

CISCO Release Notes for the StarOS Software



CISCO Release Notes for the StarOS Software User Guide

[Home](#) » [Cisco](#) » CISCO Release Notes for the StarOS Software User Guide 

Contents

- [1 CISCO Release Notes for the StarOS Software](#)
- [2 Introduction](#)
- [3 Features and Enhancements](#)
- [4 Open Bugs for this Release](#)
- [5 Resolved Bugs for this Release](#)
- [6 Operator Notes](#)
- [7 Obtaining Documentation and Submitting a Service Request](#)
- [8 Documents / Resources](#)
 - [8.1 References](#)
- [9 Related Posts](#)



CISCO Release Notes for the StarOS Software



- ## Introduction

Release Lifecycle Milestones

| Release Lifecycle Milestone | Milestone | Date |
|---|-----------|---------------|
| First Customer Ship | FCS | 30-April-2024 |
| End of Life | EoL | 29-Oct-2024 |
| End of Software Maintenance | EoSM | 29-Oct-2025 |
| End of Vulnerability and Security Support | EoVSS | 29-Oct-2025 |
| Last Date of Support | LDoS | 31-Oct-2026 |

Release Package Version Information

| | | |
|-------------------|------------|-----------------|
| Software Packages | Version | Build Number |
| StarOS Package | 2024.02.l0 | 21.28.m23.93622 |

What's New in this Release

This version of Release Notes includes a new section titled What's New in this Release comprising all new features, enhancements, and behavior changes applicable for the release.

There are no new features or enhancements for this Release.

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release.

| | |
|------------|---|
| Feature ID | Feature Name |
| FEAT-22933 | Verizon 5G CALEA N+K GR design changes – support up to 16 servers |
| FEAT-24393 | M2M ACL configuration into the SRP Checkpointing |

Related Documentation

For a complete list of documentation available for this release, go to:
<http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html>

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

There are no firmware upgrades required for this release.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.
Image checksum information is available through [Cisco.com](#) Software Download Details. To find the checksum, hover the mouse pointer over the software image you have downloaded.

ASR 5500

Release **2024.02.10**

My Notifications

Related Links

- No related links

| File Information | Release Date |
|--|--------------|
| ASR5500 Binary Software Image asr5500- 2024.02.10 zip Advisories | 31-Jan-2024 |
| ASR5500 Trusted Binary Software Image asr5500_T-:2024.02.10 zip Advisories | 31-Jan-2024 |
| StarOS SNMP MIBs, RADIUS dictionaries, ORBEM clients companion-2024.02.10 zip Advisories | 31-Jan-2024 |

At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the “...” at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop see Table 1

Table 1 – Checksum Calculations per Operating System

| Operating System | SHA512 checksum calculation command examples |
|--|---|
| Microsoft Windows | Open a command line window and type the following command > certutil.exe -hashfile <filename>.<extension> SHA512 |
| Apple MAC | Open a terminal window and type the following command \$ shasum -a 512 <filename>.<extension> |
| Linux | Open a terminal window and type the following command \$ sha512sum <filename>.<extension> Or \$ shasum -a 512 <filename>.<extension> |
| NOTES: <filename> is the name of the file. <extension> is the file extension (e.g. .zip or .tgz). | |

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

- In 2024.01 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates.
- USP ISO images are signed with a GPG key.
- For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs for this Release

The following table lists the open bugs in this specific software release.

NOTE: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Table 2 – Open Bugs in this Release

| Bug ID | Headline | Product Found |
|----------------------------|--|---------------|
| CSCwj33154 | sessmgr reload at uplane_sfw_create_nat_realm_info() | cups-up |
| CSCwi52632 | egtpu_process_update_req_evt()egtpu_handle_user_sap_event()sessmgr_uplane_gtpu_tx_update() | cups-up |
| CSCwj24130 | Inconsistency in counters in gtpu bulkstats for UP | cups-up |
| CSCwj36352 | Assertion failure at sess/mme/mme-app/app/mme_tau_proc.c:1701 | mme |
| CSCwj72131 | Improper output for PDN GW Name in 'show mme-service db record ' is a display issue. | mme |
| CSCwj66981 | Sessmgr crash-egtpc_send_ind_evt() | pdn-gw |
| CSCwj52492 | While triggerring the interim CDR, there is no aaa_sess_handle and sessmgr restart | pdn-gw |
| CSCwj25382 | UDP flows are not getting blocked when 0 quota is received from OCS | pdn-gw |
| CSCwj78838 | Assertion failure at "sit_api_rct_task_death_req" on 21.28.m23.93362 | pdn-gw |
| CSCwj70487 | Assertion failure at sess/snx/drivers/sgw/sgw_drv.c:374 | sgw |
| CSCwj68378 | ASR5500 SPGW Assertion failure at sgwdrv_send_tx_setup_to_egtpu | sgw |

| Bug ID | Headline | Product Found |
|----------------------------|---|---------------|
| CSCwj68218 | Assert observed at sgwdrv_collect_pdn_info | sgw |
| CSCwj17471 | Planned srp switchover is succeeded though bgp monitor in stby upf is down | staros |
| CSCwi59036 | Port redundancy Failed in 4-port deployment VPC SI | staros |
| CSCwd99519 | Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce | upf |

Resolved Bugs for this Release

The following table lists the resolved bugs in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Table 3 – Resolved Bugs in this Release

| Bug ID | Headline | Product Found |
|----------------------------|---|---------------|
| CSCwj51924 | VPCDI // 21.28.m15 (91862) //h Assertion failure at sess/snx/drivers/saegw/saegw_recovery.c:35 | cups-cp |
| CSCwj00472 | sessmgr 12341 error when HO between SGWs | cups-cp |
| CSCwj50864 | Assertion failure at sess/smgr/sessmgr_pgw.c:9924 | cups-cp |
| CSCwi71670 | X3 Lawful Intercept is marked as wrong EBI when using ipv6 session over dedicated bearer | cups-cp |
| CSCwi94768 | Documentation to update the max entries supported in Gx local-policy- service | cups-cp |
| CSCwi28946 | [BP-CUPS] Lot of error logs – [SXAB] Failed to remove Traffic Endpoint with Traffic Endpoint ID | cups-cp |
| CSCwj38556 | In roaming scenraio – MCC-only feature rejects the bearer after 4G3G mobility d | cups-cp |
| CSCwi53552 | sessmgr Fatal Signal 11: 11 uplane_free_nat_binding_info()uplane_free_app_data_flow() | cups-up |
| CSCwc99110 | Assertion failure at sess/smgr/sessmgr_gtpu.c sessmgr_egtpu_signalling_routine() | cups-up |
| CSCwi35960 | huge amount of “ICMP packet parse failure” logs in 21.28.m15 with NAT | cups-up |
| CSCwi69056 | VPP buffer leak caused a VPP restart | cups-up |
| CSCwj85083 | CUPS UP : npumgr crashes after upgrade to 21.28.m22 | cups-up |

| Bug ID | Headline | Product Found |
|----------------------------|--|---------------|
| CSCwj44782 | MME wrongly selecting s2b PGW record (x-3gpp-pgw:x-s2b-gtp+nc- smf) for 5G capable UE's | mme |
| CSCwi85182 | Sessmgr restart due to Assertion failure at function sn_gt_release_mm_teid() | mme |
| CSCwi55030 | Observed multiple sessmgr went to warn/over state in 21.28.m18.92419 during regression | mme |
| CSCwd25108 | DNS Failure – TCP READ, Kernel Closed – req_read_len = 0 | mme |
| CSCwi48857 | Sessmgr Assertion failure at egtpc_send_req_msg() | mme |
| CSCwc83863 | Assertion failure at sess/mme/mme-app/app/mme_app_util.c:18558 | mme |
| CSCwj29750 | Sessmgr restart after SW upgrade to 21.28.m19, mme_auth_awt_hss_h ss_resp() | mme |
| CSCwj30320 | vplmn-address option is not showing under call-control-profile | mme |
| CSCwj33658 | sessmgr crash due to Fatal Signal 11: 11 PC: [06bbc47f/X] smgr_process_iri_hi2() | pdn-gw |
| CSCwj24901 | Empty APN list in “show s8hr config” after node reload | pdn-gw |
| CSCwi54796 | VPC-SI – bfd sometimes sending ipv6 packets with udp checksum 0x0 – which is invalid | pdn-gw |
| CSCwj24886 | ipsecmgr restart seen after the rekeying process | pdn-gw |
| CSCwj15020 | ASR5500 – [SPGW] – sessctrl failure | pdn-gw |
| CSCwj72598 | user-plane traffic stops when sgw-u (Sxa) and pgw-u (Sxb) functions are hosted on the same UP | pdn-gw |
| CSCwi67492 | For gtpu-schema , few bulkstat counters not incremented | pdn-gw |
| CSCwj24899 | Few sessmgrs having TCP connect issues on Checkpointmgr | rcm |
| CSCwi68538 | RCM-Checkpointmgr crash due to fatal error concurrent map read and map write | rcm |
| CSCwi79878 | IP Pool flush enhancements for planned RCM UPF SWO | rcm |
| CSCwj36377 | Help ? for rcm-config-ep write-timeout shows inconsistency not similar with other | rcm |
| CSCwi69314 | Planned swo gives incorrect message in ops-centre | rcm |
| CSCwi87259 | StandbySessmgrDisconnected trap is not generated when upf reload due to planned switchover fails | rcm |
| CSCwi65948 | format of dateandtime used by RCM does not comply to snmpv2 | rcm |
| CSCwi73027 | Stale data in RCM post switchover | rcm |

| Bug ID | Headline | Product Found |
|----------------------------|---|---------------|
| CSCwi74961 | TCP hardening – Timeout observed during socket write during switchover | rcm |
| CSCwi23288 | session manager restart at sn_dp_utan_process_purge_req_evt function | sgsn |
| CSCwi70115 | SNS-Add messages were not sent after adding new NSVL instance | sgsn |
| CSCwj26308 | Assertion failure at sess/sgsn/sgsn-app/gtp_c/gtapp_tun_fsm.c:6936 | sgsn |
| CSCwi63250 | Despite “monitor system card-fail” config, switchover does not occur | staros |
| CSCwi59951 | TCP length issue in DNS query causing time out | staros |
| CSCwi67402 | Sessmgr restart at saegwdrv_ue_fsm_st_active_evt_snx_abortcall(), | staros |
| CSCwi65052 | [BP-CUPS] [connectedapps 203750 error CONNECTEDAPPS ERROR: Unable to open the btmp file /var/log/btmp | staros |

Operator Notes

StarOS Version Numbering System

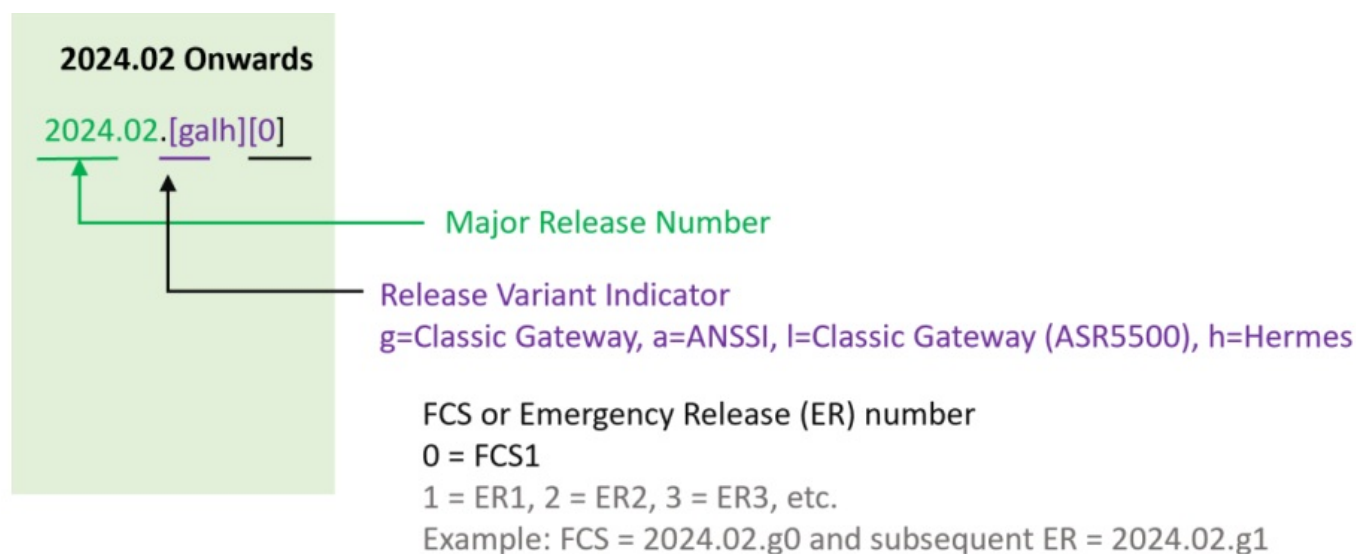
The output of the show version command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

NOTE: Starting 2024.01.0 release (January 2024), Cisco is transitioning to a new release versioning scheme. The release version is based on the current year and product. Refer to Figure 1 for more details.

During the transition phase, some file names will reflect the new versioning whereas others will refer to the 21.28.x-based naming convention. With the next release, StarOS-related packages will be completely migrated to the new versioning scheme.

Version Numbering for FCS, Emergency, and Maintenance Releases

Figure 1 – Version Numbering



Release Package Descriptions

Table 4 provides descriptions for the packages that are available with this release. For more information about the release packages up to 21.28.x releases, refer to the corresponding releases of the release note.

Table 4 – Release Package Information

| Software Package | Description |
|---------------------------------|---|
| ASR 5500 | |
| asr5500-<release>.zip | Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. |
| asr5500_T-<release>.zip | Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. |
| StarOS Companion Package | |
| companion-<release>.zip | Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants. |
| VPC-DI | |
| qvpc-di-<release>.bin.zip | Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. |
| qvpc-di_T-<release>.bin.zip | Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. |
| qvpc-di-<release>.iso.zip | Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. |

| | |
|--|---|
| qvpc-di_T-<release>.iso.zip | Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. |
| qvpc-di-template-vmware-<release>.zip | Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. |
| qvpc-di-template-vmware_T-<release>.zip | Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. |
| qvpc-di-template-libvirt-kvm-<release>.zip | Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. |
| qvpc-di-template-libvirt-kvm_T-<release>.zip | Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. |
| qvpc-di-<release>.qcow2.zip | Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. |
| qvpc-di_T-<release>.qcow2.zip | Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. |

| VPC-SI | |
|--|---|
| qvpc-si-<release>.bin.zip | Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. |
| qvpc-si_T-<release>.bin.zip | Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. |
| qvpc-si-<release>.iso.zip | Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. |
| qvpc-si_T-<release>.iso.zip | Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. |
| qvpc-si-template-vmware-<release>.zip | Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. |
| qvpc-si-template-vmware_T-<release>.zip | Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. |
| qvpc-si-template-libvirt-kvm-<release>.zip | Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. |
| qvpc-si-template-libvirt-kvm_T-<release>.zip | Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. |
| qvpc-si-<release>.qcow2.zip | Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. |
| qvpc-si_T-<release>.qcow2.zip | Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. |
| VPC Companion Package | |

| | |
|------------------------------------|--|
| companion-vpc-<release>.zip | Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORB EM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. |
| Ultra Services Platform | |
| usp-<version>.iso | The USP software package containing component RPMs (bundles). Refer to the Table 5 for descriptions of the specific bundles. |
| usp_T-<version>.iso | The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to the Table 5 for descriptions of the specific bundles. |
| usp_rpm_verify_utils-<version>.tar | Contains information and utilities for verifying USP RPM integrity. |

Table 5 – USP ISO Bundles

| USP Bundle Name | Description |
|---|--|
| usp-em-bundle-<version>-1.x86_64.rpm* | The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module. |
| usp-ugp-bundle-<version>-1.x86_64.rpm* | The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle. |
| usp-yang-bundle-<version>-1.x86_64.rpm | The Yang Bundle RPM containing YANG data models including the VNFD and VNFR. |
| usp-uas-bundle-<version>-1.x86_64.rpm | The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages. |
| usp-auto-it-bundle-<version>-1.x86_64.rpm | The bundle containing the AutoIT packages required to deploy the UAS. |
| usp-vnfm-bundle-<version>-1.x86_64.rpm | The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller). |
| ultram-manager-<version>-1.x86_64.rpm* | This package contains the script and relevant files needed to deploy the Ultra M Manager Service. |
| * These bundles are also distributed separately from the ISO. | |

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to <https://www.cisco.com/c/en/us/support/index.html>.

- THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE

SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

- THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

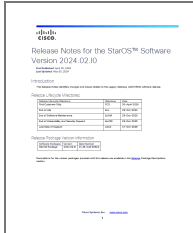
- The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright ©1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

- IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
- All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.
- Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at 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: <http://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. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

Documents / Resources

| | |
|---|---|
|  | <p>CISCO Release Notes for the StarOS Software [pdf] User Guide ASR 5500, Release Notes for the StarOS Software, Notes for the StarOS Software, StarOS Software, Software</p> |
|---|---|

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.