Release Notes for the Ultra Cloud Core Session Management Function, Version 2024.01.0

First Published: 2024-01-31

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-Jan-2024
End of Life	EoL	31-Jan-2024
End of Software Maintenance	EoSM	31-Jul-2025
End of Vulnerability and Security Support	EoVSS	31-Jul-2025
Last Date of Support	LDoS	31-Jul-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-2024.01.0.SPA.tgz	2024.01.0
NED package	ncs-5.6.8-ccg-nc-2024.01.0 ncs-6.1-ccg-nc-2024.01.0
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 9 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.01.1
Ultra Cloud CDL	1.11.6
Ultra Cloud Core UPF	2024.01.0
Ultra Cloud cnSGWc	2024.01.0

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	
3GPP Release 16-Compliant Generic UDM Enhancements	SMF supports the following enhancements in compliance with 3GPP 29.503, Release 16. • Subscription Level 3GPP Charging Characteristics: When this attribute is available in DNN configuration, this attribute takes precedence over the one received in the SessionManagementSubscriptionData. • ePDG Indication and NF Registration Time: UDM message handling configuration includes additional keyword options to allow or ignore ePDG Indication access information and NF Registration time in the N10 Registration Request. **Default Setting**: Not Applicable

Feature	Description
CHF Failure Handling at Rating Group and Application level	SMF allows you to define configurable actions to handle the failures associated with the application errors and rating group IDs. This feature introduces new command **failure-handling error-type [rg | app]** in the charging profile configuration. For more information, see the profile charging failure-handling error-type command. **Default Setting**: Disabled - Configuration Required
Dual Stack Support on N3	SMF enables the dual stack transport for N3 tunnel using the **dual-stack-transport { false | true }** CLI command in UPF network profile. **Default Setting:** Disabled – Configuration Required
EPS Fallback Reporting	SMF supports EPS Fallback Reporting functionality for PCC rules for which the EPS_FALLBACK trigger was sent by the PCF. **Default Setting**: Enabled when the compliance version 16.10.0 is set for npcf-smpolicycontrol.
Handle TFT Changes in the Absence of refQosData	SMF handles the PCC rule modification, with the following IEs as optional in smPolicyDecision. • refQosData in PCC Rule • refChgData in PCC Rule • flowInfos in PCC Rule • qosDesc in smPolicyDecision • chgDecs in smPolicyDecision • pccRules in smPolicyDecision All the valid use cases work as expected even if these optional IEs are not received.
N3IWF for Untrusted Non-3GPP Access Network	SMF supports the N3IWF interface for interworking between 5G core and untrusted non-3GPP networks. N3IWF facilitates seamless handover and uninterrupted connectivity for users when they transition between different network types. **Default Setting**: Disabled – Configuration Required
cnPGW-C	

Feature	Description
Debuggability and Logging Enhancements	For IoTaaS solutions, SMF supports the following enhancements: • Update statistics related to RADIUS, Diameter, PCC rules, and APN • Improve transaction and application level logs • Update Event trace • Improve monitor subscriber display For more information on the statistics, see the UCC 5G SMF Metrics Reference for the applicable release. **Default Setting**: Not Applicable

Behavior Changes

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

Feature	Description
3GPP-Negotiated-DSCP Attribute Information	**Previous Behavior:** SMF used to send incorrect value of 3GPP-Negotiated-DSCP attribute in the RADIUS authentication and accounting request messages. **New Behavior:** For 3GPP RADIUS dictionary, SMF populates RADIUS authentication and accounting messages with the correct value of 3GPP-Negotiated-DSCP attribute. For RADIUS authentication, SMF uses the QCI and ARP information from Create Session Request and detects an exact match in the QoS profile configuration. If not found, SMF checks for a match with only QCI and proceeds to populate the 3GPP-Negotiated-DSCP attribute value. The processing remains the same for RADIUS accounting except that SMF uses Gx authorized QCI for match finding.
Conditional Presence of IMSI IE in Change Notification Response	**Previous Behavior:** When a Change Notification Request is received with the IMSI Information Element (IE), the IMSI IE is not included in the corresponding response message. **New Behavior:**If the IMSI is received in the Change Notification Request, SMF includes the **conditional IMSI IE** in the Change Notification Response message, in compliance with 3GPP 29.274, Release 16. In the case of emergency sessions where IMSI is absent, the IMEI gets included in the Change Notification Response if it was received in the corresponding Change Notification Request.

Feature	Description
Initiation of PDU Modification on Policy Update	**Previous Behavior:** SMF did not take any action for changes to the Session-AMBR and QoS parameters in the Policy Update Response message. **New Behavior:** SMF initiates the PDU modification procedure if the Session-AMBR and QoS parameters are received in the Policy Update Response message.
Outer Header Removal IE Value During Upgrade or Activation of Dual Stack	**Previous Behavior:** SMF used to read the configured dual stack value and send the configured value to the UPF for all N4 messages. **New Behavior:** SMF saves the configured dual stack value during the session establishment. SMF uses the same dual stack value in the subsequent N4 messages until the session gets disconnected.
Processing URR During Gy CCA-I Failure	**Previous Behavior:** SMF disabled the charging for the session if the corresponding FHT action was set to CONTINUE and Sub action as NONE/UNKNOWN in Gy CCA-I. There was no communication towards OCS after Gy CCA-I for the mentioned FHT action and sub action. **New Behavior:** SMF sends Create/Update URR with high quota when the Gy CCA-I failure occurs and the FHT action for the session is set to CONTINUE and Sub action as NONE/UNKNOWN. SMF continues to stop further communication of Gy CCR-U/T towards the OCS.
Validation of Subnet Address in IPAM Configuration	**Previous Behavior:** While defining the chunk-group size, the CLI address-range allows configuring odd subnet address-range. It causes uneven or incorrect distribution of chunks across the DPs. **New Behavior:** The CLI address-range allows to configure only even subnet address-ranges. When **chunk-group** is enabled, the number of IPs in the address range should be a power of 2, which implies, the number of IPs should be even. If the address range has odd number of IPs, the following error message appears: "address range from " + startAddr +" to "+ endAddr + " is odd"

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.

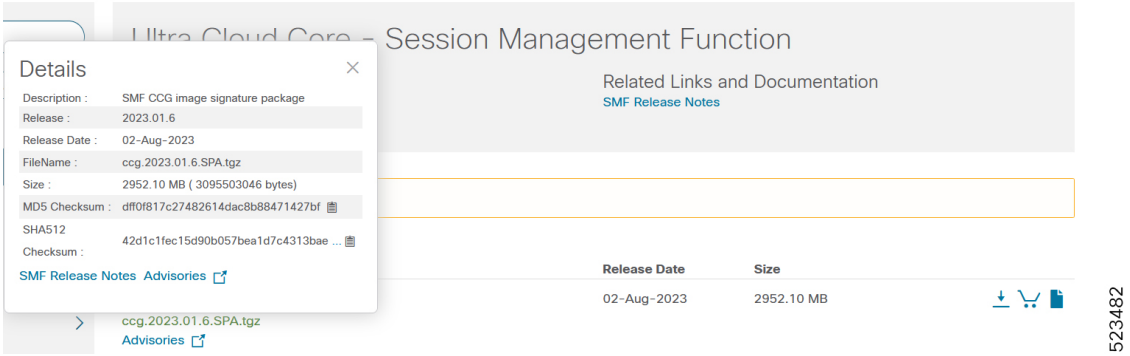
Installation and Upgrade Notes

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

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`

Operating System	SHA512 checksum calculation command examples
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
CSCwi59329	Calls got disconnected and huge Error logs being seen during longevity run
CSCwh88576	Evaluation of smf for HTTP/2 Rapid Reset Attack vulnerability
CSCwi33899	Support of clearing the subscriber for multiple UPF simultaneously, through CLI

Resolved Bugs for this Release

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

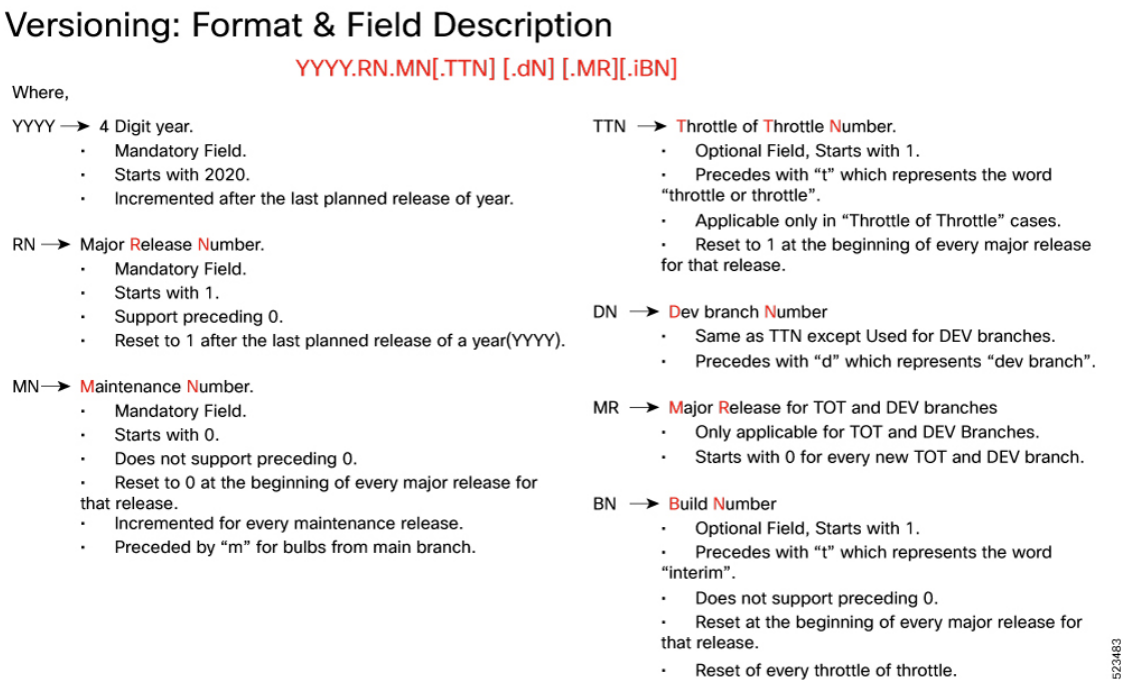
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwh83956	Gy_CCRI with CCFH AVP set to action terminate Sx mod req for Update FAR is not coming for UL	No
CSCwi25201	3GPP-Negotiated-DSCP attribute not sent in Acct msg when arp-priority-level CLI is absent	Yes
CSCwi43653	CDR generation for Secondary RAT usage report trigger is not working	Yes
CSCwi71280	3gpp-Negotiated-DSCP AVP not sent in Accounting message while matching QCI+ARP in QoS table	No
CSCwi16563	SMF does not remove the PDR for 5g-4g HO collision with IM exit	No
CSCwi07718	SMF to suppress v6 tunnel information in OHC FAR when UPF is v4	No
CSCwi00263	Ancient_Cache_Pod excludes pod affinity Once affinity stream connection flap multiple times	No
CSCwi31799	Online chf down - with NRF discovery enabled, SMF not falling back to locally configured IP	No
CSCwi00319	Multiple remove FAR with FUA-T and quota exhaust resulting in N4 MOD Cause 69	No
CSCwh97986	SMF- no radius ACCT when only online chf available and is down	No
CSCwi67146	SMF- Fallback incase of UPF blocked to different precedence not working	No
CSCwi36011	SMF should support QoS rules and QoS description with the length of two octets Option in PCO IE	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.