



# Cisco Secure Network Analytics

Release Notes 7.5.0



---

# Table of Contents

|   |           |
|---|-----------|
| <b>Introduction</b> .....                                     | <b>4</b>  |
| Overview .....  | 4         |
| Terminology .....   | 4         |
| Before You Update .....                                       | 4         |
| Software Version .....  | 4         |
| Notice of VMware Compatibility Changes .....                  | 4         |
| Supported Hardware Platforms .....                            | 4         |
| CIMC Firmware Version .....                                   | 5         |
| Cisco Bundles .....   | 6         |
| MongoDB .....   | 6         |
| Smart Licensing Transport Configuration .....                 | 6         |
| High Availability .....                                       | 6         |
| Third-Party Applications .....                                | 6         |
| Apps Version Compatibility .....                              | 6         |
| Browsers .....  | 7         |
| Alternative Access .....                                      | 7         |
| Data Store Private LAN Settings and Data Node Expansion ..... | 8         |
| Data Store Appliance Support .....                            | 9         |
| <b>What's New</b> .....                                       | <b>10</b> |
| Analytics .....   | 10        |
| Post Alerts to Cisco XDR .....                                | 10        |
| Initial Setup .....   | 10        |
| Post an Alert to Cisco XDR .....                              | 10        |
| Post Alerts using Response Management .....                   | 11        |
| Appliance Setup Tool .....                                    | 11        |
| Database Backup (Non-Data Store Domains) .....                | 11        |
| Data Store Backup .....                                       | 11        |
| Endpoint License and Network Visibility Module .....          | 11        |

---

|  |           |
|--|-----------|
| Firewall Logs for Network Detections .....   | 12        |
| Host Group Management .....  | 12        |
| IPv6 Support .....   | 12        |
| *UDP Director Support .....  | 12        |
| Network Management .....   | 13        |
| Packet Capture .....   | 14        |
| Passwords .....  | 14        |
| Restricted Command Line Interface Access .....   | 14        |
| Sending On-Premises Flows from Secure Network Analytics to Secure Cloud<br>Analytics .....           | 14        |
| SSL/TLS Certificates .....   | 15        |
| TLS Versions .....   | 15        |
| Adding Certificates to the Trust Stores (Custom Certificates) .....                                  | 15        |
| Adding Appliances to Central Management .....  | 15        |
| Replacing Unexpired Cisco Self-Signed Appliance Identity Certificates<br>(Certificate Refresh) ..... | 15        |
| Manager User Interface .....   | 16        |
| Network Diagrams .....   | 16        |
| Secure Network Analytics Apps .....  | 16        |
| Access the Apps .....  | 17        |
| Guides Moving to Help .....  | 17        |
| Known Issue: Custom Security Events .....  | 18        |
| <b>Known Issues .....</b>  | <b>19</b> |
| <b>Contacting Support .....</b>  | <b>21</b> |
| <b>Change History .....</b>  | <b>22</b> |
| <b>Release Support Information .....</b>   | <b>23</b> |

---

# Introduction

## Overview

This document provides information about the new features and improvements, bug fixes, and known issues for the v7.5.0 release of Cisco Secure Network Analytics (formerly Stealthwatch).

For additional information about Secure Network Analytics, go to [cisco.com](https://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](#).

## Software Version

To update the appliance software to v7.5.0, the appliance must have version 7.4.0, 7.4.1, or 7.4.2 installed. It is also important to note the following:

## Notice of VMware Compatibility Changes



Secure Network Analytics v7.5.0 is compatible with VMware 7.0 or 8.0. 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.

## 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, 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.

| M4 Hardware             | M5 Hardware             | M6 Hardware             |
|-------------------------|-------------------------|-------------------------|
| SMC 2200 (Manager 2200) | SMC 2210 (Manager 2210) | SMC 2300 (Manager 2300) |
| FC 4200                 | FC 4210                 | FC 4300                 |
| FC 5020 Engine          | ---                     | ---                     |
| FC 5020 Database        | ---                     | ---                     |
| FC 5200 Engine          | FC 5210 Engine          | ---                     |
| FC 5200 Database        | FC 5210 Database        | ---                     |
| FS 1200                 | FS 1210                 | FS 1300                 |
| FS 2200                 | ---                     | ---                     |
| FS 3200                 | FS 3210                 | FS 3300                 |
| FS 4200                 | FS 4210 / FS 4240       | FS 4300                 |
| UD 2200                 | UD 2210                 | ---                     |
| ---                     | DS6200                  | DN6300                  |

---

## 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.

## MongoDB

During the update to v7.5.0, we will upgrade MongoDB to v6.0.9.

**CPU Instruction Set Requirement:** Ensure that 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.

## Smart Licensing Transport Configuration

We have changed the transport configuration requirements for Smart Licensing.



If you are upgrading the appliance from v7.4.1 or earlier, make sure that the appliance is able to connect to [smartreceiver.cisco.com](https://smartreceiver.cisco.com).

## High Availability

If you have high availability configured on your UDP Directors and plan to update Secure Network Analytics to v7.5.0, 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.

## 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. 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**.
9. 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 Store Appliance Support

The following table describes Data Store appliance support:

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



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).

---

## What's New

These are the new features and improvements for the Secure Network Analytics v7.5.0 release.

### Analytics

#### Post Alerts to Cisco XDR

You can now post Cisco Secure Network Analytics alerts to Cisco XDR using the Analytics feature within your Manager. Note that when you post an alert to Cisco XDR, it will also post to SecureX.

#### Initial Setup

To post alerts to Cisco XDR, your user needs access. To give your user access, you need to set up an API Client.

Log in to Cisco XDR and complete a new API Client configuration (**Administration > API Clients**). In the **Client Name** field, type your entry. This entry will simply be the label that appears in the Client column in XDR. In the Scopes section, check all the check boxes by clicking **Select All**. For more information about Cisco XDR, go to the [Cisco XDR site](#).

#### Post an Alert to Cisco XDR

To post a Cisco Secure Network Analytics alert within Analytics, either use the **Post an Incident** field on the Alert Details page or create a rule in Response Management.

- To access the Alert Details page, from the main menu, select **Monitor > Alerts**. The Alerts Summary opens. If you click an alert, the Alert Details page for that alert opens.
- To access the Response Management Rules page, select **Configure > DETECTION > Response Management > Rules**.



Before you can use the Post an Incident field, you must first create a SecureX configuration. To do so, refer to the [Cisco SecureX Integration Guide](#).

For more details about posting Secure Network Analytics alerts to Cisco XDR, see the “Analytics: Post Alerts to Cisco XDR” topic in the Help.

---

## Post Alerts using Response Management

You can also now post Cisco Secure Network Analytics alerts using the email, syslog, and webhooks action types within Response Management (just as you currently can post Cisco Secure Network Analytics alarms using these action types). For more details about posting Secure Network Analytics alerts using Response Management, see the “Response Management: Workflow” topic in the Help.

## Appliance Setup Tool

The Appliance Setup Tool is no longer used to configure your appliances. When you log in to the appliance for the first time, you will use the First Time Setup tool to configure each appliance so it is managed by your Manager. For more information, refer to the [System Configuration Guide](#).

## Database Backup (Non-Data Store Domains)

We have removed the need to delete database snapshots when you are creating a database backup for Non-Data Store domains. For more information, refer to the [System Configuration Guide](#).

## Data Store Backup

The Data Store backup process has been updated so it is now done through the appliance console (SystemConfig). We have added a Data Store Backup menu, which allows you to configure your remote host, perform dry runs of your Data Store backup to test your backup and estimate size, manage your backup operations, and perform backups. Refer to the [System Configuration Guide](#) for more information.

## Endpoint License and Network Visibility Module

The following capabilities have been added to Data Store deployments ingesting Cisco Secure Client (including AnyConnect) Network Visibility Module (NVM) traffic in v7.5.0:

- 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

We've added two new fields to the Flow Collector Advanced Settings, **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. For details, refer to the [Secure Network Analytics Endpoint License and Network Visibility Module Configuration Guide v7.5.0](#)

## Firewall Logs for Network Detections

We've added network detections based on Cisco Security Analytics and Logging (On Premises) data. If you enable this configuration, you'll have more insight into your traffic patterns, risks, and the scope of an attack.

- **Configuration:** Follow the instructions in the [Cisco Security Analytics and Logging \(On Premises\): Firewall Event Integration Guide](#).
- **Queries:** You can query Firewall Logs in flow searches, custom security events, and Report Builder.

## Host Group Management

The Host Group Management 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.

## IPv6 Support

We provide the following support for IPv6 and Dual Stack in v7.5.0:

| 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 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 on IPv6 forwarding for UDP Directors, refer to the [Cisco Telemetry Broker User Guide](#).

- **M4 UDP Directors:** If you are configuring an M4 UDP Director (UD2200), only IPv4 is supported. For more information on M4 and M5 UDP Directors, refer to [CIMC Firmware Version](#).
- **Changing the Network Mode:** For information on 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
- IPv4 only to IPv6 only
- Dual stack to IPv6 only
- Dual stack to IPv4 only
- IPv6 to IPv4 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 v7.5.0.

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 on IPv6 forwarding for UDP Directors, refer to the [Cisco Telemetry Broker User Guide](#).



If you are configuring an M4 UDP Director (UD2200), only IPv4 is supported. For more information on M4 and M5 UDP Directors, refer to [CIMC Firmware Version](#).

For information about changing the network mode of your appliance, refer to the [System Configuration Guide](#).

Refer to the [System Configuration Guide](#) for more information.

---

## Packet Capture

The packet capture process has been updated in v7.5.0. Refer to the "Packet Capture" and "Packet Capture on the Manager" topics in the Help for more information.

## Passwords

The following password changes have been made in v7.5.0:

- There are no longer default passwords for root and root password access has been restricted. See [Restricted Command Line Interface Access](#) for more information.
- The password reset boot option and related SystemConfig plugin have been removed.
- You can reset admin and sysadmin passwords to default. The root account is inaccessible using passwords and thus has no password reset mechanism. See [Restricted Command Line Interface Access](#) for more information.
- We have changed the process for resetting the admin password on the Manager. This process is now being handled through the Appliance Console (SystemConfig) under the Security menu. Refer to the [System Configuration Guide](#) for more information.

## Restricted Command Line Interface Access

Command line interface access has been restricted due to added security measures in the v7.5.0 release. You can still use the appliance console (SystemConfig) for troubleshooting and Cisco Support. You can work with Cisco Support to gain temporary command line interface access under the following circumstances:

- Access is only used for troubleshooting or recovery.
- Access is used in accordance with the Cisco command line interface access policy.

## Sending On-Premises Flows from Secure Network Analytics to Secure Cloud Analytics

We've moved the Flow Collector configuration for sending on-premises flows from Secure Network Analytics to Secure Cloud Analytics. As part of the procedure, you will log in to the Flow Collector appliance console (SystemConfig). For instructions, refer to the [Send On-Premises Flows from Cisco Telemetry Broker or Secure Network Analytics to Secure Cloud Analytics Guide](#).

---

## SSL/TLS Certificates

We updated our requirements, security checks, and workflows for SSL/TLS appliance identity certificates. For a successful configuration in all workflows, make sure you follow the instructions in the [SSL/TLS Certificates for Managed Appliances Guide](#).

### TLS Versions

You can choose the TLS version configuration for your appliances, as shown below. Versions 1.2 and 1.3 are supported by default when you upgrade to v7.5.0.

- TLS 1.2 and 1.3 (default)
- TLS 1.3 only (not supported for Data Store)

### Adding Certificates to the Trust Stores (Custom Certificates)

To replace the appliance identity certificate with a custom certificate, we previously required uploading the identity certificate and chain (root and intermediate certificates) individually to each appliance trust store.

In v7.5.0, you only need to add the self-signed certificate or the root certificate to the appliance trust stores depending on the procedure you choose. For certificate requirements and instructions, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#).

### Adding Appliances to Central Management

Many certificate-related workflows include adding appliances to Central Management. We moved this menu from the Appliance Setup Tool to the appliance console (SystemConfig).

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



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](#).

## Manager User Interface

We changed our fonts and colors in our Manager UI.


## Network Diagrams

We moved Network Diagrams from a separate app to the core Secure Network Analytics in v7.5.0. If you are updating Secure Network Analytics from v7.4.x to v7.5.0, all of your diagrams will be preserved. However, you will now access the Network Diagrams app from a different location in the menu (see below) as part of this update.



Do not uninstall your existing Network Diagrams app. If you uninstall Network Diagrams, all files associated with it, including your diagrams and temporary files, are deleted.

Follow the instructions in the [Update Guide](#). After you've updated Secure Network Analytics to v7.5.0, access Network Diagrams as follows:

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

## 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 v7.5.0, 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.

## Guides Moving to Help

Previously we had posted the following guides to cisco.com. As of v7.5.0, this information will be available only in the Help.

| Guide Name                          | Help topics  |
|-------------------------------------|--|
| Alarm Suppression                   | Alarm Suppression Overview   |
| Default Custom Security Event Setup | <ul style="list-style-type: none"><li>• Configuring Custom Policies (Custom Security Events)</li><li>• Managing and Configuring Host Group</li></ul> |
| Using the External Lookup Feature   | Managing External Lookup   |

---

## Known Issue: Custom Security Events

When you delete a service, application, or host group, it is not deleted automatically from your custom security events, which can invalidate your custom security event configuration and cause missing alarms or false alarms. Similarly, if you disable Threat Feed, this removes the host groups Threat Feed added, and you need to update your custom security events.

We recommend the following:

- **Reviewing:** Use the following instructions to review all custom security events and confirm they are accurate.
  - **Planning:** Before you delete a service, application, or host group, or disable Threat Feed, review your custom security events to determine if you need to update them.
1. Log in to your Manager.
  2. Select **Configure > DETECTION Policy Management**.
  3. For each custom security event, click the **⋮ (Ellipsis)** icon, and choose **Edit**.
    - **Reviewing:** If the custom security event is blank or missing rule values, delete the event or edit it to use valid rule values.
    - **Planning:** If the rule value (such as a service or host group) you are planning to delete or disable is included in the custom security event, delete the event or edit it to use a valid rule value.

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

## 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  |
|----------------------------|--|
| <a href="#">CSCwi37680</a> | Data Store Retention Manager may drop too much data if a Data Node is recovering                                 |
| <a href="#">CSCwi33350</a> | Manager displays default_error when adding LDAP user authentication service using FQDN server address            |
| <a href="#">CSCwi37953</a> | Report Builder search results with filter doesn't show any data  |
| <a href="#">CSCwi37948</a> | Flow Collector shows a 500 error when saving the changes on the Flow Collector Configuration page                |
| <a href="#">CSCwi37946</a> | The XSD for SWAEntity (or SWAType) doesn't allow partner-ip-address and causes an upgrade issue                  |
| <a href="#">CSCwi37945</a> | The secondary Manager fails to recognize Flow Collector 5000 after an upgrade.                                   |
| <a href="#">CSCwi37950</a> | Update Manager is unable to upload the swu (firmware/patch update file)  |
| <a href="#">CSCwi39002</a> | Report Builder doesn't display Invalid IP Address or Range error for IP addresses separated by a space           |
| <a href="#">CSCwi37944</a> | Restoring Central Management backup configuration disables the Global Threat Alerts setting                      |
| <a href="#">CSCwi37947</a> | Appliance in IPv6 Only mode on Central Management Edit Appliance Configuration shows both IPv4 and IPv6 for eth0 |
| <a href="#">CSCwi37952</a> | System always prompts user to regenerate certificates when changing IPv6 address in IPv6 Only mode               |

---

| <b>CDETS</b>               | <b>Title</b>   |
|----------------------------|--|
| <a href="#">CSCwi19387</a> | Flow Collection Status report in Report Builder does not support all the NetFlow versions                                |
| <a href="#">CSCwi37949</a> | If a custom certificate is rejected when replacing the appliance identity, Central Management blocks uploading new files |
| <a href="#">CSCwi39016</a> | When editing ISE from different domains in the Desktop Client, the default domain ISE page is opened                     |
| <a href="#">CSCwi37951</a> | Relationship Policy doesn't show host groups when selecting Policy Management from Network Diagrams                      |
| <a href="#">CSCwi37954</a> | Device Registration Status changes from Enrolled to Unavailable when using IPv6 proxy after an upgrade                   |
| <a href="#">CSCwh66159</a> | Recovery files filling up filesystem 100% on the Manager due to failed host group configuration                          |
| <a href="#">CSCwe25793</a> | Data Node fails to block Browsing Files from UI when FIPS/CC mode is enabled   |

# 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](mailto: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              | December 13, 2023 | Initial Version.  |
| 1_1              | January 22, 2024  | General Availability (GA). Updated <i>Analytics</i> content in the <i>What's New</i> section. |

# Release Support Information

Official General Availability (GA) date for Release 7.5.0 is January 22, 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)

