Release Notes for UCC 5G UPF, Release 2025.03.0

Ultra Cloud Core - User Plane Function, Release 2025.03.0

This Release Notes identifies changes and issues related to the release of 5G User Plane Function (UPF).

The key highlights of this release include:

- **Expanded Network Functionality:** Introduces 3GPP lawful interception support and flexible DHCP-based IPv6 address allocation.
- **Cost-Effective Device Support:** Enables UPF to support reduced capability devices for wider 5G network integration.
- **Enhanced Reliability and Efficiency:** Improves serviceability through expanded Show Support Details (SSD), show output, and introduces Secondary ISE Server for operational continuity.

For more information on UPF, see the Related resources section.

Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC UPF software:

Table 1. EoL milestone information for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Milestone	Date
First Customer Ship (FCS)	14-Aug-2025
End of Life (EoL)	14-Aug-2025
End of Software Maintenance (EoSM)	12-Feb-2027
End of Vulnerability and Security Support (EoVSS)	12-Feb-2027
Last Date of Support (LDoS)	29-Feb-2028

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.

New software features

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

Table 2. New software features for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Product impact	Feature	Description
Upgrade	3GPP LI	The 3GPP LI support is introduced to adhere to the 3GPP standards for lawful interception. **Important:** This feature is fully qualified in this release. Contact your Cisco account representative for more information.
Upgrade	Reduced Capability support on UPF	This feature allows the UPF to support High Latency Communication sessions for Reduced Capabilities UEs.

Product impact	Feature	Description
		UPF supports the connectivity of Reduced Capability UEs with the 5G network by defining the new RAT type, **NR_REDCAP**. **Commands enhanced:** • **sx-protocol supported-features ddnd dbdm udbc:** This CLI is configured under Context EPC mode to indicate the support of buffering functionality. • **user-plane-service schema** schema_name: This CLI is configured under Bulkstats configuration mode. This CLI is enhanced with new RedCap-related parameters to be configured. • These show CLIs are enhanced to support RedCap functionality: ◦ **show user-plane-service statistics rat all** ◦ **show subscribers user-plane-only callid callid bar full all** ◦ **show configuration context EPC** ◦ **show bulkstats variables user-plane-service** ◦ **show bulkstats schema** ◦ **show bulkstats data** **Default Settings:** Disabled–Configuration Required to Enable **Note:** The recommended maximum buffer limit size is 50 packets, based on the performance benchmarking of 5% for RedCap Sessions.
Upgrade	DHCP-based IPv6 address allocation without prefix limitations	This feature allows the UPF to support IPv6 address allocation to the subscriber UEs through external DHCP server, without prefix limitations. **Commands introduced:** **disable ipv6-validation:** This CLI is configured under DHCP Client Profile configuration mode to disable IPv6 validation. **Commands enhanced:** **disable dhcpv6-client-unicast slot/port** slot_port_number: This CLI is configured under DHCP Client Profile configuration mode to disable unicast option for DHCPv6 client. **Default Settings:** Disabled–Configuration Required to Enable
Software Reliability	Improved serviceability through enhanced SSD and show CLI output	This feature enhances the debuggability of UPF by adding these three user plane service show CLIs in the SSD: • **show user-plane-service edr-format statistics all** • **show user-plane-service fw-and-nat policy statistics all** • **show user-plane-service inline-services firewall statistics verbose** This feature also improves monitoring and troubleshooting capability by enhancing the output of the CLI **show sx peers wide**.
Software Reliability	Secondary ISE server support on UPF	This feature allows the network operator to integrate a secondary ISE server on UPF. The secondary ISE server integration provides a failure mechanism to ensure seamless enforcement of SGACLs when the primary ISE server goes down. **Commands enhanced:** • **secondary-server { ipv4-address** ipv4_address **| ipv6-address** ipv6_address **}:** This CLI configures the secondary server IP address under the ISE server profile. • **secondary username** user_name **password** password: This CLI configures the

Product impact	Feature	Description
		secondary username and password under the ISE server profile. • **secondary-certificate** certificate_path: This CLI configures the secondary certificate path under the ISE server profile. • **secondary-ca-certificate** ca_certificate_path: This CLI configures the secondary CA certificate under the ISE server profile. • **secondary-key** key_path: This CLI configures the secondary key path under the ISE server profile. **Commands introduced**: • **max-retransmissions** max_retrans_count: This CLI configures the maximum number of retries under the ISE server profile. • **retransmission-timeout** timeout_duration: This CLI configures the retransmission timeout under ISE server profile. • **backoff-period** backoff_duration: This CLI configures the Backoff period under ISE server profile. **Default Settings:** Disabled–Configuration Required to Enable

Changes in behavior

There are no behavior changes in this release.

Resolved issues

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

Note: This software release may contain resolved 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 3. Resolved issues for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Bug ID	Description
CSCwo89406	Incorrect value in Rx port utilization counter
CSCwp04974	sessmgr crash observed for smgr_uplane_recover_instance_info()
CSCwp19441	sessmgr crash observed - sn_memblock_memcache_free()
CSCwp83463	Multeple sessmgr 12093 error logs generated in the system
CSCwq08948	vpp throws error at hatsystem_process_card_fail_msg()
CSCwq13139	Segmentation fault at sessmgr_ddn_delay_timeout()
CSCwq18455	Huge amount of logs Skipping adf creation for NAT subscriber in UPF
CSCwq34154	Recap to Wifi idle mode HO has BAR doesnt get reset even after associated FARs got removed
CSCwq34177	Redcap to 4g Combo debuffered pkts are not seen on sxa leg, neither buffered on sxa leg nor dropped

Bug ID	Description
CSCwq43695	Observed throughput value is displaying wrong value in port utlization output
CSCwq43945	sessmgr restart observed at Function: free_acct()
CSCwq46166	Segmentation fault at sessmgr_dl_buff_duration_timeout()
CSCwq58304	Peer Checksum Validation Failure during upgrade test from Apr25 FCS build to July25 EFT2 build

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 4. Open issues for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Bug ID	Description
CSCwo03399	UPF showing " 0" TX/RX counters in show port datalink counters stats after VF Driver issue
CSCwo34950	vpnctrl restart observed at Function: vc_cdr_update_xdr_reset_ind()
CSCwo92125	Sx instance checkpoint is arriving late in Sx demux
CSCwp35207	Monitor subscriber fastpath disconnect cli is not clearing the hung session in the npumgr
CSCwp36999	Continuous confdmgr restart seen due to Assertion failure in confdmgr/src/confdmgr_fsm
CSCwq24115	sessmgr Segmentation Fault (Signal 11) in smgr_match_dyn_rule_filter()
CSCwq31013	UPF does not show the Sx Mod Resp for the request packets larger than 3100
CSCwq32098	Need to support DHCPv6 Release retransmissions in scenario where reply doesnot come from Server
CSCwq36160	When sbpc is not sent after receiving dbpc buffering is done at FAR level but DBPC limits are used
CSCwq47886	UPF does not send DDN even after extended buff timer expiry
CSCwq54920	System cpu showing higher value with same callmodel on July build
CSCwq60409	Seg Fault at sessmgr_uplane_configure_ipv6_param observed after adding delay and pkt corruption through netem to n4 link between smf and upf
CSCwq60431	Assertion Failure at sessmgr_uplane_sx_update_far_apply_action() observed after adding delay and pkt corruption through netem to n4 link between smf and upf observed after adding delay and pkt corruption through netem to n4 link between smf

Bug ID	Description
	and upf
CSCwq70890	Observed sessmgr restart at uplane_drv_handle_events_from_smgr()
CSCwq68624	sessmgr restart at " dhcpv6_uninit_service_instance()"

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC UPF software.

Table 5. Compatibility information for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Product	Supported Release
ADC Plugin	2.74.10.2682
RCM	2025.03.0
Ultra Cloud Core SMI	2025.03.1.i10
Ultra Cloud SMF	2025.03.0

Supported software packages

This section provides information about the release packages associated with UCC UPF software.

Table 6. Software packages for Ultra Cloud Core - User Plane Function, Release 2025.03.0

Software Package	Description	Release
companion-vpc-2025.03.0.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.	2025.03.0 (21.28.m37.98693)
qvpc-si-2025.03.0.bin.SPA.tar.gz	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. Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.	2025.03.0 (21.28.m37.98693)
qvpc-si-2025.03.0.qcow2.zip.SPA.tar.gz	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. Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.	2025.03.0 (21.28.m37.98693)
NED Package	The NETCONF NED package. This package includes all the	ncs-6.4.5-cisco-staros-

Software Package	Description	Release
	yang files that are used for NF configuration. Note that NSO is used for the NED file creation.	5.57.1.signed.bin
NSO		6.4.5

Use this link to download the NED package associated with the software.

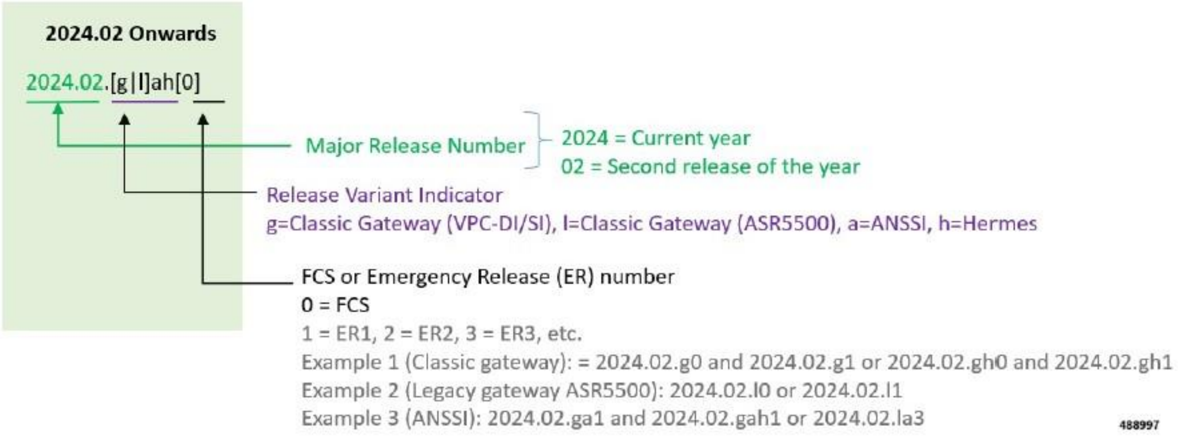
StarOS version numbering system

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 1. StarOS version numbering system format

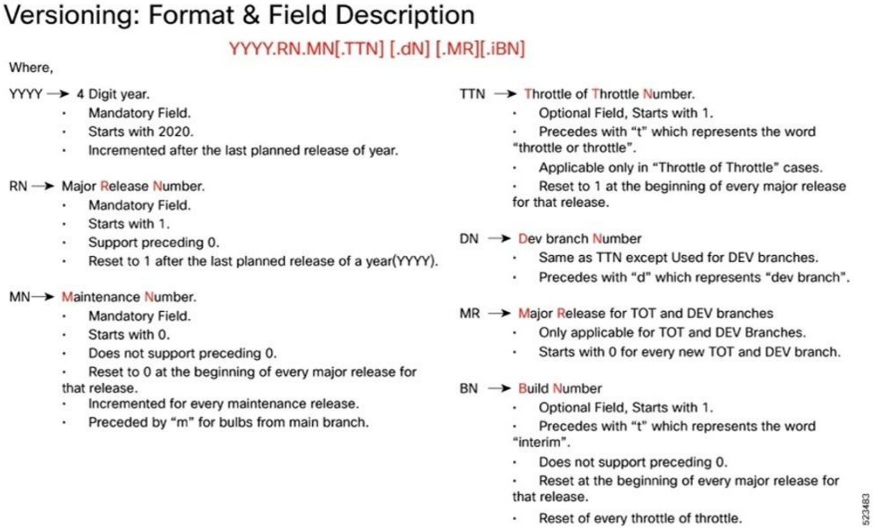

2024.02 Onwards
2024.02.[g|l]ah[0]
Major Release Number
2024 = Current year
02 = Second release of the year
Release Variant Indicator
g=Classic Gateway (VPC-DI/SI), l=Classic Gateway (ASR5500), a=ANSSI, h=Hermes
FCS or Emergency Release (ER) number
0 = FCS
1 = ER1, 2 = ER2, 3 = ER3, etc.
Example 1 (Classic 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
488997

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.

Figure 2. Cloud native product versioning format and description



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.

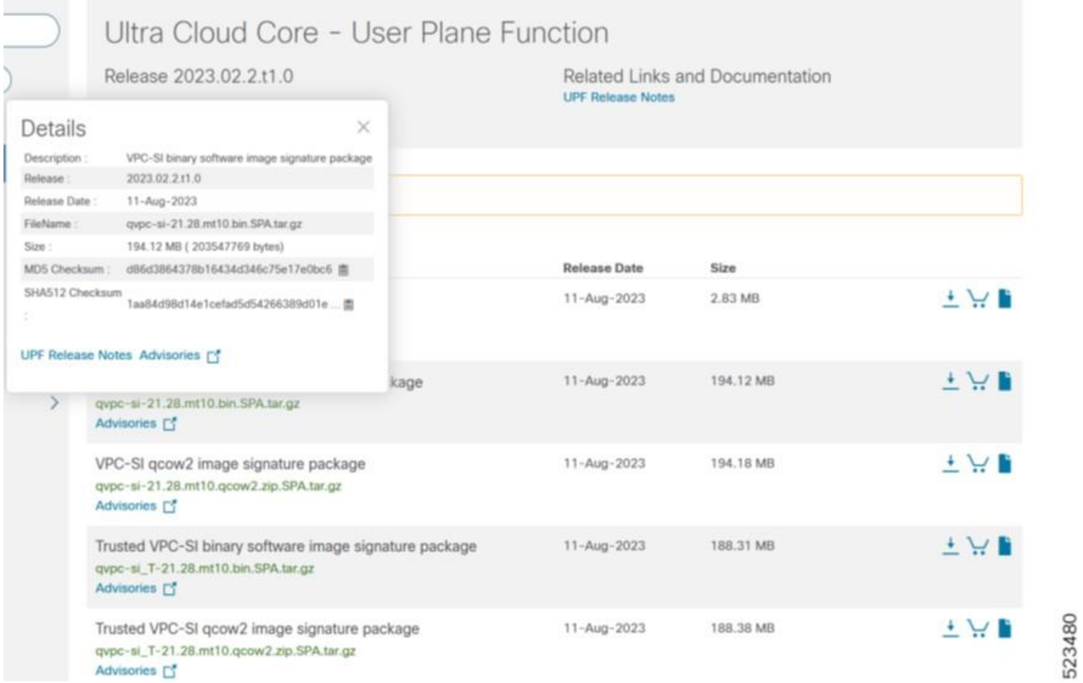
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

Software integrity version

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.

Figure 3. Sample of UPF software image



Ultra Cloud Core - User Plane Function

Release 2023.02.2.t1.0

Related Links and Documentation
UPF Release Notes

Details

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 ...

UPF Release Notes Advisories

	Release Date	Size
	11-Aug-2023	2.83 MB
kage qvpc-si-21.28.mt10.bin.SPA.tar.gz Advisories	11-Aug-2023	194.12 MB
VPC-SI qcow2 image signature package qvpc-si-21.28.mt10.qcow2.zip.SPA.tar.gz Advisories	11-Aug-2023	194.18 MB
Trusted VPC-SI binary software image signature package qvpc-si_T-21.28.mt10.bin.SPA.tar.gz Advisories	11-Aug-2023	188.31 MB
Trusted VPC-SI qcow2 image signature package qvpc-si_T-21.28.mt10.qcow2.zip.SPA.tar.gz Advisories	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 the following table and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 7. SHA512 checksum calculation commands by 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 type 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.

Related resources

Resources	Link
UPF documentation	User Plane Function
Ultra Cloud Core Subscriber Microservices Infrastructure	Subscriber Microservices Infrastructure
Ultra Cloud Core Session Management Function	Session Management Function
Ultra Cloud Core Serving Gateway Function	Ultra Cloud Core Serving Gateway Function
Service Request and Additional information	Cisco Support

Legal information

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.