Upgrade Secure Network Analytics (SNA) Best Practices

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Software Downloads and Upgrade Guides

Hardware Support Matrix

- Manager & Flow Collector (incl. Engine & Database)
- Data Store
- Flow Sensor
- Flow Replicator/UDP Director

App Compatibility Matrix

- ETA Cryptographic Audit
- Host Classifier
- Network Diagrams and Report Builder (Report Builder is integrated into the product starting 7.4.0)
- Security Analytics and Logging on Prem (integrated in product starting 7.5.1) and Visibility Assessment

Upgrades by Release

- Upgrade Release 7.3.x to 7.4.x
- Upgrade Release 7.4.x to 7.5.x
- Upgrade Release 7.5.x to 7.6.0

Software Support Timelines

End of Life (EOL) Notices

- FlexNet EOL
- Global Threat Analytics (GTA) EOL
- Endpoint License (AnyConnect Network Visibility Module Integration)
- SAL-OP License EOL
- UDP Director Virtual EOL

Upgrade Gotchas and Warnings

Introduction

This document describes some best practice information about upgrades to Secure Network Analytics (SNA) (formerly known as Stealthwatch).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SNA only supports upgrades from one major release to the next. For example, from 7.3.x to 7.4.x or 7.4.x to 7.5.x. Release skips are not supported. If the user is comfortable with reset of all data to a factory default state then a hardware appliance can be reimaged, a new VM can be installed.

Software Downloads and Upgrade Guides

- Software and guides for releases 7.3.2 and higher are at Software Download
- Software and guides for releases previous to 7.3.2 are no longer available

Hardware Support Matrix

The information in this section is pulled from the Cisco Secure Network Analytics Hardware and Software Version Support Matrix guide as of release 7.6.0.

Manager & Flow Collector (incl. Engine & Database)

● - Performs at full capacity on hardware	○ - Supported, but performance not optimal	x - Not supported

Manager

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
Manager 2200	UCSC-C220	M4S	●	●	●	●	x	x	x	x
Manager 2210	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
Manager 2300	UCSC-C225	M6SX	x	x	●	●	●	●	●	●

Flow Collector

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FC 4200	UCSC-C220	M4S	●	●	●	●	x	x	x	x
FC 4210	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
FC 4300	UCSC-C225	M6SX	x	x	●	●	●	●	●	●
FC 5200 Engine	UCSC-C220	M4S	●	●	●	●	x	x	x	x

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FC 5200 Database	UCSC-C240	M4S2	●	●	●	●	x	x	x	x
FC 5210 Engine	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
FC 5210 Database	UCSC-C240	M5SX	●	●	●	●	●	●	●	●

Data Store

Data Store

v7.4.1 and Earlier Releases

Users deploying a Data Store for v7.4.1 or earlier can configure the Manager and Flow Collector 10Gbps SFP+ interface as eth0 for increased throughput. Users not deploying a Data Store for v7.4.1 or earlier can only configure the Manager and Flow Collector 100Mbps/1Gbps/10Gbps copper interface as eth0.

v7.4.2 and Later Releases

Users deploying a Data Store for v7.4.2 can configure a Manager 2300 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. Users not deploying a Data Store for v7.4.2 can only configure the 1 Gbps/10 Gbps interface as eth0.

Appliance	Data Nodes	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
DS 6200	3	UCSC-C240	M5SX	●	●	●	●	●	●	●	●
DN 6300	1	UCSC-C225	M6SX	x	x	●	●	●	●	●	●

The following table describes Data Store appliance support:

Appliance	Required?	Supported Models
Data Store	yes	• DS 6200 multi node (v7.4.0 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	• Manager 2210 or Manager Virtual Edition (v7.4.0 or greater). Four models available for virtual edition • Manager 2300 or Manager Virtual Edition (v7.4.2 or greater).
Flow Collector	yes	• Flow Collector 4210s or Flow Collector Virtual Edition (v7.4.0 or greater)* • Flow Collector 4300s or Flow Collector Virtual Edition (v7.4.2 or greater)* • Flow Collector 5210s or Flow Collector Virtual Edition (v7.4.0 or greater)* * Four models available for Virtual Edition
Flow Sensor	no	• For M5SX generations, any model at v7.4.0 or greater. • For the M6SX generation, Flow Sensors are only supported at v7.4.2 or greater.
UDP Director	no	• UD 2210 • There are no M6 UDPDs.

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, all DN 6300).

Flow Sensor

Flow Sensor

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FS 1200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 1210	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 1300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•
FS 2200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 3200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 3210	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 3300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•
FS 4200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 4210	UCSC-C220	M5SX	•	•	•	•	•	•	•	x
FS 4240	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 4300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•

Flow Replicator/UDP Director

Flow Replicator/UDP Director

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3
UD 2200	UCSC-C220	M4S	•	•	•	•	x	x	x
UD 2210	UCSC-C220	M5SX	•	•	•	•	•	•	•

NOTE: UDPD 2210 is EOL. UDPD users are encouraged to migrate to CTB, however 7.6.0 UDPD upgrade is possible. The swu file is available at Software Download.

App Compatibility Matrix

The information in this section is pulled from the Secure Network Analytics Apps Version Compatibility Matrix

ETA Cryptographic Audit

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
ETA Cryptographic Audit	1.0.27	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None
	2.0.2	7.2.1, 7.3.0	None
	2.0.3	7.3.0	None
	3.0.0	7.3.1	None
	3.1.0	7.3.2	7.3.2 (Audit Report only)
	3.2.0	7.4.0	7.4.0 (Audit Report only)
	3.2.1	7.4.1	7.4.1 (Audit Report only)
	3.2.2	7.4.2	7.4.2 (Audit Report only)
	3.3.1	7.5.0	7.5.0 (Audit Report only)
	3.3.2	7.5.1	7.5.1 (Audit Report only)
	3.3.3	7.5.2	7.5.2 (Audit Report only)

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
	3.3.4	7.5.3	7.5.3 (Audit Report only)
	3.3.5	7.6.0	7.6.0 (Audit Report only)

Host Classifier

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Host Classifier	1.0.9, 1.0.11, 1.0.13	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None
	2.0.3	7.2.1	None
	2.0.4	7.2.1, 7.3.0, 7.3.1	None
	2.0.6	7.3.0, 7.3.1, 7.3.2	None
	3.0.0	7.4.0	None
	3.1.1	7.4.0, 7.4.1	None
	4.0.2	7.4.2	None
	4.1.1	7.5.0	None
	4.2.1	7.5.1	None
	4.2.2	7.5.2	None

	4.3.0	7.5.3	None
	4.4.0	7.6.0	None

Network Diagrams and Report Builder (Report Builder is integrated into the product starting 7.4.0)

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Network Diagrams	1.0.3	7.1.1, 7.1.2, 7.1.3	None
	2.0.2	7.2.1, 7.3.0	7.3.0
	2.0.3, 2.0.4	7.3.0, 7.3.1	7.3.0, 7.3.1
	2.0.5	7.3.2	7.3.2
	2.1.0	7.4.0	7.4.0
	2.1.1	7.4.1	7.4.1
	2.2.1	7.4.2	7.4.2
Report Builder	1.1.2, 1.1.5, 1.1.6	7.3.0	7.3.0
	1.2.1, 1.3.1, 1.3.2, 1.3.4	7.3.1	7.3.1
	1.4.1, 1.4.4, 1.4.5	7.3.2	7.3.2

Security Analytics and Logging on Prem (integrated in product starting 7.5.1) and Visibility Assessment

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Security Analytics and Logging On Prem	1.0.0	7.3.0, 7.3.1	None
	2.0.1, 2.0.2	7.3.1, 7.3.2	7.3.2
	3.0.0	7.4.0	7.4.0
	3.1.0	7.4.0, 7.4.1	7.4.0, 7.4.1
	3.2.0	7.4.2	7.4.2
	3.3.0	7.5.0	7.5.0
Visibility Assessment	1.0.4	7.0.0	None
	1.0.7, 1.0.11, 1.0.14	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None

Upgrades by Release

Upgrade Release 7.3.x to 7.4.x

Upgrades to releases: 7.4.0, 7.4.1 and 7.4.2

Software Downloads: Software is available at Software Download

Upgrade Guide: Update guide for 7.3.x to 7.4.0 or 7.4.1

Upgrade Guide: Update guide for 7.3.x to 7.4.2

Upgrade Release 7.4.x to 7.5.x

Upgrades to releases: 7.5.0, 7.5.1, 7.5.2, 7.5.3

Software Downloads: Software is available at Software Download

Upgrade Guide: Update guide for 7.4.x to 7.5.0

Upgrade Guide: Update guide for 7.4.x and 7.5.0 to 7.5.1
Upgrade Guide: Update guide for 7.4.x and 7.5.x to 7.5.2
Upgrade Guide: Update Guide for 7.4.x and 7.5.x to 7.5.3

Upgrade Release 7.5.x to 7.6.0

Upgrade to release 7.6.0

Software Downloads: Software is available at Software Download

Upgrade Guide: Update Guide for 7.5.x to 7.6.0

Software Support Timelines

Typically a release is covered under Software Maintenance for 12 months post-release and receives Vulnerability and Security Fixes for 18 months post-release. More information about the SNA software Release Model and release support timeline is available from Cisco Stealthwatch® Software Release Model and Release Support Timeline Product Bulletin.

This table lists support timelines from release 7.1.1 onwards.

Release	Release Date	End of Software Maintenance (EoS)	End of Vulnerability & Security Support (EoVSS)
7.6.0*	23 March, 2026	23 March, 2027	23 September, 2027
7.5.3	25 August, 2025	25 August, 2026	25 February, 2027
7.5.2	24 February, 2025	24 February, 2026	24 August, 2026
7.5.1	19 August, 2024	19 August, 2025	19 February, 2026
7.5.0	22 January, 2024	22 January, 2025	22 July, 2025

7.4.2	26 March, 2023	26 March, 2024	26 September, 2024
7.4.1	09 May, 2022	09 May, 2023	09 November, 2023
7.4.0	02 November, 2021	02 November, 2022	02 May, 2023
7.3.2	01 June, 2021	01 June, 2022	01 December, 2022
7.3.1	04 Feb, 2021	04 February, 2022	04 August, 2022
7.3.0	03 September, 2020	03 September, 2021	03 March, 2022
7.2.1	17 June, 2020	17 June, 2021	01 July, 2022
7.1.1	16 August, 2019	16 August, 2020	01 July, 2022

* indicates the currently recommended release

End of Life (EOL) Notices

FlexNet EOL

FlexNet licensing went EOL on Dec 31, 2022. All SNA licensing moved to CIsco Smart Licensing.

Global Threat Analytics (GTA) EOL

GTA is scheduled to go EOL on July 31, 2024. The EOL notice also discusses migration options.

Endpoint License (AnyConnect Network Visibility Module Integration)

With Secure Network Analytics Release 7.5.1, the Endpoint license is no longer necessary for the Secure Network Analytics integration with the Network Visibility Module from Cisco Secure Client (AnyConnect). Instead, consumption counts towards a customer's Flow Rate License in order to simplify the entitlement requirements.

SAL-OP License EOL

Starting with Secure Network Analytics Release 7.5.3, the SAL-OP (Secure Analytics Logging - On Prem) license is no longer required for integrating Secure Network Analytics with Secure Analytics On-Prem Logging from Cisco Firewalls. Instead, usage now contributes to a customer's Flow Rate License, streamlining the entitlement process.

UDP Director Virtual EOL

The EOL notice informs the last date of support is October 31st, 2028. UDP Director is being replaced by Cisco Telemetry Broker.

Upgrade Gotchas and Warnings

Number 1: Manager Failover: Once you start an upgrade, do **NOT** perform a Manager failover until ALL appliances are upgraded, this could result in the system becoming inoperable.

Number 2: Before you start the update (for example, to 7.6.0), make sure your appliances have been running on the same version (in this case, 7.5.0, 7.5.1, 7.5.2 or 7.5.3) for more than one month (30 days). If you've updated your system to more than one version in a short period of time, your system baselining may be impacted.