Data sheet
Cisco public

Cisco Secure Network Server 3800 Series

Designed for Cisco Identity Services Engine (ISE)

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

© 2025 Cisco and/or its affiliates. All rights reserved.

Product overview

Cisco® Identity Services Engine (ISE) plays a critical role in implementing **Universal Zero Trust Network Access (UZTNA)**, providing a comprehensive framework for identity and access management. Within the UZTNA model, Cisco ISE enforces strict access controls and continuous monitoring based on user identity, device health, and other contextual data, such as device profile, location, group membership and more. It dynamically verifies and authenticates users and devices, embodying the zero-trust principle of "never trust, always verify." By seamlessly integrating with diverse network components, Cisco ISE helps organizations maintain a secure, adaptive environment, preventing unauthorized access and reinforcing security at every layer.

The Next Generation: Cisco Secure Network Server 3800 Series

The Cisco Secure Network Server (SNS) 3800 series, powered by the Cisco UCS® C225 M8 Rack Server, sets a new standard for performance and reliability in network access control. Designed specifically for Cisco Identity Services Engine (ISE), the SNS-3800 series redefines efficiency and speed through its modern architecture.

Performance Breakthroughs with NVMe and SSD

One of the most significant advancements in the SNS-3800 series is the complete transition from traditional Hard Disk Drives (HDDs) to Non-Volatile Memory Express (NVMe) and Solid-State Drive (SSD) (Self Encrypted Drives [SED] or SED-FIPS) storage. This shift delivers:

- **Faster reboots:** Reduced boot times that get ISE nodes up and running more quickly.
- **Accelerated upgrades:** Streamlined update processes that minimize downtime and improve efficiency.
- **High-speed report generation:** Enhanced disk I/O performance enables faster analytics, troubleshooting, and visibility into network activity.
- **Improved resilience:** With no moving parts, SSDs and NVMe drives are inherently more reliable and durable than mechanical HDDs.

The SNS-3800 series supports three models to align with varying deployment sizes:

- **SNS-3815:** Ideal for small deployments, optimized for performance and cost-efficiency.
- **SNS-3855:** Configured for medium to large environments with robust redundancy in power supplies and storage. The SNS-3855 can be order in two configurations:
  - Policy Services Node (PSN) only, with a single disk
  - PAN and Monitoring and Troubleshooting Node (MnT), fully equip with four disks for medium deployments.
- **SNS-3895:** The flagship model, designed for the most demanding ISE roles such as dedicated PAN, dedicated MnT, or combined PAN/MnT personas. Equipped with enhanced memory, it handles high transaction volumes and complex data operations effortlessly.

The SNS-3800 series is fully supported by ISE 3.3 patch 7 or later, ISE 3.4 patch 3 or later, and ISE 3.5 or later, ensuring forward compatibility with the latest ISE capabilities.

© 2025 Cisco and/or its affiliates. All rights reserved.

Figure 1 shows the Cisco Secure Network Server.

Figure 1.
Cisco Secure Network Server

Product specifications

Table 1 lists specifications of the Cisco Secure Network Server.

Table 1. Secure Network Server 3800- Specifications

Product name	Cisco SNS-3815	Cisco SNS-3855	Cisco SNS-3895
Processor	AMD 9115 2.6GHz	AMD 9224 2.5GHz	AMD 9224 2.5GHz
Cores per processor	16 cores and 32 threads	24 cores and 48 threads	24 cores and 48 threads
Memory	64GB 2 X 32GB	128GB 4 X 32GB	256GB 8 X 32GB
Storage	1 960GB NVMe **Or** 960GB SSD Self Encrypted Drive **Or** 1.6TB SSD Self Encrypted Drive FIPS Certified	1 for PSN only or 4 for PAN/MnT 960GB NVMe **Or** 1 for PSN only or 4 for PAN/MnT 960GB SSD Self Encrypted Drive **Or** 1 For PSN Only or 4 for PAN/MnT 1.6TB SSD Self Encrypted Drive FIPS Certified	8 960GB NVMe **Or** 960GB SSD Self Encrypted Drive **Or** 1.6TB SSD Self Encrypted Drive FIPS Certified
Hardware Redundant Array of Independent Disks (RAID)	Level 0 Cisco 24G Tri-Mode M1 RAID Controller for SED and SED FIPS only	Level 0 for PSN only with NVMe Level 10 for PAN/MnT or when using SED or SEF-FIPS Cisco 24G Tri-Mode M1 RAID Controller	Level 10 Cisco 24G Tri-Mode M1 RAID Controller

© 2025 Cisco and/or its affiliates. All rights reserved.

Product name	Cisco SNS-3815	Cisco SNS-3855	Cisco SNS-3895
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 Or 2 X 1200W	2 X 1200W	2 X 1200W
Trusted Platform Module (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: The Policy Anchor for UZTNA

Cisco Identity Services Engine (ISE) is the policy engine at the heart of Cisco's Universal Zero Trust Network Access (UZTNA) architecture. As the industry's most comprehensive Network Access Control (NAC) platform, Cisco ISE enables organizations to implement identity-driven access controls that extend across the entire enterprise infrastructure—wired, wireless, VPN, and private 5G.

ISE plays a foundational role in delivering secure access in a Zero Trust environment by continuously verifying user and device identity, assessing contextual attributes, and enforcing adaptive access policies based on trust levels—not just credentials. This aligns with the core ZTNA principle: never trust, always verify.

With ISE, organizations can:

- **Implement identity-based segmentation** to contain lateral movement.
- **Automate device onboarding and posture validation** to support dynamic, context-aware policy enforcement.
- **Enable secure access anywhere**—supporting hybrid work, BYOD, and guest access with centralized policy control.
- **Leverage advanced profiling** to dynamically identify and classify devices on the network, enabling policy enforcement even when devices lack full identity or posture attributes.
- **Integrate seamlessly with Cisco's broader security ecosystem**, including Secure Access, Secure Access Service Edge (SASE), and third-party integrations.

ISE supports UZTNA across the full lifecycle: from initial access decisions, to posture checks, to automatic remediation and revocation of access when trust is no longer justified. Administrators can dynamically restrict access to non-compliant or high-risk endpoints, protecting critical assets from compromise.

Whether deployed as part of a self-managed infrastructure or integrated into a broader zero trust strategy, Cisco ISE provides the visibility, control, and automation needed to reduce risk, simplify operations, and accelerate secure access across distributed environments.

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Table 2. Identity Services Engine deployment scalability (ISE 3.4 P3 and later)

	Cisco Secure Network Server 3815	Cisco Secure Network Server 3855	Cisco Secure Network Server 3895
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-3895 is equipped with better memory, and 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 Cisco SNS server can be ordered with NVMe, Self Encrypted Drive (SED) or Federal Information Processing Standard (FIPS)-certified Self Encrypted Drive as a configuration option.

Table 3. Product ordering information

Server part numbers	Server description
SNS-3815-K9	Secure Network Server for ISE applications (small)
SNS-3855-K9	Secure Network Server for ISE applications (medium). For PSN only, please change number of disks from 4 to 1
SNS-3895-K9	Secure Network Server for ISE applications (large)

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

Table 4. Spare components for the Cisco Secure Network Server

Component part number	Component description
UCS-NVMEG4-M960-D=	960GB 2.5in U.3 15mm P7450 Hg Perf Med End NVMe
UCS-SD960GM2NK9-D=	960GB 2.5in Enter Value 6G SATA Micron G2 SSD (SED)
UCS-SD16TBKANK9-D=	1.6TB 2.5in Enter Perf 12G SAS Kioxia G2 SSD (3X SED-FIPS)
UCSC-PSU1-1200W-D=	1200W power supply
UCSC-RAIL-D=	Rail kit
UCSC-FAN-C22XM7=	Fan

© 2025 Cisco and/or its affiliates. All rights reserved.

Network connective

Copper PID:

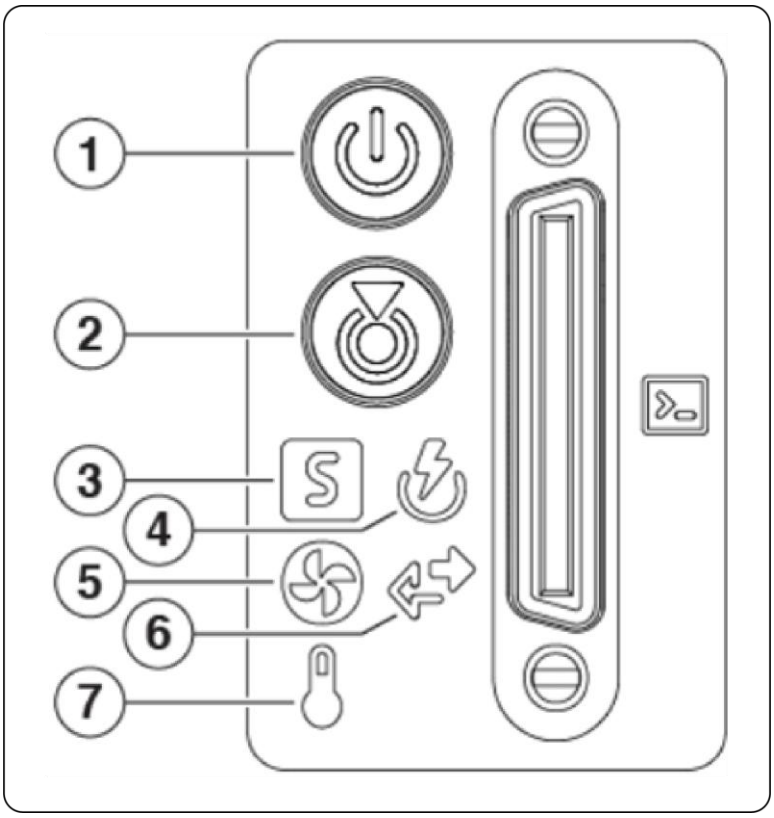
GLC-TE - 1000BASE-T SFP transceiver module for Category 5 copper wire.

Fiber PIDs: UCS M6 10G NIC Interoperability with Cisco Cables/Optics.

Supported Cisco ISE versions

The Cisco Secure Network Server 38xx supports Cisco ISE 3.3 P7 and later, 3.4 P3 and later, and 3.5 versions only. Upon receiving the SNS-38xx, it is recommended to install the latest patch of the Cisco ISE suggested release.

Connectors and LEDs



© 2025 Cisco and/or its affiliates. All rights reserved.

Table 5 lists Connectors and LEDs on the Cisco SNS-3815, SNS-3855, and SNS-3895.

Table 5. Cisco SNS-3815, SNS-3855, and SNS-3895 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 Integrated Management Controller (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.
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 Dual In-line Memory Modules (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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Form factor

Physical dimensions (H x W x D) 1RU: 1.7 x 16.9 x 30 in. (4.3 x 42.9 x 76.2 cm).

Power Specifications

Table 6 lists power specification for the Cisco Secure Network Servers 3800.

Table 6. Secure Network Server 3800- Power Specifications

Parameter	Specification			
Input Connector	IEC320 C14			
Input Voltage Range (Vrms)	100 to 240			
Maximum Allowable Input Voltage Range (Vrms)	90 to 264			
Frequency Range (Hz)	50 to 60			
Maximum Allowable Frequency Range (Hz)	47 to 63			
Maximum Rated Output (W)[1]	1100		1200	
Maximum Rated Standby Output (W)	48			
Nominal Input Voltage (Vrms)	100	120	208	230
Nominal Input Current (Arms)	12.97	10.62	6.47	5.84
Maximum Input at Nominal Input Voltage (W)	1300	1264	1343	1340
Maximum Input at Nominal Input Voltage (VA)	1300	1266	1345	1342
Minimum Rated Efficiency (%)[2]	90	90	91	91
Minimum Rated Power Factor[2]	0.97	0.97	0.97	0.97
Maximum Inrush Current (A peak)	20			
Maximum Inrush Current (ms)	0.2			
Minimum Ride-Through Time (ms)[3]	12			

Notes:

[1]Maximum rated output is limited to 1100W when operating at low-line input voltage (100-127V).

[2]This is the minimum rating required to achieve 80 PLUS Titanium certification, see test reports published at http://www.80plus.org/ for certified values.

[3]Time output voltage remains within regulation limits at 100% load, during input voltage dropout.

© 2025 Cisco and/or its affiliates. All rights reserved.

Environmental

Table 7 lists environmental information for the Cisco Secure Network Servers.

Table 7. Environmental Specifications

Description	Specification
Temperature, operating	41°F to 95°F (5°C to 35°C) (supports ASHRAE Class A4 and/or Class A3 and/or Class A2). ASHRAE Class A3 will be generic test profile unless otherwise specified by product engineering. System shall continue to operate with a single fan failure (one failed impeller in dual impeller housings) across the ASHRAE recommended operating range of 64.4°F to 80.6°F (18 °C to 27 °C). While undesired, increased power consumption and/or acoustic noise is permitted during a fan fail event.
Nonoperating Temperature (when the server is stored or transported)	Dry bulb temperature of -40°F to 149°F (-40°C to 65°C) ()
Humidity (RH), operating	8% to 90% relative humidity, non-condensing, with maximum wet bulb 82.4°F (28°C) within operational temperature range of 41°F to 122°F (5°C to 50°C)
Humidity (RH), nonoperating (when the server is stored or transported)	5% to 93% relative humidity, non-condensing, with a maximum wet bulb temperature of 82.4°F (28°C) across the 68°F to 104°F (20°C to 40°C) dry bulb range.
Altitude, operating	0 to 10,006 feet (0 to 3050 meters)
Altitude, nonoperating (when the server is stored or transported)	0 to 39,370 feet (0 to 12,000 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

© 2025 Cisco and/or its affiliates. All rights reserved.

Compliance requirements

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

Table 8. Compliance Specifications

Parameter	Description
Regulatory compliance	Products should comply with CE Markings per directives 2014/30/EU and 2014/35/EU
Safety	UL 60950-1/62368-1 CAN/CSA-C22.2 No. 60950-1/62368-1 IEC/EN 60950-1/62368-1 AS/NZS 62368.1 GB 4943.1-2022 CNS 15598-1:2020
EMC - Emissions	47CFR Part 15 (CFR 47) Class A AS/NZS CISPR32 Class A CISPR32 Class A EN55032 Class A ICES003 Class A VCCI-CISPR32 Class A EN61000-3-2 EN61000-3-3 KS C 9832 Class A EN 300386 Class A
EMC - Immunity	EN55035 EN55024 CISPR24/35 EN300386 KS C 9835 IEC/EN61000-6-1

© 2025 Cisco and/or its affiliates. All rights reserved.

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/UCS.

Document history

New or revised topic	Described in	Date
Initial Draft		May 20, 2025

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)

Printed in USA C78-5189670-00 06/25

© 2025 Cisco and/or its affiliates. All rights reserved.