ılıılı
CISCO
The bridge to possible

Cisco Secure Network Server

Contents

Product overview

Granting and denying network access has evolved beyond simple username and password verifications. Today, additional attributes related to users and their devices are used as decision criteria in determining authorized network access. Additionally, network service provisioning can be based on data such as the type of device accessing the network, including whether it is a corporate or personal device.

The Cisco® Secure Network Server is a scalable solution that helps network administrators meet complex network access control demands by managing the many different operations that can place heavy loads on applications and servers, including:

- Authorization and authentication requests

- Queries to identity stores such as Active Directory (on-premise or Azure), LDAP, and other databases

    ◦ API queries to fetch attributes from third-party systems (such as ServiceNow)

- Device profiling and compliance checking

- Enforcement actions to remove devices from the network

- Reporting

The Cisco Secure Network Server is based on the Cisco UCS® C220 Rack Server and is configured specifically to support the Cisco Identity Services Engine (ISE) security application. The Secure Network Server supports these applications in three versions. The Cisco Secure Network Server 3715 is designed for small deployments. The Secure Network Server 3755 and 3795 have several redundant components such as hard disks and power supplies, making it suitable for larger deployments that require highly reliable system configurations.

Figure 1 shows the Cisco Secure Network Server.

Figure 1.
Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server

Product specifications

Table 1 lists specifications of the Cisco Secure Network Server.

Table 1.

Product name	SNS-3715	SNS-3755	SNS-3795
Processor	Intel 4310 2.1GHz	Intel 4316 2.3GHz	Intel 4316 2.3GHz
Cores per processor	12 Cores and 24 Threads	20 Cores and 40 Threads	20 Cores and 40 Threads
Memory	32GB 2 X 16GB	96GB 6 X 16GB	256GB 8 X 32GB
Hard disk	1 60012G SAS 10K RPM SFF HDD **Or** 800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance) **Or** 960GB 2.5 in Enterprise value SATA SSD Self Encrypted Drive (1X , SED)	4 60012G SAS 10K RPM SFF HDD **Or** 800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance) **Or** 960GB 2.5 in Enterprise value SATA SSD Self Encrypted Drive (1X , SED)	8 60012G SAS 10K RPM SFF HDD **Or** 800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance) **Or** 960GB 2.5 in Enterprise value SATA SSD Self Encrypted Drive (1X , SED)
Hardware RAID	Level 0	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network interface	2 X 10Gbase-T 4 X 10GE SFP	2 X 10Gbase-T 4 X 10GE SFP	2 X 10Gbase-T 4 X 10GE SFP
Power supplies	1 X 1050W	2 X 1050W	2 X 1050W
TPM chip	Yes	Yes	Yes

Security applications

The Cisco Secure Network Server supports Cisco's powerful network access and control security applications:

Cisco Identity Services Engine

An integral component to Cisco's cybersecurity initiative, the Cisco Identity Services Engine (ISE) is a revolutionary product that extends the network access and admission control capabilities. Looking beyond username and password, the Identity Services Engine delivers unprecedented abilities to acquire user and device identity and context information to forge flexible and powerful policies that govern authorized network access. ISE is an all-in-one enterprise policy control platform that can reliably provide secure access for wired, wireless, VPN, and Private 5G networks. ISE can also help IT with secure BYOD on-boarding and allow IT to provide differentiated Guest Access. The Identity Services Engine provides enforcement actions that allow administrators to restrict devices from the network that are violating access and policies.

Table 2 lists ISE endpoint scalability metrics for the Secure Network Servers.

Table 2. Identity Services Engine deployment scalability (ISE 3.1 P6 and later)

	Secure Network Server 3715	Secure Network Server 3755	Secure Network Server 3795
Concurrent active endpoints supported by a dedicated PSN **(Cisco ISE node only has PSN persona.)**	50,000	100,000	100,000
Concurrent active endpoints supported by a shared PSN **(Cisco ISE node has multiple personas.)**	25,000	50,000	50,000

Note: Cisco SNS-3795 is equipped with better RAM, Disk R/W performance. It is best suited for dedicated PAN, dedicated MnT or dedicated PAN/MnT personas.

Ordering information

Table 3 lists ordering information for the Cisco Secure Network Servers.

Each SNS server can be ordered with HDD, SSD or SED as a configuration option.

Table 3. Product ordering information

Server part numbers	Server description
SNS-3715-K9	Secure Network Server for ISE applications (small)
SNS-3755-K9	Secure Network Server for ISE applications (medium)
SNS-3795-K9	Secure Network Server for ISE applications (large)

SSD offers improved performance in disk read/write operations and other ISE operations like reboot, installation, upgrades, database intensive tasks like backup and restore, reports generation, and so on.

Performance improvements vary between an average of 15% in fresh installation, 40% in upgrades, and 80% in exporting extensive reports with tens of millions of records.

Table 4 lists the Secure Network Server component spares that can be used as Field Replaceable Units (FRUs).

Table 4.   Spare components for the Cisco Secure Network Server

Secure network server	Component part number	Component description
3715/3755/3795	UCS-HD600G10K12N=	600-GB 12-Gb SAS 10K RPM SFF hard disk; hot pluggable; drive sled mounted
3715/3755/3795	UCS-SD800GK3XEP=	800GB 2.5 in Enterprise Performance 12G SAS SSD (3X endurance)
3715/3755/3795	UCS-SD960GM2NK9=	960GB Enterprise value SATA SSD (1X , SED)
	UCSC-PSU1-1050W=	1050W power supply
3715/3755/3795	UCSC-PSU1-1050ELV=	UCSC-PSU1-1050ELV is required for Low Line Voltage 110VAC and below (e.g., Japan)
3715/3755/3795	N20-BKVM=	KVM cable
3715/3755/3795	UCSC-RAIL-M6=	Rail kit

Network connective

Copper PID:

GLC-TE – 1000BASE-T SFP transceiver module for Category 5 copper wire

Fiber PIDs:

[UCS M6 10G NIC Interoperability with Cisco Cables/Optics](#)

Supported ISE versions

The Cisco Secure Network Server 37XX supports ISE 3.1 P6 and later versions only. Upon receiving the SNS-37XX, it is recommended to install the latest patch of the ISE suggested release.
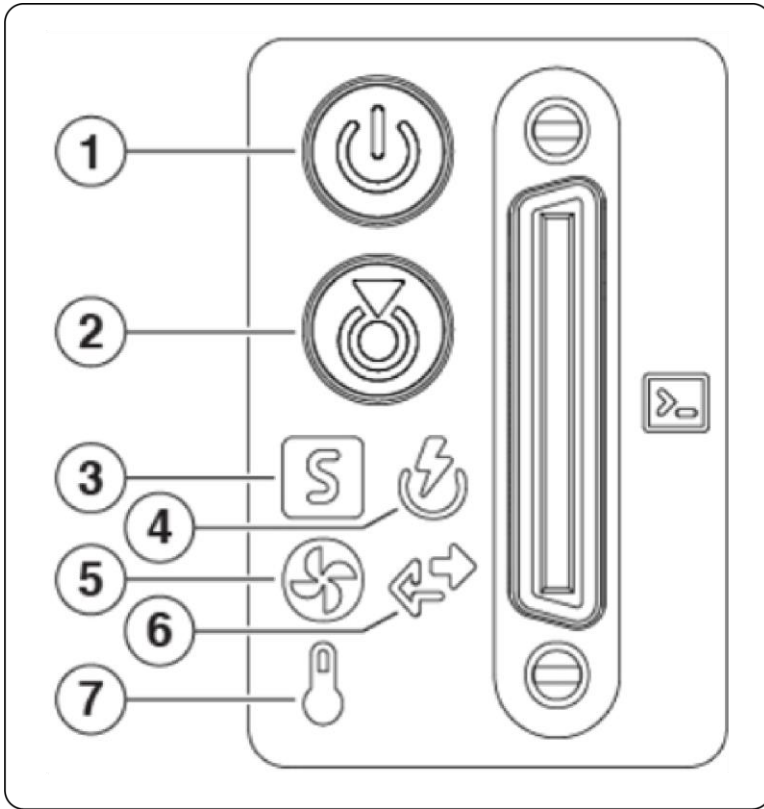
Connectors and LEDs

Table 5 lists Connectors and LEDs on the Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Servers.

Table 5.   SNS-3715, SNS-3755, and SNS-3795 Connectors and LEDs

	LED Name	States
1	**Power LED**	**Off** – There is no AC power to the server.
		Amber – The server is in standby power mode. Power is supplied only to the Cisco IMC and some motherboard functions.
		Green – The server is in main power mode. Power is supplied to all server components.
2	**Unit Identification**	**Off** – The unit identification function is not in use.
		Blue, blinking – The unit identification function is activated.

	LED Name	States
3	**System Health**	**Green** – The server is running in normal operating condition.
		Green, blinking – The server is performing system initialization and memory check.
		Amber, steady – The server is in a degraded operational state (minor fault). For example:
		• Power supply redundancy is lost.
		• CPUs are mismatched.
		• At least one CPU is faulty.
		• At least one DIMM is faulty.
		• At least one drive in a RAID configuration failed.
		Amber, 2 blinks – There is a major fault with the system board.
		Amber, 3 blinks – There is a major fault with the memory DIMMs.
		Amber, 4 blinks – There is a major fault with the CPUs.
4	**Power Supply Status**	**Green** – All power supplies are operating normally.
		Amber, steady – One or more power supplies are in a degraded operational state.
		Amber, blinking – One or more power supplies are in a critical fault state.
5	**Fan Status**	**Green** – All fan modules are operating properly.
		Amber, blinking – One or more fan modules breached the nonrecoverable threshold.
6	**Network Link Activity**	**Off** – The Ethernet LOM port link is idle.
		Green – One or more Ethernet LOM ports are link-active, but there is no activity.
		Green, blinking – One or more Ethernet LOM ports are link-active, with activity.
7	**Temperature Status**	**Green** – The server is operating at normal temperature.
		Amber, steady – One or more temperature sensors breached the critical threshold.
		Amber, blinking – One or more temperature sensors breached the nonrecoverable threshold.

Form factor

Physical dimensions (H x W x D) 1RU: 1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm).

Environmental

Table 6 lists environmental information for the Cisco Secure Network Servers.

Table 6.

Description	Specification
Temperature, operating	50 to 95°F (10 to 35°C)
	Extended environment 41 to 104°F (5 to 40°C)
	Derate the maximum temperature by 1°F for every 547 feet (1°C per every 300 meters) of altitude above 3117 feet (950 m).
	Note: Although the ASHRAE guidelines define multiple classes with different operating ranges, the recommended temperature and humidity operating range is the same for each class. The recommended temperature and humidity ranges are:
	Operating Temperature: 64.4 to 80.6°F (18 to 27°C)
	For general information, see the [Cisco Unified Computing System Site Planning Guide: Data Center Power and Cooling](#).
Temperature, nonoperating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
	Maximum rate of change (operating and nonoperating)
	20°C per hour (36°C per hour)
Humidity (RH), operating	8% to 90% and 75°F (24°C) maximum dew point temperature, noncondensing environment
Humidity (RH), nonoperating (when the server is stored or transported)	5 to 95% and 91°F (24°C) maximum dew point temperature, noncondensing environment
Altitude, operating	0 to 10,000 feet (0 to 3050 meters)
Altitude, nonoperating (when the server is stored or transported)	0 to 40,000 feet (0 to 12,192 meters)
Sound power level **Measure A-weighted per ISO7779 LwAd (Bels)** **Operation at 73°F (23°C)**	5.5
Sound pressure level **Measure A-weighted per ISO7779 LpAm (dBA)** **Operation at 73°F (23°C)**	40

Compliance requirements

Table 7 lists compliance requirements information for the Cisco Secure Network Servers.

Table 7.

Parameter	Description
Regulatory compliance	Products should comply with CE Markings per directives 2014/30/EU and 2014/35/EU.
Safety	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition AS/NZS 60950-1 GB4943 2001
EMC - Emissions	47CFR Part 15 (CFR 47) Class A AS/NZS CISPR32 Class A CISPR32 Class A EN55032 Class A ICES003 Class A VCCI Class A EN61000-3-2 EN61000-3-3 KN32 Class A CNS13438 Class A
EMC - Immunity	EN55024 CISPR24 EN300386 KN35

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

How to buy

To view buying options and speak with a Cisco sales representative, visit www.cisco.com/c/en/us/buy.html.

For more information

For more information, please visit the following resources:

- Cisco Identity Services Engine: www.cisco.com/go/ISE
- Cisco UCS Servers: www.cisco.com/go/unifiedcomputing

Document history

New or revised topic	Described in	Date
Add SED disk	[Table 1](#)	July, 2023
Updated performance	[Table 2](#)	July, 2023
Updated PIDs	[Table 4](#)	July, 2023

Printed in USA   C78-726524-12   07/23