UCC 5G UPF Release Notes, Release 2024.03.0

First Published: 2024-07-31

Last Modified: 2024-08-02

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	31-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-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-2024.03.0.zip.SPA.tar.gz	2024.03.0 (21.28.m25.94479)
qvpc-si-2024.03.0.bin.SPA.tar.gz	2024.03.0 (21.28.m25.94479)
qvpc-si-2024.03.0.qcow2.zip.SPA.tar.gz	2024.03.0 (21.28.m25.94479)
NED package	ncs-6.1.11-cisco-staros-5.52.12
NSO	6.1.11

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 9 section.

Verified Compatibility

Products	Version
ADC Plugin	2.74.2.2209
RCM	2024.03.0
Ultra Cloud Core SMI	2024.03.1.12
Ultra Cloud Core SMF	2024.03.0

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
Enable IP Source Violation for Uplink Packets	The IP Source Violation feature on cnSGWc allows UPF to check if the origin of uplink packets is from the correct subscriber. This feature enhances the security and privacy of subscribers by preventing the leakage of their data to unauthorized parties. This feature further reduces the risk of legal and regulatory issues for the service provider by complying with lawful interception requirements. **Default Setting**: Disabled – Configuration Required to Enable
Initiate PFCP Association Release Request from UPF	This feature lets UPF to send notifications to cnSGWc and SMF on PFCP Session Release. This notification indicates to clear the calls simultaneously in UPF and SMF, or UPF and cnSGWc. If SMF or cnSGWc is not notified, the call remains connected until UPF receives the next Session Modify Request from SMF or cnSGWc. This leads to loss of subscriber usage reports. Here, the Enhanced PFCP Association Release (EPFAR) feature improves the signalling efficiency and effective handling of usage reports by SMF or cnSGWc. **Default Setting**: Disabled – Configuration Required to Enable
UCS C220 M7 Server Qualification	In this release, UPF is functionally qualified on the Cisco UCS C220 M7 server. The Cisco UCS C220 M7 Rack Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization and bare-metal applications.

Feature	Description
User Access Control through SGACL	UPF supports Cisco ISE integration for SGACL (Secure Group Tag-based Access Control List) enforcement on the downlink packets. SGACL controls and manages the authorization of security group members. UPF fetches the SGACL matrix from ISE through an API query based on Destination SGT (D-SGT). SMF sends the D-SGT value to UPF over Sx or N4. UPF then applies the SGACLs based on the D-SGT and S-SGT (Source SGT) mapping for downlink packets. Therefore, you can enable policy enforcement from Cisco ISE. **Default Setting**: Disabled – Configuration Required to Enable

Behavior Changes

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

Behavior Change	Description
IP Chunk Processing at UPF	**Previous Behavior:** UPF did not have a comprehensive validation criterion to process requests from SMF during IP chunk deletion or allocation. **New Behavior:** The robustness of UPF is improved to prevent corruption of chunk lists. UPF rejects or ignores any incorrect requests from SMF, and only processes requests with correct parameters. The parameters include peer address, VRF name, chunk ID, chunk size, and start address. This release supports the following new commands and logs: • The **show ip chunks all-vrf** command lists all IPv4 chunks under each VRF in the configured context. • The **show ipv6 chunks all-vrf** command lists all IPv6 chunks under each VRF in the configured context. • VPN error logs to track errors: • Event ID 5585 is reported when conflicting chunk add request (mismatched parameters) is received at UPF VPNMgr. • Event ID 5586 is reported when conflicting chunk delete request (chunk-id mismatch) is received at UPF VPNMg. • Event ID 5587 is reported when conflicting chunk delete request (chunk-id matches but other parameters are mismatched) is received at UPF VPNMgr. • Event ID 5588 is reported when invalid prefix allocation request is received at UPF VPNMgr for which the chunk is not yet allocated. • Event ID 5589 is reported when invalid prefix release request is received at UPF VPNMgr for which the chunk is not yet allocated.

Behavior Change	Description
Elimination of Hash Entries in VPP for ICMPv6 Flows	**Previous Behavior:** The session manager created both stream and hash entries in VPP for ICMPv6 data flows. **New Behavior:** For ICMPv6 data flows, the session manager only creates the streams and does not create hash entries in VPP. This behavior ensures uniform ICMPv4 and ICMPv6 data flow, and reduced number of hash entries.

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.

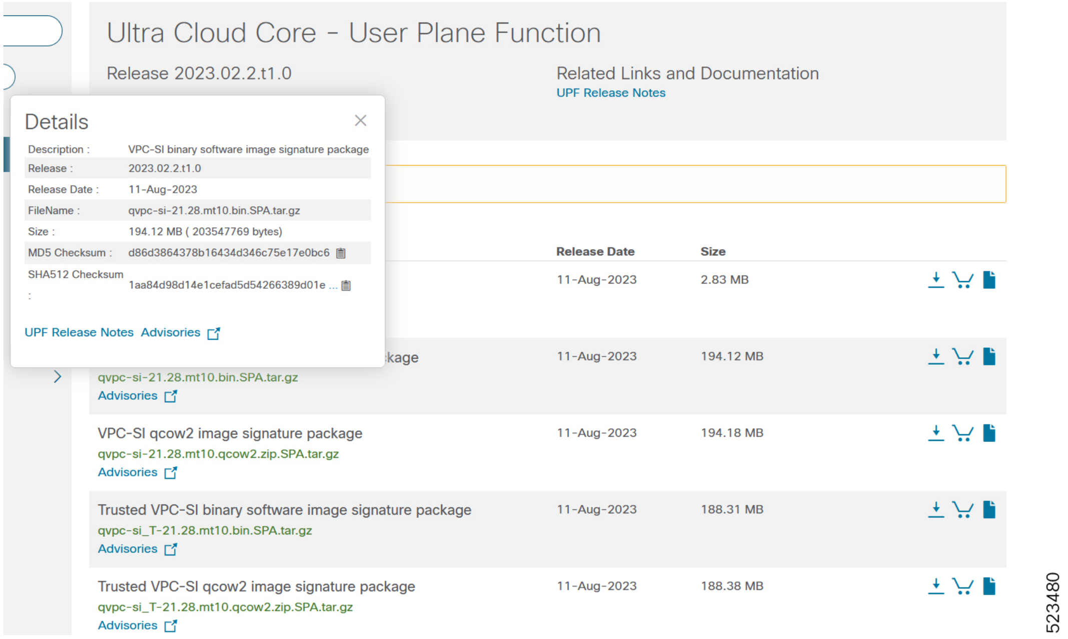
Software Integrity Verification

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:



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 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: `> 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 (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 open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwi68993	OHR not displayed post sessctrl/sessmgr recovery for Sxa Access PDR created midsession

Bug ID	Headline
CSCwj44610	Pkt on the new flow getting charged eventhough flow action is configured with terminate-flow
CSCwj60896	sx-demux instance goes in OVER state while doing srp switchover
CSCwj89977	Sx heartbeat is not always seen though it is enabled
CSCwk07729	UPF statistics are not showing correct value of converged calls.
CSCwk27158	Continuous sxdemux error logs "MISMATCH: IMSI ENTRY [SMGR-ID:10 IMSI:123456773200320]"
CSCwk27555	Incorrect reporting when reporting trigger is changed for a URR.
CSCwk30363	Error log: Sessmgr-1: [CDR 1966 - URR ID -2147483646] seen while Usage updation on Session delete
CSCwk63546	mTLS connection breaks after multiple swo
CSCwk66799	UPF performance improvement for DATA call model
CSCwk67358	UPF Monitor Subscriber logs are unavailable when W - UP PCAP Trace (ON) is enabled at CP
CSCwk74985	Hatsystem throws error at hatsystem_process_card_fail_msg()
CSCwk83794	PDN Released stats are not pegged in show user-plane-service stats in ERIR release
CSCwk84615	vpnmgr resiliency event takes around 9-10 min to program the vrf

Resolved Bugs for this Release

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

Note This software release may contain resolved 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	Behavior Change
CSCwj56071	Old timestampd and incorrect load in load reporting in some scenario during ICSR switchover.	No
CSCwj60766	VPP and hatsystem restart while doing UPF build upgrade to latest	No
CSCwj66773	CNSGW charging has issues in ICSR/Modify bearer rejection scenario.	No

Bug ID	Headline	Behavior Change
CSCwj81778	vpnmgr throws error at vpnmgr_rcm_send_msg_pool()	No
CSCwj83319	UPF vpnmgr crash during Sxa_Sxb_N4_Link_Flap "vpnmgr_release_cups_up_ip4_by_addr()"	Yes
CSCwj96763	sx monitor is not detecting sx interface down after sxdemux restart	No
CSCwk23684	Incorrect logs when user plane service goes down	No
CSCwk23718	Sessmgr restart at sessmgr_uplane_lc_counters_update_for_clp()	No
CSCwk27237	Continues sessmgr error log on new active rcm UPF "Peer version is not populated yet" post swo	No
CSCwk28656	No Online Offline URRs created on RAR modify when another ADC rule exists with same RG/SI	No
CSCwk30067	sessmgr restart seen at smgr_uplane_check_for_handover()	No
CSCwk30067	sessmgr restart seen at smgr_uplane_check_for_handover()	No
CSCwk31685	FP stats accounted against rulematch / flow but not in ACL	No
CSCwk40563	Negotiated EPFAR not effective post UPF Switchover	No
CSCwk42150	IP chunks are not getting allocated to HUPF after clear sx-association	No
CSCwk45098	Issue is seen when epfar capability is disabled when PFCP association is down	No
CSCwk46887	Bulkstats counter for qci1 are not getting fetched correctly	No
CSCwk47110	Sessmgr throws error at acsmgr_dcca_srp_config_wait_timer()	No
CSCwk47258	SGACL ICSR Active Standby issues	No
CSCwk47303	SGACL update doens't work for existing streams when ACL is changed mid-session	No
CSCwk48476	UPF doesn't update SGACL when mid-flow SGT changes for a drop state stream	No
CSCwk48737	TCP based flows are matched against wrong ACL as SSGT is not considered	No
CSCwk52911	ssgt set to 256 when no SSGT is received in DL paket earlier it was zero	No
CSCwk55661	Sessmgr restart at sessmgr_uplane_process_sx_update_far_update_tep_teid_n4	No

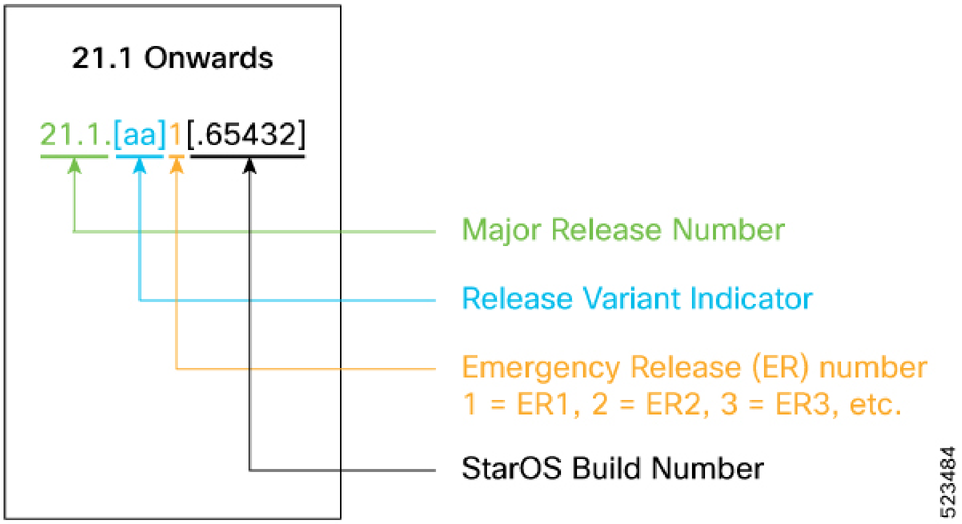
Bug ID	Headline	Behavior Change
CSCwk61579	SGACLs not getting updated during refresh despite different genID received	No
CSCwk61791	Post mid session de-association and apimgr recovery, ACL defs are seen for new call	No
CSCwk62069	Difference in behaviour of icmpv4 vs icmpv6 while creating hash entry in vpp.	Yes
CSCwk62728	N3IWF: SMF is encoding incorrect Rat-Type, for N4 Modify procedure triggered by PCF	No
CSCwk62888	UPF doesn't apply refresh timer for new calls when old call query fails during retries	No
CSCwk63070	Incorrect sgacl rule match on the default sgacl change	No
CSCwk63859	DL Pkts dropped at Sessmgr with Ip readdressing and deny ACL configured on DL	No

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 5x00 or Cisco Virtualized Packet Core platform.

The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".

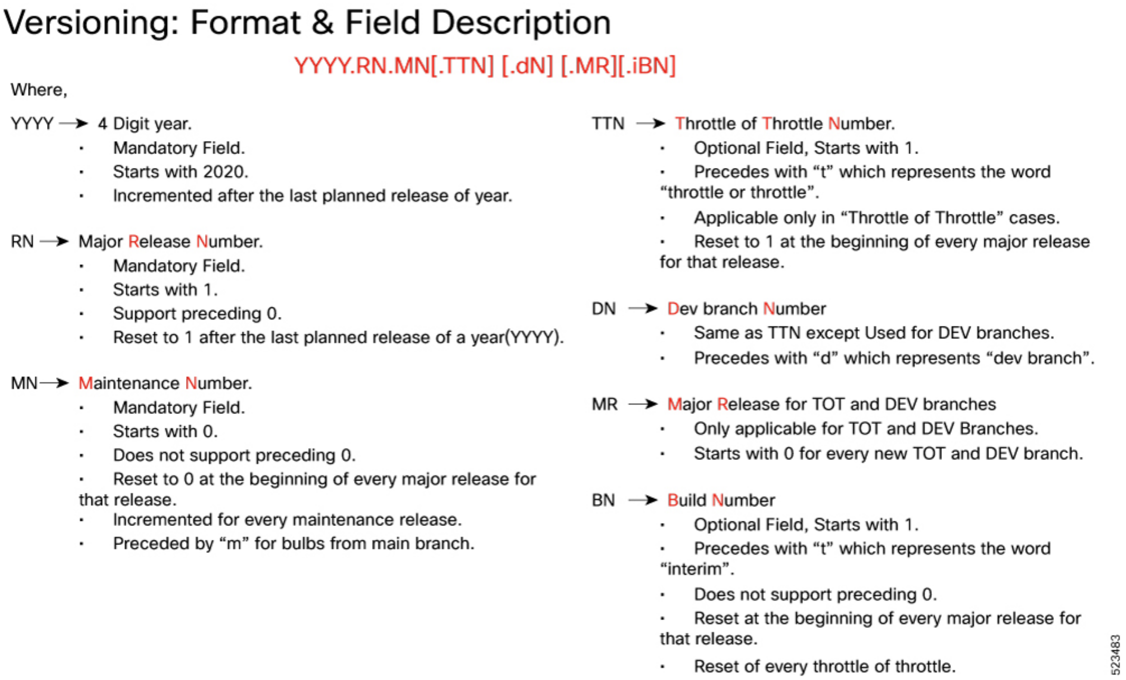

21.1 Onwards
21.1.[aa]1[.65432]
Major Release Number
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number
523484

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.

Note The 5G UPF software is based on StarOS and implements the version numbering system described in this section. However, as a 5G network function (NF), it is posted to Cisco.com under the Cloud Native Product Numbering System as described in Cloud Native Product Version Numbering System, on page 9.

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.

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.
qvpc-si-<staros_version>.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.
qvpc-si-<staros_version>.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.
ncs-<nso_version>-cisco-staros-<version>.signed.bin	The NETCONF NED package. This package includes all the files that are used for NF configuration. Note that NSO is used for NED file creation.

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.