



Cisco Secure Network Analytics

Release Notes 7.4.0



Table of Contents

Introduction	4
Overview	4
Rebranding	4
Terminology	6
Before You Update	6
Software Version	6
Supported Hardware Platforms	6
CIMC Firmware Version	7
Certificate Check	7
Cisco Bundles	8
High Availability	8
Third-Party Applications	8
Browsers	8
Alternative Access	9
What's New	11
Certificate Expiry	11
DoDIN and Common Criteria Compliance	11
Diagnostic Packs	11
Flow Collector Databases Password	11
Session Settings	12
Cisco Security Analytics and Logging (On Premises)	12
Report Builder	13
Server Identity Verification	13
Server Identity Verification: Preparing for the Update	14
Audit Log Destination Requirements	14
SMTP Configuration Requirements	14
Strict ISE Server Identity Verification	15
Secure Network Analytics Apps	15

Analytics Beta	15
Alarm Suppression	16
NetFlow and sFlow Support for a Single Flow Collector Image	16
Enabling Data Compression in the Data Store	16
Data Store Deployment Options	16
Hardware and Virtual Edition (VE) Appliances Combined	16
Hardware Appliances Only	18
Virtual Edition (VE) Appliances Only	19
Contacting Support	20
What's Been Fixed	21
Version 7.4.0	21
Known Issues	24
Change Log	29
Release Support Information	30

Introduction

Overview

This document provides information on new features and improvements, bug fixes, and known issues for the Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.0 release. 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 version 7.4.0, the appliance must have version 7.3.0, 7.3.1, or 7.3.2 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., and then update from v7.2.x to v7.3.2. 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
SMC 2220	SMC 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, FS 4240
UD 2200	UD 2210

Certificate Check

The update to v7.4.0 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 present 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, 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.

What's New

These are the new features and improvements for the Secure Network Analytics v7.4.0 release.

Certificate Expiry

When your Manager appliance identity certificate is going to expire in 60 days or less, Secure Network Analytics shows a warning on the login page. If the certificate expires, you will be unable to access the system. To change the certificate validity period or replace the certificate, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#).

DoDIN and Common Criteria Compliance

To configure Secure Network Analytics for the Department of Defense Information Network (DoDIN) or Common Criteria (CC) compliance, follow the instructions in the *DoDIN Military Unique Deployment Guide* or the *Common Criteria Administrative Guide*. We are no longer publishing the *Stealthwatch Compliance Guide*.

Diagnostic Packs

We moved the Diagnostics Packs menus from the Appliance Administration interface to System Configuration in the appliance console. Having a diagnostics pack can be invaluable if you need to work with [Cisco Support](#) to troubleshoot an issue. To create a diagnostics pack for an appliance in v7.4.0, follow the instructions in the [System Configuration Guide](#).

Flow Collector Databases Password

You can now change your default password for all Flow Collector databases by selecting the Database tab on the Central Management page. Cisco recommends that you change the default password for your Flow Collector databases.



This option is not supported for Flow Collectors in a Data Store deployment.

Session Settings

User sessions have a maximum of 12 hours. After 12 hours, users need to log in again. This setting cannot be changed.

In Protected Sessions Time-Out, you may set the Administrator-Only Functions or User Inactivity time to exceed 12 hours. However, your settings will not change the overall system user session time-out. Users need to log in again after 12 hours.

Cisco Security Analytics and Logging (On Premises)



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) v3.0.0 through the App Manager after you've updated the system to v7.4.0. Previous versions of the app are not compatible with v7.4.0. 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:

- **Multi-node:** The multi-node solution collects and analyzes ASA events from FTD, ASA, or NGIPS devices.
- **Event Viewer:** The Event Viewer allows you to filter ASA events based on the exporting device type (FTD, ASA, or NGIPS).
- **Event Type:** The Event Type column allows you to filter ASA events.
- **ASA-specific Events:** You can search for ASA events using columns which are specific to ASA events.

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

- [Cisco Security Analytics and Logging \(On Premises\) Release Notes](#)
- [Getting Started with Cisco Security Analytics and Logging \(On Premises\)](#)
- [Cisco Security Analytics and Logging \(On Premises\): Firepower Event Integration Guide](#)

Report Builder

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



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 v7.4.0, you can access the Report Builder dashboard in the same location as previous versions:

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

Server Identity Verification

We've added more stringent security checks for TLS connections in v7.4.0 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."
- **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

As part of the update to v7.4.0, 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, you can choose to enable this setting. If you install a new version of Secure Network Analytics, 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 Beta

As of v7.4.0, Analytics Beta works only with systems deployed with a Data Store. If you are running Analytics Beta on a system that does not have a data store and you upgrade to v7.4.0 or higher, Analytics Beta will no longer be available on your system.

You can now see the MITRE ATT&CK tactics and technique tags on the Alert Details page and the Alerts Settings page.

Alarm Suppression

You can now configure rules, based on alarm attributes, for known communication between devices which is expected and known to never be malicious. When the communication matches the rule criteria (such as for ports, protocols, and IP addresses), Analytics suppresses any alarms that would normally be generated, resulting in a less noisy and more efficacious system.

 When you perform a configuration backup, the alert suppression list is included.

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.

Enabling Data Compression in the Data Store

You can now enable data compression to reduce bandwidth usage between a Flow Collector and the Data Store. It is especially helpful in scenarios where the network bandwidth from a Flow Collector to the Data Store is limited. By enabling compression, you can reduce bandwidth usage by up to 90%.

Data Store Deployment Options

In addition to an exclusive hardware deployment or virtual deployment for Secure Network Analytics with a Data Store, we also provide a mixed hardware and virtual deployment option in v7.4.0. Starting in v7.4.0, Secure Network Analytics now supports the combination of a Virtual Manager and Flow Collector with a DS6200 hardware Data Store.

Make sure all appliances have the same version of Secure Network Analytics installed, and review the documentation for the deployment you choose. It is important to understand all requirements before you start.

- [Hardware and Virtual Edition \(VE\) Appliances Combined](#)
- [Hardware Appliances Only](#)
- [Virtual Edition \(VE\) Appliances Only](#)

Hardware and Virtual Edition (VE) Appliances Combined

Use the following guides to deploy your Data Store 6200 with the Manager VE and Flow Collector VE.

Procedure	Document	Description
Preparation	Release Notes	Review the latest information about the current Data Store release, including last-minute information.
Preparation	Data Store 6200 Specification Sheet	Review the physical layout and capabilities.
1.	x2xx Series Hardware (with Data Store) Appliance Installation Guide	Install the physical hardware appliance (rack, cables, etc.).
2.	Data Store Virtual Edition Deployment and Configuration Guide	<p>Deploy and configure the Manager VE. Refer to the Manager Configuration for Use with a Data Store section.</p> <ul style="list-style-type: none"> For details about resource requirements, deploying the ISO, and First Time Setup, refer to the Virtual Edition (with Data Store) Appliance Installation Guide. For more information about the Appliance Setup Tool, refer to the System Configuration Guide.
3.	x2xx Series Hardware (with Data Store) Appliance Installation Guide and Data Store Hardware Deployment and Configuration Guide	<p>Deploy and configure each Data Node.</p> <p>Make sure you follow the instructions in the Data Node Configuration section to configure the inter-Data Node communication port settings.</p> <p>Refer to the Data Store Hardware Deployment and Configuration Guide for deployment considerations and prerequisites.</p>
4.	Data Store Virtual Edition Deployment and Configuration Guide	Deploy and configure the Flow Collector VE. Refer to the Flow Collector Configuration for Use with a Data Store section.

		<ul style="list-style-type: none"> For details about resource requirements, deploying the ISO, and First Time Setup, refer to the Virtual Edition (with Data Store) Appliance Installation Guide. For more information about the Appliance Setup Tool, refer to the System Configuration Guide.
5.	Data Store Virtual Edition Deployment and Configuration Guide	<p>Initialize the Data Store. Refer to the Data Store Initialization and Configuration section.</p> <p>Configure the flow interface statistics retention and Data Store compression.</p>
6.	Smart Licensing Guide	License your Secure Network Analytics deployment and appliances before the evaluation period (90 days) expires.

Hardware Appliances Only

Use the following guides to deploy Secure Network Analytics hardware with a Data Store 6200.

Procedure	Document	Description
Preparation	Release Notes	Review the latest information about the current Data Store release, including last-minute information.
Preparation	Hardware and Software Version Support Matrix	Review the Manager and Flow Collector appliance models that you can use with a Data Store.
Preparation	Appliance Specification Sheets	Review the physical layout and capabilities for your appliances.
1.	x2xx Series Hardware (with Data Store) Appliance Installation Guide	Install your Manager, Data Store, and Flow Collector hardware.

2.	x2xx Series Hardware (with Data Store) Appliance Installation Guide and Data Store Hardware Deployment and Configuration Guide	<p>Configure your appliances in the order shown in the Data Store Hardware Deployment and Configuration Guide (refer to the Data Store Installation section):</p> <ol style="list-style-type: none"> 1. Manager 2. Data Nodes: Make sure you follow the instructions to configure the inter-Data Node communication port settings. 3. Flow Collector 4. Initialize the Data Store. 5. Configure the flow interface statistics retention and Data Store compression. <p>For more information about installing the hardware and First Time Setup, refer to the x2xx Hardware (with Data Store) Appliance Installation Guide.</p> <p>For more information about the Appliance Setup Tool, refer to the System Configuration Guide.</p>
3.	Smart Licensing Guide	<p>License your Secure Network Analytics deployment and appliances before the evaluation period (90 days) expires.</p>

Virtual Edition (VE) Appliances Only

Use the following guides to deploy Secure Network Analytics Virtual Edition with a Data Store Virtual Edition.

Procedure	Document	Description
Preparation	Release Notes	Review the latest information about the current Data Store release, including last-minute information.
1.	Data Store Virtual Edition Deployment and	Deploy and configure your appliances in the order shown in the Data Store Virtual Edition Deployment and Configuration Guide (refer to the Data Store

	<p>Configuration Guide and Virtual Edition (with Data Store) Appliance Installation Guide</p>	<p>Installation section):</p> <ol style="list-style-type: none"> 1. Manager VE 2. Data Nodes: Make sure you follow the instructions to configure the inter-Data Node communication port settings. 3. Flow Collector VE 4. Initialize the Data Store. 5. Configure the flow interface statistics retention and Data Store compression. <p>For details about resource requirements, deploying the ISO, and First Time Setup, refer to the Virtual Edition (with Data Store) Appliance Installation Guide.</p> <p>For more information about the Appliance Setup Tool, refer to the System Configuration Guide.</p>
2.	<p>Smart Licensing Guide</p>	<p>License your Secure Network Analytics deployment and appliances before the evaluation period (90 days) expires.</p>

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 7.4.0

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	Flow based Identities are missing on 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

Defect	Description
	Retention is not 7 days.
SWD-16369	Corrected the Syslog message for reoccurring Recon Alarm. (LSQ-5527)
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 SMC 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-16417	Fixed an issue in the v7.3.1 Flow Collector engine SIGSEGV for "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	The 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 Webhook 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.	<p>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.</p> <p>Mitigation Options: If you configure Active Directory Lookup:</p> <ul style="list-style-type: none"> • Limit the user account privileges and monitor the account for misuse. • Encrypt your backup configuration files. Refer to "Backup Configuration Encryption" in the Help. <p>If you prefer to disable Active Directory Lookup:</p> <ul style="list-style-type: none"> • 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.
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.

Defect	Description	Workaround
SWD-13964	The database restore does not include the encrypted configuration backup.	Make sure to perform the database restore without restoring the configuration backup by adding <code>-r</code> to the <code>doDbRestore</code> command, then manually restore the encrypted backup.
SWD-14057	The Packet Capture page is blank in the Manager Appliance Administration.	We've removed Packet Capture from the Manager Appliance Administration. Alternative Method: Select Help > Help , and then follow the instructions for the Manager packet capture.
SWD-14855	When using Firefox, the Flow Sensor AST may not present Step 6: Add the appliance to Central Management.	Use a different browser . If using Firefox, clear cache, and refresh the page.
SWD-15002	Configuration restore fails after RFD.	If you reset an appliance to its factory defaults, you can't restore the configuration using Central Management. For assistance, contact Cisco Support .
SWD-16378	The system alarms for Data Nodes on the dashboard, and in reports, may not indicate the correct issue. The time frame indication (top right of the box) may display a much shorter amount of time since the Data	<p>In the System Report, you can use the Search box at the top of the Alarm column to type the description of the specific alarm. Then you can sort on the Date/Time column to see the oldest and/or newest occurrence of the specific alarm.</p> <p>You can also select a Day from the calendar, then select the Search icon values with Is Before to find the first day it occurred.</p>

Defect	Description	Workaround
	<p>Node went down, than the actual amount of time.</p> <p>When you select View Details, then select View System Report, alarms for the last 30 days display.</p>	
SWD-16382	When a user on the FMC specifies an IP subnet filter (i.e., 10.10.1.0/24), the query is unsuccessful at the Data Store query-service backend.	A workaround is available for the FMC by using the ipRange comparison operator. However, it requires a code change, which may not be possible either architecturally or due to release timing.
SWD-16408	The ISE client does not parse user sessions containing a non-UTC time zone.	A workaround is to set ISE to UTC time.
SWD-16733	SWUv2 changes updating process in Data Store.	Make sure to wait until the SMC is updated before you apply the Data Node finalizer SWU. If you're concerned about the downtime required, contact Cisco Support .
SWD-16781	The <code>Connection Status: Failed</code> message displays when you access Cisco Identity Services Engine	Before you update to v7.4.0, make sure the certificate chain in ISE is complete. Refer to the "Option 1 - Deploying Certificates Using ISE Internal Certificate Authority (Recommended)" section starting on page 5 of the Cisco Secure Network Analytics ISE and ISE-PIC

Defect	Description	Workaround
	<p>(ISE).</p> <p>When the log displays <code>Service <service name> cannot be found on this ISE Cluster</code>, it indicates the ISE integration failing with empty services list.</p>	<p>Configuration Guide 7.4 for details. Make sure to also correct any replication alarm issues in ISE by performing a manual sync.</p> <p>Note: For more details, see the ISE Troubleshooting TechNotes article, Troubleshoot Secure Network Analytics - ISE Integration "Connection Failed - Service Cannot Be Found On This ISE Cluster".</p> <p>If you have already updated to v7.4.0 and see this message, contact Cisco Support.</p>
SWD-16858	<p>When updating from v7.3.0, the SMC on the Data Store system stops the Data Store database.</p>	<p>Restart the database manually on a Data Node as dbadmin user:</p> <pre>admintools -t start_db -d sw -p <dbadmin password></pre>
SWD-16862	<p>SWUv1 finalizer patch blocks upgrade if it's used instead of SWUv2 finalizer.</p>	<p>After the incorrect patch installation fails, install the correct patch.</p>
SWD-16929	<p>When ISE receives a message larger than 8,192 bytes, the ISE sessions' topic doesn't function as it normally would due to an insufficient buffer size for receiving ISE session with pxGrid</p>	<p>None currently available, but a patch is planned.</p>

Defect	Description	Workaround
	2.0.	
SWD-17936 CSCwc25672	When upgrading to v7.4.1, an UNREGISTERED error displays when installing the Flow Sensor (FS4240).	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: <pre>sed -i 's/platform="ST-FS4240-K9" nicspeed="eth+,40000"/platform="ST-FS4240-K9"/' /lancope/admin/lib/model.xml</pre> 3. Reboot the appliance.
NA	On the Flow Sensor VE, “Export Application Identification” is off by default.	To enable application identification, the advanced setting will need to be selected manually.

Change Log

Revision	Revision Date	Description
1_0	September 30, 2021	Initial version.
2_0	November 2, 2021	General Availability (GA).
2_1	November 18, 2021	Added the Enabling Data Compression in the Data Store section.
3_0	December 13, 2021	Added the Data Store Deployment Options section and updated the What's Been Fixed section.
3_1	April 7, 2022	Updated the What's Been Fixed section.
3_2	July 1, 2022	Added SWD-17936 to the Known Issues section.

Release Support Information

Official General Availability (GA) date for Release 7.4.0 is Nov. 2, 2021.

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

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)

