



Cisco Secure Network Analytics

Release Notes 7.4.2



Table of Contents

Introduction	4
Overview	4
Rebranding	4
Terminology	6
Before You Update	6
Software Version	6
Supported Hardware Platforms	7
CIMC Firmware Version	7
Notice of VMware Compatibility Changes	8
Certificate Check	8
Cisco Bundles	8
High Availability	8
Third-Party Applications	8
Apps Version Compatibility	8
Browsers	9
Alternative Access	9
Data Store Private LAN Settings and Data Node Expansion	10
Data Node Patch SWU	10
What's New	11
Menu Structure	11
Former Menu Structure (v7.4.1, v7.4.0, and v7.3.x)	11
New Menu Structure (v7.4.2)	11
Certificate Expiration Alarms and Email Notifications	15
Replacing Unexpired Cisco Self-Signed Appliance Identity Certificates (Certificate Refresh)	16
ECDSA Certificate Compatibility	16
Report Builder	16
Server Identity Verification	17
Server Identity Verification: Preparing for the Update (7.3.x to 7.4.2 only)	17

Audit Log Destination Requirements	18
SMTP Configuration Requirements	18
Strict ISE Server Identity Verification	18
Secure Network Analytics Apps	19
Access the Apps	19
Analytics	20
Enable Analytics	22
Access Analytics	22
Data Store Appliance Support	23
Data Store Enhancements	24
Transitioning Non-Data Store Flow Collectors to Data Store Flow Collectors	24
Transitioning Data Store Flow Collectors Identified with a "Data Store" Transition Tag	25
Database Passwords Cannot be Changed for Transitioning Flow Collectors	26
Oldest Data in Data Store Table	26
Synchronizing Data Store and Non-Data Store Domains	27
Redundant Site Configuration	27
Data Store System Configuration Menu	27
Endpoint License and Network Visibility Module Enhancements	28
Use Flow Collector Advanced Settings to Configure Newly Added Fields	28
MTU Configuration	30
New Flow Collector System Alarm	30
What's Been Fixed	31
Version 7.4.2	31
Version 7.4.1	36
Version 7.4.0	39
Known Issues	42
Contacting Support	45
Change History	46
Release Support Information	47

Introduction

Overview

This document provides information about the new features and improvements, bug fixes, and known issues for the v7.4.2 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](#).

Software Version

To update the appliance software to v7.4.2, the appliance must have version 7.3.0, 7.3.1, 7.3.2, 7.4.0, or 7.4.1 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**.
- **Uploading Files:** Make sure you upload all SWU files to the Update Manager before you start installing rollup patches or software update files. Follow the instructions in the [Update Guide](#).
- **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.
- **Baselining:** Before you start the update to v7.4.2, make sure your appliances have been running on the same version of **v7.3.0, v7.3.1, v7.3.2, v7.4.0, or v7.4.1** for more than 1 month (30 days). If you've updated your system to more than one version in a short period of time, your system baselining may be impacted. For assistance, please contact [Cisco Support](#).
- **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

Secure Network Analytics is available on the latest generation of UCS hardware (M6). 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 2200	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

Notice of VMware Compatibility Changes



Secure Network Analytics v7.4.2 is compatible with VMware 7.0 and 8.0. We do not support VMware 6.0, 6.5, or 6.7 with Secure Network Analytics v7.4.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

Certificate Check

Updating to v7.4.2 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 v7.4.2, 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.

Apps Version Compatibility



If you have previously installed apps, make sure they are compatible with the version of Secure Network Analytics you will be installing.

To learn how to confirm the list of your installed apps and to see the latest Secure Network Analytics apps compatibility information, refer to the [Secure Network Analytics Apps Version Compatibility Matrix](#).

Browsers

- **Compatible Browsers:** Secure Network Analytics supports the latest rapid release 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 v7.4.2.

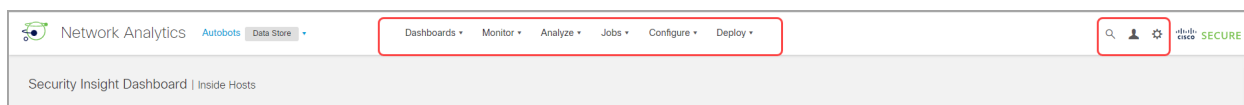
What's New

These are the new features and improvements for the Secure Network Analytics v7.4.2 release.

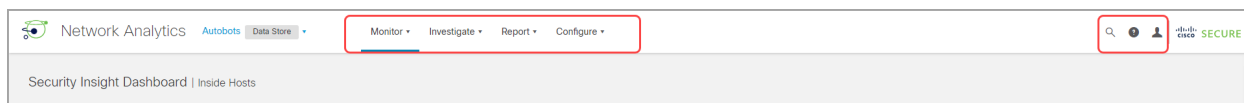
Menu Structure

We changed our menu structure and page names in v7.4.2 for a more simplified experience. We also updated our Help menu organization to match the new structure.

Former Menu Structure (v7.4.1, v7.4.0, and v7.3.x)



New Menu Structure (v7.4.2)



The following table is organized by the Former Menu Location and shows the new page names and menu locations.








Some of the new menus also include categories, such as **Configure > GLOBAL Central Management** (where Global is the category), and we've listed them here.

Former Page Name	New Page Name	Former Menu Location	New Menu Location
Network Security	Security Insight Dashboard	Dashboards	Monitor
Secure Cloud Analytics	Secure Cloud Analytics	Dashboards	Monitor > Integrations
Visibility Assessment	Visibility Assessment	Dashboards	Report
Report Builder	Report Builder	Dashboards	Report
Global Threat Alerts	Global Threat Alerts	Dashboards	Monitor > Integrations

Former Page Name	New Page Name	Former Menu Location	New Menu Location
ETA Cryptographic Audit	ETA Cryptographic Audit	Dashboards	Apps
Host Classifier	Host Classifier	Dashboards	Apps
Network Diagrams	Network Diagrams	Dashboards	Apps
Security Analytics and Logging	Security Analytics and Logging (OnPrem) Firewall Events	Dashboards	Apps
Hosts	Hosts	Monitor	Investigate > Assets
Host Groups	Host Groups	Monitor	Investigate > Assets
Users	Users	Monitor	Investigate > Assets
ISE ANC Assignments	ISE ANC Policy Assignments	Monitor	Monitor > Integrations
Interfaces	Interfaces	Monitor	Investigate > Assets
Alerts	Alerts	Monitor	Monitor
Observations	Observations	Monitor	Monitor
Flow Search	Flow Search	Analyze	Investigate
Saved Searches	Saved Searches	Analyze	Investigate > Search Management
Saved Results	Saved Results	Analyze	Investigate >

Former Page Name	New Page Name	Former Menu Location	New Menu Location
			Search Management
Host Search	Host Search	Analyze	Investigate
Copyright Infringement	Copyright Infringement	Analyze	Investigate
Job Management	Job Management	Jobs	Investigate > Search Management
Policy Management	Policy Management	Configure	Configure > Detection
Alarms	Alarm Severity	Configure	Configure > Detection
Analytics	Analytics	Configure	Configure > Detection
Alerts	Alerts	Configure	Configure > Detection
Host Group Management	Host Group Management	Configure	Configure > Detection
Network Classification	Network Scanners	Configure	Configure > Detection
Services	Services	Configure	Configure > System
Applications	Applications	Configure	Configure > System
Response Management	Response Management	Configure	Configure > Detection

Former Page Name	New Page Name	Former Menu Location	New Menu Location
Domain Properties	Domain Properties	Configure	Configure > System
Flow Collectors	Flow Collectors	Configure	Configure > System
Exporters	Exporters	Configure	Configure > System
Cisco ISE Configuration	Cisco ISE	Deploy	Configure > Integrations
Active Directory	Active Directory	Deploy	Configure > Integrations
Secure Cloud Analytics Configuration	Secure Cloud Analytics	Deploy	Configure > Integrations
Help	Help	 (User) icon	 (Help) icon
Resources	Resources	 (User) icon	 (Help) icon
About	About	 (User) icon	 (Help) icon
Profile	Profile	 (User) icon	 (User) icon
Logout	Logout	 (User) icon	 (User) icon
Central Management	Central Management	 (Global Settings) icon	Configure > Global Note: Appliance Manager is now named Inventory.
Manager Configuration	Manager	 (Global Settings) icon	Configure > Global

Former Page Name	New Page Name	Former Menu Location	New Menu Location
Packet Analyzer Configuration	Packet Analyzer	 (Global Settings) icon	Configure > Global
UDP Director Configuration	UDP Director	 (Global Settings) icon	Configure > Global
External Lookup Configuration	External Lookup	 (Global Settings) icon	Configure > Global
User Management	User Management	 (Global Settings) icon	Configure > Global
SecureX Configuration	SecureX	 (Global Settings) icon	Configure > Integrations
Select Language	Language	 (Global Settings) icon	 (User) icon

Certificate Expiration Alarms and Email Notifications

If you have appliance identity certificates expiring, the following system alarms will begin displaying on your dashboard:

- Appliance Certificate Expiration less than 90 days
- Appliance Certificate Expiration less than 60 days
- Appliance Certificate Expiration less than 30 days
- Appliance Certificate Expiration less than 14 days
- Appliance Certificate Expiration less than 3 days
- Appliance Certificate has expired

These system alarms are enabled by default and will continue to display until you've replaced the appliance identity certificates, as required.

If you've previously set up email notifications through Response Management, you'll also receive email messages indicating that your appliance identity certificates will be expiring.

If you'd like to modify which email notifications you'll receive, refer to the "Receiving Notifications for Expiring Certificates" section of the [SSL/TLS Certificates for Managed Appliances Guide](#) for more information.

Replacing Unexpired Cisco Self-Signed Appliance Identity Certificates (Certificate Refresh)

We have simplified the workflow for generating new Cisco self-signed appliance identity certificates when your existing certificates have not expired. You can generate identity certificates for all managed appliances or for selected, individual appliances using the Certificate Refresh menu in the Manager appliance console (System Configuration).

- **Host Information:** The appliance host information (IP address, host name, domain name) is preserved.
- **Required Patch:** Follow the instructions in the [Secure Network Analytics Manager Update Patch v7.4.2](#) to install patch ROLLUP20230928-01 (or later) on your Managers.
- **Instructions:** Follow the instructions in the [SSL/TLS Certificates for Managed Appliances Guide](#).
- **Custom Certificates:** The appliance identity certificate is replaced automatically with a Cisco self-signed appliance identity certificate in this certificate refresh procedure. To use custom certificates, follow the instructions for Replacing the SSL/TLS Appliance Identity Certificate in [SSL/TLS Certificates for Managed Appliances Guide](#).

ECDSA Certificate Compatibility

When you install an appliance, generate an appliance identity certificate, or generate a client identity certificate, Secure Network Analytics generates the certificate with an RSA key.

In v7.4.2, you can replace the system certificates with custom certificates that use ECDSA keys generated with NIST P-256, P-384, or P-521 curves.

You can also upload custom certificates that use ECDSA keys (generated with NIST P-256, P-384, or P-521 curves) to the appliance Trust Stores in Central Management.

For instructions, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#).

Report Builder

We moved Report Builder from a separate app to the core Secure Network Analytics in v7.4.0. If you are updating Secure Network Analytics from v7.3.x to v7.4.2, your app will be removed automatically as part of this update.



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.

Follow the instructions in the [Update Guide](#). After you've updated Secure Network Analytics to v7.4.2, access the Report Builder dashboard as follows:

1. Log in to the Manager.
2. Select the **Report** menu.
3. Select **Report Builder**.
4. For instructions, click (**Help**) icon > **Help**.



Before you run a report, select the Data Store domain or Non-Data Store domain that includes your data.

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 (**Help**) icon > **Help**, and search "Audit Log Destination." In v7.4.1 and later, 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 (**Help**) icon > **Help**, and search "SMTP Configuration."

Server Identity Verification: Preparing for the Update (7.3.x to 7.4.2 only)

As part of the update from 7.3.x to 7.4.2, 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 **Configure > GLOBAL 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 **Configure > GLOBAL 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](#)

Access the Apps

After you've upgraded to v7.4.2, do the following to access the apps:

1. From the main menu, select **Configure > GLOBAL Central Management**.
2. Click the Secure Network Analytics App Manager tab.

The App Manager page opens. A list of installed apps are listed in the Apps table.

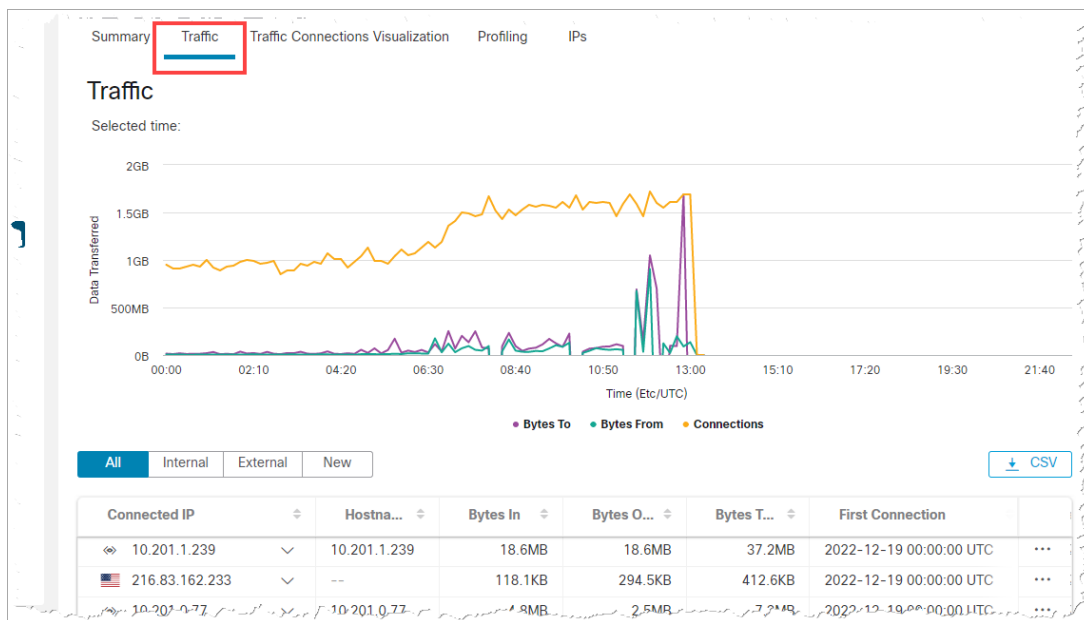
Analytics

The following enhancements to Analytics have been made in Secure Network Analytics v7.4.2:

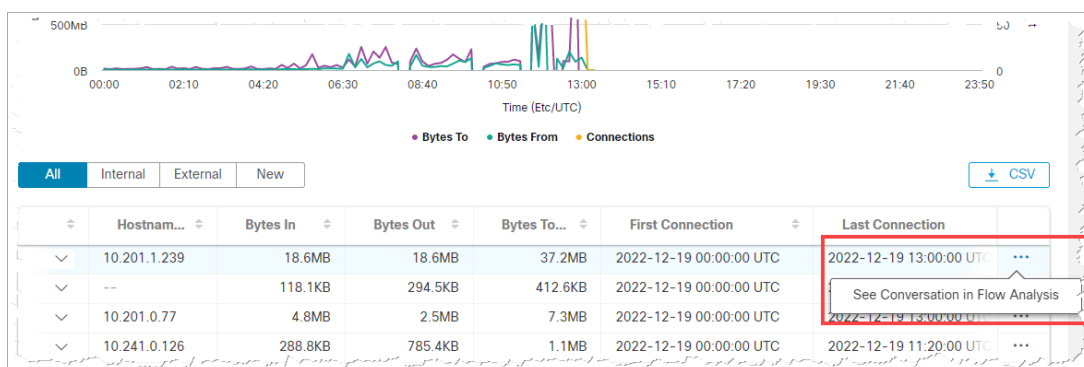
- Alerts and Observations now has SMC Failover support. Alerts and Observations data is processed and stored only on the Manager that is currently in the primary role. When you promote the original primary Manager back to the primary role, you will not be able to view any alerts and observations data that was processed on the original secondary Manager while it served in the primary role.
- When upgrading from v7.4.1 to v7.4.2, customer's data does not persist.
- Added the following new alerts:
 - LDAP Connection Spike
 - Outbound LDAP Spike
 - Protocol Forgery
 - Repeated Umbrella Sinkhole Communications
- Added the following new observation:
 - Umbrella Sinkhole Hit Observation
- Renamed the Outbound SMB Spike alert to Outbound SMB Connection Spike
- Added the following new system alarms:
 - Analytics does not support more than 1 Data Store domain
 - Analytics Performance has degraded
 - Analytics results are incomplete
- Device Report:
 - Moved the alerts data from the Summary tab to the main page.



- Added the Traffic Connections Visualization tab.



- Added the “See Conversation in Flow Analysis” link to the last column in the table on the Traffic tab.



- Added the Roles page (select **Investigate > ASSETS Roles** from the menu).

Roles
Investigate

This page shows the Active Roles with at least one matching device for the selected timeframe. The default timeframe is the last 7 days, with a maximum timeframe of the last 90 days. Active Roles is an automated list that depends on what types of telemetry are being ingested. When you select Roles, the Matching Sources table will display the devices associated with the Roles.

Active Dates: 2022-12-12 13:22:31 UTC - 2022-12-19 05:00:00 UTC

Active Dates: 2022-12-12 13:22:31 UTC | 2022-12-19 05:00:00 UTC

Reset Apply

Active Roles from 2022-12-12 13:22:31 UTC to 2022-12-19 05:00:00 UTC

Database Server	3
DNS Server	5
Domain Controller	5
Kerberos Node	318
Mail Server	3
NetFlow Exporter	3

CSV

Matching Sources	Role Names
10.10.30.12	Database Server
10.10.31.48	Database Server
10.201.0.55	Database Server

20 Per Page 1-3 of 3 results |<< 1 / 1 >>|

Enable Analytics

To enable Analytics, select **Configure > DETECTION Analytics** from the main menu. On the Welcome page that opens, in the upper right corner of the page, click the switch so that the label displays *Analytics On*.

Access Analytics

If Analytics is already enabled, select **Monitor > Alerts** from the main menu. The Alerts Summary opens.

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	<ul style="list-style-type: none"> DS 6200 multi node (v7.4 or greater) or single node (v7.4.1 or greater), Virtual Edition DN 6300 multi node or single node (v7.4.2 or greater), Virtual Edition
Manager	yes	<ul style="list-style-type: none"> Manager 2200, Virtual Edition Manager 2210 or Manager Virtual Edition (v7.4 or greater). Four models available for virtual edition Manager 2300 or Manager Virtual Edition (v7.4.2 or greater).
Flow Collector	yes	<ul style="list-style-type: none"> Flow Collector 4200s, 5200s, Virtual Edition Flow Collector 4210s or Flow Collector Virtual Edition (v7.4 or greater)* Flow Collector 4300s or Flow Collector Virtual Edition (v7.4.2 or greater)* Flow Collector 5210s or Flow Collector Virtual Edition (v7.4 or greater)* <p>* Four models available for Virtual Edition</p>
Flow Sensor	no	<ul style="list-style-type: none"> For M5SX and earlier generations, any model at v7.4 or greater. For the M6SX generation, Flow Sensors are only supported at v7.4.2 or greater.
UDP Director	no	<ul style="list-style-type: none"> any model at v7.3 or greater



Mix and match of Data Nodes is not supported. Data Nodes must be either all virtual or all hardware and they must be from the same hardware generation (all DS 6200 or all DN 6300).

Data Store Enhancements

The following Data Store enhancements are included in v7.4.2. For more information, refer to the [Secure Network Analytics Appliance Installation Guide \(Hardware or Virtual Edition\)](#) and the [System Configuration Guide](#).

Transitioning Non-Data Store Flow Collectors to Data Store Flow Collectors

Transitioning Non-Data Store Flow Collectors to Data Store Flow Collectors 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, which can alleviate your current ingest capacity limitations. Flow Collectors in Data Store mode can exhibit up to a 200% increase in performance.
- **Multi-Telemetry Support:** Data Store deployments are capable of handling NetFlow, Remote Worker/Endpoint (NVM), 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, which 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, which in some cases is 10x faster or more when 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.

You can transition your existing Flow Collectors to use the Data Store database without loss of pre-transition data or visibility. Once you have completed the initial transition process, you can preserve your pre-existing data until you no longer need it.

By completing the transition process, your Flow Collector will solely become a Data Store Flow Collector. All of the pre-existing Non-Data Store data that the Flow Collector is storing will be deleted and resources will be recovered, thereby improving the performance of your Flow Collector.

For more information about transitioning Non-Data Store Flow Collectors to Data Store Flow Collectors, refer to the [System Configuration Guide](#).

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

If a Flow Collector has a Data Store Transition tag shown on the Inventory or Update Manager tabs, it is configured to send flows to your Data Store. Refer to the [System Configuration Guide](#) for more information.

The screenshot shows the Cisco Central Management console interface. The top navigation bar includes 'Central Management', 'Inventory', 'Data Store', 'Update Manager', 'App Manager', and 'Smart Licensing'. The 'Inventory' tab is active, displaying '3 Appliances found'. Below this is a search filter 'Filter Appliance Inventory Table'. The main content is a table with columns: Appliance Status, Host Name, Type, IP Address, and Actions. The first row is highlighted and has a red box around the 'Data Store Transition' tag in the 'Type' column.

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-192.168.0.74-144-0	Flow Collector Data Store Transition FCNFVE-192.168.0.74-144-0	10.0.74.144	...
Connected	sdbn-192.168.0.74-147-4	Data Node DNODEVE-192.168.0.74-147-4	10.0.74.147	...
Connected	smc-192.168.0.74-144-0	Manager SMCVE-192.168.0.74-144-0	10.0.74.144	...

Database Passwords Cannot be Changed for Transitioning Flow Collectors

When you change a database password, only Non-Data Store Flow Collectors and Transition Flow Collectors will receive the new password. For information on changing your Data Store passwords, refer to the [System Configuration Guide](#).

Oldest Data in Data Store Table

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.

For more details, refer to the [System Configuration Guide](#).

The screenshot displays the 'Data Store' configuration page in the Cisco Central Management console. The navigation bar includes 'Central Management', 'Inventory', 'Data Store', 'Update Manager', 'App Manager', and 'Smart Licensing'. The 'Data Store' section is active, showing 'Database Retention', 'Database Control', and 'Database Update Status' tabs. The 'Database Retention' section includes a 'Database Fullness' pie chart (Used: 28%, Free: 72%, System: 0%) and a 'Per Telemetry Contribution' pie chart (NetFlow: 100%, NVM: 0%, Firewall Log: 0%). The 'Daily Storage' table shows a total capacity of 0.020 TB and a daily storage rate of 0.000 GB/Day for all telemetry types. The 'Oldest Data in Data Store' table, highlighted with a red box, shows 'No data to display' for all categories. The 'Store Flow Interface Data' section at the bottom has 'Up to (days)' set to 7.

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

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		

Synchronizing Data Store and Non-Data Store Domains

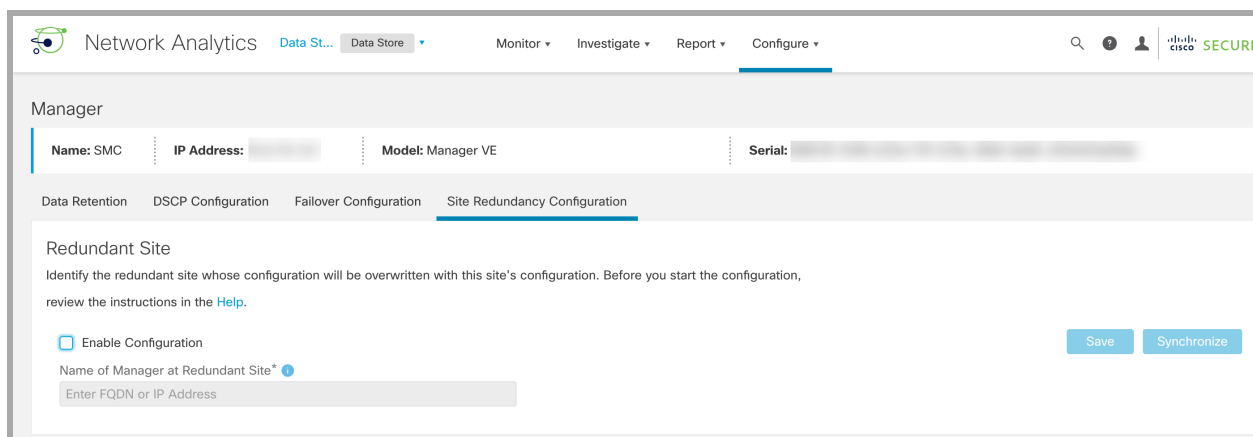
During your Flow Collector transition, you may want to keep your configurations and tuning synchronized between your pre-transition Non-Data Store domain and your Data Store domain. Refer to the [System Configuration Guide](#) for more information.

Redundant Site Configuration

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.

For more information about Site Redundancy, refer to the [System Configuration Guide](#).



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.
- **Transition:** Use this menu to transition a Non-Data Store Flow Collector to a Data Store Flow Collector.

Endpoint License and Network Visibility Module Enhancements

The following capabilities have been added Data Store deployments ingesting Cisco Secure Client (including AnyConnect) Network Visibility Module (NVM) traffic in v7.4.2:

- Adding endpoints to host groups via NVM traffic endpoint IPs
- Creating Custom Security Events based on the endpoint connections
- NetFlow detections based on NVM traffic
- Storing and viewing off-network flows in Report Builder

Use Flow Collector Advanced Settings to Configure Newly Added Fields

We've added two new fields, `nvm_to_flow_cache` and `nvm_filter_untrusted_flows`, both of which default to **0** and must be changed to **1** for improved handling of NVM untrusted traffic.

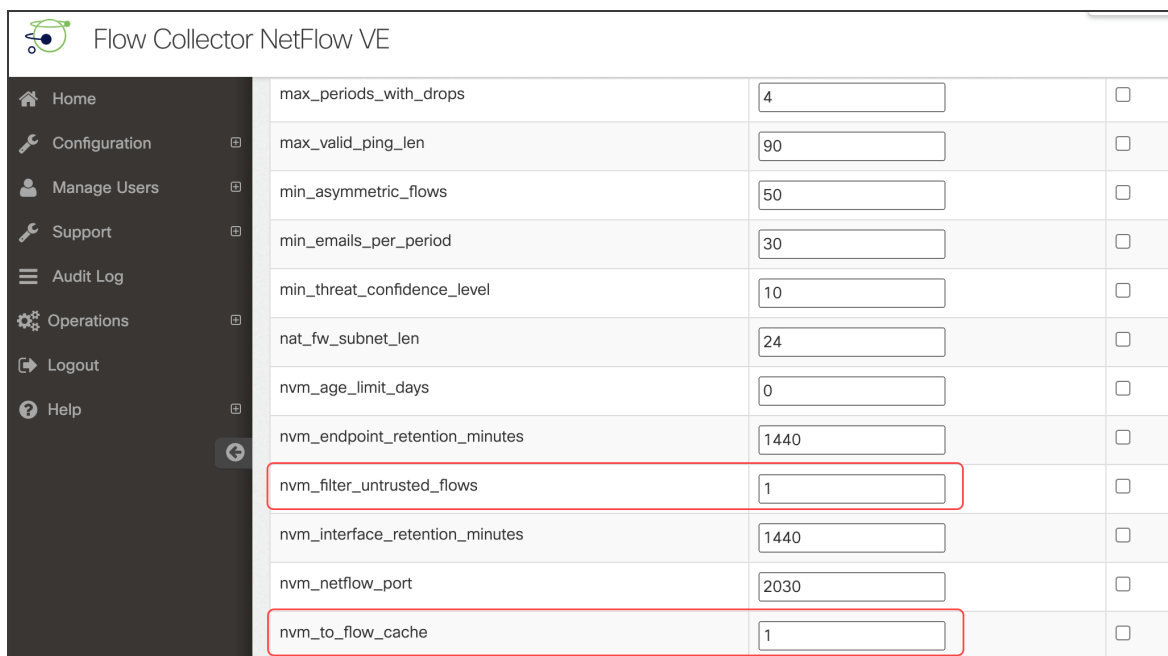


Make sure to install the [latest Flow Collector NetFlow rollup patch](#) before you begin this procedure.

Complete the following steps:

1. Log in to your Manager.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. On the Inventory page, click the **⋮ (Ellipsis)** icon for your Flow Collector, then select **View Appliance Statistics**. The Flow Collector Admin interface opens.
4. Select **Support > Advanced Settings**.

5. In the **nvm_to_flow_cache** field, set the value to **1** to capture network-based detections of NVM ingest flows. This field defaults to **0**.
6. In the **nvm_filter_untrusted_flows** field, set the value to **1**. When you activate this field, it filters out untrusted traffic from network-based detections and averts possible issues such as conflicting IP addresses. This field defaults to **0**.



Field Name	Value	Checkbox
max_periods_with_drops	4	<input type="checkbox"/>
max_valid_ping_len	90	<input type="checkbox"/>
min_asymmetric_flows	50	<input type="checkbox"/>
min_emails_per_period	30	<input type="checkbox"/>
min_threat_confidence_level	10	<input type="checkbox"/>
nat_fw_subnet_len	24	<input type="checkbox"/>
nvm_age_limit_days	0	<input type="checkbox"/>
nvm_endpoint_retention_minutes	1440	<input type="checkbox"/>
nvm_filter_untrusted_flows	1	<input type="checkbox"/>
nvm_interface_retention_minutes	1440	<input type="checkbox"/>
nvm_netflow_port	2030	<input type="checkbox"/>
nvm_to_flow_cache	1	<input type="checkbox"/>

7. Click **Apply**.
8. When the confirmation message displays, click **OK**.



If you have Data Store and set the **nvm_filter_untrusted_flows** field value to **1**, untrusted traffic is filtered out but remains stored in the NVM tables used to build the Endpoint Traffic (NVM) report. If you don't have Data Store, the untrusted traffic is not retained.

For more information, refer to the [Secure Network Analytics Endpoint License and Network Visibility Module Configuration Guide v7.4.2](#).

MTU Configuration

In v7.4.2, you can configure the maximum transmission unit (MTU) for the appliance eth0 network interface. The configuration sets the maximum packet size the eth0 interface can transmit per transaction. Enter 1500 (default), 9000, or a number that meets your network configuration requirements. For instructions, refer to the [System Configuration Guide](#). 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.



The MTU impacts your network processing. If you change this number, make sure it is configured consistently in your network.

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](#).

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 7.4.2

Defect	Description
LVA-719	Fixed an issue with Active Directory lookup configuration storing passwords in plaintext.
SWD-15689	Fixed an issue related to a mistranslation on the Smart Licensing page. (LSQ-5156)
SWD-15941	Updated documentation to show the Rest API 2k limit. (LSQ-5262)
SWD-15957	Fixed an issue related to the Authenticated NTP that was occurring due to an unsuccessful ntpdate execution. (LSQ-5285)
SWD-16424	Fixed an issue where the interface order was incorrect after installing a Flow Sensor Virtual Edition on VMware and configuring it with PCI pass-through. Note: If you configure PCI pass-through with VMware, confirm the virtual interface is eth0 and additional interfaces are eth1, eth2, etc.
SWD-16577	Fixed a problem where basic auth wasn't working when registering for a Smart Licensing account. (LSQ-5449)
SWD-16603	Fixed an issue where a blank window displayed when logging in to the Web UI.
SWD-16606	Fixed an issue where the Flow Search was not working in Japanese language on the Manager. (LSQ-5106)
SWD-16618	Fixed an issue where Response Management displayed a warning message when attempting to edit or create an email action with the SMTP username that contained the backslash (\) character.

Defect	Description
SWD-16724	Fixed an issue related to Smart License Reservation (SLR).
SWD-16844	Fixed an LDAP timeout issue. (LSQ-5652)
SWD-17233	Fixed an issue related to receiving an email error message during SMTP server.
SWD-17309	Fixed an issue where fields (SGT, SGT ID, and Username) were missing from active user sessions after a Flow Collector rebooted.
SWD-17379	Fixed an issue related to the UDP Director memory alarm.
SWD-17394	Updated documentation related to the SecureX integration.
SWD-17452	Fixed an issue where the observations table on the Selected Observations page showed inaccurate results.
SWD-17526	Updated documentation related to exfiltration alarm details.
SWD-17599	Improved how the Desktop Client functions with macOS Monterey versions 12.2.1 and 12.3. Note: If your environment includes the Desktop Client, make sure you download the latest version.
SWD-17612	Fixed an issue where the banner was not shown for installation errors when installing software updates using the Update All Data Nodes button in Update Manager.
SWD-17617	Updated documentation related to the <i>Enable baselining for hosts in this group</i> topic.
SWD-17628	Fixed an issue where the group index in the baseline file being equal to the number of host groups generated a SIGABRT problem.
SWD-17648	Increased the Web UI Top Report retention setting from 24 hours to 48 hours for MongoDB to provide customers more time to access long-running report(s).

Defect	Description
SWD-17653	Fixed an issue where a welcome message created with quotes could not be edited or saved.
SWD-17656	Fixed an error that was occurring when loading the Flow Sensorpacket capture page.
SWD-17668	Fixed an issue where under Interfaces, Top Application Traffic did not show any data.
SWD-17672	Fixed an issue where Flow Search results showed negative TCP retransmission values for flows.
SWD-17675	Addressed an issue related to high CPU usage by the Manager.
SWD-17681	Fixed an issue where selecting Monitor > Interfaces displayed "5020 Internal Server Error" when certain alarms appeared on exporters.
SWD-17743	Enhanced the Flow Collector engine to ensure it's processing all telemetry (including NVM) in all interfaces (eth0 and eth1).
SWD-17745	Fixed an issue where UEFI mode enabled in VMware prevented users from accessing the Appliance Setup Tool (AST).
SWD-17756	Added support for IPFIX AVC fields.
SWD-17788	Enhanced the Flow Collector engine to ensure that it would accept the templates 272 and 273, which are exported by AnyConnect version 4.10.0407 (or newer).
SWD-17832	Fixed an issue where the system-stats folder was missing from v7.4.1 diag packs.
SWD-17872	Updated documentation related to the SecureX ribbon.
SWD-17874	Fixed an issue where TrustSec data stored in the Manager exceeded the storage allowed in the Vertica database table.

Defect	Description
SWD-17888	Fixed an issue which allows any valid MTU range that the operating system kernel permits.
SWD-17936	Fixed an issue where UNREG or Unregistered was shown in the Flow Sensor 4240 appliance console when upgrading to v7.4.1.
SWD-17950	Updated release documentation for a Known Issue.
SWD-17964	Modified the Flow Sensor engine to ignore the ECN bits when matching flows. The engine had been putting packets from the same flow into different flows due to the changing ECN bits in the IP headers.
SWD-17966	Implemented a configurable app filter so PACE2 app IDs can be filtered out and not sent from the Flow Sensor.
SWD-17972	Fixed an issue where restoring a configuration on the Manager failed.
SWD-18019	Added a netflow tool and a script that can be modified to send specific NBAR IDs to the Flow Collector.
SWD-18033	Addressed an issue related to MongoDBRestore.
SWD-18036	Fixed an issue where nicspeed attribute was removed for the Flow Sensor 4240.
SWD-18136	Fixed an issue where the Host Summary REST endpoint made unnecessary database queries for alarms.
SWD-18170	Addressed an issue where the Mail Server Classifier was providing inaccurate results.
SWD-18237	Fixed an issue so that when the Flow Collector engine applies a Host SGT tag to a flow, it remains only until a new one is applied.
SWD-18264	Updated documentation related to backing up data store.

Defect	Description
SWD-18297	Fixed an issue where an error message "413 payload too large" was displayed when creating a new Response Management Rule.
SWD-18329	Confirmed documentation content related to updating data nodes to be accurate.
SWD-18330	Resolved an issue related to the new inactive_purge_days Advanced Setting.
SWD-18343	Fixed an issue with the SecureX Orbital queries integration.
SWD-18357	Fixed an issue where the SMTP settings were re-initialized to default settings after installing an update.
SWD-18404	Fixed an issue related to the Flow Collector engine processing large XML files.
SWD-18424	Fixed an issue where the API displayed incorrect characters for the host group names instead of multi-byte character codes.
SWD-18453	Fixed an issue where the Flow Collector engine showed decode errors when the MTU range was set to higher than 2048 bytes.
SWD-18501	Fixed an issue with the UDP Director related to false alarm issues.
SWD-18650	Addressed an issue related to Cisco Bundles.
SWD-18674	Fixed a translation issue where the Manager wasn't allowing SNMP polling be disabled.
SWD-18775	Addressed an issue related to processing a particularly large number of jobs.

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.
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.

Defect	Description
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.
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).

Defect	Description
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 NullPointerException 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 NullPointerException 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 provides information about the bugs (defects) which may exist in this release. For each defect, there is a corresponding Cisco Defect and Enhancement Tracking System (CDETS) number. Click the CDETS link to view details about an issue.

Defect	CDETS	Title
SWD-17388	CSCwc17092	Cloud specific telemetry types are shown in Secure Network Analytics Alert Configuration page
SWD-17425	CSCwc17091	Vertica database does not rebalance after one or more Data Nodes are added
SWD-17516	CSCwc17082	Some Observations are disabled by default due to underlying job inconsistency
SWD-17635	CSCwc17079	Missing data on Database Control tab when two Data Nodes with lower IP addresses are shut down
SWD-18076	CSCwe51387	Vertica database backup does not remove snapshot after backup failure
SWD-18184	CSCwe25791	Data Store private SSH key is not removed when SSH window is closed
SWD-18304	CSCwe25801	Inactive exporters cleanup feature is not working
SWD-18466	CSCwe25789	SecureX menu doesn't work on Analytics pages if SecureX is configured
SWD-18592	CSCwe25806	Observations failed to download CSV with more than 14869 observations due to timeout

Defect	CDETS	Title
SWD-18642	CSCwe25792	Manager backup omits key Data Store files
SWD-18667	CSCwd86030	Threat Feed Alerts can be received after disabling Threat Feed
SWD-18684	CSCwe25803	Smart Licensing - Changing failover roles results in communication errors with CSSM
SWD-18686	CSCwe25799	Smart Licensing - Registration errors and communication errors with CSSM cause background jobs
SWD-18694	CSCwe25800	Analytics - Observations - Negative values for 'bytes_in' on Device Report page
SWD-18714	CSCwe25794	Retention Management not working properly with SAL enabled - partition issue
SWD-18716	CSCwe25793	Data Node fails to block Browsing Files from UI when in FIPS/CC mode
SWD-18730	CSCwe67091	Certificate Expiry Alarm incorrectly states Certificate has expired
SWD-18765	CSCwe25798	Uploading an identity certificate can break inter-appliance communications due to hostname verification
SWD-18776	CSCwe25795	Central Management shows Config Channel Down error when adding a certificate with the same Common Name to trust store
SWD-18803	CSCwe67090	Flow Sensor upgrade from 7.3.x to

Defect	CDETS	Title
		7.4.2 fails via the GUI upgrade method
SWD-18814	CSCwe25802	Manager fails to extract 7.4.2 SWU before timeout is reached
SWD-18822	CSCwe25805	Audit Log 'Generating random EngineID config value' seen after any configuration change
SWD-18823	CSCwe25796	Unable to restore Central Management backup if Data Store appliance has internal failure
SWD-18826	CSCwe25790	Analytics requests fail with 504 on Device Report, Observations pages
SWD-18835	CSCwe25788	Apply Settings button in Central Management becomes available for unchanged Internet Proxy configuration
SWD-18863	CSCwe32908	Manager menu header is not shown in the UI
SWD-18869	CSCwe49107	Analytics Performance 3-node hardware - Critical alarm raised approximately every 10 minutes on high FPS
SWD-19402	CSCwh17718	Deletion of a service, application, or host group, or disabling Threat Feed, can invalidate custom security events and cause missing alarms or false alarms.

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	March 1, 2023	Initial Version.
1_1	March 27, 2023	Updated the <i>Known Issues</i> section.
2_0	May 26, 2023	Updated the <i>Analytics and Endpoint License and Network Visibility Module Enhancements</i> sections.
3_0	October 12, 2023	Added the <i>Replacing Unexpired Cisco Self-Signed Appliance Identity Certificates (Certificate Refresh)</i> section. Updated the <i>Known Issues</i> section.
3_1	October 20, 2023	Added VMware 8.0 support.
3_2	January 22, 2024	Updated format.

Release Support Information

Official General Availability (GA) date for Release 7.4.2 is March 27, 2023.

For support timeline information regarding general software maintenance support, patches, general maintenance releases, or other information regarding Cisco Secure Network Analytics software lifecycle support, refer to the [Cisco Secure Network Analytics® Software Lifecycle Support Statement](#).

Copyright Information

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

