UCC 5G SMF Release Notes, Release 2024.04.1

First Published: 2024-11-26

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-Oct-2024
End of Life	EoL	30-Oct-2024
End of Software Maintenance	EoSM	30-Apr-2026
End of Vulnerability and Security Support	EoVSS	30-Apr-2026
Last Date of Support	LDoS	30-Apr-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**
ccg-2024.04.1.SPA.tgz	2024.04.1
NED package	ncs-5.6.8-ccg-nc-2024.04.1 ncs-6.1.12-ccg-nc-2024.04.1
NSO	5.6.8 6.1.12

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 8 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.04.1.14
Ultra Cloud CDL	1.11.9.1
Ultra Cloud Core UPF	2024.04.1
Ultra Cloud cnSGWc	2024.04.1

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 that are introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
Duplicate Static IP Detection and Resolution	This feature provides a mechanism to handle error scenarios where the same static IP gets allocated to two different UEs or two different PDU sessions belonging to the same UE or DNN. This feature ensures that such duplicate IP allocations are detected and appropriate actions are taken to prevent conflicts. **Command introduced**: **condition duplicate-ip** — Use this command in policy rule management configuration to detect the duplicate static IP allocations and reject or terminate such session requests.

Feature	Description
Enhancements to N3IWF: Network-Initiated Service Requests, Inter-PLMN Handover, and Core-Agnostic Location Parameters	Following are the additional enhancement to the N3IWF for the seamless communication between the Wi-Fi network and the cellular network. • Network initiated service request through N3IWF • Inter PLMN Wi-Fi to NR handover • Inter PLMN NR to Wi-Fi handover • Wi-Fi (N3IWF) to Evolved Universal Terrestrial Radio Access (EUTRA) HO • EUTRA to Wi-Fi (N3IWF) HO • Next Generation Core-Agnostic (N3GA) location parameters
Load and Overload Control over SBI, GTP-C, and N4 Interfaces	This feature handles the load and overload control mechanism for GTPC, N4, and SBA Interfaces. This feature improves the network robustness by considering the load and overload status of self and the peer nodes. **Commands Enhanced:** • **profile overload-exclude** *overload_exclude_profile_name***message-priority [n4 | n7 | n10 | n11 | n16 | n40 | s5] upto** *message_priority* • **profile overload-exclude** *overload_exclude_profile_name* **procedure-list [session-delete | new-call | xnho | modify | chf-reauth | inter-rat-ho | intra-rat-ho | imexit-nw | imexit-ue | usar]** **Default Settings**: Disabled—Configuration Required to Enable
Message Priority Negotiation for High Priority Messages	At any given circumstance, the SMF must ensure that the high-priority messages (WPS, emergency, etc.) continue uninterruptedly. SMF uses Message Priority (MP) Negotiation as the method to ensure uninterrupted communication between SMF and peer nodes. This mechanism allows the SMF to compare the message priority value present in the inbound message with the message priority value present in the local configuration. This way, the high priority inbound and outbound messages in a WPS Session get prioritized and processed on SMF. **Default Setting:** Always Enabled

Behavior Changes

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

Behavior Change	Description
SMF	

Behavior Change	Description
CLI for Load Factor Calculation and Pod Exclusion	**Previous Behavior:** The frequency of calculating the load factor was fixed at an interval of 30 seconds. As there was no support to change this interval, it was causing an overloaded system to stay overloaded until the next interval of 30 seconds. There was no mechanism to change this frequency according to the situations. Also, by default all the pods that were not participating in message-handling were getting excluded from the load factor calculation. **New Behavior:** The process of load factor calculation is enhanced to allow the user to configure the suitable interval. This enhancement also provides the capability to configure the specific non-participating pods to be excluded from the load factor calculation. Also, the show resources output is enhanced to display the load factor of the various pod instances. The following new CLI is introduced as part of this enhancement: **load factor { calc-frequency** *calc_frequency_time* **| exclude-pods** *exclude_pod_name* **}** **Note:** This CLI is backward-compatible. Therefore, if these load factor parameters are not configured, it considers the old behavior for calculating the load factor.
Enhanced Show CLI Output to Display the GR Instance ID of the Overloaded Peers	**Previous Behavior:** The network operator did not have the visibility into the instances of the peers that are overloaded. **New Behavior:** The show CLI **show overload-info peer all** is enhanced to display the GR Instance ID of the peers that are overloaded. This allows the peers to have detailed information about the peer overload status. **Customer Impact:** The network operator has detailed information about the overloaded peer.
Message Priority Negotiation for High Priority Messages	**Previous Behavior:** SMF was not considering the message priority of the incoming messages over N4, GTPC, and SBA interfaces. SMF used to send the message priority in outgoing messages. **New Behavior:** SMF extracts the message priority of the incoming messages, negotiates the extracted MP value with the configured interface specific MP value, and sends out the best among them in the outgoing message.
SMF Handling of SmContextStatusNotify for WiFi (N3IWF) to NR Handover	**Previous Behavior:** By default, SMF sends the SmContextStatusNotify to AMF without checking the "3GPP 23.502" compliance version for "WiFi (N3IWF) to NR" and "NR to WiFi" handover in intra-PLMN scenarios. **New Behavior:** SMF now sends the SmContextStatusNotify to AMF only if the compliance profile for "3GPP 23.502" is configured to be greater than 15.4.0 for "WiFi (N3IWF) to NR" and "NR to WiFi" handover in intra-PLMN scenarios. If the compliance profile is 15.4.0, SMF does not send the SmContextStatusNotify message to AMF.

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.

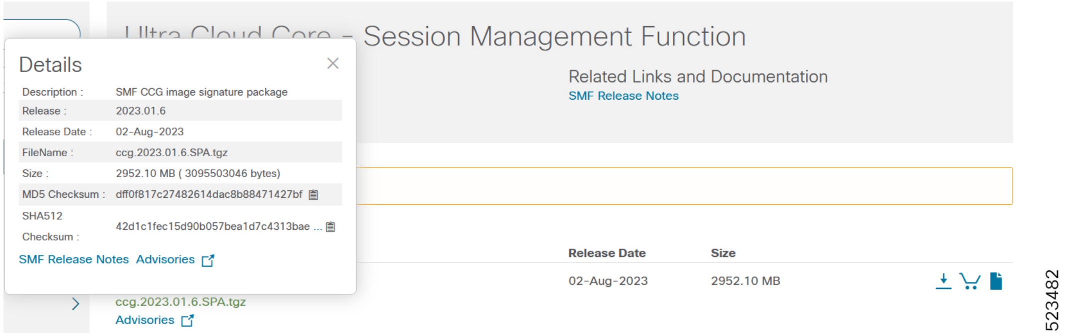
Installation and Upgrade Notes

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 Version

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.



Ultra Cloud Core – Session Management Function

Details

Description :	SMF CCG image signature package
Release :	2023.01.6
Release Date :	02-Aug-2023
FileName :	ccg.2023.01.6.SPA.tgz
Size :	2952.10 MB (3095503046 bytes)
MD5 Checksum :	dff0f817c27482614dac8b88471427bf
SHA512 Checksum :	42d1c1fec15d90b057bea1d7c4313bae ...

SMF Release Notes Advisories

Related Links and Documentation
SMF Release Notes

	Release Date	Size
ccg.2023.01.6.SPA.tgz Advisories	02-Aug-2023	2952.10 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 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
SMF	
CSCwn12767	Service restart - processFailedFlowList - RB and QCI change
CSCwn33214	GR switchback results in GR Instance detecting false overload and throttling happens for 10 mins
IoT	
CSCwk82318	Clear sub CLI did not clear all active sessions
CSCwm73549	show peers all interfaceName Gz not showing all peers on dynamic config change
CSCwm86970	Rolling Upgrade Async/SendNotification support validation for IOT

Resolved Bugs for this Release

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

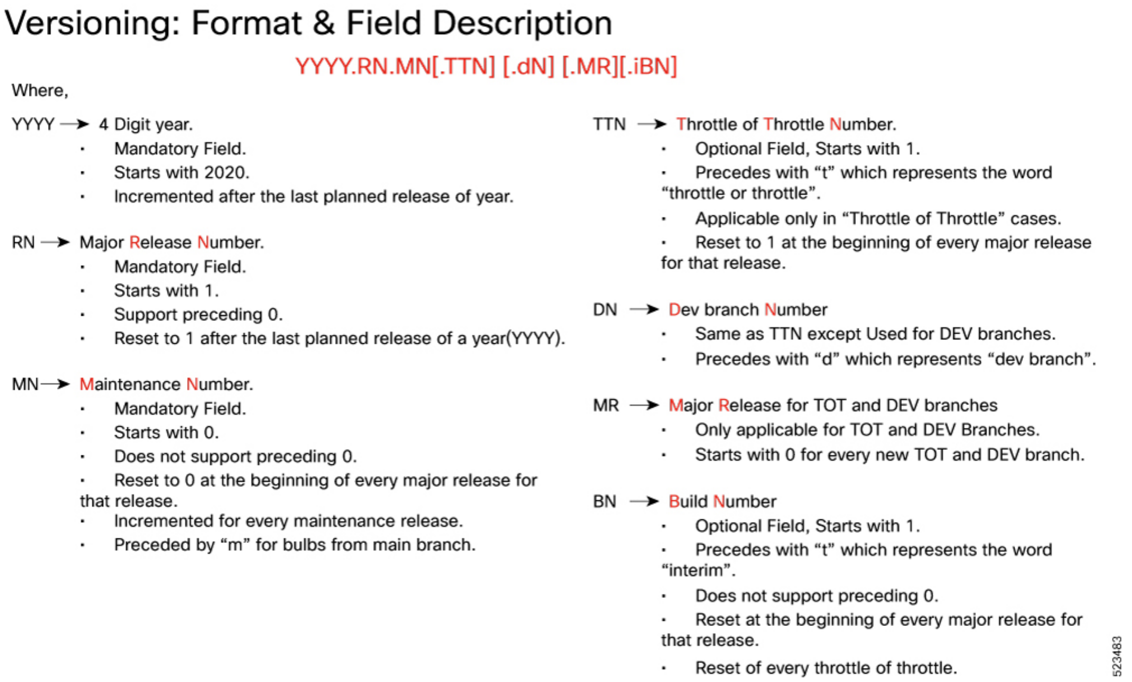
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
SMF		
CSCwn05114	Release procedure KPI impact, sending 500 instead of 204	No
CSCwn13440	N2 PDU FAIL in the IM exit case, KPI impact	No
CSCwm77385	Does not trigger IM exit for DLDR in case of ue init & n/w IM entry	No
CSCwm82520	Not removing imsi entry after disabling tap from etcd dump	No
CSCwm83584	ARP missing in charging update request - PCF Revalidation case	Yes
CSCwm86027	show subscriber count nf-specific updating wrongly after upgrade	No
CSCwm87196	Service restart - cdl session content in released state	No
CSCwm92840	Cdl ep is not able to fetch the key from cdl index pod, and sending empty response to smf service	No
CSCwm82203	LI taps clear functionality not working	No
IoT		
CSCwm94697	"mode debug exec attributes" cli pushing two ip chunks to UPF instead of one	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.



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.

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.