Release Notes for the StarOS™ Software Version 2025.02.ga0

First Published: April 30, 2025

Introduction

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

Products Qualified and Released in this Release

Products	Qualified?
CUPS	Yes
MMEs	Yes
ePDG	Yes
P-GW	Yes
SAEGW	Yes
SGSN	Yes
Platforms	
ASR5500	No
VPC-DI	Yes
VPC-SI	Yes

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	30-Apr-2025
End of Life	EoL	20-Apr-2025
End of Software Maintenance	EoSM	29-Oct-2026
End of Vulnerability and Security Support	EoVSS	29-Oct-2026
Last Date of Support	LDoS	31-Oct-2027

Release Package Version Information

StarOS Packages	Version	Build Number
StarOS Package	2025.02.ga0	21.28.14.97802

Descriptions for the various packages provided with this release are available in the Release Package Descriptions section.

Verified Compatibility

Products	Version
ADC P2P Plugin	2.74.8.2658
RCM	20250423-050401Z

Note Use only these compatible software versions for the products qualified in this release.

What's New in this Release

Features and Enhancements

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

Feature Title	Description	Product
Support for 16K UE Radio Capability	MME is enhanced to configure **s1-mme ue-radio-cap** parameter with greater than 9000 Bytes.	MME
Extend the explicit route limit	The explicit route advertisement limit is enhanced from 24,000 to 40,000 on the ASR5500 platform to accommodate the increasing network requirements. A new command extend-**explicit-route-limit** is introduced at the context level to extend the explicit route limit. The **show ip pool** command is modified to display the maximum supported explicit route as either 40,000 or 24,000, based on the configuration. **Note**:. In an ICSR environment, when upgrading the standby chassis to the latest StarOS 21.28.14 version, the 'Total explicit host route' value in the **show ip pool** CLI output on the active chassis may temporarily double. This issue will resolve automatically once the active chassis is upgraded to the latest image.	

Behavior Changes

There is no behavior changes introduced in this release.

Related Documentation

For a complete list of documentation available for this release, go to: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-%20list.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.

Synchronizing Boot File for Service Function Cards

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 21.28.11 to version 21.28.11 or versions higher than 21.28.11.

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.

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 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 -a512 <filename>.<extension>`

Linux	Open a terminal window and type the following command:
	
	`$sha512sum <filename>.<extension>`
	
	Or
	
	`$shasum -a512 <filename>.<extension>`

Operating System	SHA512 checksum calculation command examples
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.

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.

Firmware Updates

There is no firmware upgrade required for this release.

Open Bugs

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
CSCwo93460	sxmgr_pfcp_read_callback()	cups-cp
CSCwo47679	Buffered bytes dropped due to flow action discard in charging action incorrect under input byte drop	cups-up
CSCwk65512	ipsecmgr cpu warn/over during make-break sessions with 4096 keysize device certificate	epdg
CSCwo37912	Vpnmgr crash observed in sn_tacacs_authen_login_cleanup function	pdn-gw
CSCwo75863	Sessmgr restarts after enabling VoLTE for specific inroamer IMSIs ranges	pdn-gw
CSCwo74921	Error log for SGW - wrong 'recordOpeningTime' in CDR	sgw

Resolved Bugs

This document uses the following conventions. The following table lists the resolved bugs in this specific software release.

Note: This software release may contain open bugs first identified 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
CSCwm40394	Sx-IPSec - clear crypto security-association results in Sx failure	cups-cp
CSCwn12297	Cannot change monitoring key at session level on CUPS when changing rulebase and ruledef	cups-cp
CSCwo10621	[CUPS / LIVE / CP / 21.28.h7] CLI crash : PC: [f6fe1b6f/X] libc.so.6/__strlen_ia32()	cups-cp
CSCwk39766	Memory usage kept increasing for ipsecmgr instances on ePDG when server certificate config used	epdg
CSCwo75859	Legacy-GW: ICSR : Value of Total explicit host route count doubled in active chassis on reloading standby chassis	sae-gw

Operator Notes

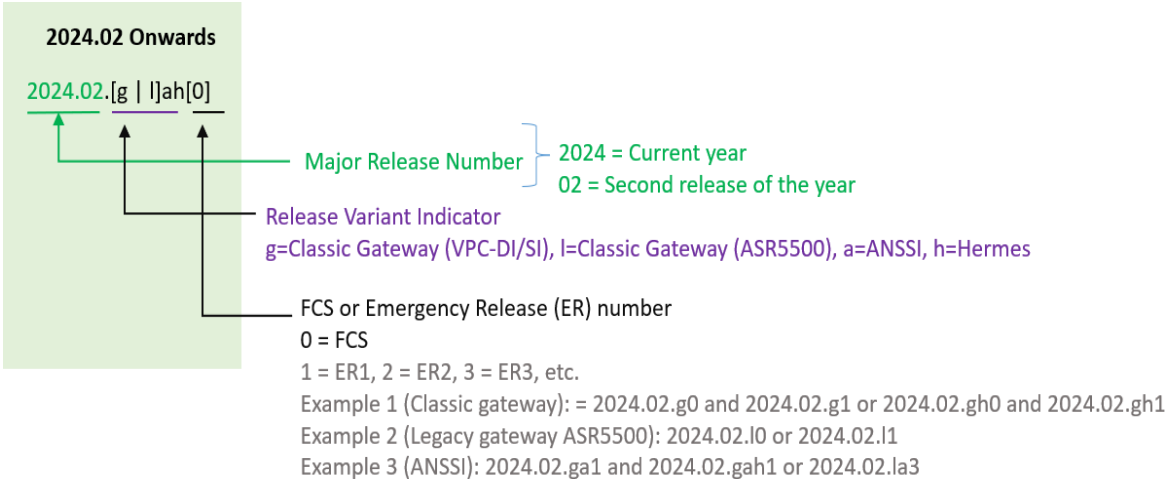
Software Version Numbering System

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



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

Release Package Descriptions

The table provides examples of packages according to the 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.
VPC Companion Package	
companion-vpc-<release>.zip For example, companion-vpc- 2024.02.gh2.i4.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-<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	
intelligent_onboarding-<release>.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-<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.
RCM	
rcm-vm-airgap-<release>.ova.zip	Contains the RCM software image that is used to on-board the software directly into VMware.
rcm-vm-airgap-<release>.qcow2.zip	Contains the RCM software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
rcm-vm-airgap-<release>.vmdk.zip	Contains the RCM virtual machine disk image software for use with VMware deployments.
Ultra Services Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles).
usp_T-<version>.iso	The USP software package containing component RPMs (bundles). This bundle contains trusted images.
usp_rpm_verify_utils-<version>.tar	Contains information and utilities for verifying USP RPM integrity.

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, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax 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: 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)