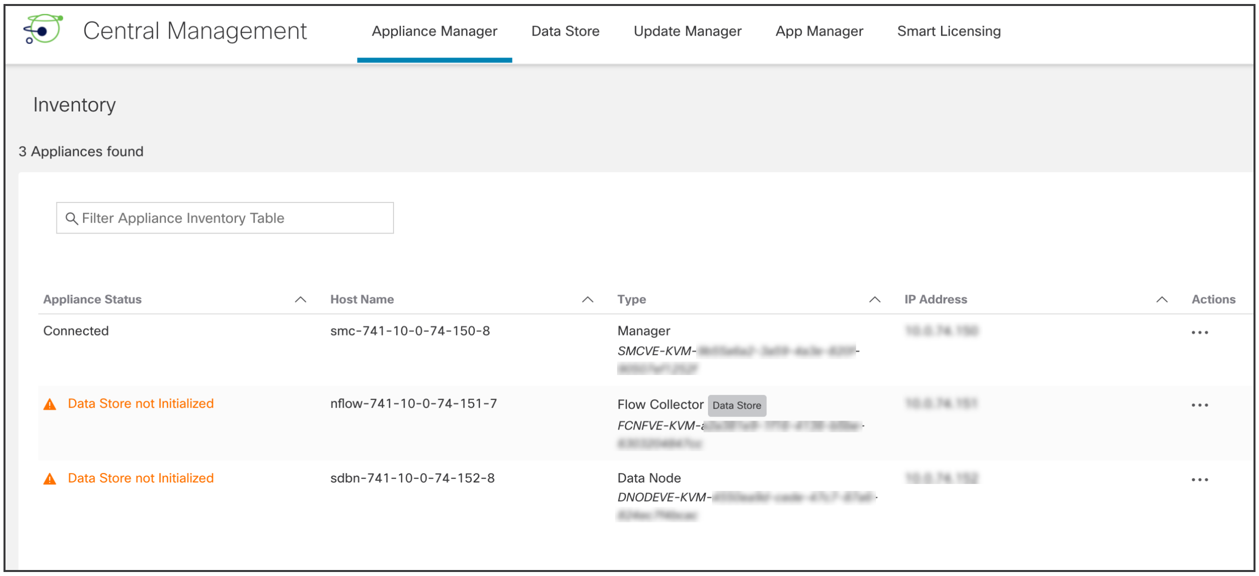
The following Data Store enhancements are included in v7.4.1. For more information, refer to the Secure Network Analytics Appliance Installation Guide (Hardware or Virtual Edition) and the System Configuration Guide.

New Appliance Error States

The following new appliance error states have been added.

Data Store Not Initialized

The Appliance Status column on the Central Management Appliance Manager tab displays a "Data Store not Initialized" message when a Data Store has not been initialized. If you see this error, you need to initialize the Data Store after you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory. Please note that the order is critical. Follow the instructions in the System Configuration Guide.



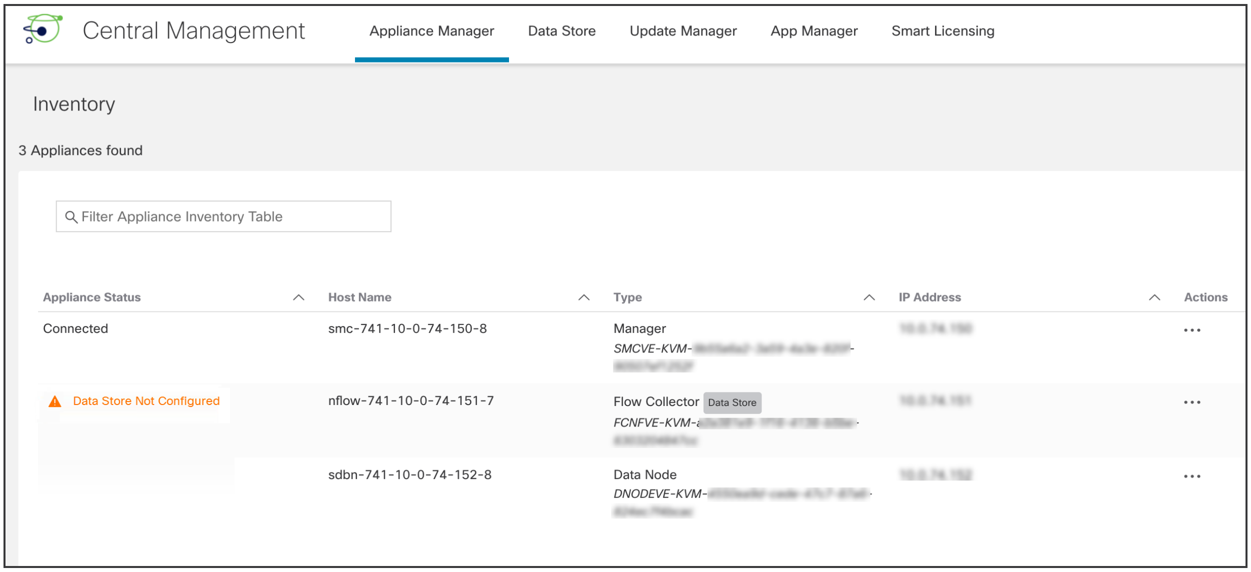
Inventory

3 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	smc-741-10-0-74-150-8	Manager SMCVE-KVM-[redacted]	[redacted]	...
⚠ Data Store not Initialized	nflow-741-10-0-74-151-7	Flow Collector Data Store FCNFVE-KVM-[redacted]	[redacted]	...
⚠ Data Store not Initialized	sdbn-741-10-0-74-152-8	Data Node DNODEVE-KVM-[redacted]	[redacted]	...

Data Store Not Configured

The Appliance Status column on the Central Management Appliance Manager tab displays a "Data Store not Configured" message when a Data Store has not been configured. If you see this error, you need to configure your new appliances for secure communication with your Data Store after you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory. Please note that the order is critical. Follow the instructions in the System Configuration Guide.



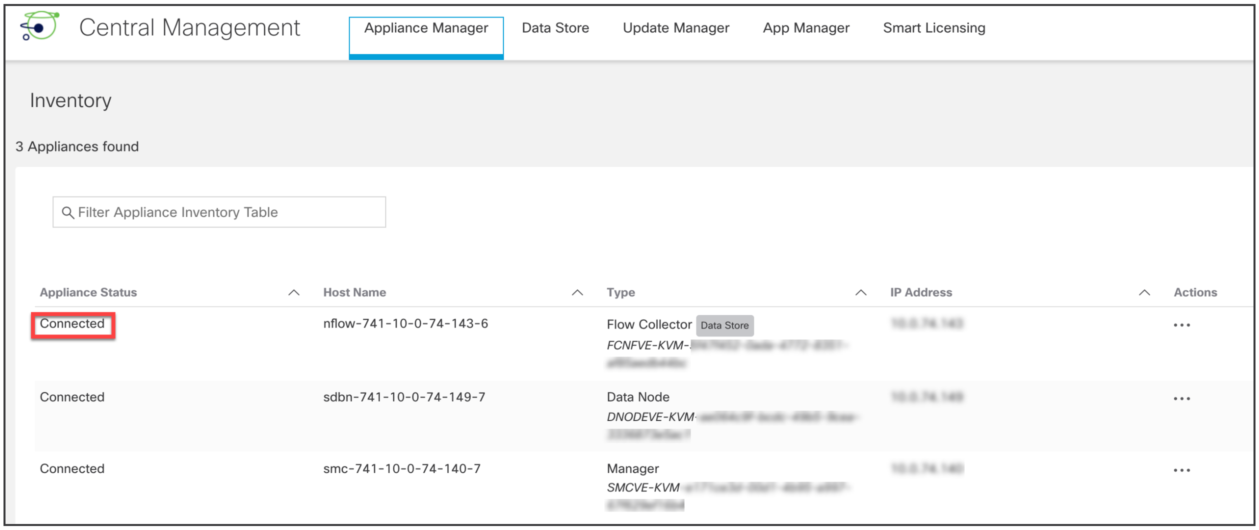
Inventory

3 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	smc-741-10-0-74-150-8	Manager *SMCVE-KVM-*[redacted]	[redacted]	...
Data Store Not Configured	nflow-741-10-0-74-151-7	Flow Collector Data Store *FCNFVE-KVM-*[redacted]	[redacted]	...
	sdbn-741-10-0-74-152-8	Data Node *DNODEVE-KVM-*[redacted]	[redacted]	...

Central Manager Appliance States - "Up" to "Connected".

The Appliance Status column on the Central Management Appliance Manager tab displays an Appliance Status of "Connected" where it previously referred to the Appliance Status as "Up".



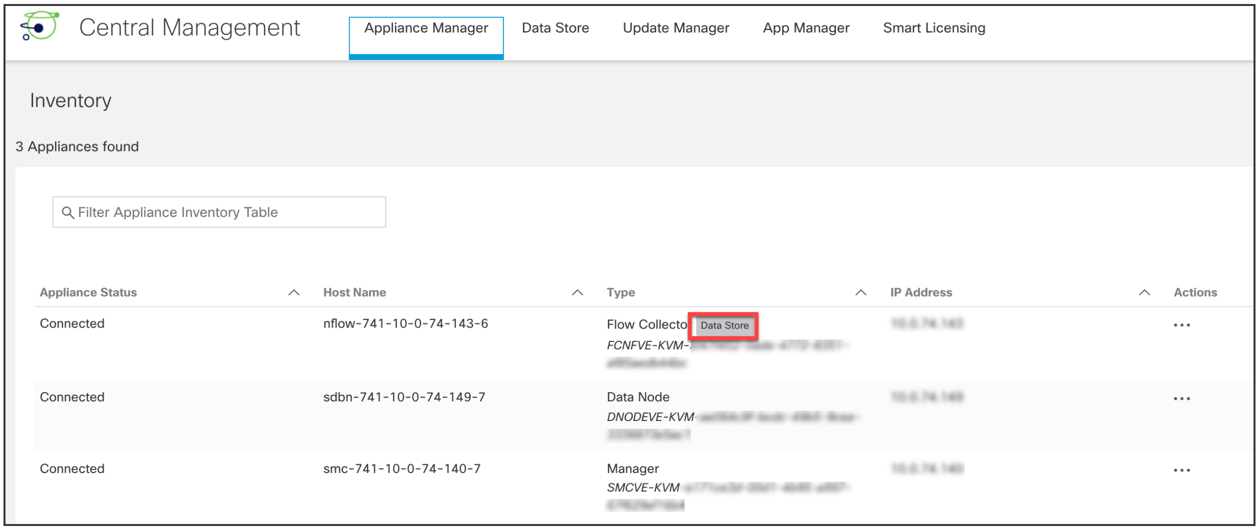
Inventory

3 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-741-10-0-74-143-6	Flow Collector Data Store *FCNFVE-KVM-*[redacted]	[redacted]	...
Connected	sdbn-741-10-0-74-149-7	Data Node *DNODEVE-KVM-*[redacted]	[redacted]	...
Connected	smc-741-10-0-74-140-7	Manager *SMCVE-KVM-*[redacted]	[redacted]	...

Data Store Flow Collectors Identified with a "Data Store" Tag

If a Flow Collector has a Data Store tag, it is configured to send flows to your Data Store. For more information about Data Store domains, refer to **Configure Domains as a Data Store Domain** .



Inventory

3 Appliances found

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-741-10-0-74-143-6	Flow Collecto Data Store *FCNFVE-KVM-*[redacted]	[redacted]	...
Connected	sdbn-741-10-0-74-149-7	Data Node *DNODEVE-KVM-*[redacted]	[redacted]	...
Connected	smc-741-10-0-74-140-7	Manager *SMCVE-KVM*[redacted]	[redacted]	...

Data Store Tab

We've added a new tab to Central Management, the Data Store tab, which has the following sub-tabs:

- **Database Control Tab**
- **Database Retention Tab**
- **Database Update Status Tab**

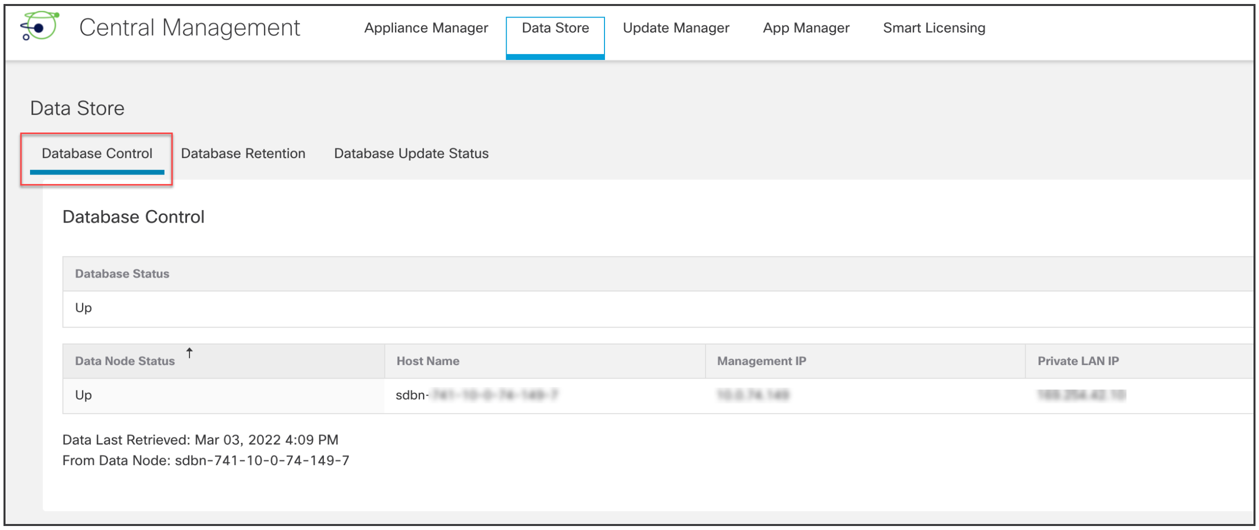
You can use these Data Store sub-tabs to do the following:

- View the status of your database or any Data Node
- View the current storage usage statistics for your database
- View the status of all Data Nodes during updates
- Start or stop the database or any Data Node
- Modify retention status for flow interface data

Database Control Tab

You can use the Database Control 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).



Central Management

Data Store

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

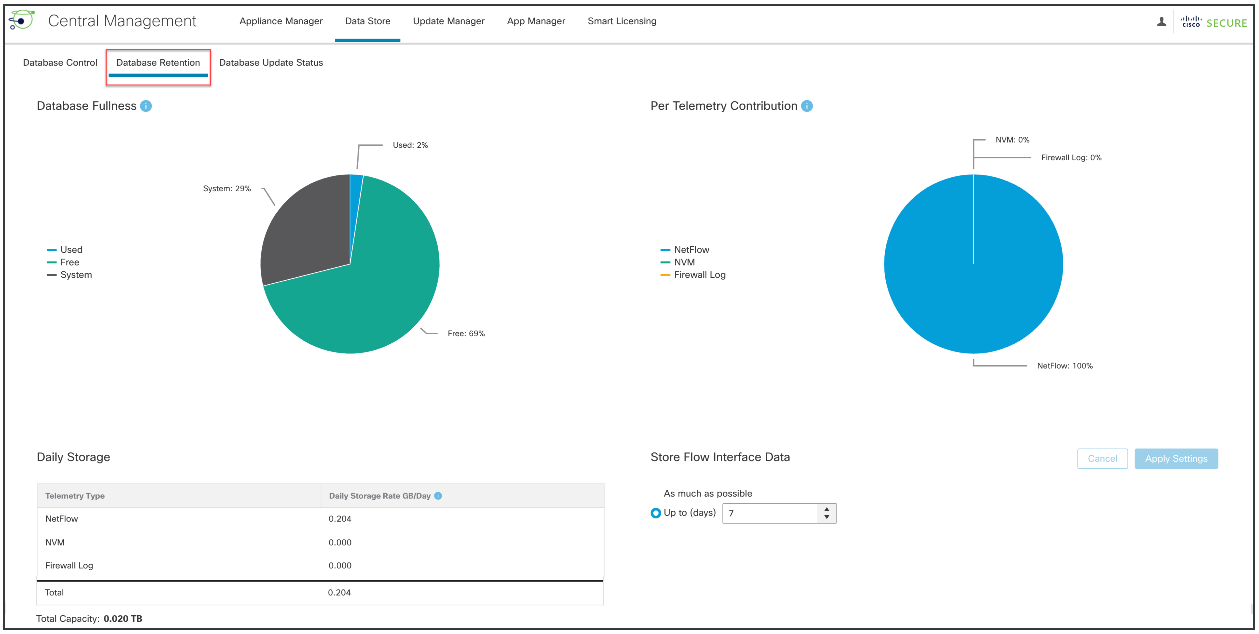
Database Retention Tab

Use the Database Retention tab to review:

- database fullness (used and free space),
- storage by telemetry type, and
- the incremental amount of data added to your database on the previous day.

We show the storage status of your database for the previous day (computed nightly).

> You'll see only the database storage status for the previous day. The database storage status is evaluated nightly; it's not updated throughout the day.



Central Management

Database Fullness

Per Telemetry Contribution

Daily Storage

Telemetry Type	Daily Storage Rate GB/Day
NetFlow	0.204
NVM	0.000
Firewall Log	0.000
Total	0.204

Total Capacity: **0.020 TB**

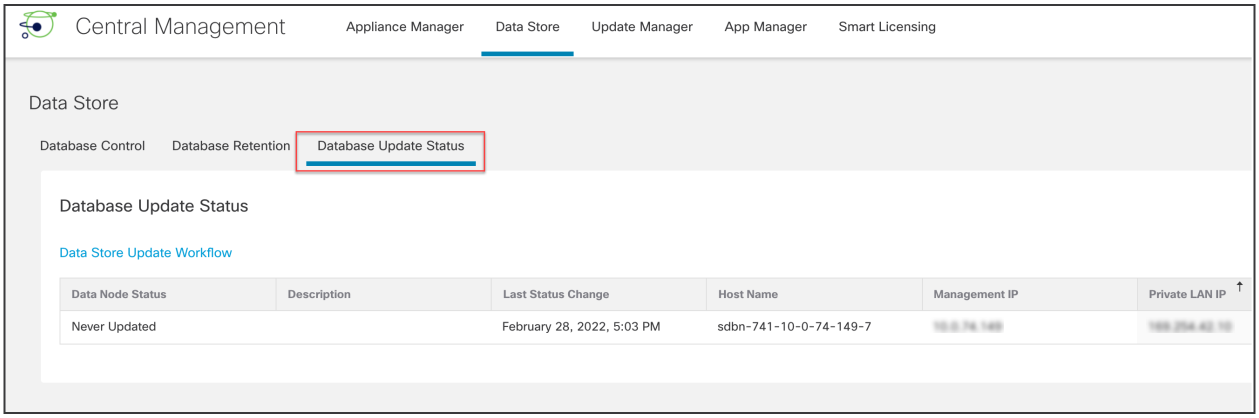
Store Flow Interface Data

As much as possible
● Up to (days) 7

Database Update Status Tab

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 **Database Control Tab** to confirm your database status is Connected. For more information, refer to the Update Guide.

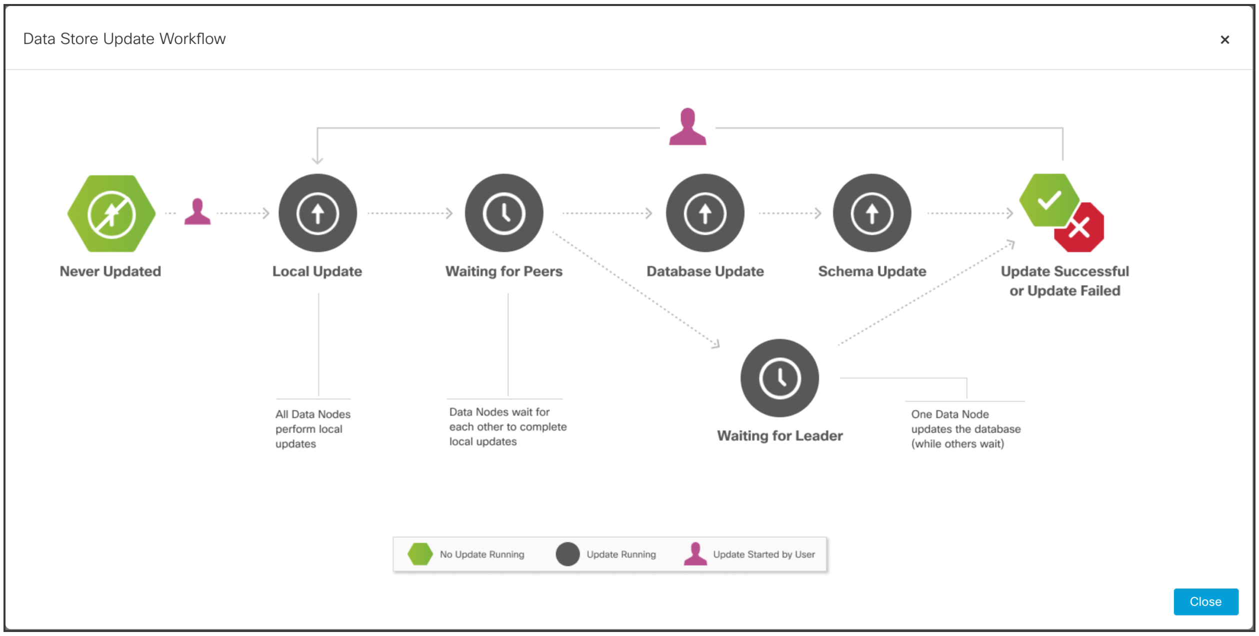


Database Update Status

Data Store Update Workflow

Data Node Status	Description	Last Status Change	Host Name	Management IP	Private LAN IP ↑
Never Updated		February 28, 2022, 5:03 PM	sdbn-741-10-0-74-149-7	[redacted]	[redacted]

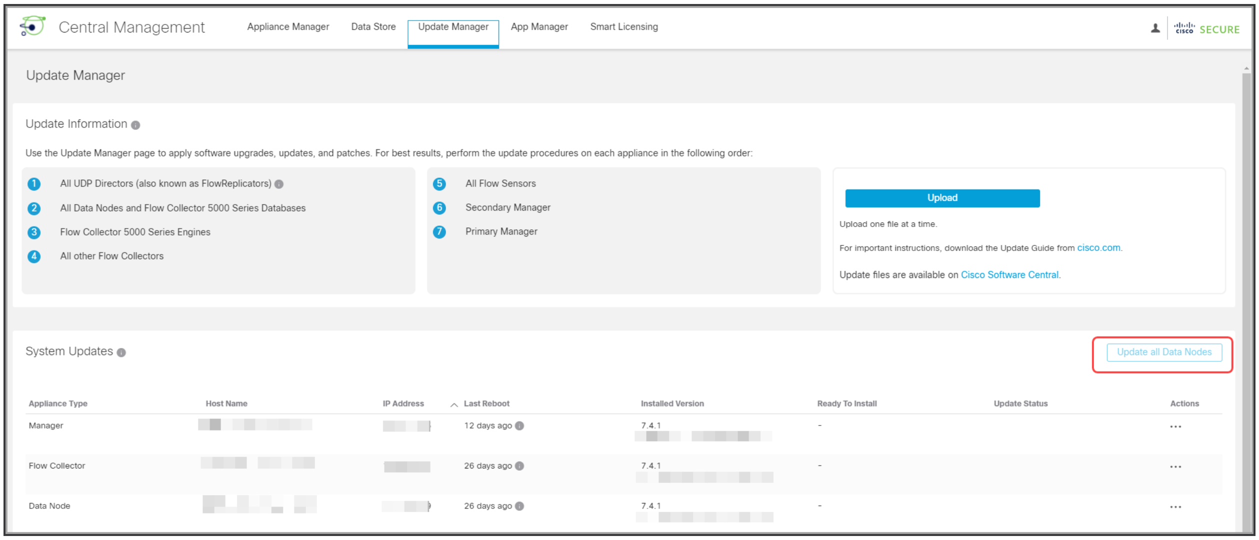
The following image shows the Data Store update workflow.


Data Store Update Workflow
×
Never Updated
Local Update
Waiting for Peers
Database Update
Schema Update
Update Successful or Update Failed
All Data Nodes perform local updates
Data Nodes wait for each other to complete local updates
Waiting for Leader
One Data Node updates the database (while others wait)
No Update Running
Update Running
Update Started by User
Close

Update All Data Nodes Button

We've added an **Update all Data Nodes** button to Central Management > Update Manager so you can update your Data Nodes at the same time.

- **Status:** The Update Manager shows the overall update status, and the new installed version is shown after the update is completed. The appliances reboot during the update process, so the status information may be delayed when the appliance goes offline. To monitor the progress of the database services update on each Data Node, go to the **Data Store** > **Database Update Status Tab**. Also, refresh each page to see the most recent status.
- **Instructions:** For a successful update, follow the update order and instructions in the Cisco Secure Network Analytics System Update Guide or patch readme file.
- **Best Practices:** Although you can update each Data Node individually, we recommend using **Update all Data Nodes** button to update your Data Nodes at the same time.



Update Information

Use the Update Manager page to apply software upgrades, updates, and patches. For best results, perform the update procedures on each appliance in the following order:

1. All UDP Directors (also known as FlowReplicators)
2. All Data Nodes and Flow Collector 5000 Series Databases
3. Flow Collector 5000 Series Engines
4. All other Flow Collectors
5. All Flow Sensors
6. Secondary Manager
7. Primary Manager

Upload one file at a time.

For important instructions, download the Update Guide from cisco.com.

Update files are available on Cisco Software Central.

System Updates

Appliance Type	Host Name	IP Address	Last Reboot	Installed Version	Ready To Install	Update Status	Actions
Manager	[redacted]	[redacted]	12 days ago	7.4.1 [redacted]	-		...
Flow Collector	[redacted]	[redacted]	26 days ago	7.4.1 [redacted]	-		...
Data Node	[redacted]	[redacted]	26 days ago	7.4.1 [redacted]	-		...

Documentation

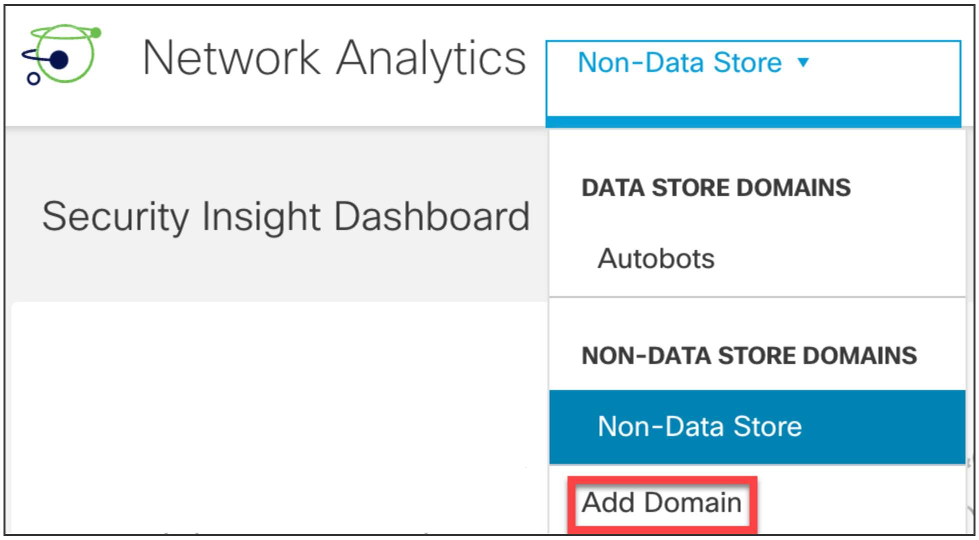
We've restructured our documentation in v7.4.1. For new v7.4.1 deployments, follow the instructions in these guides at https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html:

1. x2xx Series Hardware Appliance Installation Guide v7.4.1 or Virtual Edition Appliance Installation Guide v7.4.1
2. System Configuration Guide v7.4.1

Configure Domains as a Data Store Domain

From the Secure Network Analytics Home page, you can now add Data Store domains, which enables you to migrate to a Data Store system. Follow the instructions in the System Configuration Guide.

- **Non-Data Store Domain:** A domain without a Data Store deployed. Flows are stored in the Flow Collector database (5000 Series only).
- **Data Store Domain:** A domain with a Data Store deployed. Flows are stored in the Data Nodes.



Data Store System Configuration Menu

We've updated the Data Store menu in System Configuration. You will use these menus for new deployments or expanding your existing deployment. For a successful system configuration, follow the instructions in the System Configuration Guide.

- **SSH:** Use this menu to enable SSH temporarily, which is required for the other procedures in the Data Store menu. When you exit System Config, the system restores your previous SSH settings.
- **Initialization:** After you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory, use this menu to initialize your Data Store.
- **New Appliances:** After you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory, use this menu to configure your new Managers and Flow Collectors for secure communication with your Data Store.
- **New Data Nodes:** After you add all Managers, Flow Collectors, and Data Nodes to your Central Management inventory, use this menu to configure your new Data Nodes for secure communication with your Data Store.
- **Passwords:** Change your Data Store database passwords (dbadmin and readonlyuser). To change your Flow Collector database passwords in a Non-Data Store domain, go to Central Management > Database tab.

New Flow Collector System Alarm

The Flow Collector Database Updates Dropped alarm has been added to Secure Network Analytics. This alarm indicates that database updates for the following telemetry types (if enabled) are currently being dropped:

- Firewall log event updates
- NVM flow updates
- NetFlow flow updates

This condition typically occurs when your Flow Collector either cannot reach the Data Store database or your Data Store database has remained unreachable for an extended period of time.

For more information, refer to both the Help topic entitled "Alarm List: Flow Collector System Alarms" and the Secure Network Analytics Internal Alarm IDs Guide.

Multi-Telemetry Support

If you have a Data Store deployment, you can configure your Flow Collectors to ingest the following telemetry types simultaneously:

- NetFlow
- Network Visibility Module (NVM)
- Firewall Logs for Cisco Security Analytics and Logging (On Premises).

Multi-telemetry can be configured using:

- First Time Setup
- Flow Collector Advanced Settings. To access Advanced Settings, log in to your Flow Collector (formerly known as Appliance Administration (Admin) interface), then select **Support > Advanced Settings**.

> - Make sure your telemetry ports are unique when configuring multi-telemetry. If you configure duplicate telemetry ports, the ports will be reset to their internal defaults to avoid loss of flow data.
> - 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.

Additional Configuration Documentation

For more information about configuring:

- **Multi-telemetry during First Time Setup**: Refer to the System Configuration Guide v7.4.1.
- **Multi-telemetry using Flow Collector Advanced Settings**: Follow the instructions in the Help. Select 👤 (**User**) icon and search "Advanced Settings."
- **Network Visibility Module (NVM)**: Refer to the Endpoint License and Network Visibility Module (NVM) Configuration Guide v7.4.1.
- **Security Analytics and Logging (OnPrem)**: Refer to the Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide.

Cisco Security Analytics and Logging (On Premises) Enhancements

> ⚠ Do not uninstall the previous version of Security Analytics and Logging (OnPrem) or your existing data will be deleted.

Make sure to upgrade to Security Analytics and Logging (OnPrem) v3.1.0 through the App Manager after you've updated the system to v7.4.1. Previous versions of the app are not compatible with v7.4.1. If you don't upgrade, you won't be able to access Security Analytics and Logging (OnPrem).

Security Analytics and Logging (OnPrem) enhancements include the following:

- **Branding**: The deployment options are now Manager-only and Data Store instead of Single-node and Multi-node. This update is to avoid confusion due to similar terms in Secure Network Analytics.
- **Multiple Flow Collectors**: Secure Firewall Management Center (formerly Firepower Management Center) v7.2 supports up to five Flow Collectors.
- **Data Store Deployment Enhancements**:
  - The Data Store deployment supports one Data Node. Refer to the Single Node Deployment section for more information about requirements.
  - The Data Store deployment supports ingesting Firewall Logs, NetFlow, and NVM flows at the same time. Refer to the Multi-Telemetry section for more information.

For more information about Security Analytics and Logging (OnPrem) deployment, refer to following documents:

- Security Analytics and Logging (On Premises) Release Notes v3.1.0
- Getting Started with Cisco Security Analytics and Logging (On Premises)
- Security Analytics and Logging (On Premises) v3.1.0: Firewall Event Integration 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: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

What's Been Fixed

This section summarizes fixes made in this release for issues (bugs/defects) reported by customers in previous releases. The Secure Network Analytics Defect (SWD or LSQ) number is provided for reference.

Version 7.4.1

Defect	Description
SWD-16381	Fixed an issue where the Audit Category wasn't showing system-level tasks. (LSQ-5564)
SWD-16394	Corrected a documentation error in the Data Store Virtual Edition Deployment Overview Guide v7.3.2 (LSQ-5592).
SWD-16406	Fixed an issue where customers were seeing incorrect dates for alarms from the Dashboard. (LSQ-5440)
SWD-16487	Fixed an issue related to the Host Classifier Domain Controllers query causing a high CPU usage on the Flow Collector. (LSQ-5614)
SWD-16501	Updated documentation to indicate that SSO SAML Request Signing is not supported.
SWD-16599	Fixed an issue where the login page wasn't displaying after upgrading to v7.3.1.
SWD-16634	Fixed an issue where the SSE Connector wasn't communicating with the svc-ctr-service using public certificates.
SWD-16718	Fixed an issue where the Tomcat log file permissions changed when upgrading from v7.1.1 to v7.2.1.
SWD-16755	Fixed an issue where the Flow Collector Interfaces Count Exceeded alarm initiated unnecessarily.
SWD-16764	Fixed an issue where the UDPD was interfering with the templates of ASA that go through VPN and Checkpoint.

Defect	Description
SWD-16828	Fixed an issue where the Interface Top reports showed inaccurate results.
SWD-16844	Improved performance of the LDAP authentication query method to address an inconsistent time-out issue.
SWD-16856	Fixed an issue where the Smart License manager showed 0 consumption for End Point (AnyConnect NVM).
SWD-16868	Fixed an issue in v7.3.2 where the Flow Sensor wasn't supporting management and data interfaces on same subnet (for example, eth0 and eth1).
SWD-16891	Fixed an issue where the Flow Collector database wasn't coming up after upgrading to v7.2.1.
SWD-16897	Fixed an issue with the CTR Enabled Metrics reports provided inaccurate results.
SWD-16902	Updated the Cognitive Installation guide to provide additional information about domains.
SWD-16929	Fixed an issue where there was an insufficient buffer size for receiving ISE session with pxGrid 2.0.
SWD-17057	Fixed an issue where the engine produced a flex_security_events file containing an invalid JSON variable.
SWD-17097	Fixed an issue where users installed v7.4.0 from an ISO and rebooted, but they couldn't navigate past the first AST configuration screen.
SWD-17172	Enhanced the Flow Sensor Virtual Edition to support 1G interfaces for large VMs.
SWD-17178	Fixed an issue in v7.4.0 where GRUB wasn't recognizing disk partitions with type 0700.

Defect	Description
SWD-17252	Updated the ISE integration port information in documentation v7.3.2 and later.
SWD-17265	Fixed an issue related to unexpected http error codes in reporting api (/tenants/{tenantId}/flows/queries).
SWD-17311	Reviewed how to more thoroughly integrate Network Based Application Recognition (NBAR) functionality with Secure Network Analytics.
SWD-17361	Fixed an issue with the engine's scaling cap to insure the host and flow caches scale properly on Flow Collector 5K appliances.
SWD-17376	Fixed an issue where the engine caused the SWAAgent to reset its message server during Host Group configuration updates resulting in a mutex locked up condition.
SWD-17409	Fixed an issue where the FC agent (fc-core) wasn't working properly if sending unsupported messages to the engine.
SWD-17424	Fixed an alarms issue by increasing the maximum number of ROS containers from 1024 to 2048 and increasing the alarm lever from 700 to 1700.
SWD-17439	Fixed a SIGABRT issue that occurred whenever a group ID with a number greater than the current number of groups was deleted from the baseline file.
SWD-17450	Fixed an issue where the engine shut down process needed to call the stop_smc_agent() function on non-graceful shutdowns.
SWD-17532	Fixed an issue with the Flow Collector Exporter Count Exceeded indicators display.
SWD-17551	Fixed a SIGABRT issue related to the log_backtrace function.
SWD-17574	Updated the ASA port assignment content in Secure Analytics and Logging (On-Prem) documentation.

Version 7.4.0

Defect	Description
SWD-15701	Fixed an issue with NullExceptionPointer that occurred when attempting to disable a custom mitigation script. (LSQ-5159)
SWD-16053	Removed references to the Endpoint Concentrator in documentation. (LSQ-5930)
SWD-16075	Enhanced Smart Licensing. (LSQ-5431)
SWD-16087	Fixed an issue where Flow Based Identities were missing on the Users report.
SWD-16206	Fixed an issue related to the ASA flow byte counts showing 0 client bytes and is displaying the NAT source address. (LSQ-5320)
SWD-16217	Fixed an issue where the segfault errors in v7.2.1 Flow Sensor console due to file /etc/udev/rules.d/70-persistent-net.rules being empty.
SWD-16296	Fixed an issue where IDs generated from idgen were getting lost.
SWD-16314	Fixed an issue where the Flow Search for sFlow at the exporter level was not returning results in v7.3.0. (LSQ-5508)
SWD-16340	Fixed an issue with the "Associated Flows" search was not filtering for IP address or the protocol.
SWD-16346	Fixed an issue where the incorrect status was coming back from the engine for inactive exporters.
SWD-16366	Added this content to documentation: Default Data Store Retention is not 7 days.
SWD-16369	Updated the Syslog message for reoccurring Recon Alarm.
SWD-16383	Fixed an issue related to SAL CONNECTION_END_EVENT last_ packet_second computation.

Defect	Description
SWD-16396	Fixed an issue where the Flow Sensor related to the eth0's MTU for exporter when dpdk is used.
SWD-16401	Fixed an issue that occurred with the Manager NullExceptionPointer when attempting to Disable a Custom mitigation script. (LSQ-5159)
SWD-16413	Fixed an issue related to cognitive reports TLS TCP (HTTPS) traffic with client port 443.
SWD-16416	Fixed an issue for the v7.3.1 Flow Collector engine where there was a "Thread interrupted" message after the archive hour due to a particularly high rate of security events.
SWD-16417	Fixed an issue in the v7.3.1 Flow Collector engine SIGSEGV for the host_flow_condition due to a particularly high rate of security events.
SWD-16428	Fixed an issue where the SNMP Polling in v7.3.0 and v7.3.1 stalled at Pending with no results returning for days and sometimes weeks. (LSQ-5521, LSQ-5496)
SWD-16432	Fixed an issue where the Flow Sensor was sometimes sending an incorrect FlowSensorInitiator element.
SWD-16441	Fixed an issue so that baseline data files are now excluded from backup. (LSQ-5617)
SWD-16453	Documented the default policy for the All Inside host group and what happens when you disable "When Host Is Target" setting.
SWD-16489	Fixed an issue where the Proxy Ingest option was grayed out without a license file for v7.3.1. (LSQ-5624)
SWD-16503	Updated documentation to clarify that Vertica Backup Restore (VBR) for the Flow Collector database is not supported. (LSQ-5636)

Defect	Description
SWD-16576	Fixed an issue where the CDS TopConversations default query was failing for order-by flows.
SWD-16588	Fixed an issue where the SecureX User Role was unable to access the SecureX Ribbon.
SWD-16626	Fixed an issue with the Decode Error processing the AVC Subapplication Value field and 1 Byte TCP Flag fields.
SWD-16629	Updated documentation to include details about the syslog variables related to each alarm type.
SWD-16635	Updated documentation to include the ISE integration prerequisite for resolvable ISE nodes.
SWD-16647	Added documentation content about using the flow search advanced parameters for the Web UI.
SWD-16669	Added information to the UI to indicate that the Web hook URL is limited to 200 characters.
SWD-16844	Fixed an LDAP timeout issue related to the authentication query method performance. (LSQ-5652)
SWD-16902	Updated the Cognitive Analytics Configuration Guide to include more detailed content about domains.

Known Issues

This section summarizes issues (bugs) that are known to exist in this release. Where possible, workarounds are included. The defect number is provided for reference.

Defect	Description	Workaround
LVA-719	The Active Directory Lookup Configuration password is stored in cleartext in configuration files.	**Details:** The password is accessible in the local file system, the File Browser in the Appliance Administration interface (admin credentials required), and in unencrypted backup configuration files. **Mitigation Options:** If you configure Active Directory Lookup: • Limit the user account privileges and monitor the account for misuse. • Encrypt your backup configuration files. Refer to "Backup Configuration Encryption" in the Help. If you prefer to disable Active Directory Lookup: • Delete your Active Directory Lookup configurations. Go to Deploy > Active Directory in your Manager. • Delete any unencrypted backup configuration files. Refer to "Backup Configuration Encryption" and "Backup Configuration Files" in the Help.
SWAPP-477	When you have installed Host Classifier v3.1.0 on either v7.4.0 or v7.4.1, and your system contains a combination of several Data Store	Install Host Classifier v3.1.1 when it is released.

Defect	Description	Workaround
	and Non-Data Store domains, the domain monitor that runs every 5 minutes loops at 1-minute intervals, which produces a large number of logs. This increases the disk usage on the Manager.	
SWD-12574	If a user logs in to the command line interface without any failed attempts, the EPOCH date (January 1, 1970) might display.	None currently available.
SWD-17388	On the Configure Priorities page, the only telemetry source displayed in the Telemetry drop-down list that is currently supported by Cisco Secure Network Analytics is **Netflow**. All other source types are not supported.	None currently available.
SWD-17425	When one or more Data Nodes is added to an existing Vertica database, a rebalance of the data to utilize the new node fails to automatically occur.	Manually initiate a rebalance by performing the following steps: 1. Use a root shell via SSH or a console (without SSH) to connect to any pre-existing UP Data Node. 2. Type **su dbadmin**

Defect	Description	Workaround
		3. Execute the following command: `/opt/vertica/bin/admintools -t rebalance_data -d sw -p -k 1<dbadmin password>`
SWD-17452	When you initially open the Observation Types page and click the ➡ (**Arrow Right**) icon next to an observation type that has no data (0), no related data is displayed on the Selected Observations page that opens, which is correct functionality. If you perform one or more searches on other observations and then search again for the observation that initially showed no results, the Time and Device columns now incorrectly show data, even though the results in the lower right corner of the table correctly shows **0-0 of 0 results**.	None currently available.
SWD-17516	The Analytics observation jobs, InternalIPScanner and WormPropagation,	None currently available.

Defect	Description	Workaround
	aren't running as they should.	
SWD-17612	When you install an update on an individual Data Node (by clicking the ··· (**Ellipsis**) icon in the Actions menu), a fail banner is provided if the database **Up**. However, when you use the **Update all Data Nodes** button, the error occurs but no banner is displayed (it fails silently).	None currently available.
SWD-17635	When two Data Nodes with lower IPs are shut down, there is missing data under the Database Control tab.	None currently available.
SWD-17644	When upgrading with failover from v7.4.0 to v7.4.1, activating the failover causes a "Data Store Not Initialized" error.	Make sure to complete your setup; follow system prompts.
SWD-17668	The message, "No data to display," appears in the Top Application Traffic area of Network Analytics.	None currently available.

Defect	Description	Workaround
SWD-17676	When upgrading from v7.3.x, the appliance status for the Flow Sensor might display as **Config Changes Pending**, particularly if you choose to update the Flow Sensor last.	Continue with the upgrade process, the issue is resolved after the primary Manager is updated.
SWD-17936 CSCwc25672	When upgrading a Flow Sensor 4240 to v7.4.1, a 404 error displays, and UNREG or Unregistered is shown in the appliance console.	**Do this first:** Make sure you have the latest SWU file for your Flow Sensor. See the "SWU Files" section of the v7.4.1 Update Guide for more details. To access the appliance, remove the 40 GB requirement as follows: 1. Use a root shell via SSH or a console (without SSH). 2. Execute the following command: `sed -i 's/platform="ST-FS4240-K9" nicspeed="eth+,40000"/platform="ST-FS4240-K9"/' /lancope/admin/lib/model.xml` 3. Reboot the appliance.
SWD-18329	The "Last Status Change" and "Data Node Update Status" fields on the Data Store > Database Update tab in Central Management do not change following a rollup installation of a Data Node.	None currently available.

Defect	Description	Workaround
N/A	If you have enabled Analytics within a single node deployment, unpublished alerts will behave inaccurately. Unpublished alerts are alerts that Secure Network Analytics still considers to be in the experimental phase and therefore have not yet been officially published. They are Off by default. Listed below are the unpublished alerts: • NetBIOS Connection Spike • New IP Scanner • New SNMP Sweep • Outbound SMB Spike • SMB Connection Spike • Suspected Remote Access Tool Heartbeat • Worm Propagation	None currently available.
NA	On the Flow Sensor	To enable application identification, the

Defect	Description	Workaround
	Virtual Edition, the “Export Application Identification” indicator is off by default.	advanced setting will need to be selected manually.

Change History

Revision	Revision Date	Description
1_0	April 18, 2022	Initial version.
1_1	May 9, 2022	General Availability (GA).
1_2	July 1, 2022	Updated the **Multi-Telemetry Support** section, and added SWD-17936 to the **Known Issues** section.
1_3	July 15, 2022	Updated the SWD-17936 workaround in the **Known Issues** section.
1_4	August 5, 2022	Added note for Compliance Customers to the **Before You Update** section.
1_5	November 1, 2022	Added SWD-18329 to the **Known Issues** section.
1_6	February 7, 2023	Updated the **Analytics Requirements** section.

Release Support Information

Official General Availability (GA) date for Release 7.4.1 is May 9, 2022.

For support timeline information regarding general software maintenance support, patches, general maintenance releases, or other information regarding Cisco Stealthwatch Release Support lifecycle, please refer to Cisco Stealthwatch® Software Release Model and Release Support Timeline Product Bulletin.

Copyright Information