Release Notes for the Ultra Cloud Core Session Management Function, Version 2024.02.0

First Published: 2024-04-30

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	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
ccg-2024.02.0.SPA.tgz	2024.02.0
NED package	ncs-5.6.8-ccg-nc-2024.02.0 ncs-6.1-ccg-nc-2024.02.0
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	2024.02.1.14
Ultra Cloud CDL	1.11.7
Ultra Cloud Core UPF	2024.02.0
Ultra Cloud cnSGWc	2024.02.0

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

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	
Event Failure Logs	SMF provides the following support: • Consistent event failure logs for Create, and Idle or Active procedures across pods • Configurable logs at pod type • Inclusion of request and response details in a single-line format The consistent error log message format across various pods helps in analytics and minimized number of log generations by the system. The single-line log format display enhances the readability. **Default Setting:** Not applicable

Feature	Description
Ga/N40 Interface Enhancement for correlation of the CGF Feeds	This feature enables GTPP-EP to support the CHF record with ASN1 encoding and send the record to the configured CGF server through GTPP protocol. GTPP-EP additionally supports the base features for CHF record, such as batcher for GTPP records, archival, peer management, and CGF selection. This feature will be consumed by the CHF service by invoking new APIs to send the GTPP CHF records.
P-CSCF Address Restoration and Re-Selection	SMF supports restoration and reselection of P-CSCF addresses when a P-CSCF failure event occurs. The CLI **pcscf-restoration trigger [UDM][action [mark-down]]** is used for configuring P-CSCF address reselection. This feature enables the 5G/4G/Wi-Fi RAT subscribers to restore a failed IMS connectivity with UE by connecting to a working P-CSCF address. **Default Setting:** Disabled – Configuration required to enable
Preemptive Quota Requests for Static and Predefined Rules	In SMF, Preemptive Quota is enabled by default for dynamic rules. Through this feature enhancement, SMF can request preemptive quota for static and predefined rules during the initial attach session creation procedure. The preemptive quota is configurable using the **preemptively-request-n-validate** command in the Charging Action Configuration mode. **Default Setting**: Enabled – Always-on
Rolling Upgrade Optimization	Converged Core Gateway provides the following support: • Retry mechanism at service and protocol pods during upgrades • Configuration-based rolling upgrade enhancements This optimization helps in reduced session and Call Events Per Second (CEPS) loss during the upgrade procedure. The configurable rolling upgrade enhancements enable smooth rollout of the changes. This feature introduces the new CLI command **supported-features [app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra]** in the converged core profile. **Default Setting:** Disabled – Configuration required to enable

Feature	Description
Selection of Alternate AMF	This feature allows the SMF to choose an available AMF from the set when the AMF connected to the UE experiences an outage. SMF performs AMF selection based on the configuration of query parameters or NRF query response local filters. This feature addresses the need for uninterrupted service continuity in the event of an AMF becoming unavailable. This feature introduces the following new CLI commands: • **filter-discovery-response filter match { all | any } attributes { target-nf-instance-id }** • **filter-discovery-response filter failure-action { use-discovery-response }** These configurations allow SMF to locally filter the received NRF discovery response and select the appropriate one which matches the configured filters. This feature additionally supports region and set ID configuration as part of NRF query parameters. **Default Setting**: Disabled – Configuration required to enable
Mobile IoT	
DNN Inheritance for 4G Sessions on Legacy Interfaces	SMF with legacy interfaces supports the DNN inheritance feature. **Default Setting:** Disabled – Configuration required to enable
Dynamic ADC Rules Over Gx Interface	SMF allows the users to install, modify, or remove the dynamic ADC rules. SMF forwards the new or updated rules to UPF for traffic classification. This feature allows the service providers to manage the IoT devices, such as connected cars, and charge their subscribers based on the traffic flows classified by SMF/UPF. With this traffic classification, the service providers enable service monetization. **Default Setting**: Enabled – Always On
M6 Server Performance and Scaling	With this release, the SMF (with Legacy Interfaces) was tested and validated for 5 million sessions scale for IoT use cases using the M6 based UCS systems with published call model including Modeled CEPS and DNN/IP pool configuration. **Default Setting**: Not Applicable
M7 Server Functional Qualification	With this release, the SMF (with Legacy Interfaces) was functionally qualified for IoT use cases using the M7 based UCS systems. **Default Setting**: Not applicable

Feature	Description
Troubleshooting GTP-C Services	This feature allows the cnSGW and SMF+PGW-C to send the GTPC test echo command to peer nodes to: • Troubleshoot and monitor the connectivity of peer nodes. • Test a Round Trip Time (RTT) of the peer. • Supports S11, S5E, S5, S2B and S8 GTPC interfaces, and IPv4 and IPv6 transport types. **Default Setting**: Enabled – Always On
Troubleshooting GTPP Services	This feature allows the SMF+PGW-C to send a GTPP test echo command to the CGF server to: • Troubleshoot and monitor the connectivity of CGF servers. • Test Round Trip Time (RTT) of the peer. **Default Setting**: Enabled – Always On

Behavior Changes

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

Feature	Description
Enhancing Local Policy Statistics for N7 Connectivity	**Previous Behavior**: SMF triggers the **local_policy** label as part of **smf_service_stats** to represent all the N7 connectivity event triggers. **New Behavior**: To provide more granular information on the various N7 events, the **local_policy** label is renamed as **policy_status**. The **policy_status** label has the following values: • **N7Skip**: Specify that the PCF interaction is disabled. • **N7DisableLocalPolicy**: Specify that a local policy is enabled or used. • **N7Active**: Specify that the PCF provided policies are used.
Event Trace Log for SMF-initiated PDU Session Release	**Previous Behavior**: The error log "EVENT TRACE for RelProcType" was generated for create over create scenarios, that is, when SMF initiates the PDU session release procedure for existing session. **New Behavior**: Error log "EVENT TRACE for RelProcType" is no longer added to avoid log flooding in a valid scenario of create over create.

Feature	Description
Handling Terminate Sub Action FHT in CCA-I	**Previous Behavior**: SMF terminates the session without sending the Gy CCR-T whenever the Gy CCR-I has failed with FHT action Terminate and subaction WITH_TERM_REQUEST. **New Behavior**: SMF terminates the session and sends the Gy CCR-T when the Gy CCR-I fails with FHT action Terminate and subaction WITH_TERM_REQUEST.
Preemptive Quota Request for Static and Predefined Rules	**Previous Behavior**: SMF didn't have the capability to request for preemptive quota for during the initial attach scenario. **New Behavior**: SMF can now request preemptive quota for both static and predefined rules during the initial attach procedure through a **preemptively-request-n-validate** CLI command in the Charging Action configuration.
Presence of Dummy Charging Information in Show Subscriber Output	**Previous Behavior**: SMF used to display dummy data under PolicySubData in the **show subscriber** output if there's no charging data generated for both online and offline charging. **New Behavior**: Dummy data is no longer part of the **show subscriber** output when there's no charging data for the PCC rules.
S-NSSAI IE over N4 Interface	**Previous Behavior**: SMF doesn't send S-NSSAI of PDU session to UPF. **New Behavior**: SMF includes S-NSSAI IE in the PFCP Session Establishment Request message over the N4 interface. SMF sends this IE to UPF during the PDU session establishment.
Unique Charging Identifiers for Default and Dedicated Bearers in Converged Calls	**Previous Behavior**: SMF used to allocate the same charging ID to all the dedicated bearers for visiting LBO sessions in the 4G network. SMF forwards the same charging ID to S-GW through the Create Bearer Request message, Due to this behavior, differentiating the CDRs for the default and dedicated bearers becomes difficult. **New Behavior**: SMF generates and allocates a unique charging ID to each dedicated bearer for visiting LBO sessions only when QoS flow Based Charging (QBC) charging is enabled. This unique identifier helps S-GW to easily identify the CDR records generated for default and dedicated bearers.

Feature	Description
Validation Check Enabled for show peers Command	**Previous Behavior**: The **show peers** command used to display the peer information with duplicate entries in different table outputs. **New Behavior**: It is mandatory that you specify one of the following options with a **show peers** command. • **all** • **ipv4** • **ipv6** If the **show peers** command is executed without any option, SMF returns a command syntax error message. Through this validation check, display of duplicate records is avoided. Similar behavior is additionally observed with the following commands: • **show rpc** • **show endpoint** • **show vrf-info**
Validation of Load Metric IE	**Previous Behavior**: SMF didn't accept the UPF Load Metric IE with value 0 and rejected the Sx Session Report Request message with mandatory_IE_Missing cause. **New Behavior**: SMF complies with 3GPP TS- 29.244, release 16 and accepts the Load Metric IE with the value 0. This action results in no rejections while processing the Sx request messages.

Related Documentation

For the complete list of documentation available for this release, go to:

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

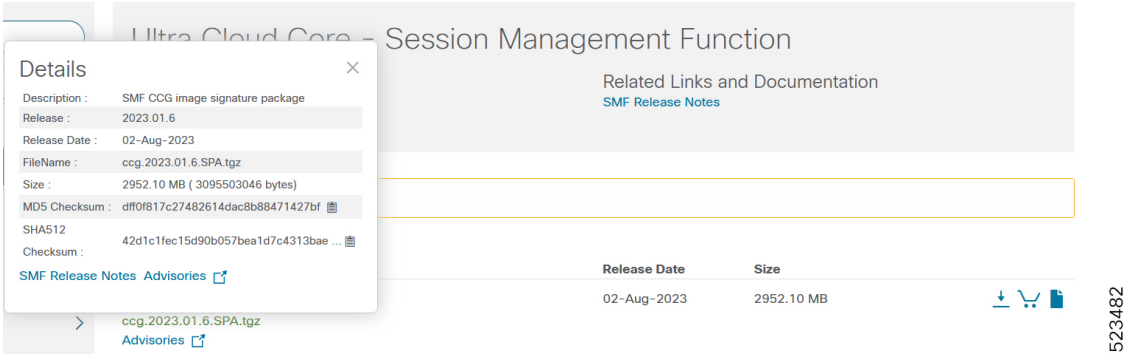
Installation and Upgrade Notes

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

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
SMF	
CSCwf98183	Flood of error logs on active RCM UPF "Active and Inactive RAT pdr CH validation failed"
CSCwh88576	Evaluation of smf for HTTP/2 Rapid Reset Attack vulnerability
CSCwj48323	Observing CEPS Loss while rolling upgrade from April Mainline (i88) to Target Branch
CSCwj60638	Evaluation of smf for HTTP/2 CONTINUATION Attack vulnerability
CSCwj66531	pcf_req_ded_brr_create | failures | rpc_failure | IPC_Error|failures seen during Rolling Upgrade
Mobile IoT	
CSCwj62733	Context not found. Errtype 1601 error logs observed in 5M call model
CSCwj75299	SMF is showing higher ip pool utilization than the actual subs count on the node

Resolved Bugs for This Release

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

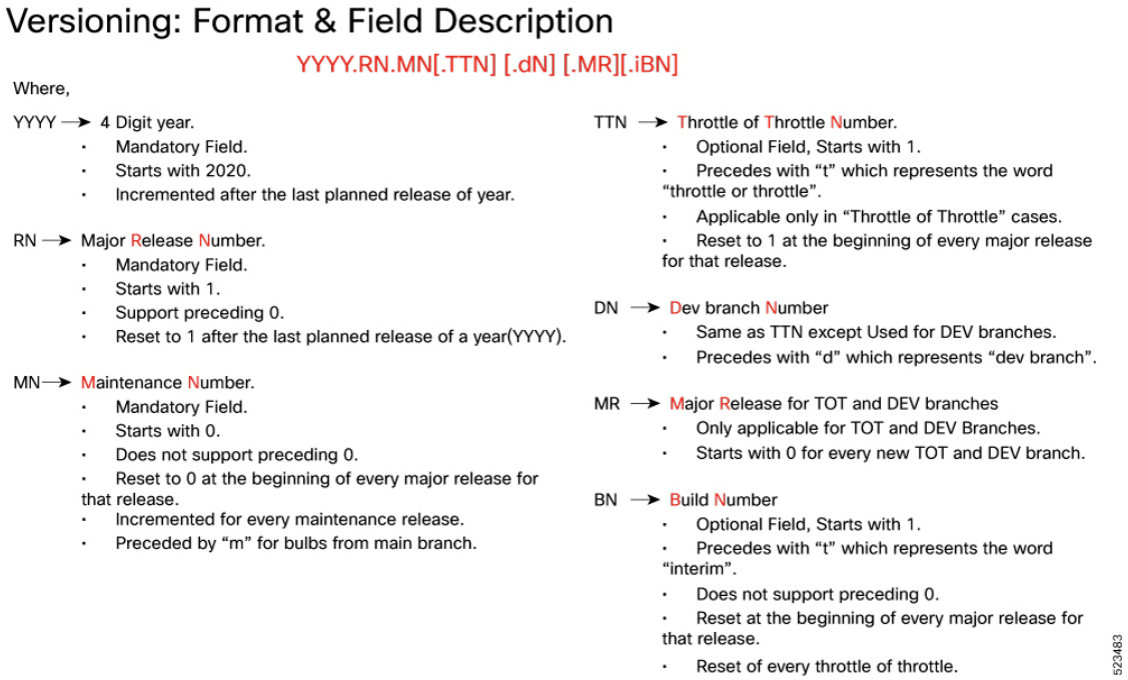
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
SMF		
CSCwj30314	BGP pod not doing bd switch if BGP link towards the leaf is down during reboot scenario.	No
CSCwj31295	udp-proxy is listening to all the IPs/Ports; needs to have some restrictions around it.	No
CSCwj38878	Create bearer response is not handled by smf	No
CSCwj41076	SMF dont fallback to precedence 2 during UPF selection when precedence 1 does not match	No
CSCwj51130	Online chf marked down, reauth not triggering release.	No
CSCwj51370	3gpp-sbi-message-priority in N7 not set when optimization enabled	No
CSCwj56507	SMF node sending traffic to UPF after SxPathFailure	No
CSCwj57597	R16 ePDG Indication - Policy Control Request message sent with null value for /userLocationInfo/n	No
CSCwj64328	smf-service: Additional transaction error logging during HO - WLAN to LTE	Yes
Mobile IoT		
CSCwi71280	3gpp-Negotiated-DSCP AVP not sent in Accounting message while matching QCI+ARP in QoS table	No
CSCwi96372	smf-service crash while running mon sub (version ccg.2024.01.0)	No
CSCwj04000	Routes are still connected even after removing IP chunks for a VRF	No
CSCwj43377	pdn_ho_location_change stats incorrectly getting updated	No
CSCwj59580	500k session loss observed after node reboot in 5M call model execution	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.