



Cisco Secure Network Analytics

Release Notes 7.5.1



Table of Contents


Introduction	5
Overview	5
Terminology	5
Before You Update	5
Software Version	5
Smart Licensing	5
Third-Party Applications	5
Supported Hardware Platforms	6
CIMC Firmware Version	6
Data Store Appliance Support	7
IPv6 Support	8
Network Management	8
SSL/TLS Appliance Identity Certificates	9
Cisco Bundles	9
Apps Version Compatibility	9
Browsers	10
Alternative Access	10
Data Store Private LAN Settings and Data Node Expansion	11
UDP High Availability	11
Notice of VMware Compatibility Changes	12
What's New	13
Changes in Design	13
Cisco SecureX End-of-Sale and End-of-Life	13
Cisco XDR Analytics	13
Increased Minimum Storage Requirements for Flow Collector Virtual Edition with Data Store	14
Flow Collector with Data Store	14
Delete All SWU Files Button Added to the Update Manager	14
Direct Software Downloads (Beta)	15

Direct Upload of Diag Packs or Files in the Appliance Console (SystemConfig)	16
Enable/Disable SSH in SystemConfig	16
Firewall Events	17
Global Threat Alerts	17
Google Analytics	17
Host Group Management	17
ISE ANC Policy Action for Alarms or Alerts	18
M4 Appliances No Longer Supported	19
MongoDB	19
Multi-Factor Authentication	19
NTLM v1 Removal	19
Network Visibility Module (NVM) Configuration	20
OpenSSL Version Upgraded to OpenSSL3	21
Packet Analyzer	21
Report Scheduling for Report Builder	21
Network Insights Dashboard	22
Additional Report Builder Enhancements	24
Flow Collection Status Report - Added Ability to Select Multiple Flow Collectors	24
Alarms Report - Added the Ability to Select Multiple Host Groups	24
Added Identifying Information to PDF Outputs	24
Fixed Mixed Time Axis and Failure to Show Date	24
SNMP Updates	24
Secure Network Analytics Apps	25
Access the Apps	25
Security Analytics and Logging (On Premises)	26
Smart Licensing Transport Configuration	26
Supported TLS Versions	26
Known Issues	27
Contacting Support	30
Change History	31

Introduction

Overview

This document provides information about the new features and improvements, bug fixes, and known issues for the v7.5.1 release of Cisco Secure Network Analytics (formerly Stealthwatch).

 To review release notes for previous releases, go [here](#).

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

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](#). It is important to note the following:


Software Version

To update the appliance software to v7.5.1, the appliance must have version 7.4.x or 7.5.0 installed.

Smart Licensing

We have changed the transport configuration requirements for Smart Licensing.

 If you are upgrading the appliance from v7.4.1 or earlier, make sure the appliance is able to connect to smartreceiver.cisco.com.

 You no longer need to purchase an Endpoint license for NVM telemetry starting with v7.5.1. NVM traffic is now included along with NetFlow when calculating Flow Rate (FPS) licensing requirements.

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](#).

M4 Appliances No Longer Supported: Make sure to remove all M4 appliances from your cluster, and make sure you're using only M5, M6, or Virtual appliances when you upgrade to Secure Network Analytics v7.5.1.

M4 appliances are not supported for v7.5.1 and later.

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 M5 common update patch applies to M5 hardware and the M6 common update patch applies to M6 hardware for the appliances shown in the following table.

M5 Hardware	M6 Hardware
SMC 2210 (Manager 2210)	SMC 2300 (Manager 2300)
FC 4210	FC 4300
FC 5210 Engine	---
FC 5210 Database	---
FS 1210	FS 1300
FS 3210	FS 3300
FS 4210 / FS 4240	FS 4300
UD 2210	---
DS6200	DN6300

Data Store Appliance Support

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 4200, 5200, Virtual Edition Flow Collector 4210 or Flow Collector Virtual Edition (v7.4 or greater)* Flow Collector 4300 or Flow Collector Virtual Edition (v7.4.2 or greater)* Flow Collector 5210 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).

IPv6 Support

We provide the following support for IPv6 and Dual Stack in v7.5.1:

Appliance/Desktop Client	IPv6 and Dual Stack Support	IPv4 Only Support
Managers	✓	✓
Flow Collectors	✓	✓
Flow Sensors	✓	✓
Data Nodes		✓
Desktop Client		✓
UDP Directors*		

* UDP Director Support

- **M5 UDP Directors:** When configuring M5 UDP Director (UD2210), your options are IPv4 and Dual Stack. If you select the Dual Stack option, UDP will only forward over IPv4. You can, however, use IPv6 for management. For information about IPv6 forwarding for UDP Directors, refer to the [Cisco Telemetry Broker User Guide](#).
- **Changing the Network Mode:** For information about changing the network mode of your appliance, refer to the [System Configuration Guide](#).

Network Management

With the exception of your Data Node appliances and UDP Directors, you can change the network mode of your appliances in any of the following ways:

IPv4 only to Dual stack	Dual stack to IPv4 only	IPv6 to IPv4 only
IPv4 only to IPv6 only	Dual stack to IPv6 only	IPv6 only to Dual stack



The only supported network mode for Data Nodes is IPv4 only. Changing the network mode of Data Nodes is not supported in v7.5.1.

When configuring an M5 UDP Director (UD2210), your options are IPv4 and Dual Stack. If you select the Dual Stack option, UDP will only forward over IPv4. You can, however, use IPv6 for management. For information about IPv6 forwarding for UDP Directors, refer to the [Cisco Telemetry Broker User Guide](#). For information about changing the network mode of your appliance, refer to the [System Configuration Guide](#).

SSL/TLS Appliance Identity Certificates



Make sure you replace your appliance identity certificates before they expire. To check expiration dates, follow the instructions in the [SSL/TLS Certificates for Managed Appliances Guide](#).

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 (SystemConfig).

- **Host Information:** The appliance host information (IP address, host name, domain name) is preserved.
- **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 the [SSL/TLS Certificates for Managed Appliances Guide](#).

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). It includes a core certificate bundle and an external certificate bundle, which are used for connecting to Cisco services and to non-Cisco services.

Apps Version Compatibility

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



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

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

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. If you do not intend to leave SSH enabled, make sure that you disable SSH when you have finished using it.

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

1. Log in to the Manager.
2. Select **Configure > Global > Central Management**.
3. Click the **⋮ (Ellipsis)** icon in the **Actions** column for the appliance.
4. Select **Edit Appliance Configuration**.
5. Select the **Appliance** tab.
6. Locate the **SSH** section.
7. Check the **Enable SSH** check box to allow SSH access on the appliance.
8. Click **Apply Settings**, then 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](#).

UDP High Availability

If you have high availability configured on your UDP Directors and plan to upgrade to v7.5.1, make sure to record your high availability settings on your UDP Director before you begin the update. You will need to reconfigure high availability once your upgrade to v7.5.1 is complete. For more information about updating Secure Network Analytics, refer to the [Update Guide](#).

Notice of VMware Compatibility Changes

We do not support VMware 6.0, 6.5, or 6.7 with Secure Network Analytics v7.5.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

 Secure Network Analytics v7.5.1 is compatible with VMware 7.0 or 8.0.

What's New

These are the new features and improvements for the Secure Network Analytics v7.5.1 release.

Changes in Design

We've changed our design to be consistent with the Breach Protection Suite. The following changes have occurred:

- The colors of the user interface, as well as a few icons, have changed.
- The top navigation menu is now a left navigation menu.
- The Security Analytics and Logging OnPrem menu is now under the Investigate menu.

Cisco SecureX End-of-Sale and End-of-Life

Cisco SecureX will no longer be available for purchase. If you have an active Cisco SecureX environment, you will continue to have access for support through the Cisco Technical Assistance Center (TAC) until July 31, 2024.

After this date, Cisco SecureX environments will be disabled and all capabilities will become unavailable. For more details, refer to [End-of-Sale and End-of-Life Announcement for Cisco SecureX](#).

Cisco XDR Analytics

Secure Cloud Analytics (SCA) is now a part of Cisco XDR and is referred to as Cisco XDR Analytics.

Increased Minimum Storage Requirements for Flow Collector Virtual Edition with Data Store

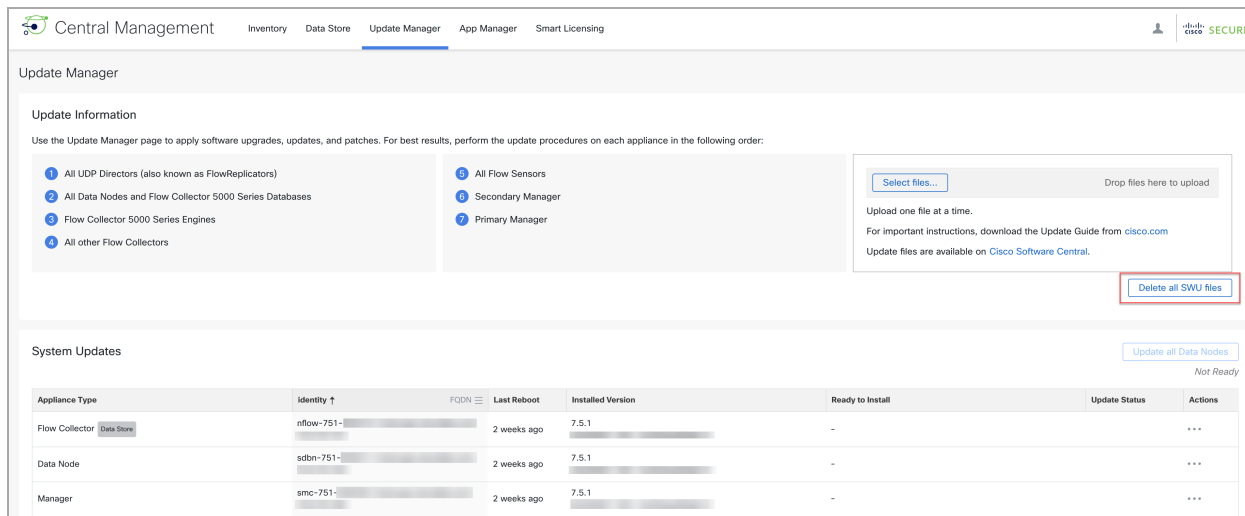
The minimum storage requirements for Flow Collector Virtual Edition with Data Store has been increased beginning with 30,000 flows per second and above. Refer to the following table for more information.

Flow Collector with Data Store

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage	Interfaces	Exporters	Internal Hosts
Up to 10,000	2	24 GB	200 GB	Up to 65535	Up to 1024	25,000
Up to 30,000	6	32 GB	300 GB	Up to 65535	Up to 1024	50,000
Up to 60,000	8	64 GB	400 GB	Up to 65535	Up to 2048	100,000
Up to 120,000	12	128 GB	500 GB	Up to 65535	Up to 4096	250,000

Delete All SWU Files Button Added to the Update Manager

We have added a "Delete all SWU files" button to the Update Manager page. Selecting this button will delete SWU files (upgrades and patches) from all appliances.

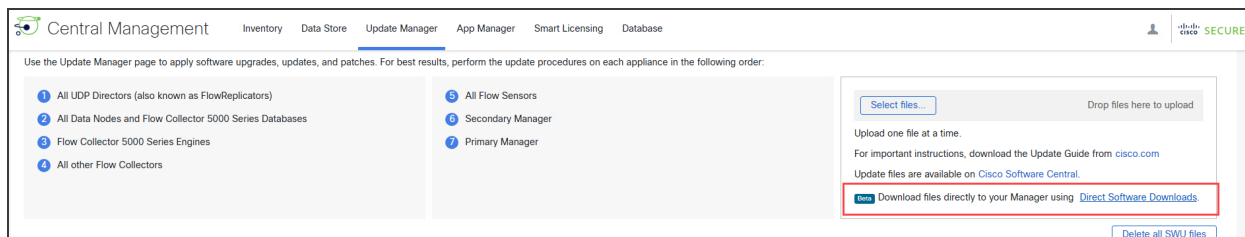


Direct Software Downloads (Beta)

We've added Cisco Automatic Software Distribution to the Update Manager. After you've updated Secure Network Analytics to v7.5.1, you can use this Beta integration to download patches and update files directly to your Update Manager.

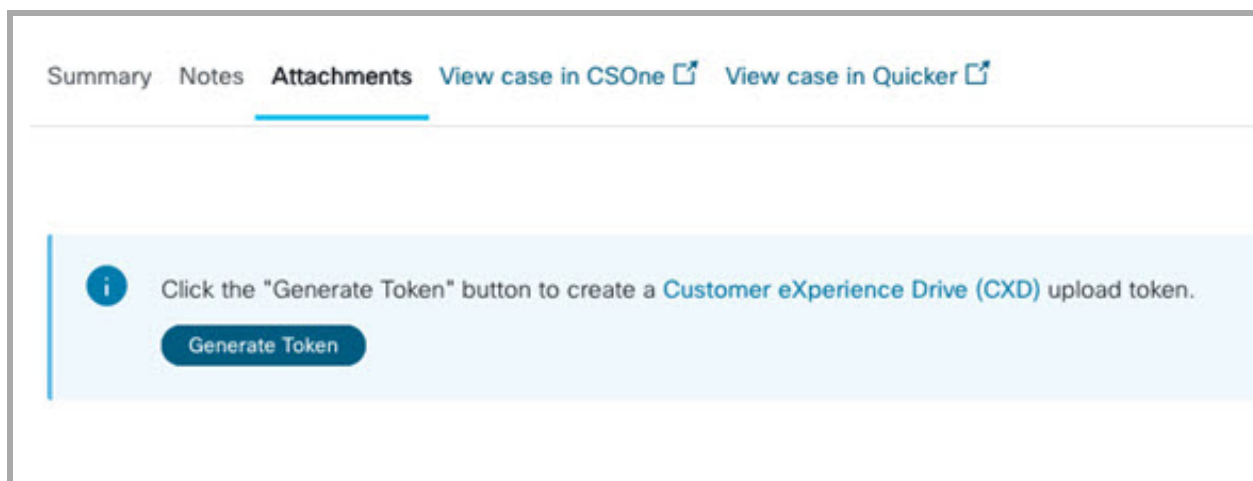
1. Go to **Configure > Global > Central Management > Update Manager**.
2. Click **Direct Software Downloads**. Follow the on-screen prompts.

For instructions, refer to the patch readme or update guide.



Direct Upload of Diag Packs or Files in the Appliance Console (SystemConfig)

When a TAC case is opened for a customer, we have added the ability to upload a diag pack (or any file) directly to the case. This saves time and effort on getting that information from your system to Cisco for triage. Since access to the Diag Pack is already in the appliance console (SystemConfig) menu, we have added a way to type/copy the case number and required token and let the appliance console (SystemConfig) application execute this command for you.



Enable/Disable SSH in SystemConfig

We have added the ability to enable or disable SSH using the appliance console (SystemConfig). Perform the following steps to access this option.

1. Log in to your appliance console (System Config).
2. Select **Advanced > SSH**.
3. Select your desired option.
4. Click **OK** to save your changes.

Firewall Events

We've added support for the latest Firewall event fields through Firewall Threat Defense release v7.7.0.

- **Configuration:** Follow the instructions in the [Cisco Security Analytics and Logging \(On Premises\): Firewall Event Integration Guide](#).
- **Firewall Events:** Go to **Investigate > Security Analytics and Logging (OnPrem)**. Click **Columns** to review the list of fields and add them to your queries.

Global Threat Alerts

In order to have a cohesive Cisco XDR solution, Global Threat Alerts has been removed from Secure Network Analytics. You can now have a more complete solution by adopting Cisco XDR as part of the Breach Protection Suite. For more information about Cisco XDR, go [here](#).

Google Analytics

Google Analytics has been removed from Secure Network Analytics. Google Analytics has enabled us to better understand user behavior in order to drive innovation and iterate on product functionality. It will be replaced in a future release with a tool that is better suited for users' current needs.

Host Group Management

The Host Group Management page has been updated to sort IP addresses alphanumerically. For more information about Host Group Management, refer to "Managing and Configuring Host Groups" in the Help.

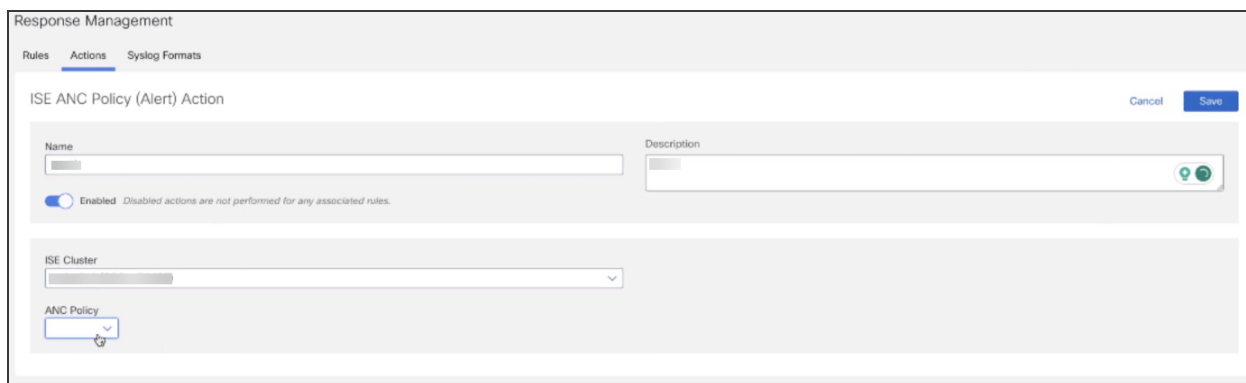
ISE ANC Policy Action for Alarms or Alerts

You can now configure an ISE ANC Policy action for Alarms and Alerts through Response Management. To create an ISE ANC Policy action, do the following:

1. From the main menu, choose **Configure > Detection > Response Management** and choose the Actions tab.
2. From the Add New Action dropdown menu, choose either **ISE ANC Policy (Alarm)** or **ISE ANC Policy (Alert)**.



3. Enter a name for the ISE ANC Policy action. It does not have to be unique.




4. (Optional) Enter a description for the automated ISE ANC Policy action.
5. Choose the applicable ISE cluster from the ISE Cluster drop-down list. The domain is shown in parentheses after the ISE cluster name. The ISE ANC Policy action executes only for rules created for the domain name shown in this field. Secure Network Analytics will not implement this action for any rule it's assigned to that is configured for another domain.
6. Choose the applicable ANC policy from the ANC Policy drop-down list. These are policies that have been created in the ISE management interface.
7. Indicate whether you want this action to apply to the source host or target host (for alarms only).

To monitor ISE ANC policy assignments, review the ISE ANC Policy Assignments Report. You can quickly determine which hosts need policy changes because the report shows which hosts have been assigned an ANC policy using Response Management.


M4 Appliances No Longer Supported

M4 appliances are not supported for v7.5.1 and later.

-  Before you upgrade to v7.5.1, make sure you've removed all M4 appliances from your cluster, and make sure you're using only M5, M6, or Virtual appliances.

MongoDB

When upgrading to v7.5.1, you'll also be upgrading MongoDB to v7.0.5.

-  **CPU Instruction Set Requirement:** Make sure your CPU is capable of the AVX/AVX2 instruction sets. For ESXi, select a VM hardware version of 11 or greater. For KVM, we recommended that you utilize host passthrough.

Multi-Factor Authentication

SSO Multi-Factor Authentication services are supported for v7.5.1. The supported identity providers include, but are not limited to, the following:

- Microsoft ADFS
- Okta
- Login.gov
- Microsoft Entra ID

To configure SSO multi-factor authentication, refer to the "Configuring Authentication and Authorization" topic in the Help.

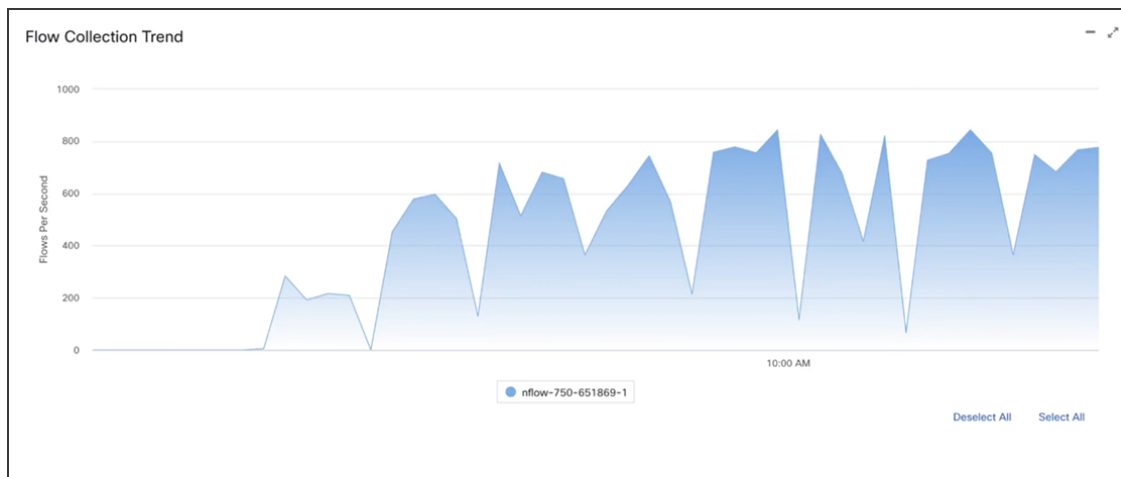
NTLM v1 Removal

Any previous configurations for the Remote File System on the Manager or Flow Collector utilizing NT LAN Manager (NTLM) v1 will be cleared and will require reconfiguration following an upgrade to v7.5.1.

-  Only NTLM v2 connections are supported in v7.5.1.

Network Visibility Module (NVM) Configuration

You no longer need to purchase an Endpoint license for NVM. NVM traffic is now included along with NetFlow when calculating Flow Rate (FPS) licensing requirements. You might notice an increase in FPS when viewing the Flow Collection Trend on your dashboard, as in this example.



You might observe changes in the Flow Trend by Exporter Report and the Flow Collection Trend by Flow Collector Report.

For NVM traffic, the Flow Collector IP address is shown as the Exporter.

The screenshot shows the "Flow Collection Status (38)" table in the Cisco Secure Network Analytics interface. The table lists various flow collectors and their associated exporters. A red box highlights the "Exporter" column, which shows the IP address of the flow collector for each entry. The table includes columns for Status, Flow Collector, Exporter, Flow Type, Average Flow Rate (fps), Average NetFlow Traffic (bps), Interface Count, and Utilization Inbound (%).

Status	Flow Collector	Exporter	Flow Type	Average Flow Rate (fps)	Average NetFlow Traffic (bps)	Interface Count	Utilization Inbound (%)	Utiliza
Active	nflow-751-687595-1	10.10.10.1	IPFIX	25	35.43K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	23	33.15K	1	1	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	18	24.65K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	16	22.23K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	15	21.67K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	15	20.13K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	14	18.88K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	12	15.9K	1	0	0
Active	nflow-751-687595-1	10.10.10.1	IPFIX	12	15.43K	1	0	0

For more information about NVM telemetry, refer to the [Network Visibility Module \(NVM\) Configuration Guide v7.5.1](#).

OpenSSL Version Upgraded to OpenSSL3

The OpenSSL library version has been upgraded to OpenSSL3. If you are uploading a .p12, .pfx, or .pks certificate file, it needs to be encrypted with one of the algorithms supported by OpenSSL's default OSSL Provider.

You can find this list of supported algorithms here:

https://www.openssl.org/docs/man3.0/man7/OSSL_PROVIDER-default.html. If you are using openssl to generate your .p12, .pfx, or .pks file to upload certificates to Central Management, make sure you're using OpenSSL 3.0+.

Packet Analyzer

The Packet Analyzer appliance has reached end of support. For details, refer to the [End-of-Sale and End-of-Life Announcement for the Cisco Security Packet Analyzer 2400](#).

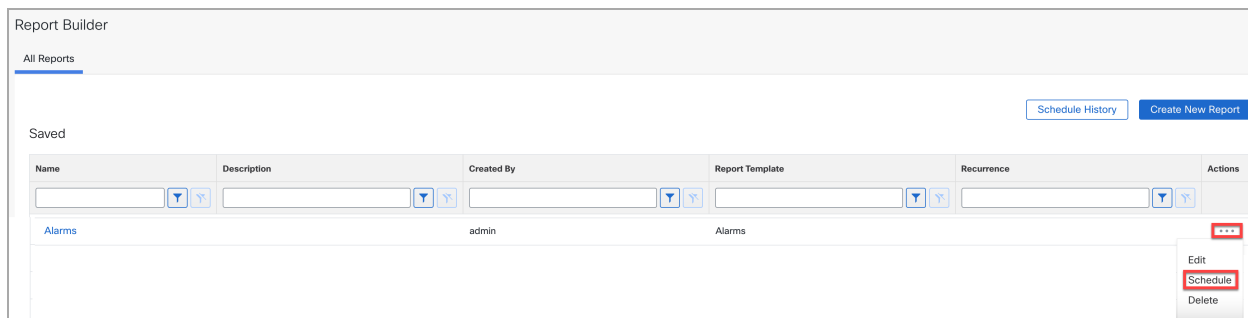
Report Scheduling for Report Builder

You can set up report scheduling for Report Builder reports in v7.5.1. If your report supports scheduling, you can designate a custom schedule and Email delivery list to ensure the .csv file gets delivered to the desired recipients at the preferred time.

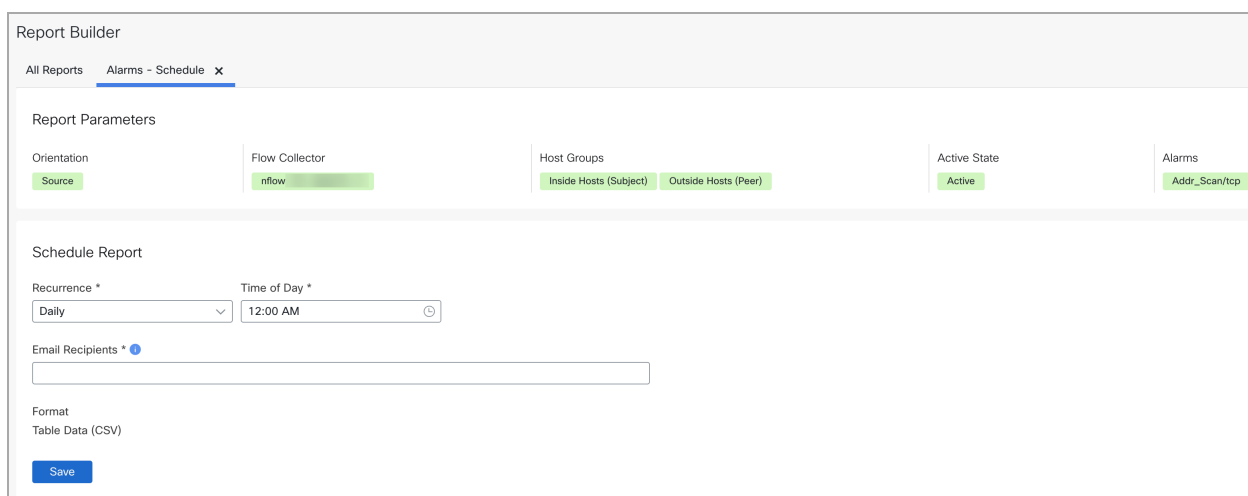
Scheduling is supported in the following reports:

<ul style="list-style-type: none"> Alarms 	<ul style="list-style-type: none"> DSCP Status
<ul style="list-style-type: none"> Firewall Log Collection Trend 	<ul style="list-style-type: none"> Firewall Log Database Ingest Trend
<ul style="list-style-type: none"> Flow Collection Status 	<ul style="list-style-type: none"> Flow Collection Trend by Exporter
<ul style="list-style-type: none"> Flow Collection Trend by Flow Collector 	<ul style="list-style-type: none"> Flow Database Ingest Trend
<ul style="list-style-type: none"> Host Group Application Traffic 	<ul style="list-style-type: none"> Host Group Flow Traffic
<ul style="list-style-type: none"> Interface Application Traffic 	<ul style="list-style-type: none"> Interface Network Traffic
<ul style="list-style-type: none"> Interface Network Traffic 	<ul style="list-style-type: none"> NVM Collection Trend
<ul style="list-style-type: none"> NVM Log Database Ingest Trend 	<ul style="list-style-type: none"> Network and Server Performance
<ul style="list-style-type: none"> Security Events 	<ul style="list-style-type: none"> System Alarms

To schedule a report, click the **⋮ (Ellipsis)** icon in the **Actions** column for the report. Then click **Schedule** to open the scheduling window.



Use the **Email Recipients** field to enter the Email addresses that will be receiving the report updates. To save your changes, select your report parameters and click **Save**. For detailed instructions, refer to the "Scheduling a Report" topic in the Help.



Network Insights Dashboard

The Network Insights dashboard is a customizable dashboard template that contains the following reports by default:

- Firewall Log Collection Trend Report
- Flow Collection Trend by Flow Collector Report
- Flow Collection Trend by Exporter Report
- Host Group Application Traffic Report
- Host Group Flow Traffic Report
- Network and Server Performance Report
- NVM Collection Trend Report

To add, edit, delete, rearrange, or re-size reports, do the following:

1. On the Report Builder - All Reports Tab page, click **Create New Report**.
2. Click the **Dashboard** template to select it.
3. Click **Add Report** to add a report to your dashboard.
4. Scroll through the **Select report type** menu, then select the report you want to add to your dashboard.

Add Report

Select report type
Host Group Application Traffic

Time Range * Start Time * End Time *
Custom 4/14/2024 2:53 PM 4/15/2024 2:53 PM

Subject
Include

Host Group * Applications
Select Outside Hosts X Include Exclude
authentication X
business systems X

Cancel Save

After you have added your reports, you can rearrange them by clicking the header of the report tile and dragging it to your desired location. For detailed instructions, refer to the "Creating a Network Insights Dashboard" topic in the Help.

Additional Report Builder Enhancements

The following additional enhancements have been added to Report Builder for v7.5.1.

Flow Collection Status Report – Added Ability to Select Multiple Flow Collectors

The Flow Collection Status report now gives you the ability to select multiple Flow Collectors. It also gives you the option to select all or deselect all of your Flow Collectors.

Alarms Report – Added the Ability to Select Multiple Host Groups

The Alarms report now gives you the ability to select multiple Host Groups.

Added Identifying Information to PDF Outputs

The following identifying information has been added to the PDF outputs of reports in v7.5.1:

- Report Title
- Report selection criteria (date range, Host Group, etc)
- Legend
- Description on X and Y axis
- "Cisco Secure Network Analytics" label
- Notes (open field, content provided by user)

Fixed Mixed Time Axis and Failure to Show Date

Reports that included specific time frames were showing a mixed 12/24 hour time axis and were also failing to show the date. This has been corrected in v7.5.1. All reports that include specific time frames are now based on a 24 hour time axis and are including the date.

SNMP Updates

We have added the following SNMP updates for v7.5.1:

- SNMPv3 supports SHA-2 authentication protocols
- SNMPv3 supports AES256 encryption
- Crypto control is available in Central Manager for configuration and reference

For more information, refer to the following Help topics: "SNMP Agent," "Exporter SNMP Profiles: Add an Exporter SNMP Configuration," and "Response Management: Action Types."

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 updated to v7.5.1, 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.

Security Analytics and Logging (On Premises)

We've moved Security Analytics and Logging (OnPrem) from a separate app to the core Secure Network Analytics. If you are updating Secure Network Analytics from v7.4.x or 7.5.0 to v7.5.1, you can uninstall the app after the update to v7.5.1 is completed.



Do not uninstall your existing app before completing the update to v7.5.1. If you uninstall it beforehand, 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 v7.5.1, access the Security Analytics and Logging (OnPrem) menu as follows:

1. Log in to the Manager.
2. Select the **Investigate** menu.
3. Select **Security Analytics and Logging (OnPrem)**.

For instructions, click the  (**Help**) icon > **Help**.

Smart Licensing Transport Configuration

We have changed the transport configuration requirements for Smart Licensing. If you are upgrading the appliance from Secure Network Analytics v7.4.1 or earlier, make sure the appliance is able to connect to smartreceiver.cisco.com.

Supported TLS Versions

The following TLS versions are supported for Secure Network Analytics v7.5.1.

Identity Provider	Supported TLS Version
Microsoft Active Directory Federation Services (ADFS) for SAML/SSO	1.2
Okta	1.2
Login.gov	1.2, 1.3
Microsoft Entra ID	1.2, 1.3

To change the TLS version on an appliance, refer to the "Configuring Authentication and Authorization" topic in the Help.

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.

CDETS	Title
CSCwh11361	Alarms by Type in dashboard does not match the Report Builder Alarm Count
CSCwk33783	Poor LDAP filter performance when finding roles for remote authorization
CSCwk33798	Incorrect NetFlow parsing after template pointer update causes unexpected flow search results
CSCwk45893	Exporter/Interface cleaner routine causes Flow Collector engine crash in remove_unused_interfaces
CSCwk53075	Slow flow queries caused by Data Store histogram statistics
CSCwk56511	Decryption fails on diagnostic packs uploaded through SystemConfig Upload menu
CSCwk57518	Session Timeout does not work when using Direct Software Downloads Beta
CSCwk57519	Report Builder Dashboard: column filter values are saved without clicking the Apply Filters to Total
CSCwk57520	Analytics Device Report shows inconsistent data after Manager role change
CSCwk57521	Unable to save Report Builder Dashboard when a specific column filter is applied to some report types
CSCwk57522	Report Builder allows deleting a schedule created by someone else

CDETS	Title
CSCwk57523	The ISE ANC Policy Action shows incorrect navigation path to configure a Cisco ISE cluster
CSCwk57524	Security Analytics and Logging On Premises app is shown on the App Manager after 7.5.1 upgrade
CSCwk57525	Security Insights Dashboard shows inaccurate number of alarms for Alarms by Type
CSCwk57526	Changes lost or not saved due to missing confirmation message (before leaving edit mode in Network Diagrams and other components)
CSCwk57527	The Host Summary report shows host policy description instead of the policy name
CSCwk57528	Unable to register or add the Manager to Central Management after removing it from inventory
CSCwk57529	After Flow Collector transition to Data Store, no data shown in flow search queries, top applications, and alarms
CSCwk57530	Assigning IPv6 address using SLAAC protocol fails intermittently
CSCwk57531	The Browser tab title does not match with the Secure Network Analytics user interface title
CSCwk57532	The Browser tab title does not match with the Secure Network Analytics user interface title
CSCwk57533	Missing confirmation message to save configuration changes in Central Management before leaving a page
CSCwk57534	Syslog over TLS certificate revocation check with non-default OCSP/CRL ports is not working on non-Manager appliances

CDETS	Title
CSCwk57535	Report Builder NVM Report: removing one filter value removes all values
CSCwk57536	Changing the appliance network mode from IPv6 SLAAC to IPv4 fails
CSCwk57537	After the Manager is rebooted, Analytics jobs are lagging and shows "Analytics performance has degraded" alarm
CSCwk57541	Manager configured for TLS 1.3 doesn't connect to ISE 3.3
CSCwk57542	Flow Sensor 4240 shows Dropped Packets (DPP)
CSCwk57543	Tooltip text doesn't fit in the box on Investigate Interfaces page
CSCwk57544	Direct Software Download: duplicate status notifications are shown and cannot be closed
CSCwk57929	Help link redirects to general search page instead of service-specific page
CSCwk58048	Secure Network Analytics Alerts not included in Cisco XDR Incident Correlation
CSCwk58049	Simplified XDR-Secure Network Analytics Integration for Incident Correlation (SSX Integration) - Pending Cisco XDR Release
CSCwk69281	Port Order confirmation not shown in SystemConfig on Flow Collector 4210
CSCwk73828	Desktop Client inaccurately shows Flow Collector as unlicensed

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	July 24, 2024	Initial version.
1_1	August 1, 2024	<i>Added Increased Minimum Storage Requirements for Flow Collector VE with Data Store</i> to the What's New section.
1_2	August 1, 2024	Corrected a heading style.
1_3	August 19, 2024	General Availability (GA).

Release Support Information

Official General Availability (GA) date for Release 7.5.1 is August 19, 2024.

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)

