Release Notes for StarOS™ Software, Release 2025.03.gh0

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

Contents

StarOS™ Software, Release 2025.03.gh0

This Release Notes identifies changes and issues that are related to the Legacy Gateway, Control, and User Plane Separation (CUPS) software release.

The key highlights of this release include:

- UEFI-based secure boot for VM-based RCM: Ensures only authenticated software runs at boot by verifying cryptographic signatures, enhancing system security.
- Option to disable SRP monitor-based switchovers for ICSR nodes: Allows operators to maintain session integrity and system stability by preventing SRP monitor-triggered switchovers.
- Timezone enhancements: Streamlines operations by removing the need for manual timezone workarounds and ensuring local time alignment.
- Multiple P-CSCF payload attributes support: Enables configuration of up to 10 IPv4/IPv6 P-CSCF address values, providing greater flexibility and simplifying complex setups.

Qualified products and platforms

Table 1. Products and platforms qualified in this release

Component	Qualified?
Products	
CUPS	Yes
MME	Yes
ePDG	Yes
P-GW	Yes
SAEGW	Yes
SGSN	Yes
Platforms	
ASR 5500	No
VPC-DI	Yes
VPC-SI	Yes

New software features

This section provides a brief description of the new software features introduced in this release.

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

Table 2. New software features for StarOS™ Software, Release 2025.03.gh0

Product impact	Feature	Description
Software Reliability	Disabling SRP monitor-based switchovers for ICSR nodes	This feature lets operators disable Service Redundancy Protocol (SRP) monitor-based switchovers in the ICSR pair nodes preventing interruptions and ensuring session integrity during such events. Command introduced: **srp-monitor-based-switchover** {**enable** | **disable**}
Software Reliability	UEFI-based secure boot support for VM-based RCM	This feature introduces UEFI-based Secure Boot support for VM-based RCM, enhancing system security by ensuring only authenticated and trusted software is executed during the boot process. Secure Boot leverages cryptographic signatures to validate each stage of the bootloader and kernel, preventing unauthorized or tampered software from running. The implementation supports both Cisco and customer code signing, integrates with Cisco's certificate infrastructure, and provides clear guidelines for VM configuration, partitioning, and binary signing to maintain a secure and verifiable boot chain.
Ease of use	Timezone enhancements	To reflect the recent removal of Central Daylight Time (CDT) by the Government of Mexico, the Classic Gateway (GW) has been updated to support the revised Mexico timezone. This enhancement eliminates the need for workarounds, ensures seamless network operations, aligns with local time standards, and improves operational efficiency.
Upgrade	Support for multiple P-CSCF payload attributes	This feature allows the network operator to configure multiple types for P-CSCF attributes in CFG_REQUEST and CFG_REPLY messages as part of the CP payload in the IKE_AUTH Request and Response messages that ePDG sends and receives from the UEs. Using this feature the network operator can configure a range of 10 values or up to 10 different values for IPv4 and IPv6 P-CSCF address attributes type. Command enhanced: **[no] configuration-payload private-attribute-type { imei imei_value | p-cscf-v4 { v4_value | range start_value end_value } | p-cscf-v6 { v6_value | range start_value end_value } }:** This CLI is configured under Crypto Template Configuration mode Default setting: Disabled–Always Enabled

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Table 3. Behavior changes for StarOS™ Software, Release 2025.03.gh0

Description	Behavior changes
Automatic SRP switchover for MAV	**Previous Behavior**: On ASR 5500 systems, when a Control Function (CF) failure occurred and a redundant CF instance was available, the system would attempt to switch over to the standby CF to

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

Description	Behavior changes
issues during CF failover	minimize service disruption. For example, if CF1 failed (such as a reboot), the system would automatically switch to the standby CF2—even if CF2 had a Multi Attach Volume (MAV) issue. In such cases, the chassis (active VNF) could enter an unrecoverable state. **New Behavior**: If a CF failure occurs and the newly active CF card (for example, CF2) has a MAV issue, the system now automatically initiates a Service Redundancy Protocol (SRP) switchover. This SRP switchover process helps ensure system recovery and typically completes in approximately 3 minutes.
MME Handling of NR UE Security Capability in Path Switch Procedures	**Previous Behavior**: MME includes the NR UE Security Capability Information Element (IE) over the S1AP interface in the following messages: • INITIAL-CONTEXT-SETUP-REQUEST • PATH-SWITCH-REQUEST-ACK If the MME receives the NR UE Security Capability in a PATH SWITCH REQUEST from the eNodeB, it uses this value in the PATH SWITCH ACK. Otherwise, it parses and uses the NR UE Security Capability from the UE Additional Security Capability received in one of these messages: • ATTACH REQUEST • TAU REQUEST • UE-CONTEXT-MODIFICATION-REQUEST • HANDOVER REQUEST • DOWNLINK-NAS-TRANSPORT **New Behavior**: If the MME receives the NR UE Security Capability in a PATH SWITCH REQUEST from eNodeB, it now ignores this value. Instead, the MME always uses its backed-up value parsed from the UE Additional Security Capability received in the ATTACH or TAU request when sending the PATH SWITCH ACK.
Updated cause to handle SGW errors during 4G to 5G handover	**Previous behavior**: For Pure S call, if the Update Bearer Request is received while the SGW is already processing Modify Bearer Request for the PRA change, then the Update Bearer Request message was rejected with the cause No Resource Available. **New behavior**: For Pure S call, if the Update Bearer Request is received while the SGW is already processing Modify Bearer Request for the PRA change, then the Update Bearer Request is silently dropped. The P-GW retries the Update Bearer Request message and S-GW processes it.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

Table 4. Resolved issues for StarOS™ Software, Release 2025.03.gh0

Bug ID	Description	Product Found
CSCwq20529	vpnmgr restart at function vpnmgr_lookup_pool_by_id_slow()	cups-cp

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

Bug ID	Description	Product Found
CSCwq09903	Corrupted Diameter Realm value in STR	cups-cp
CSCwq30875	Session manager recovery status instability	cups-cp
CSCwq00805	CUPS-CP not triggering CCRU to PCRF after wifi to wifi handover	cups-cp
CSCwp03503	CDR corruption after CP switchover	cups-cp
CSCwp16586	Generated URR's are not associated with PDR's when the Online Charging System (OCS) is in a Server Unreachable (SU) state	cups-cp
CSCwp84482	Mapping of Default IMS bearer QCI set 1 by PGW so no dedicated created for the reason UE faced Issue while connecting to call once to comes back to volte from vowifi	cups-cp
CSCwo94253	3GPP-Reporting-Reason VALIDITY_TIME in the CCR-U after GY RAR	cups-cp
CSCwq22329	Lack of P-CSCF address in EGTP_CREATE_SESSION_RESPONSE in case of VoWiFi	cups-cp
CSCwq31050	sessmgr reload after ECS configuration modification	cups-cp
CSCwq18010	MBR-UBR collision in CUPS-SGW during handover	cups-cp
CSCwp10751	Periodic updates not being sent when 'diameter send-ccri session-start' is configured	cups-cp
CSCwk31021	On CUPS-CP node multiple session manager restarts observed after SRP switchover	cups-cp
CSCwn52078	Data stall issue is reported for CUPS	cups-up
CSCwo87056	Wrong UP behavior after getting CREDIT_LIMIT_REACHED	cups-up
CSCwp83463	Multiple sessmgr 12093 error logs generated in the system	cups-up
CSCwn78141	packet drops when GSU in CCA-I only provides CC-TIME with FUI terminate without volume quota	cups-up
CSCwq18455	huge amount of logs Skipping adf creation for NAT subscriber in UPF	cups-up
CSCwo47679	Buffered bytes dropped due to flow action discard in charging action incorrect under input byte drop	cups-up
CSCwp14183	IPSECDEMUX is in WARN state	epdg
CSCwo64859	Frequent authentication failures in the second PDN on ePDG	epdg
CSCwn30866	mme sessmgr crash-mme_pdn_fsm_connect_pending_brr_evt	mme
CSCwo87872	Code change to drop a PDN Connection Request for an existing PDN with same APN when Service Request Procedure is ongoing and 'policy pdn-reconnection restart' is configured	mme
CSCwp84512	To send unauthenticated IMSI in Location Report Request for unauthenticated emergency attach with IMSI	mme
CSCwq12952	During X2 handover MME modifies NR UE Security Capabilities received in Path Switch	mme

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

Bug ID	Description	Product Found
	Request prior returning it to eNB	
CSCwo68956	Handling of enodeb transmission to avoid mmemgr crash	mme
CSCwp19640	UE loses NAT IP Address after SRP switchover	pdn-gw
CSCwo37912	Legacy-GW ATT : vpnmgr crash observed in sn_tacacs_authen_login_cleanup function	pdn-gw
CSCwo66261	CLI not working after upgrade " show subscribers data-rate summary active-charging-service XXXX"	sae-gw
CSCwo74921	Error log for SGW - wrong 'recordOpeningTime' in CDR	sgw
CSCwq14804	" starBusyoutReason" and " starSxPeerIP" are used/referenced and not defined.	staros
CSCwo02043	ePDG VPCDI: iftask warn during SR tests	staros
CSCwj67156	RTNETLINK socket recv buffer under run error code 105 on hermes branch sw build on CUPS CP	staros
CSCwo89406	Incorrect value in Rx port utilization counter	staros
CSCwo65162	Incorrect output in command " show bulkstats internal intervals"	staros
CSCwo01479	Unplanned SF migration caused diamproxy instance # out of range	staros
CSCwp65651	VzW OSP17 vPGW CF multi-attach volume feature (MAV) - use cases	staros

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

Table 5. Open issues for StarOS™ Software, Release 2025.03.gh0

Bug ID	Description	Product Found
CSCwp28316	Sx peer failure with demux SF unplanned migration	cups-cp
CSCwp20248	CP is not sending Delete session request to UP in case of GTPU Path Failure	cups-cp
CSCwq56869	Periodic updates not being sent when 'diameter send-ccri session-start' is configured and when FUI with terminate is received in CCA-I	cups-cp
CSCwq56872	Generated URR’s are not associated with PDR's when the Online Charging System (OCS) is in a Server Unreachable (SU) state.	cups-cp
CSCwo82799	CUPS UP UL/DL packets dropping	cups-up

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

Bug ID	Description	Product Found
CSCwq29508	After SGW relocation (S1-HO), traffic not sent.	cups-up
CSCwq36099	ePDG VPC-SI: dhmgr mem warn	epdg
CSCwq48299	Incorrect VLR Status Displayed on MME Post sgs vlr-failure/vlr-recover with Pooled VLRs.	mme
CSCwq50254	Fatal Signal 11: failures observed due to sessmgr_dhcpv6app_api_release_address	pdn-gw
CSCwq22148	Legacy-GW ATT: ASR5500 chassis hwctrl process shows warn state in show task resources	pdn-gw
CSCwq55405	Updates to a Group of Ruledefs triggers an mtree data structure rebuild, the configuration under the GOR retains old hash causing packet mismatches	pdn-gw
CSCwq56385	Assertion failure at midplane/libsn_midplane.c in SPGW	sae-gw
CSCwp60108	session manager crash with an unknown signature time encoding data at smgr_gr_encode_uplane_call_info_uchckpt_cmd	sae-gw

Known issues

This section describes the known issue that may occur during the upgrade of the StarOS image.

Install 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.

When upgrading the StarOS image from a previous version to the latest version, issues may arise if there is a problem with the Cisco SSH/SSL upgrade. To avoid such issues, ensure that the boot file for Service Function (SF) cards is properly synchronized.

To synchronize the boot file for all the Service Function (SF) VPC-DI non-management cards, use the following CLI command:

```
[local] host_name# system synchronize boot
```

This ensures that the changes in boot file are identically maintained across the SF cards.

Note: Execute the system synchronize boot command before reloading for version upgrade from any version earlier than 21.28.mh14 to version 21.28.mh14 or versions higher than 21.28.mh14.

Compatibility

This section provides compatibility information about the StarOS package version, and the hardware and software requirements for the Legacy Gateway and CUPS software release.

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

Compatible StarOS package version

Table 6. Release package version information

StarOS packages	Version	Build number
StarOS package	2025.03.gh0	21.28.mh28.98642

Compatible software and hardware components for CUPS

This table lists the CUPS compatible components that operate on bare metal server when deployed in a VPC-SI environment.

Table 7. Compatibility information for CUPS User Plane deployed on bare metal server with VPC-SI, Release 2025.03.gh0

Supported hardware	Version
Server requirements	UCSC-C220-M75 UCSC-C220-M6S
CPU	Intel(R) Xeon(R) Gold 6438N @2GHz Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz
NIC	E810C
Base OS	Ubuntu 22.04.1 LTS (Jammy Jellyfish) Red Hat Enterprise Linux release 8.4 (Ootpa)
Supported orchestrator and software	
ESC	6.0.0.54
CVIM	5.0.4
NSO	nso-mob-fp-3.5.2
ADC P2P plugin	2.74.h7.2683
RCM	20250723-132226Z **Note**: Use this link to download the RCM package associated with the software.

This table lists the CUPS compatible components that operate on an OpenStack when deployed in a VPC-SI environment.

Table 8. Compatibility information for CUPS User Plane deployed on OpenStack with VPC-SI, Release 2025.03.gh0

Supported hardware	Version
Server Requirements	Cisco UCS C220 M7S

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

Supported hardware	Version
CPU	Intel(R) Xeon(R) Gold 6438N @2GHz
NIC	E810C
Base OS	Ubuntu 22.04.1 LTS (Jammy Jellyfish)
Supported orchestrator and software	
ESC	6.0.0.54
CVIM	5.0.4
NSO	nso-mob-fp-3.5.2
ADC P2P plugin	2.74.h7.2683
RCM	20250723-132226Z

This table lists the CUPS compatible components that operate on an OpenStack when deployed in a VPC-SI environment.

Table 9. Compatibility information for CUPS Control Plane deployed on OpenStack with VPC-SI, Release 2025.03.gh0

Supported hardware	Version
Server Requirements	UCSC-C220-M6S
CPU	Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz
NIC	E810C
Base OS	Ubuntu 22.04.3 LTS (Jammy Jellyfish)
Supported orchestrator and software	
ESC	6.0.0.54
CVIM	5.0.4
NSO	nso-mob-fp-3.5.2
ADC P2P plugin	2.74.h7.2683
RCM	20250723-132226Z

Compatible software and hardware components for non-CUPS

This table lists the compatible P-GW components that operate on a bare metal server (CNDP) when deployed in a VPC-DI environment.

Table 10. Compatibility information for P-GW deployed on bare metal server with VPC-DI, Release 2025.03.gh0

Supported hardware	Version
Server Requirements	UCSC-C220-M6S
CPU	Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz
NIC	E810C
Base OS	Ubuntu 22.04.5 LTS (jammy Jellyfish)
Supported orchestrator and software	
ESC	—
CVIM	—
NSO	ncs-6.4.3
ADC P2P plugin	2.74.h7.2683

This table lists the P-GW compatible components that operate on an OpenStack when deployed in a VPC-DI environment.

Table 11. Compatibility information for P-GW deployed on OpenStack with VPC-DI, Release 2025.03.gh0

Supported hardware	Version
Server Requirements	UCSC-C220-M5
CPU	Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz
NIC	XL710
Base OS	RHEL 9.2
Supported orchestrator and software	
ESC	6.0.0.54
CVIM	5.0.4
NSO	nso-mob-fp-3.5.2
ADC P2P plugin	2.74.h7.2683
RHOSP	17.1

This table lists the ePDG compatible components that operate on a bare metal (CNDP) server when deployed in a VPC-DI environment.

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

Table 12. Compatibility information for ePDG deployed on bare metal server with VPC-DI, Release 2025.03.gh0

Supported hardware	Version
Server requirements	UCSC-C220-M6S
CPU	Intel(R) Xeon(R) Gold 6338N CPU @ 2.20GHz
NIC	E810C
Base OS	Red Hat Enterprise Linux release 8.4 (Ootpa
Supported orchestrator and software	
ESC	6.0.0 or later
CVIM	–
NSO	–
ADC P2P plugin	–
RHOSP	16.2

This table lists the compatible MME components that operate on a bare metal server when deployed in a VPC-DI environment.

Table 13. Compatibility information for MME deployed on bare metal server with VPC-DI, Release 2025.03.gh0

Supported hardware	Version
Server requirements	UCSC-C220-M5SX
CPU	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz
NIC	XL710
Base OS	RHEL Fedora 8.4
Supported orchestrator and software	
ESC	6.0.0.52
CVIM	5.0.1
NSO	–
ADC P2P plugin	–

Supported software packages

This section provides information about the release packages associated with StarOS Classic Gateway, Control, and User Plane Separation (CUPS) software.

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

Table 14. Software packages for Release 2025.03.gh0

Software package	Description
NSO	
nso-mob-fp-3.5.2-2025.03.gh0.zip	Contains the signed NSO 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.
VPC companion package	
companion-vpc-2025.03.gh0.zip	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants.
VPC-DI	
qvpc-di-2025.03.gh0.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-2025.03.gh0.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-2025.03.gh0.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-2025.03.gh0.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-2025.03.gh0.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-2025.03.gh0.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-2025.03.gh0.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-2025.03.gh0.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-2025.03.gh0.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.
VPC-SI	
intelligent_onboarding-2025.02.gh0.zip	Contains the VPC-SI onboarding signature package that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-2025.03.gh0.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.

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

Software package	Description
qvpc-si-2025.03.gh0.iso.zip	Contains the VPC-SI ISO used for new deployment. A new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template-vmware-2025.03.gh0.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-2025.03.gh0.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-2025.03.gh0.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.

Release lifecycle milestones

The following table provides EoL milestones for Cisco StarOS software:

Table 15. EoL milestone information for StarOS™ Software, Release 2025.03.gh0

Milestone	Date
First Customer Ship (FCS)	31-Jul-2025
End of Life (EoL)	31-Jul-2025
End of Software Maintenance (EoSM)	29-Jan-2027
End of Vulnerability and Security Support (EoVSS)	29-Jan-2027
Last Date of Support (LDoS)	31-Jan-2028

StarOS product version numbering system

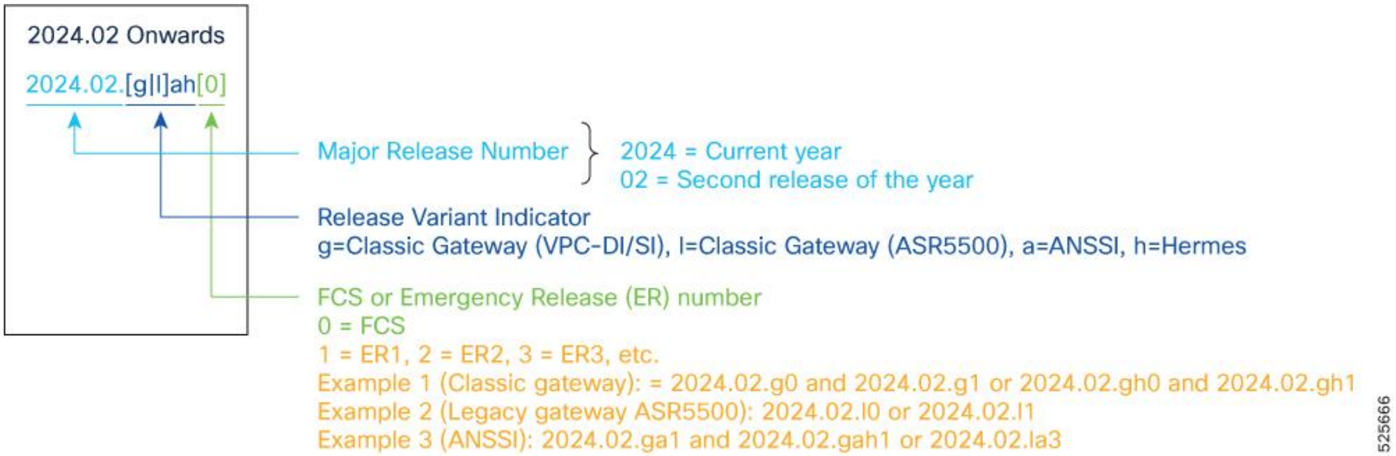
The output of the show version command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

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 the figure for more details.

Note: 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.

Figure 1. **Version numbering for FCS, emergency, and maintenance releases**

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


2024.02 Onwards
2024.02.[g|l]ah[0]
Major Release Number
2024 = Current year
02 = Second release of the year
Release Variant Indicator
g=Classic Gateway (VPC-DI/SI), l=Classic Gateway (ASR5500), a=ANSSI, h=Hermes
FCS or Emergency Release (ER) number
0 = FCS
1 = ER1, 2 = ER2, 3 = ER3, etc.
Example 1 (Classic gateway): = 2024.02.g0 and 2024.02.g1 or 2024.02.gh0 and 2024.02.gh1
Example 2 (Legacy gateway ASR5500): 2024.02.l0 or 2024.02.l1
Example 3 (ANSSI): 2024.02.ga1 and 2024.02.gah1 or 2024.02.la3
525666

Note: For any clarification, contact your Cisco account representative.

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. Click Linux and then choose the Software Image Release Version.

To find the checksum, hover the mouse pointer over the software image you have downloaded. 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 the table and verify that it matches the one provided on the software download page. To calculate a SHA512 checksum on your local desktop see the table.

Table 16. 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`

Note: **filename** is the name of the file. **extension** is the file extension (for example, .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.

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

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.

Related resources

This table provides key resources and links to the support information and essential documentation for StarOS and CUPS products.

Table 17. Related resources and additional information

Resource	Link
Cisco ASR 5500 documentation	StarOS documentation
Cisco Ultra Packet Core documentation	CUPS documentation
Service request and additional information	Cisco Support

Legal information

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: 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)

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.

© 2025 Cisco Systems, Inc. All rights reserved.