UCC 5G UPF Release Notes, Release 2024.02.0

First Published: 2024-04-30

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-2024
End of Life	EoL	30-Apr-2024
End of Software Maintenance	EoSM	29-Oct-2025
End of Vulnerability and Security Support	EoVSS	31-Oct-2025
Last Date of Support	LDoS	31-Oct-2026

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-21.28.m23.tgz.SPA.tar.gz	21.28.m23
qvpc-si-21.28.m23.bin.SPA.tar.gz	21.28.m23
qvpc-si-21.28.m23.qcow2.tgz.SPA.tar.gz	21.28.m23
NED package	ncs-6.1.3-cisco-staros-5.52.9
NSO	6.1.3

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 10 section.

Verified Compatibility

Products	Version
ADC Plugin	2.74.0.2084
RCM	2024.02.0
Ultra Cloud Core SMI	2024.02.1.14
Ultra Cloud Core SMF	2024.02.0

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
ADC Dynamic Rules over N4	UPF leverages the dynamic ADC rules for traffic matching and charging. This feature allows the service providers to manage IoT devices, such as connected cars, and charge their subscribers based on the traffic flows classified by SMF or UPF. With this traffic classification, the service providers enable service monetization. In summary, SMF first processes the dynamic ADC rules received from PCF with TDF-App-Identifier, Service ID, and Rating group. SMF then sends this information to UPF to classify ruledefs and perform charging. **Default Setting**: Enabled – Always-on
Charging Support for Converged Calls	UPF supports S-GW Charging Data Record (CDR) volume reporting for converged calls. This feature allows you to use these CDRs for reporting and charging during inbound LBO roaming scenario. This feature introduces a new CLI command **converged-sxa-usage-reporting** in the ACS Service Configuration mode, to generate the usage report with volume count. **Default Setting**: Disabled – Configuration Required to Enable
Dual Stack Support on S5u Interface	UPF supports dual stack to handle IPv4 and IPv6 connections between SGW-U and PGW-U on the S5u interface. **Default Setting**: Enabled – Always-on

Feature	Description
EDR Attributes for DSCP Mapping	UPF supports two new EDR attributes **sn-dscp-uplink** and **sn-dscp-downlink** as part of Flow and Transaction EDRs in the EDR Format configuration. These attributes help you to understand the QoS flow information of uplink and downlink traffic in the network. The attributes report the DSCP mapping value of the user plane traffic. UPF derives the DSCP values either from SMF through the Transport Level Marking AVP in FAR or locally through the IP ToS configured under charging-action. **Default Setting**: Disabled – Configuration Required to Enable
EDR Attribute for S-NSSAI Reporting	UPF supports a new EDR attribute **sn-nssai** as part of Flow and Transaction EDRs in the EDR Format configuration. This attribute reports the S-NSSAI value that UPF receives from SMF in PFCP Session Establishment Request. **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
Accurate Correlation of Application Instance IDs for Traffic Optimization	When you configure the **adc app-notification once-per-app** CLI in ACS Rulebase, UPF optimizes the reporting once per application. Upon detecting traffic for an application, UPF sends an APP-START notification to SMF with an Application Instance ID. This ID is the flow-id for the first data flow of an application. **Previous Behavior**: When the last data flow of the application gets terminated, the flow-id of that data flow is used as the Application Instance ID in APP-STOP notification. This causes issues for PCF to correlate the APP-START and APP-STOP notifications. **New Behavior**: UPF caches the Application Instance ID from the first data flow. When the last data flow of an application terminates, UPF sends the cached Instance ID with the APP-STOP notification. This behavior enables PCF to correlate the APP-START and APP-STOP notifications and identify the application traffic appropriately.
GTPU Statistics for Combo Calls	**Previous Behavior**: For combo calls on the N4 interface, the count for uplink and downlink packets/bytes were not incremented correctly in the **show user-plane-service gtpu statistics** CLI output. **New Behavior**: For combo calls on the N4 interface, the count for uplink and downlink packets/bytes will be incremented three times for each GTPU interface. The fields Uplink Packets, Downlink Packets, Uplink Bytes, and Downlink Bytes in the **show user-plane-service gtpu statistics** CLI output will display the correct packet count.

Behavior Change	Description
LCI Reporting to Control Plane	UPF sends the load control information (LCI) to the control plane, to inform the operating status of its resources at the node level. The control plane uses this information to augment UPF selection procedures. **Previous Behavior**: UPF reported only one LCI per session manager to the control plane because of which some associated CPs did not receive the LCI. **New Behavior**: UPF reports one LCI to each PFCP peer per session manager. The control plane will be able to distribute calls evenly over multiple UPFs. • For cnSGW or legacy S-GW, LCI is reported only if the CP sends the load bit in the CP Function Features IE during Sx Association Setup or Update. • By default, UPF enables LCI reporting to SMF. Hence, the load bit in CP Function Features IE is optional for SMF. • The debug CLI **show session subsystem facility sessmgr all debug-info** displays the current and reported load metrics on UPF. • Error logs will be generated when the load metric is reported to the control plane. The following is an example of an error log: `2024-Mar-15+08:12:54.517 [sx 221333 info] [1/0/8083 <sessmgr:6> sx_fsm.c:1311] [context: EPC2-UP, contextID: 2] [software internal system critical-info syslog] LCI with load-metric = 19 and sequence-number = 1710489965 sent to Peer: 20.20.20.54` **Customer Impact**: Each CP that supports LCI reporting will now receive multiple messages with the same LCI value from a UPF.
Redirected Packet Drop Statistics	**Previous Behavior**: The drop counters were not incremented for redirected packets when the **flow action redirect-url** CLI was configured. **New Behavior**: The drop counter is incremented for redirected packets with the **flow action redirect-url** configuration. The new **Redirect-URL** field under **Flow apply action** in the output of the **show user-plane-service statistics drop-counter** command displays the number of redirected packets that are dropped. **Customer Impact**: For each redirected packet, you can view the incremented packet drop counter.

Behavior Change	Description
SxDemux Stops IP Pool Deregistration Request towards VPNmgr on Standby UPF	**Previous Behavior**: After receiving the Sx peer delete checkpoint, SxDemux initiated the IP pool deregistration request towards VPNMgr on a standby UPF. This behavior led to IP chunk deletion resulting in call preallocation failure on a standby UPF. **New Behavior**: SxDemux does not initiate IP pool deregistration request towards VPNMgr on a standby UPF, after receiving the Sx peer delete checkpoint. This behavior prevents call preallocation failure on a standby UPF.

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.

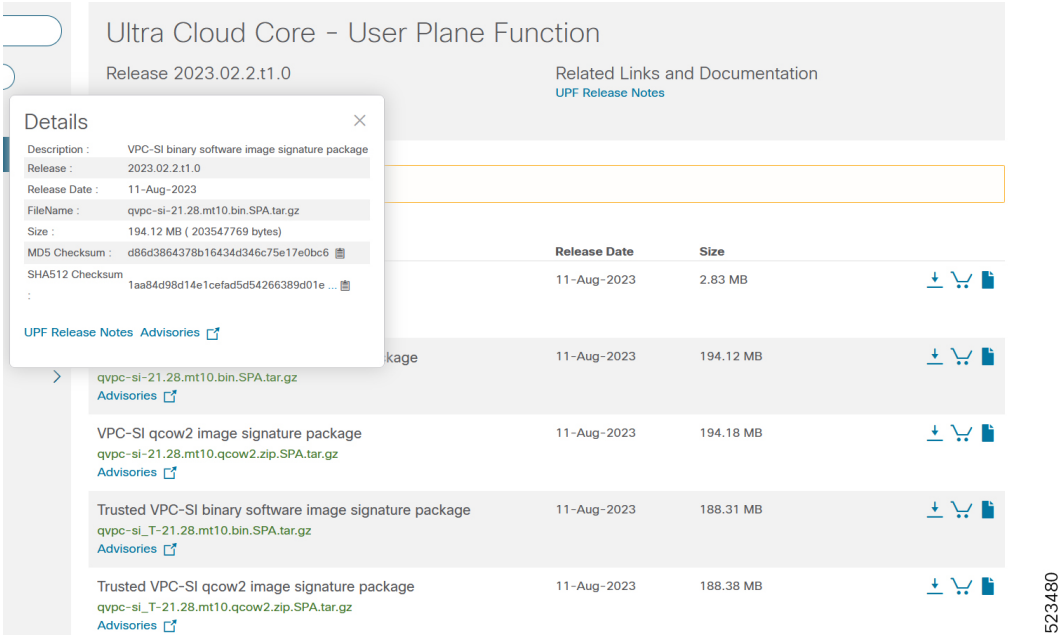
Software Integrity Verification

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:



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
CSCwf08057	Observed Update FAR not found with FAR ID

Bug ID	Headline
CSCwh02919	4g converged and non converged calls getting drop with echo req/res on MPLS over N9
CSCwh25088	VUPF doesn't update proper counts in show user-plane-service statistics for RA packet
CSCwi59700	SN-Charge volume parameter in EDR is wrongly pegged in case of flow redirect and delay charging
CSCwi68993	OHR not displayed post sessctrl/sessmgr recovery for Sxa Access PDR created midsession
CSCwi80353	sessmgr is in over state post sessmgr task kill
CSCwi99148	callid 00004e21 adc statistics CLI not working,adc app failure statistics required at userplane stat
CSCwj04184	UPF doesn't report volume measurement when dynamic ADC rule removal happens mid-session
CSCwj16848	StarOS is not supporting wild card character in Password in EDR push
CSCwj17224	SNMP sysLocation was not updated by change system location
CSCwj17471	Planned srp switchover is succeeded though bgp monitor in stby upf is down
CSCwj32627	Sgw Charging for predefined dedicated bearer is getting additionally accounted in default bearer URR
CSCwj44610	Pkt on the new flow getting charged eventhough flow action is configured with terminate-flow
CSCwj56071	Old timestamp and incorrect load in load reporting in some scenario during ICSR switchover
CSCwj60766	VPP and hatsystem restart while doing UPF build upgrade to latest
CSCwj60896	sx-demux instance goes in OVER state while doing srp switchover
CSCwj66773	CNSGW charging has issues in ICSR/Modify bearer rejection scenario
CSCwj72602	UDP data is not seen in fast path pcap while its seen in show cli
CSCwj78716	Sessmgr error logs on UPF [N4] UE IP Address is different in PDR with PDR ID 0x1e2
CSCwj81778	vpnmgr throws error at vpnmgr_rcm_send_msg_pool()

Resolved Bugs for this Release

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

Note This software release may contain bug fixes first introduced 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
CSCwf99786	Bulkstats docs cuto-dnlink-forward, cuto-dnlink-tx, cuto-dnlink-rx, cuto-dnlink-hold insufficient	No
CSCwi03248	Some of non-std QCI bulkstats counters are zero	No
CSCwi10931	UPF GTPU statictis displays incorrect Downlink Packets / Bytes counters	Yes
CSCwi47535	First-Packet-Time is wrongly set for RB URR whn recal measmnt IE is receivd & data sent again	No
CSCwi59951	TCP length issue in DNS query causing time out	No
CSCwi63250	Despite "monitor system card-fail" config, switchover does not occur	No
CSCwi65052	Unable to open the btmp file /var/log/btmp	No
CSCwi75020	Data drop is seen on UPF, when Pure p call (using cnPGW) attached with Dual stack cli	No
CSCwi83803	UPF rejects SX Modification Request msg to install ADC Dynamic Rule from SMF	Yes
CSCwi94430	Need to stop IP chunk deregistration reqest on sxdemux on standby chassis	Yes
CSCwi97129	Application instance identifier correlation is incorrect with ADC optimization	Yes
CSCwi99071	Crash observed in UPF when 14 dynamic ADC rules are sent from SMF	Yes
CSCwj01285	UPF doesn't display TDF / ADC related information in PDR cli	No
CSCwj03102	UPF needs to send LCI to all supported CP	Yes
CSCwj12799	UPF behavior not correct to flip the byte order in ID field	No
CSCwj24604	sessmgr restart at sessmgr_uplane_threshold_check_and_reset_hcf()	No
CSCwj24690	sessmgr restart observed at sessmgr_uplane_periodic_reset_counter_values	No

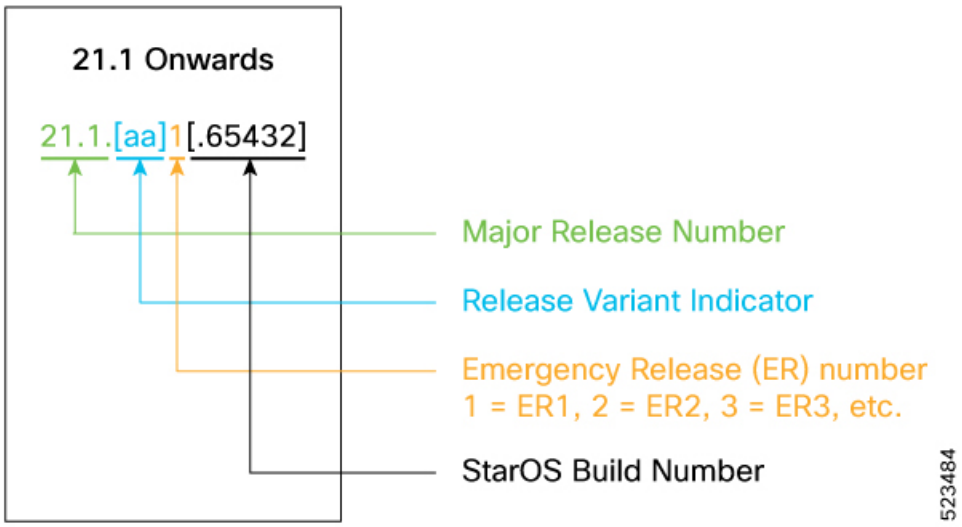
Bug ID	Headline	Behavior Change
CSCwj38192	IMEI value truncated and congestion level IE seen in show CLI for a call post UPF recovery	No
CSCwj38533	SMF sends CDR with timestamp of 1970-01-01 for first and last usage,_User Plane Functions_21.28.M16	No
CSCwj60743	FAPI err log on 4G Combo call: fapi_tp_process_sync_row_request() returned error 0x80002001	No
CSCwj85083	npumgr crashes after upgrade to 21.28.m22	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".

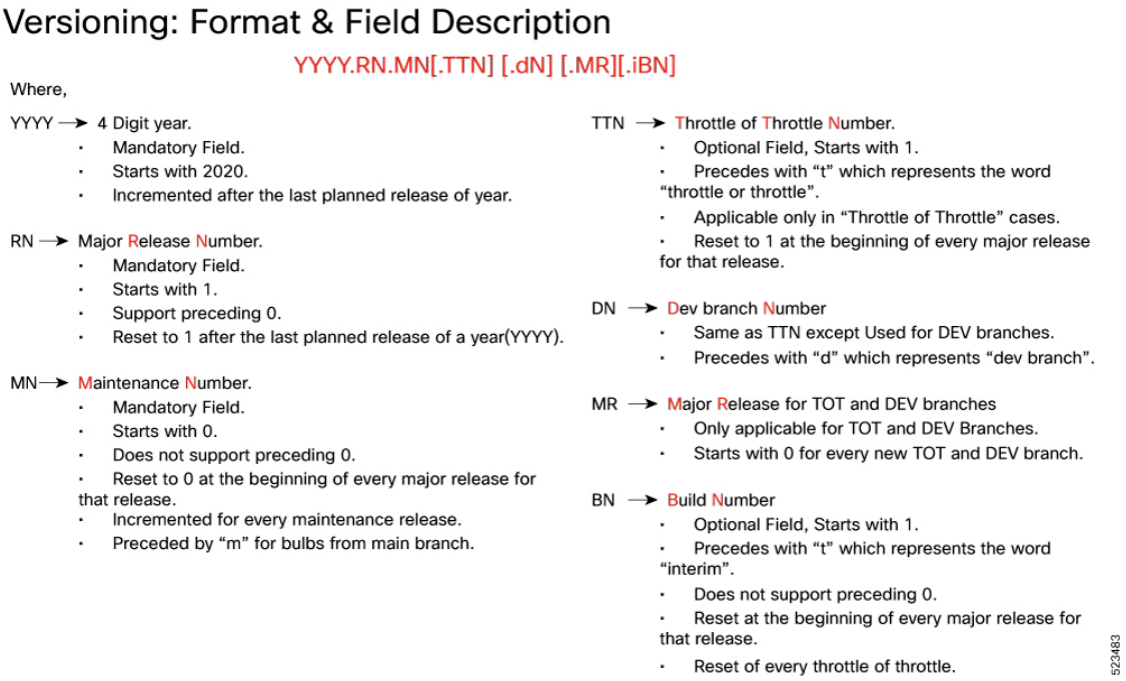


The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 10.

Cloud Native Product Version Numbering System

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



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.

Software Packages	Description
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.