



# UCC 5G UPF Release Notes, Release 2025.02.0

First Published: 2025-04-29

## Ultra Cloud Core User Plane Function

### Introduction

This Release Notes identifies changes and issues related to this software release.

### Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	30-Apr-2025
End of Life	EoL	30-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

These milestones and the intervals between them are defined in the [Cisco Ultra Cloud Core \(UCC\) Software Release Lifecycle Product Bulletin](#) available on cisco.com.

### Release Package Version Information

Software Packages	Version
companion-vpc-2025.02.0.zip.SPA.tar.gz	2025.02.0 (21.28.m35.97821)
qvpc-si-2025.02.0.bin.SPA.tar.gz	2025.02.0 (21.28.m35.97821)
qvpc-si-2025.02.0.qcow2.zip.SPA.tar.gz	2025.02.0 (21.28.m35.97821)
NED package	ncs-6.4.3-cisco-staros-5.56.1
NSO	6.4.3

Use this [link](#) to download the NED package associated with the software.

Descriptions for the various packages provided with this release are available in the [Release Package Descriptions, on page 8](#) section.

## Verified Compatibility

Products	Version
ADC Plugin	2.74.8.2658
RCM	2025.02.0.i46
Ultra Cloud Core SMI	2025.02.1.i17
Ultra Cloud Core SMF	2025.02.0

## What's New in this Release

### Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
DHCP-based IP Address Allocation	<p>This feature allows the network operator to use an external DHCP server to receive IP addresses for subscriber UEs.</p> <p>Allocating IP addresses using a DHCP server enables the enterprises with complex 5G networks to manage and control the IP address allocation centrally.</p> <p><b>Important</b></p> <p>While enabling the DHCP feature, it is always recommended to enable the DHCP service on the standby UPF first and then on the active UPF. After making the feature CLI changes, save the changed config at boot config to enable the feature.</p> <p>If you enable this feature for an existing DNN, the ongoing calls will experience service interruptions. If you enable this feature for a new DNN, there will be no service disruptions, as the new call will always have IP allocation from the DHCP server.</p> <p><b>Commands Introduced:</b></p> <p><b>dhcp server enable-discover slot/port slot_port_number dhcp-node-id node_id:</b> This CLI is configured under DHCP service configuration mode to allow UPF to discover the DHCP server.</p> <p><b>Commands Enhanced:</b></p> <p><b>dhcp ip skip-validation:</b> This CLI is configured under the DHCP service configuration mode to skip the IPv4 address validation.</p> <p><b>Default Settings:</b> Disabled—Configuration Required to Enable</p>

## Behavior Changes

There are no behavior changes in this release.

# 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.

## 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.

The following screenshot is an example of a UPF release posted in the Software Download page.

**Figure 1:**

The screenshot shows the Cisco Software Download page for the Ultra Cloud Core - User Plane Function, Release 2023.02.2.t1.0. A 'Details' modal is open, displaying the following information:

- Description: VPC-SI binary software image signature package
- Release: 2023.02.2.t1.0
- Release Date: 11-Aug-2023
- FileName: qvpc-si-21.28.mt10.bin.SPA.tar.gz
- Size: 194.12 MB ( 203547769 bytes)
- MD5 Checksum: d86d3864378b16434d346c75e17e0bc6
- SHA512 Checksum: 1aa84d98d14e1cefad5d54266389d01e ...

The main table lists the following software packages:

Package Name	Release Date	Size
VPC-SI binary software image signature package	11-Aug-2023	2.83 MB
qvpc-si-21.28.mt10.bin.SPA.tar.gz	11-Aug-2023	194.12 MB
VPC-SI qcow2 image signature package	11-Aug-2023	194.18 MB
qvpc-si-21.28.mt10.qcow2.zip.SPA.tar.gz	11-Aug-2023	188.31 MB
Trusted VPC-SI binary software image signature package	11-Aug-2023	188.38 MB
qvpc-si_T-21.28.mt10.bin.SPA.tar.gz	11-Aug-2023	188.38 MB

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, refer to the following 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: <b>&gt; certutil.exe -hashfile <i>filename.extension</i> SHA512</b>
Apple MAC	Open a terminal window and type the following command: <b>\$ shasum -a 512 <i>filename.extension</i></b>
Linux	Open a terminal window and type the following command: <b>\$ sha512sum <i>filename.extension</i></b> OR <b>\$ shasum -a 512 <i>filename.extension</i></b>
<b>NOTES:</b> <i>filename</i> is the name of the file. <i>extension</i> 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.

## Certificate Validation

UPF software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

## 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 resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Headline
<a href="#">CSCwk27158</a>	Continuous sxdemux error logs "MISMATCH: IMSI ENTRY [SMGR-ID:10 IMSI:123456789123456]"
<a href="#">CSCwm59995</a>	sessmgr restart function sessmgr_uplane_gtpu_tx_setup_n4

Bug ID	Headline
<a href="#">CSCwn61589</a>	CRR recovery failure recovery-invalid-crr-clp-uplane-record-info observed with ICSR UPF swo
<a href="#">CSCwo34203</a>	UPF should allow to configure dhcpv6 service without server-profile under apn
<a href="#">CSCwo34950</a>	vpnctrl restart observed at Function: vc_cdr_update_xdr_reset_ind()
<a href="#">CSCwo53463</a>	UPF should send Decline if DHCP Server assigns same IP to a second UE
<a href="#">CSCwo65306</a>	DHCP Partially allocated calls are not recovered on new ICSR Active after SW
<a href="#">CSCwo65746</a>	UPF sends different chaddr after session recovery
<a href="#">CSCwo65802</a>	Incorrect disconnect reasons and cause codes during DHCP failure scenarios
<a href="#">CSCwo68401</a>	UPF showing incorrect disconnect reason when dhcp serve or vlan port shut down & new call attach
<a href="#">CSCwo75158</a>	DHCPv6 solicit - sessmgr wrongly sending sw_if_index to VPP causing packet to be blackholed packets
<a href="#">CSCwo89553</a>	sessmgr restart observed at libc.so.6/__memset_sse2_rep()
<a href="#">CSCwo89554</a>	sessmgr restart observed at sessmgr_uplane_send_ddn_n_buff_dl_pkts_before_processing()
<a href="#">CSCwo89625</a>	smp-fp-strm-chrg-oper-failure pegging in session disconnect-reasons on RCM UPFs
<a href="#">CSCwo90153</a>	Sessmgr restart at sessmgr_Uplane_collect_pdr_info()
<a href="#">CSCwo92125</a>	Sx instance checkpoint is arriving late in Sx demux is not included
<a href="#">CSCwo96983</a>	GR Checkpoint ignored for callid<> and cmd 232 as clp audit is completed

## Resolved Bugs for this Release

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 open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Headline	Behavior Change
<a href="#">CSCwe29094</a>	Seen Uplane received invalid far id in PDU on task kill	No
<a href="#">CSCwe30498</a>	Time quota is not reset post UPF 1:1 ICSR, in case new quota is not provisioned.	No

Bug ID	Headline	Behavior Change
<a href="#">CSCwe60139</a>	Idletimer is triggered post switchover, even if UE is not in idle state for defined duration.	No
<a href="#">CSCwf89394</a>	Nat IP and Port chunk struck in scenario of ICMPv6 traffic involving config modification	No
<a href="#">CSCwi98822</a>	Need cli enhancement to clear monsub session at npu and sessmgr.	No
<a href="#">CSCwm05166</a>	UPF Crash - Assertion failure at sess/smgr/sessmgr_uplane.c:32102	No
<a href="#">CSCwn40724</a>	EDRs w/non-zero byte count and w/o NAT IP in CUPS UP	Yes
<a href="#">CSCwn52078</a>	Data stall issue is reported for CUPS	No
<a href="#">CSCwn96859</a>	DIMM failure induced b2b switchover results in all session loss	No
<a href="#">CSCwn99718</a>	TCP OOO observed in Converged core only for Pure S SGW-U session after exiting VPP	No
<a href="#">CSCwo00106</a>	Continuous sessmgr restart with function dhcpv6app_server_fsm_handler()	No
<a href="#">CSCwo20496</a>	'show rcm monitor' CLI may report 'SX monitors down' even though peers are up	No
<a href="#">CSCwo33410</a>	sessmgr gives error at libc.so.6/___strncpy_sse2()	No
<a href="#">CSCwo36802</a>	Seen sessmgr restarted at sessmgr_uplane_sx_update_far_apply_action()	No
<a href="#">CSCwo37027</a>	HTTP GET packets not getting forwarded from CUPS	No
<a href="#">CSCwo58564</a>	sessmgr restart @ sessmgr_uplane_start_self_protection_call_cleanup_timer	No
<a href="#">CSCwo81815</a>	DNS Snoop rules changes causing high CPU in UPF	No

## Operator Notes

### StarOS Version Numbering System

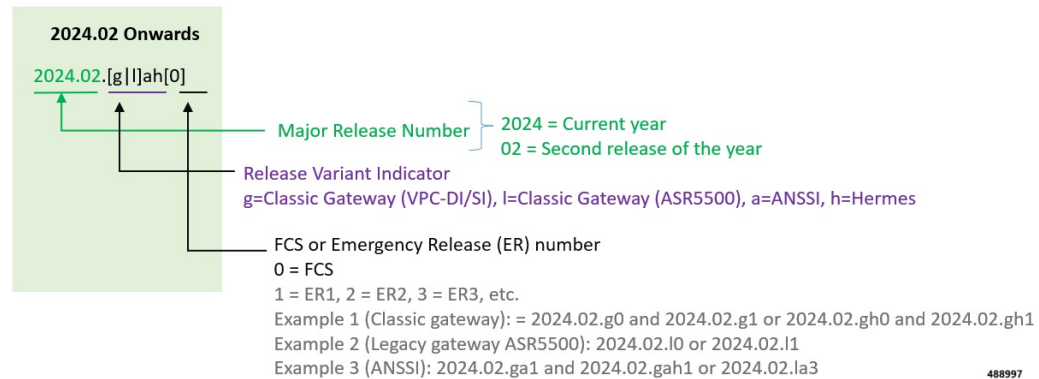
The output of the **showversion** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.



**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 the figure 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.

**Figure 2: Version Numbering for FCS, Emergency, and Maintenance Releases**



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

## Cloud Native Product Version Numbering System

The show helm list command displays detailed information about the version of the cloud native product currently deployed.

Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.

- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.

- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.

- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number

- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches

- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Software Packages	Description
companion-vpc-<staros_version>.zip.SPA.tar.gz	Contains files pertaining to VPC, including SNMP MIBs, RADIUS dictionaries, ORBEM clients, etc. These files pertain to both trusted and non-trusted build variants. The VPC companion package also includes the release signature file, a verification script, the x.509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpv-si-<staros_version>.bin.SPA.tar.gz	<p>The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.</p> <p>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.</p>



Software Packages	Description
qvpc-si-<staros_version>.qcow2.zip.SPA.tar.gz	<p>The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.</p> <p>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.</p>
ncs-<nso_version>-cisco-staros-<version>.signed.bin	<p>The NETCONF NED package. This package includes all the files that are used for NF configuration.</p> <p>Note that NSO is used for NED file creation.</p>

## 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>.

