Release Notes for the 5G Converged Core Session Management Function Version 2023.04.0

First Published: 2023-10-17

5G Converged Core Session Management 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-Oct-2023
End of Life	EoL	31-Oct-2023
End of Software Maintenance	EoSM	30-Apr-2025
End of Vulnerability and Security Support	EoVSS	30-Apr-2025
Last Date of Support	LDoS	30-Apr-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
ccg-2023.04.0.SPA.tgz	2023.04.0
NED package	ncs-5.6.8-ccg-nc-2023.04.0 ncs-6.1-ccg-nc-2023.04.0
NSO	5.6.8 6.1.3

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 11 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2023.04.1
Ultra Cloud CDL	1.11.5
Ultra Cloud Core UPF	2023.04.0
Ultra Cloud cnSGWc	2023.04.0

For information on the Ultra Cloud Core products, refer to the documents for this release available at:

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-serving-gateway-function/products-installation-and-configuration-guides-list.html

What's New in this Release

New in Documentation

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all the 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.01, the RCR document will be deprecated.

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
SMF	
Creation of GBR Bearer Based on Local Policy	SMF allows creating GBR bearers based on local policies in 4G and 5G RATs. **Default Setting**: Disabled – Configuration required to enable
DRB Level Data Forwarding in IDFT for N2-based Handover	SMF supports DRB level data forwarding, in case the Data forwarding response DRB List is present in the Handover Request Acknowledge message and it doesn't meet the criteria for Session Level Forwarding.

Feature	Description
MBFR, Semantic and Syntactic Error Handling for 4G and 5G	SMF handles MBFR, semantic and syntactic errors in QFI, QoS and indicates 5GSM cause. Configurations using event names, rules, and actions are included for 4G and 5G errors. **Default Setting**: Disabled – Configuration required to enable
Minimizing SMF and PCF interactions on the N7 interface	For the N7 optimization support, the SMF skips the N7 Update message by sending the UE IP address in the N7 Create message. **Default Setting**: Enabled – Always-on
Minimizing SMF and UDM interactions on N10 interface through fail open support	With the fail open feature, the SMF supports the ignore and continue failure handling actions as well for the call during the N10 message failures. These failures include the UDM registration, Subscriber Fetch, and Subscribe to Notify for all RAT types. **Default Setting**: Enabled – Always-on
Minimizing Session Loss During Application VIP switchover	The High Availability redundancy support is enhanced in SMF in a way that when the gRPC IPC stream breaks, the App-Infra library retries immediately and the IPC connection is reestablished between gRPC endpoints within milliseconds.
N4 Resource or Association Release	SMF supports clearing resources related to a particular UPF from the SMF using a CLI **release-resource**. **Default Setting**: Disabled – Configuration required to enable
Network Address Translation Binding Updates	SMF supports NAT Binding Record functionality where, N4 Session Report Request Message is used for providing NAT Binding Record Information from UPF to SMF. After SMF receives NAT Binding Record Information from UPF, it sends the corresponding NAT Binding Updates to the AAA Server over the RADIUS interface. **Default Setting**: Disabled – Configuration required to enable
SBI Message Priority Enhancement	The SBI Message Priority (SMP) mechanism uses the "3gpp-Sbi-Message-Priority" custom HTTP header to set and carry the message priority between the client and the server. The custom HTTP header enforces the message priority end to end between the client and the server through one or more proxies. **Default Setting**: Disabled – Configuration required to enable
Support for ePCO length and Local IP in TFT	SMF allows ePCO length with two octets for QoS rules and QoS descriptions and indicate local IP address in TFT. **Default Setting**: Enabled – Always-on
cnPGWc	

Feature	Description
Asynchronous and Synchronous Usage Report for Offline Bearer Recalculation	As part of Gz Usage Reporting, SMF receives Asynchronous and Synchronous Usage Reporting for Offline Bearer recalculation. **Default Setting**: Disabled – Configuration required to enable
EGCDR Final Record Closing Cause	This feature allows you to send a unique record closure reason for final CDR through CLI configuration. **Default Setting**: Enabled – Always-on
Final Unit Indication (FUI) support in CCR-U	As part of Gy Usage Reporting, SMF supports FUI in CCA-U from OCS.FUI is enabled or activated during the session creation or update. After FUI activation, when there's any update triggers due to an event trigger or Usage report, SMF sends subsequent CCR-U toward OCS without requesting further Quota and receives CCA-U.
Gz Default Bearer Modification	This feature allows PCRF-initiated modification of a default Bearer through Gx CCR-U and Gx RAR. You can perform the following functions: • Add rules to the Default Bearer • Delete rules from the Default Bearer • Rulebase Modification • Default-bearer QoS change • APN-AMBR change
HSS-Initiated Bearer QoS Modification	SMF supports the HSS Initiated Bearer QoS Modification procedure to modify APN-AMBR and optionally one or more of the EPS Bearer QoS parameters. **Default Setting**: Enabled – Always-on
Handling Modify Bearer Request Triggers	SMF receives the Modify Bearer Request from S-GW for the User Location and TimeZone changes, change notifications. SMF supports N4 Query Interface and Recalculate Interface IEs for Rulebase change, Secondary RAT Usage limit, and Record closing triggers. **Default Setting**: Disabled – Configuration required to enable
Periodic Report of Secondary RAT Usage	This feature allows SMF to handle periodic Secondary RAT data volume report messages from the MME over the S5 or S8 interface in the Modify Bearer Request, Change Notification Request, Delete Session Request, and Delete Bearer Response **Default Setting**: Disabled – Configuration required to enable

Feature	Description
Same dictionary support extended to RAR messages.	In the previous releases, for CCR-I, CCA-U, and CCA-T messages, the dictionary specified under the client, which is a custom dictionary, was applied. For a RAR message, a common dictionary was being used. With this release, RAR messages also use the same dictionary that CCR-I, CCA-U, and CCA-T messages use.
Use of Credit-Control-Failure-Handling AVP for Gy request failure handling	The SMF uses the value of Credit-Control-Failure-Handling AVP to derive the Gy request failure handling behavior when the requests are prevented due to a network problem. **Default Setting**: Enabled – Always-on
VRF support for Diameter Gx and Gy interfaces	SMF supports the client-side VRF for the Diameter Gx and Gy interfaces. The profile Diameter endpoint refers to the VRF name and interface name that you configure from the Diameter endpoint. The Diameter endpoint uses the VRF name to create a TCP connection from the Diameter client. **Default Setting**: Enabled – Always-on
Zero CDR Suppression Support on the Gz Interface	This feature allows you to suppress CDR records based on the **egcdr suppress-cdrs zero-volume** CLI. **Default Setting**: Disabled – Configuration required to enable

Behavior Changes

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

Feature	Description
Call Handling in the Absence of PCF Configuration in DNN Profile	**Previous Behavior**: SMF mandated the configuration of PCF/PCRF in DNN profile even when the local policy was configured through the **pcf-interaction** command. **New Behavior**: PCF or PCRF configuration remains optional if the local policy is configured. Subscriber call setup is successful even in the absence of PCF or PCRF configuration in the DNN profile.
DLDR Handling for N3 Connection Reactivation	**Previous Behavior**: SMF didn't trigger the N1N2 setup request on the N11 interface when UPF received the Downlink Data Request (DLDR). The difference in the upContext state between SMF and UPF resulted in UPF triggering the DLDR. With the N3 in an inactive state, UPF used to send the session report request to SMF. **New Behavior**: The new CLI command **reactivate-n3-on-dupl-activation-dldr** is added in the supported features at SMF to reactivate the N3 when DLDR is received in the N3 activated state. After this CLI is enabled and if the DLDR is received in the ACTIVATED state, then SMF changes the upState to DEACTIVATED and reactivates the N3 connection.

Feature	Description
DWR/DWA Message Handling	**Previous Behavior**: Diameter peer was considered down only if sending Device Watchdog Request (DWR) failed. Even if the Device Watchdog Answer (DWA) wasn't received or was received with an error result-code, the peer wasn't considered in the error state. **New Behavior**: In addition to the failure in sending a DWR, even if the DWA isn't received or is received with the error result-code, the peer is considered to be in the error state.
Non-Standard PLMN List Configuration for MccMncExceptionList Dynamic Update	**Previous Behavior**: No CLI command existed for the nonstandard PLMN values. **New Behavior**: The new **non-standard-plmn-list** CLI command is added in the SMF profile. Use this command to enable SMF to update the MccMncExceptionList dynamically.
Processing GTPv2 Modify Bearer Request Messages	**Previous Behavior**: At the time of GTPv2 MBReq message processing, Modify Bearer Request (MBR) from a Visitor PLMN (V-PLMN) or any PLMN was accepted by PGW-C+SMF. **New Behavior**: If the inter-plmn CLI isn't configured in PGW-C+SMF, MBR from a V-PLMN is rejected by PGW-C+SMF. To handle handovers from V-PLMN, configuring the **inter-plmn-ho** in the DNN profile is mandatory.
QER Request Creation to UPF During N4 Session Establishment	**Previous Behavior**: If the predefined rules are mapped to a dedicated flow or dedicated bearer, the SMF didn't send the Create QER Request to the UPF. **New Behavior**: If the predefined rules are mapped to a dedicated flow or dedicated, the SMF sends the Create QER Request for both default and dedicated flows to the UPF.
Routing CCR-U/CCR-T Message to the Bounded Peer from CCR-I/U or CCA-I/U Message	**Previous Behavior**: No bounded peer existed. **New Behavior**: The peer with which the last CCR-I/U interaction happened is considered as the bounded peer. Route matching the bounded peer is given the highest priority for sending subsequent CCR-U/T messages.
Statistics Updates for Internal Transaction Triggered for RAR Scenario	**Previous Behavior**: When the Modify Bearer Request (MBR) or Modify Bearer Command (MBC) triggered a RADIUS update towards the RADIUS accounting server, the **procType** label was updated as PDU Session Modify - SMF initiated. For Gy metrics, the **proc_name** label displayed the PDU Session Modify - SMF initiated value. **New Behavior**: The new statistics **PDN Session Modify - PCRF initiated** is added for this scenario.

Feature	Description
Wait Time Display for Ongoing Bulk clear Subscriber CLI and Blocking the Consecutive CLI	**Previous Behavior**: The Ops Center didn't display the expected waiting time for an ongoing bulk **clear subscriber** CLI command. In addition, you could run the **clear subscriber** CLI while the processing of the earlier CLI was still in progress. **New Behavior**: The Ops Center displays the expected waiting time for an ongoing bulk **clear subscriber** CLI command. In addition, the **clear subscriber** CLI gets blocked while the processing of the earlier CLI is in progress. **Customer Impact**: Ease of use and maintenance in processing of the subscriber profiles.

Related Documentation

For the complete list of documentation available for this release, see https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/products-installation-and-configuration-guides-list.html.

Installation and Upgrade Notes

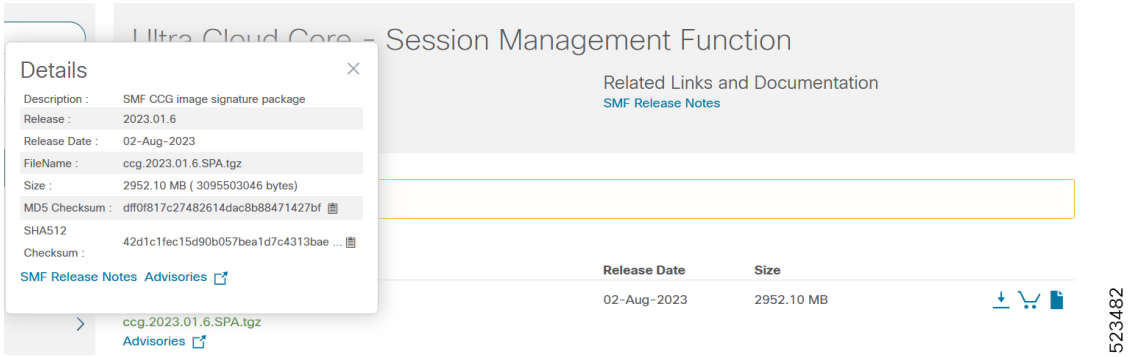
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Note ETCD v3.5.x does not support in-service downgrade to 3.4.x. If you are downgrading from 2023.04.0 builds to previous releases, perform system mode shutdown before downgrade.

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.



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: Checksum Calculations per Operating System 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 table below.

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`

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.

Certificate Validation

SMF 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
CSCwf93945	Observing CC69 mandatory-IE failures in N4 during cdl ep, index rollout test
CSCwh84424	RS-RA does not work when N4 VIP in VRF

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.

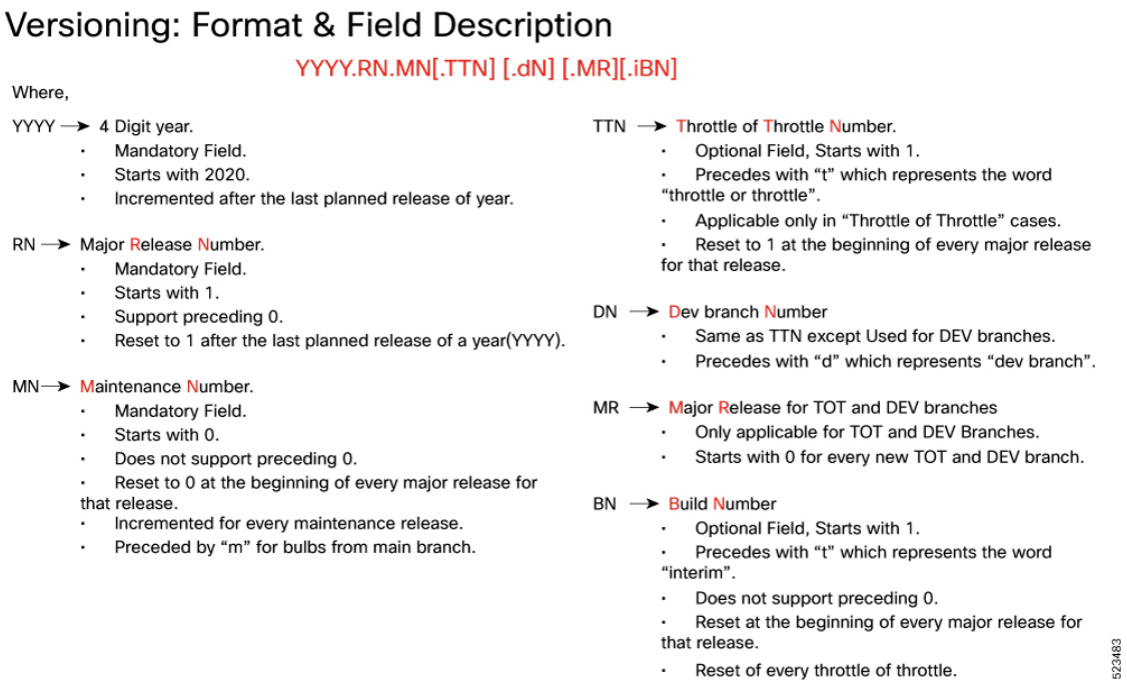
Bug ID	Headline	Behavior Change
CSCwf22947	Route CCR-U/CCR-T to the bound peer from CCR-I/CCA-I	Yes
CSCwf90525	MBC msg not displayed with mon sub	Yes
CSCwf92324	Incorrect sequence number observed in UBReq which was triggered for MBC	Yes
CSCwh01133	BEARER_QOS IE is seen in UBReq msg, even when def QoS is not changed	Yes
CSCwh37515	Radius/Gy stats LABEL procType/proc_name is getting updated for "PDU Session Modify - SMF initiated"	Yes
CSCwh43258	GTPv2 Retry/Retransmit behavior for CNR	Yes
CSCwh49329	SMF opscenter timed out to display output of show rpc all command	No
CSCwh53385	RS not replied during WLAN to 4G HO with active voice-call	No
CSCwh53948	SGW_POD Restart after DIMM error causing IPC Streams failed on gtpc-ep1 streams to sgw-Service	No
CSCwh66800	SMF-Service pod crash with Panic Message during WIFI to NR HO - MsgPduSessionReleaseRequest	No

Bug ID	Headline	Behavior Change
CSCwh68478	Gy ep pod is in CrashLoopBackOff error	No
CSCwh69654	SMF sending DSResp with incorrect h-teid for DSREq from ePDG received post wlan to 4g HO	No
CSCwh72328	Diameter peer down detection criterion in SMF	Yes
CSCwh78460	IPC stream down observed between sgw-service(s) to s11-gtpc after disabling resmgr batch processing	Yes
CSCwh79228	[SMF] - session deletion during 5g-4g HO with Deactivate from AMF after MBR procedure	No
CSCwh81800	Charing char - policy match issue	No
CSCwh82366	SEPCF005 / SESMFM33 - MVNO IoT CC Integration on CNDP | PGW-C is sending wrong IMEI value in Radius Auth and Acct messages	No
CSCwh72362	SGW service reusing smf service ip after upgrade, results into sgw pod entry deletion from cache pod	No

Operator Notes

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.

Table 2: Release Package Information

Software Packages	Description
ccg.<version>.SPA.tgz	The SMF offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-ccg-nc-<version>.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration. Note that NSO is used for the 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.