

Cisco Secure Network Server

Product overview

Granting and denying network access has evolved beyond simple user name 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 and LDAP databases
- Device profiling and posture 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 five versions. The Cisco Secure Network Server 3515 and 3615 are designed for small deployments. The Secure Network Server 3595, 3655, and 3695 has several redundant components such as hard disks and power supplies, making it suitable for larger deployments that require highly reliable system configurations. The Secure Network Server 3615, 3655, and 3695 are recommended for new installations whereas the Secure Network Server 3515 and 3595 are recommended for existing installations.

Figure 1 shows the Cisco Secure Network Server.

Figure 1. Cisco SNS-3515 and SNS-3595 Secure Network Server



Figure 2. Cisco SNS-3615, SNS-3655, and SNS-3695 Secure Network Server



Product specifications

Table 1 lists specifications of the Cisco Secure Network Server.

Table 1. Product specifications

Product Name	Secure Network Server 3515	Secure Network Server 3595	Secure Network Server 3615	Secure Network Server 3655	Secure Network Server 3695
Processor	1 – Intel Xeon 2.40 GHz E5-2620	1 – Intel Xeon 2.60 GHz E5-2640	1 – Intel Xeon 2.10 GHz 4110	1 – Intel Xeon 2.10 GHz 4116	1 – Intel Xeon 2.10 GHz 4116
Cores per processor	6	8	8	12	12
Memory	16 GB (2 x 8 GB)	64 GB (4 x 16 GB)	32 GB (2 x 16 GB)	96 GB (6 x 16 GB)	256 GB (8 x 32 GB)
Hard Disk	1 - 2.5-in. 600-GB 6Gb SAS 10K RPM	4 - 2.5-in. 600-GB 6Gb SAS 10K RPM	1 - 2.5-in. 600-GB 6Gb SAS 10K RPM	4 - 2.5-in. 600-GB 6Gb SAS 10K RPM	8 - 2.5-in. 600-GB 6Gb SAS 10K RPM
Hardware RAID	No	Level 10 Cisco 12G SAS Modular RAID Controller	No	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network Interfaces	6 x 1GBase-T	6 x 1GBase-T	2 X 10Gbase-T 4 x 1GBase-T	2 X 10Gbase-T 4 x 1GBase-T	2 X 10Gbase-T 4 x 1GBase-T
Power Supplies	1 x 770W	2 x 770W	1 x 770W	2 x 770W	2 x 770W

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 first offered in Cisco NAC and Cisco Secure ACS. Looking beyond user name 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 and VPN 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 2.6 and Greater)

	Secure Network Server 3515	Secure Network Server 3595	Secure Network Server 3615	Secure Network Server 3655	Secure Network Server 3695
Endpoints supported in a standalone configuration	7,500	20,000	10,000	25,000	50,000
Endpoints supported per Policy Services Node	7,500	40,000	10,000	50,000	100,000

Ordering information

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

Table 3. Product ordering information

Server Part Numbers	Server Description
SNS-3515-K9	Secure Network Server for ISE applications (small)
SNS-3595-K9	Secure Network Server for ISE applications (medium)
SNS-3615-K9	Secure Network Server for ISE applications (small)
SNS-3655-K9	Secure Network Server for ISE applications (medium)
SNS-3695-K9	Secure Network Server for ISE applications (large)

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
3515/3595/3615/3655/3695	UCS-HD600G10K12N	600-GB 12-Gb SAS 10K RPM SFF hard disk; hot pluggable; drive sled mounted
3515/3595/3615/3655/3695	UCSC-PSU1-770W=	770W power supply
3515/3595/3615/3655/3695	N20-BKVM=	KVM cable
3515/3595/3615/3655/3695	UCSC-RAILB-M4=	Rail kit

Cisco UCS C220 Server

The Cisco UCS C220 Rack Server is designed for performance and density over a wide range of business workloads, from web serving to distributed databases.

The Cisco UCS C220 Rack Server is a high-density general-purpose server optimized to deliver high performance for a large range of workloads. Cisco UCS C-Series servers extend unified computing innovations to an industry-standard form factor to help reduce Total Cost of Ownership (TCO) and increase business agility. Designed to operate both in standalone environments and as part of Cisco UCS, the Cisco UCS C-Series Rack Servers employ Cisco technology to help customers handle the most challenging workloads.

Connectors and LEDs

Table 5 lists Connectors and LEDs on the Cisco SNS-3515 and SNS-3595 Secure Network Servers. Table 6 lists Connectors and LEDs on the Cisco SNS-3615, SNS-3655, and SNS-3695 Secure Network Servers.

Table 5. SNS-3515 and SNS-3595 Connectors and LEDs

Connector/LEDs	Description
Front-panel connector	One KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)
Front-panel locator LED	Indicator to help direct administrators to specific servers in large data center environments
Additional rear connectors	Additional interfaces, including a VGA video port, 2 USB ports, an RJ-45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports

Table 6. SNS-3615, SNS-3655, and SNS-3695 Connectors and LEDs

Connector/LEDs	Description
Front-panel connector	One KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)
Front-panel locator LEDs	Power status, fan status, system status, power supply status, unit identification, and network link activity
Additional rear connectors	Additional interfaces, including a VGA video port, 2 USB ports, an RJ-45 serial port, 1 Gigabit Ethernet management port, and dual 10 Gigabit Ethernet ports

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 7 lists environmental information for the Cisco Secure Network Servers.

Table 7. Regulatory standards compliance: Safety and EMC

Item	Specification
Temperature: Operating	41 to 95°F (5 to 35°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Temperature: Nonoperating	-40 to 149°F (-40 to 65°C)
Humidity: Operating	10 to 90% noncondensing
Humidity: Nonoperating	5 to 93% noncondensing
Altitude: Operating	0 to 10,000 ft (0 to 3000m); maximum ambient temperature decreases by 1°C per 1000 ft
Altitude: Nonoperating	0 to 40,000 ft (12,000m)
Heat Dissipation	Approximately 2500 BTU/h

Regulatory standards

Table 8 lists regulatory standards compliance information for the Cisco Secure Network Servers.

Table 8. Regulatory standards compliance: Safety and EMC

Specification	Description
Safety	<ul style="list-style-type: none">• UL 60950-1 No. 21CFR1040 Second Edition• CAN/CSA-C22.2 No. 60950-1 Second Edition• IEC 60950-1 Second Edition• EN 60950-1 Second Edition• IEC 60950-1 Second Edition• AS/NZS 60950-1• GB4943 2001
EMC: Emissions	<ul style="list-style-type: none">• 47CFR Part 15 (CFR 47) Class A• AS/NZS CISPR22 Class A• CISPR2 2 Class A• EN55022 Class A• ICES003 Class A• VCCI Class A• EN61000-3-2• EN61000-3-3• KN22 Class A• CNS13438 Class A

Specification	Description
EMC: Immunity	<ul style="list-style-type: none"> • EN55024 • CISPR24 • EN300386 • KN24 (SNS-3515 and SNS-3595) • KN35 (SNS-3615, SNS-3655, and SNS-3695)

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.](#)

For more information

For more information, please visit the following resources:

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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

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. (1110R)