End–of–Sale and End–of–Life Announcement for the Cisco Secure Network Server 3715, 3755 and 3795

Contents

Overview

EOL15685 - Amended

Cisco announces the end-of-sale and end-of-life dates for the Cisco Secure Network Server 3715, 3755 and 3795. The last day to order the affected product(s) is December 30, 2025. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as shown in Table 1 of the EoL bulletin. Table 1 describes the end-of-life milestones, definitions, and dates for the affected product(s). Table 2 lists the product part numbers affected by this announcement. For customers with active and paid service and support contracts, support will be available under the terms and conditions of customers' service contract.

End-of-life milestones

Table 1. End-of-life milestones and dates for the Cisco Secure Network Server 3715, 3755 and 3795

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	July 1, 2025
End-of-Sale Date: HW,App SW	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	December 30, 2025
Last Ship Date: HW,App SW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	March 30, 2026
End of SW Maintenance Releases Date: HW,App SW	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.	December 30, 2026
End of Vulnerability/Security Support: HW	The last date that Cisco Engineering may release a planned maintenance release or scheduled software remedy for a security vulnerability issue.	December 31, 2030
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.	December 30, 2026
End of New Service Attachment Date: HW,App SW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	December 30, 2026
End of Service Contract Renewal Date: HW,App SW	The last date to extend or renew a service contract for the product.	March 27, 2030
Last Date of Support: HW,App SW	The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.	December 31, 2030

HW = Hardware   OS SW = Operating System Software   App. SW = Application Software

Product part numbers

Table 2. Product part numbers affected by this announcement

End-of-Sale Product Part Number	Product Description	Replacement Product Part Number	Replacement Product Description	Additional Information
SW-37X5-ISE-K9	Cisco ISE Software Load on SNS-36x5-K9 appliance	There is currently no replacement product available for this product.	-	-
SNS-3715-K9	Small Secure Network Server for ISE Applications	SNS-3815-K9	Small Secure Network Server for ISE Applications	-
SNS-3715-K9-CHAS	Small Secure Network Server Chassis for ISE Applications	SNS-3815-K9-CHAS	Small Secure Network Server Chassis for ISE Applications	-
SNS-3755-K9	Medium Secure Network Server for ISE Applications	SNS-3855-K9	Medium Secure Network Server for ISE Applications	-
SNS-3755-K9-CHAS	Medium Secure Network Server Chassis for ISE Applications	SNS-3855-K9-CHAS	Medium Secure Network Server Chassis for ISE Applications	-
SNS-3795-K9	Large Secure Network Server for ISE Applications	SNS-3895-K9	Large Secure Network Server for ISE Applications	-
SNS-3795-K9-CHAS	Large Secure Network Server Chassis for ISE Applications	SNS-3895-K9-CHAS	Large Secure Network Server Chassis for ISE Applications	-
SNS-CPU-I4310	Intel 4310 2.1GHz/120W 12C/18MB DDR4 2667MHz	There is currently no replacement product available for this product.	-	-
SNS-CPU-I4316	Intel 4316 2.3GHz/150W 20C/30MB DDR4 2667MHz	There is currently no replacement product available for this product.	-	-
SNS-HD600G10K12NM6	600GB 12G SAS 10K RPM SFF HDD	There is currently no replacement product available for this product.	-	-
SNS-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	There is currently no replacement product available for this product.	-	-
SNS-MR-X32G2RW	32GB RDIMM DRx4 3200 (8Gb)	There is currently no replacement product available for this product.	-	-

End-of-Sale Product Part Number	Product Description	Replacement Product Part Number	Replacement Product Description	Additional Information
SNS-PCIE-IQ10GF	Intel X710 quad-port 10G SFP+ NIC	There is currently no replacement product available for this product.	-	-
SNS-PSU-M5BLK	Power Supply Blanking Panel for SNS-3700 servers	There is currently no replacement product available for this product.	-	-
SNS-PSU1-1200W	1200W Titanium power supply for C-Series Servers	There is currently no replacement product available for this product.	-	-
SNS-PSU1-1200W-2	2nd 1200W Titanium power supply for C-Series Servers	There is currently no replacement product available for this product.	-	-
SNS-RAID-220M6	Cisco 12G SAS RAID Controller w/4GB FBWC (16 Drv) w/1U Brkt	There is currently no replacement product available for this product.	-	-
SNS-SD800GK3XEP	800GB 2.5in Enter Perf 12G SAS Kioxia G1 SSD (3X)	There is currently no replacement product available for this product.	-	-
SNS-SD800GS3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD(3X endurance)	There is currently no replacement product available for this product.	-	-
SNS-SD960GM2NK9	960GB Enterprise value SATA SSD (1X, SED)	There is currently no replacement product available for this product.	-	-
SNS-TPM-002C	TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, for M6 servers	There is currently no replacement product available for this product.	-	-

Product migration options

Customers may be able to use the Cisco Technology Migration Program (TMP) where applicable to trade-in eligible products and receive credit toward the purchase of new Cisco equipment. For more information about Cisco TMP, customers should work with their Cisco Partner or Cisco account team. Cisco Partners can find additional TMP information on Partner Central at
https://www.cisco.com/web/partners/incentives_and_promotions/tmp.html.

Customers may be able to continue to purchase the Cisco Secure Network Server 3715, 3755 and 3795 through the Cisco Refresh (certified remanufactured) program. Remanufactured units may be available in limited supply for sale in certain countries on a first-come, first-served basis until the Last Date of Support has been reached. For information about the Cisco Refresh program, go to:
https://www.cisco.com/c/en/us/products/remanufactured.html.

The Cisco Takeback and Recycle program helps businesses properly dispose of surplus products that have reached their end of useful life. The program is open to all business users of Cisco equipment and its associated brands and subsidiaries. For more information, go to:
https://www.cisco.com/c/en/us/about/takeback-and-reuse/product-recycling.html.

For more information

For more information about the Cisco End-of-Life Policy, go to: https://www.cisco.com/c/en/us/products/eos-eol-policy.html.

For more information about the Cisco Product Warranties, go to:
https://www.cisco.com/c/en/us/products/warranty-listing.html.

To subscribe to receive end-of-life/end-of-sale information, go to: https://cway.cisco.com/mynotifications.

Any authorized translation issued by Cisco Systems or affiliates of this end-of-life Product Bulletin is intended to help customers understand the content described in the English version. This translation is the result of a commercially reasonable effort; however, if there are discrepancies between the English version and the translated document, please refer to the English version, which is considered authoritative.