



# UCC 5G SMF Release Notes, Release 2025.02.0

First Published: 2025-04-29

## 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-2025
End of Life	EoL	30-Apr-2025
End of Software Maintenance	EoSM	29-Oct-2026
End of Vulnerability and Security Support	EoVSS	29-Oct-2026
Last Date of Support	LDoS	31-Oct-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-2025.02.0.SPA.tgz	2025.02.0
NED package	ncs-6.4.3-ccg-nc-2025.02.0 ncs-6.1.14-ccg-nc-2025.02.0
NSO	6.4.3 6.1.14

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	2025.02.1.17
Ultra Cloud CDL	1.12.1
Ultra Cloud Core UPF	2025.02.0
Ultra Cloud cnSGWc	2025.02.0

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
<a href="#">2G and 3G session attach and detach procedures for S4-SGSN</a>	<p>This feature adds support to the SMF for managing attach and detach functions originating from S4-SGSN (Serving GPRS Support Node). This allows the consolidation of 2G/3G and 4G/5G network control within a single converged core. By integrating the networks, you can simplify the network management and reduce the operational costs.</p> <p><b>Commands Introduced:</b></p> <p><b>profile converged-core activated-features 2g3g</b>—This CLI command enables S4-SGSN support for 2G and 3G RAT type in SMF.</p> <p><b>Default Settings:</b> Disabled - Configuration Required to Enable</p>

Feature	Description
Blocking UPF to handle N4 session establishment failures	<p>This feature allows the SMF to blocklist a specific UPF node when it continuously rejects session establishment requests. The UPF may reject these requests from the SMF due to various errors, such as licensing issues.</p> <p>However, without information on the issues at the UPF, the SMF might repeatedly select the same UPF, leading to an increased number of session creation failures.</p> <p>By enabling this feature, the network operators can prevent the SMF from repeatedly selecting the same UPF for a defined time interval.</p> <p><b>Commands Introduced:</b></p> <ul style="list-style-type: none"> <li>• <b>[no] activated-features upf-blocklisting [ use-alert <i>custom_rule_name</i> ]:</b> This CLI is configured under converged core profile configuration mode to enable UPF blocklisting feature on SMF.</li> <li>• <b>reactivate-peer condition [blocked] attributes [frequency <i>frequency_timer</i> ]:</b> This CLI is configured under the endpoint configuration mode to reactivate blocked UPF after the frequency timer is over.</li> </ul> <p><b>Default Setting:</b> Disabled—Configuration Required to Enable</p>
External DHCP-based IP Address Allocation	<p>The enterprises with large and complex 5G networks require centralized IP address allocation and management.</p> <p>This feature helps achieve centralization of IPAM by allowing the SMF to allocate IPs through a DHCP server.</p> <p><b>Commands Introduced:</b></p> <ul style="list-style-type: none"> <li>• <b>ipam dhcp:</b> This CLI is configured under the DNN profile to indicate the IPAM as DHCP.</li> <li>• <b>dhcp:</b> This CLI is configured under the IPAM profile to tag the address pool as DHCP.</li> <li>• <b>vlan <i>vlan_id</i>:</b> This CLI is configured under the IPv4 and IPv6 modes to attach the VLAN IDs.</li> </ul> <p><b>Default Settings:</b> Disabled—Configuration Required to Enable</p>
NF Discovery based on Preferred Locality	<p>SMF includes the "3gpp-Sbi-Discovery-preferred-locality" HTTP header when communicating with the SCP. By populating this header, SMF enables more efficient NF selection based on locality during peer NF discovery, resulting in optimized network function interactions and improved service delivery.</p> <p><b>Important</b> This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.</p>

## Behavior Changes

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

Behavior Change	Description
Encode quotaManagementIndicator in the charging request	<p><b>Previous Behavior:</b> The offline converted rating group SMF did not send the quotaManagementIndicator to the CHF in charging requests.</p> <p><b>New Behavior:</b> The offline converted rating group SMF now sends the quotaManagementIndicator as CONVERTED_OFFLINE to the CHF in charging requests.</p>
Explicit TEID setting in GTPv2 messages for Context Not Found scenario	<p><b>Previous Behavior:</b> SMF did not explicitly set the Tunnel Endpoint Identifier (TEID) flag to 0 in certain GTPv2 messages when sending a response with the Cause IE set to "Context Not Found (64)." This led to stale TEID values being used inadvertently.</p> <p><b>New Behavior:</b> SMF explicitly sets the TEID flag to 0 in the GTPv2 header for the following messages when the Cause IE is "Context Not Found (64)":</p> <ul style="list-style-type: none"> <li>• Modify Bearer Response</li> <li>• Delete Session Response</li> <li>• Modify Bearer Failure Indication</li> <li>• Delete Bearer Failure Indication</li> <li>• Change Notification Response</li> </ul> <p>This update ensures compliance with GTPv2 specifications and aligns with 3GPP standards, providing improved handling for error scenarios.</p>
Handling of FQDN in smContextStatusUri	<p><b>Previous Behavior:</b> Receiving an FQDN in the <b>smContextStatusUri</b> within the <b>N11CreateSmContextReq</b> led to service restart, as only IPv4 and IPv6 addresses were correctly processed.</p> <p><b>New Behavior:</b> The system now properly decodes FQDNs in the smContextStatusUri, integrating them into the nfFqdn IE within the ServingNetworkFunctionInformation IE in ChargingDataReq. This ensures seamless handling alongside IPv4 and IPv6 addresses.</p> <p><b>Customer Impact:</b> Customers can now use FQDNs in the smContextStatusUri, which will be accurately processed and included in the relevant information elements, enhancing network configuration flexibility and functionality</p>
Implement RPC limits to prevent CLI timeouts	<p><b>Previous Behavior:</b> Previously, there were no limits on the number of Remote Procedure Calls (RPCs) collected from each pod instance and included in the response, which could result in a CLI timeout.</p> <p><b>New Behavior:</b> The system now limits the number of RPCs received per pod instance to 50,000 and the total number of RPCs from all pod instances to 200,000. The <b>show rpc all</b> command displays a maximum of 200,000 lines in its output.</p>

Behavior Change	Description
Interface type display for overload information	<p><b>Previous Behavior:</b> The interface type was incorrectly displayed in the output of the <b>show overload-info peer all</b> command. For instance, the peer type "MME" was shown as "S5" instead of its correct interface type.</p> <p><b>New Behavior:</b> The interface type is now correctly assigned based on the peer type:</p> <ul style="list-style-type: none"> <li>• ePDG → "S2B"</li> <li>• MME → "S11"</li> <li>• SGW → "S5"</li> </ul> <p>This correction aligns the command output with expected network behavior, ensuring precise representation of interface types.</p> <p><b>Customer Impact:</b> The update rectifies the interface type display errors in the command output, improving the clarity and accuracy of the system's overload information.</p>
Load Control Information Calculation Update	<p><b>Previous Behavior:</b> For active and standby types of pods, such as protocol, GTPC, LI, UDP-proxy, GTPP, and Diameter, the Load Control Information (LCI) was calculated by taking the average of loads of the pods. Due to this calculation, the system did not detect overload even though the active pod was heavily loaded.</p> <p><b>New Behavior:</b> The Load Control Information (LCI) is now calculated by taking the maximum load among the standby and active pods. This behavior helps the system to correctly identify the overloaded active pod.</p>
Name change for RAN Cause IE on N7 interface	<p><b>Previous Behavior:</b> In 3GPP standard releases 15.4.0 and 16.0, certain Information Elements (IEs) on the N7 interface were sent with an invalid prefix "_". The affected IEs included _5gSmCause, _5gMmCause, and _3gppPsDataOffStatus.</p> <p><b>New Behavior:</b> The invalid prefix "_" has been removed from the IEs on the N7 interface.</p> <p><b>Customer Impact:</b> Customers will observe a change in the naming of a few IEs on the N7 interface. This change ensures consistency and compliance with standard naming practices.</p>

Behavior Change	Description
NF Discovery based on Preferred Locality	<p><b>Previous Behavior:</b> The 3gpp-sbi-discovery-preferred-locality header was not sent to the SCP, even if the following conditions were met:</p> <ul style="list-style-type: none"> <li>• "locality preferred-server" was enabled under "profile nf-pair" of the respective targetNF.</li> <li>• "locality client" had the same value as the configuration of "locality" under "profile smf".</li> </ul> <p><b>New Behavior:</b> The 3gpp-sbi-discovery-preferred-locality header is sent to the SCP when the following conditions are met:</p> <ul style="list-style-type: none"> <li>• "locality preferred-server" is enabled under "profile nf-pair" of the respective targetNF.</li> <li>• "locality client" matches the configuration of "locality" under "profile smf".</li> </ul>
Retry-Terminate mechanism for HSMF roaming	<p><b>Previous Behavior:</b> In HSMF roaming scenarios, the retry-terminate mechanism was not functional. The system failed to apply the retry-terminate action as part of N4 failure handling even when the following configurations are available:</p> <pre>interface pfcf   message N4SessionEstablishmentReq     cause-code pfcf-entity-in-congestion action   retry-terminate max-retry 2</pre> <p><b>New Behavior:</b> The retry-terminate mechanism is now effectively implemented for HSMF roaming scenarios. This update provides the necessary retry procedures during the UPF setup, ensuring that roaming cases are managed accurately and efficiently.</p>
Updated Cause Code for Rejected N11 Retrieve Message during Disabled Interworking	<p><b>Old behavior:</b> Previously, during the EPS fallback scenario, if the IWK is marked as disabled the SMF rejected N11 retrieve message with a failure cause code 403 forbidden-'UPIP_REQ_DENIED_IN_RAT'.</p> <p><b>New behavior:</b> With this enhancement, during the EPS fallback scenario, if the IWK is marked as disabled the SMF rejects N11 retrieve message with a failure cause code 403 forbidden with an updated cause code as "SUBSCRIPTION_DENIED".</p>

Behavior Change	Description
Enhancements in UPIP Functionality to Support Roaming, Session Modification, and N16 Interface	<p><b>Old Behavior:</b> During the resource setup process at gNB, such as idle-active, N2 ho, xn ho, the SMF recalculated UPIP for existing sessions and updated the latest UPIP values to the gNB. The dynamic configuration change for UPIP under the DNN configuration was applicable for the existing sessions.</p> <p>Also, previously the UPIP feature did not support roaming and session modification functionalities.</p> <p><b>New behavior:</b> As part of the UPIP enhancement process, the SMF decides to enable UPIP based on UDM SM data, UE data rates, and the local configuration during the 5G session create processes or handover to 5G. The SMF does not recalculate the UPIP values again during handovers, it uses the UPIP values decided during session create time. The dynamic configuration change for UPIP under the DNN configuration does not apply to the existing session.</p> <p>Also, the UPIP functionality is enhanced to support roaming and UE init modification for UPIP data rate change.</p>

## 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.

**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](#)

Ultra Cloud Core Session Management Function

Related Links and Documentation

[SMF Release Notes](#)

Release Date	Size
02-Aug-2023	2952.10 MB

ccg.2023.01.6.SPA.tgz

[Advisories](#)

523482

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 the following table 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:  <code>&gt; certutil.exe -hashfile filename.extension SHA512</code>
Apple MAC	Open a terminal window and type the following command:  <code>\$ shasum -a 512 filename.extension</code>
Linux	Open a terminal window and type the following command:  <code>\$ sha512sum filename.extension</code> OR <code>\$ shasum -a 512 filename.extension</code>
<b>Note</b> 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 list an open bug 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
<a href="#">CSCwo88928</a>	Show subs file writing with failed-open option returning "Unable to perform Subscriber Search"

## 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 is available in the [Cisco Bug Search Tool](#).

Bug ID	Headline	Behavior Change
<b>SMF</b>		
<a href="#">CSCwn14934</a>	create_bearer_request procedures failed without a reason label being pegged	No
<a href="#">CSCwn47741</a>	Enhancements in UPIP (User plane integrity protection) feature	Yes
<a href="#">CSCwn55179</a>	Nodemgr dumps continuous errors when issued the command to clear the taps	No
<a href="#">CSCwn59558</a>	show rpc all shows no entries with log "Read timed out" in product-confd-callback logs	Yes
<a href="#">CSCwn80324</a>	LCI value is not calculated correctly for active/standby type of pods like gtpc-ep	Yes
<a href="#">CSCwn82411</a>	Not hitting the START_OF_SERVICE_DATA_FLOW; multiple predefined sharing CA	No
<a href="#">CSCwo20179</a>	Create over create with SLA timeout	No
<a href="#">CSCwo21940</a>	Not handling smContextStatusUri value as fqdn, svc crashes while creating n40req	Yes
<a href="#">CSCwo26437</a>	rest-ep-nx-x stopped sending HB post crash	No
<a href="#">CSCwo28264</a>	CCG is forwarding the RAN NAS cause code within the _5gSmCause AVP in the N7 update	Yes

Bug ID	Headline	Behavior Change
<a href="#">CSCwo39461</a>	SMF wrongly considers SGW as Overload MME Peer	Yes
<a href="#">CSCwo49656</a>	ops-center pods crashed due to concurrent commands executed	No
<a href="#">CSCwo58551</a>	nodemgr restart - Failed to read System Up Time from cache maxRetry:30	No
<a href="#">CSCwo71954</a>	Not restricting the PCO length when slice present	No
<a href="#">CSCwo73071</a>	slice sst matching for three digit not working	No
<a href="#">CSCwo77322</a>	Not restricting the PCO length when slice present	No
<a href="#">CSCwo83066</a>	Back to back FOP sessions file writing is taking SMF into overload state	Yes
<b>IoT</b>		
<a href="#">CSCwn80092</a>	Handling N4 failure during UPF Association	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 "i" 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.

523483

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
csg.<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>-csg-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>.