Release Notes for the Ultra Cloud Core Session Management Function, Version 2024.01.2

First Published: 2024-03-26

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-Apr-24
End of Life	EoL	30-Apr-24
End of Software Maintenance	EoSM	29-Oct-25
End of Vulnerability and Security Support	EoVSS	31-Oct-25
Last Date of Support	LDoS	31-Oct-26

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-2024.01.2.SPA.tgz	2024.01.2
NED package	ncs-5.6.8-ccg-nc-2024.01.2 ncs-6.1-ccg-nc-2024.01.2
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	2024.01.1
Ultra Cloud cnSGWc	2024.01.2

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
IoT	
Enable IPv6 Connectivity for SMF with Legacy Interfaces	SMF with legacy interfaces allows IPv6 address configuration to enable communication with the GTP, N4, Gx, and Gy interfaces. With this support, both IPv4 and IPv6 addresses can be used for peer connections. One peer connection can use either IPv4 or IPv6 address. To enable IPv6 connectivity, SMF uses the existing **endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }** and **dual-stack-transport { false | true }** CLI commands. **Default Setting:** Disabled – Configuration Required
SMF	

Feature	Description
Configuration-based Control of UDM Registration Messages	SMF allows the user to ignore the UDM registration messages during the PDU setup and Wi-Fi attach procedures. **Note** If the UDM registration message is ignored, SMF reattempts to send the registration message during the handover between 5G and Wi-Fi. With this controlled UDM registrations, the interactions between SMF and UDM over the N10 interface are minimized to handle the message overload and attach failures on the N10 interface. This feature introduces the new CLI command **skip-n10-registration rat-type [NR | WIFI | ALL]** in the DNN profile. **Default Setting:** Disabled – Configuration Required
Handling Traffic Flow for Dedicated UE Services	This feature allows specific UEs, like PTTs, to connect on the 5G RAT using specific TFTs. To enable this functionality, PCF sets the value of the **PacketFilterUsage** IE attribute to **true** in the dynamic PCC rule. This rule causes the SMF to only send the PCC Rule TFTs instead of the IP "Any-Any". This feature is only applicable for default flow. **Default Setting:** Enabled - Always-on
SMF Instance-based UPF Selection	This feature allows you to customize SMF instances in the **Subscriber Policy Configuration** and to bind SMF instances to the colocated UPFs in the inter-site GR deployment model. When the user selects operator policies, the SMF instances act as a filter and allow the SMF to select a specific DNN profile. The DNN selection helps in finding the closest and active Network functions (for example, UPFs) and ensures routing the user traffic only to the colocated UPFs. This implementation reduces the latency and improves user experience. To implement this feature, the following keywords are added under the policy subscriber command: **instance-start-range** **instance-stop-range** **Default Setting**: Disabled – Configuration required to enable

Behavior Changes

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

Feature	Description
ARP Configuration for WPS Profile during SMF Upgrade	**Previous Behavior**: For any SMF upgrades prior to Release 2023.03, the ARP configuration in the WPS profile was retained as is. **New Behavior**: For any SMF upgrades from Release 2023.03 to later releases, the ARP configuration gets removed. It is mandatory that you manually reconfigure the ARP parameter after the upgrade is complete.
GTP Echo Interval Configuration during SMF Upgrade	**Previous Behavior**: For any SMF upgrades prior to Release 2023.03, the GTP echo interval configuration in the S5 interface was retained as is. **New Behavior**: For any SMF upgrades from Release 2023.03 to later releases, the GTP echo interval configuration gets removed. It is mandatory that you manually reconfigure the GTP echo interval for the S5 interface after the upgrade is complete.
Handling Multiple PCC Rules on N1 Interface and Sending Additional QER Per PDR on N4 Interface	**Previous Behavior:** On the N1 interface, if multiple PCC rules are associated to the default flow, the SMF sends multiple QoS Rules with DQR=1 and Packet filters for the PCC Rules. SMF sends or adds up the bitrates of all PCC rules associated to default flow in FBR IE. On the N4 interface, for each of the PCC Rule associated to the default flow, SMF sends a CREATE_QER with the MBR set to the values of maxbrUl & maxbrDl sent by PCF in the QoS description for that PCC Rule. As QERs are unique for each PDR, SMF includes the gate status in the same QER as and when applicable based on the TC data associated to the PCC rule received from PCF. **New Behavior:** As per the new behavior, on the N1 interface, SMF sends only one QoS Rule for default flow with DQR=1 and the Packet filter as “Any-Any” or specific TFT. SMF doesn’t send or add up the bitrates in the QoS description of the PCC Rules in FBR IE. The MBR value in UE is derived from session AMBR. On the N4 interface, SMF doesn’t send a CREATE_QER for the PCC Rules QoS descriptions. The QER IDs in the PDRs for the PCC Rules are set to the Session Rules QER IDs. SMF includes an additional QER in the PDR of the PCC rule (along with the existing two QERs) specifically to display the gate status as enabled or disabled. The QER doesn’t contain any MBR information. **Note** This behavior change is applicable only for the dynamic rules.

Feature	Description
Handling Peer Delete Log during Reload	**Previous Behavior**: The application error log was captured even if the ETCD entry was deleted for a valid scenario. Following is an example of error log where this log is marked as ERROR. 2024/03/08 06:22:38.700 smf-service-6 [ERROR] [MemoryCache.go:446] [infra.memory_cache.core] Reload cache, key C.GR.1.peergtpnodeinfo1.x.x.x.x deleted **New Behavior**: The log level of this error log is changed to debug as this log is getting printed in the valid scenario.
Prioritized Processing of EDR Reporting for Subscribers	**Previous Behavior**: The **edr reporting subscriber** command when configured, didn't allow the user to configure **edr all subscribers** command. It is expected that the user first disables the edr reporting with **no edr reporting subscriber** command and then configure **edr all subscribers** command. **New Behavior**: The **edr all subscribers** command takes precedence over the **edr reporting subscriber** command when enabled. Through this prioritized processing, the user requires no additional configuration to remove the edr reporting subscriber.
SGW Peer Detection in Roaming Scenario	**Previous Behavior**: Roaming S-GW peers were showing as UNKNOWN_PEER in nodemgr logs and not tagged as "Roaming" in the SMF CCG software release 2023.03.m0.d8.0.i45 when seen with **show peers all** command. **New Behavior**: Roaming S-GW peers are tagged as "Roaming" when seen with **show peers all** command.
UDM Registration Reattempt during 5G and Wi-Fi Handovers	**Previous Behavior**: If the UE registration failed during a 5G or Wi-Fi attach and if the UDM failure handling template (FHT) was configured as continue or ignore, then SMF didn't attempt registration in Wi-Fi to 5G and 5G to Wi-Fi handovers. **New Behavior**: If the UE registration fails during a 5G or Wi-Fi attach and if the UDM FHT is configured as continue or ignore, then SMF reattempts the registration during Wi-Fi to 5G and 5G to Wi-Fi handovers.

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.

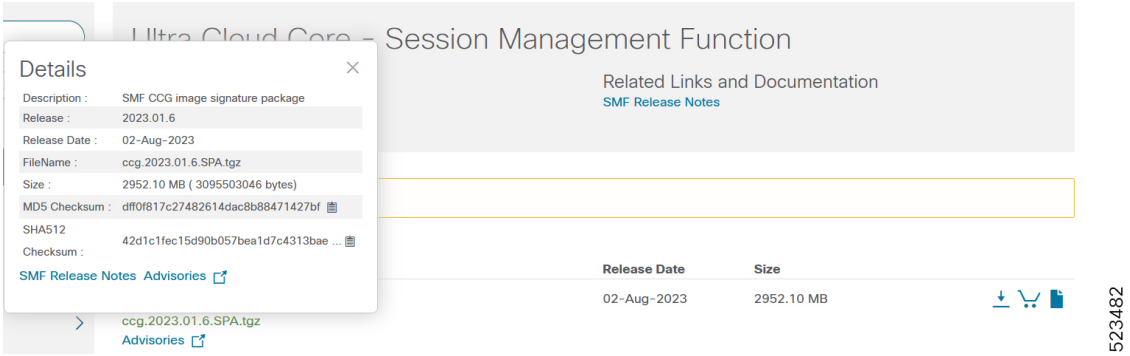
Installation and Upgrade Notes

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
CSCwj04000	Routes are still connected even after removing IP chunks for a VRF
CSCwj30314	Bgp pod not doing bd switch if bgp link towards the leaf is down during reboot scenario
CSCwj34474	ITC bandwidth drops are seen for dyn rule on default bearer 4G combo call instead of APN AMBR
CSCwj41076	SMF doesn't fallback to precedence 2 during UPF selection when precedence 1 does not match

Resolved Bugs for this Release

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

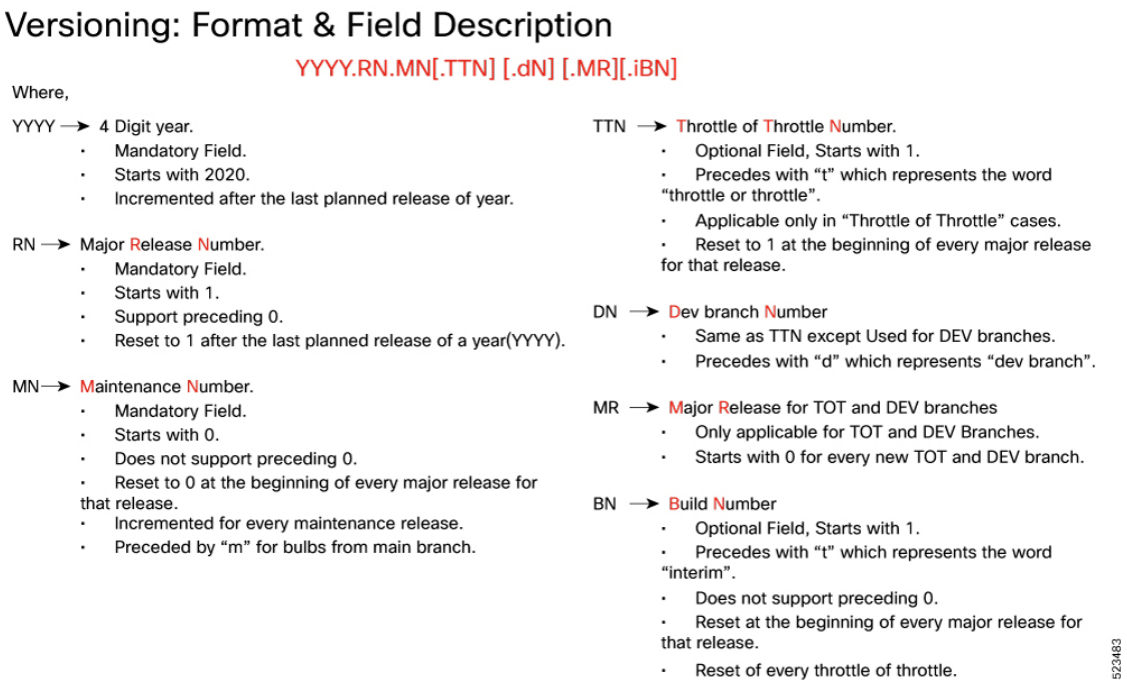
Note This software release may contain open bugs first identified in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwi19577	Frequent Reload cache peerInfo deleted errors in OAM logs	Yes
CSCwi59329	Calls got disconnected and huge Error logs being seen during longevity run	No
CSCwi95005	Customer wanted a procedure to show /clear local policy session using (local keyword)	No
CSCwi99821	SMF not sending the MTU info when ePCOSI flag set	No
CSCwj08989	PTI and Pdu Session ID not set in the Establishment Reject (HO case)	No
CSCwj19242	s11-gtpc-ep2-2 is unable to communicate to cache_pod_1	No
CSCwj19934	SMF Handling Policy decisions in SmPolicyControl_UPDATE response in 4G RAT	No
CSCwj21675	During incoming DSR and onging WIFI to LTE ho, SMF delets all the PDRs.	No
CSCwj27775	High count of etcd DELETE/PUT operations observed when roaming peer sends MBR with RC IE	No
CSCwj28003	Abort Ho not triggered : incoming DSR and onging WIFI to LTE ho await CBRes	No
CSCwj30058	GBR failure during idle active procedure, smf not sending rule report to pcf	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.