



Release Notes for UCC 5G SMF, Release 2025.03.2



Ultra Cloud Core – Session Management Function, Release 2025.03.2 3

New software features 3

Changes in behavior 3

Resolved issues 3

Open issues 4

Compatibility 4

Supported software packages 5

Related resources 6

Legal information 7

Ultra Cloud Core - Session Management Function, Release 2025.03.2

This Release Notes identifies changes and issues related to the 5G Converged Core Session Management Function (SMF).

For more information about Ultra Cloud Core - Session Management Function, see the [Related resources](#) section.

Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC SMF software:

Table 1. EoL milestone information for Ultra Cloud Core - Session Management Function, Release 2025.03.2

Milestone	Date
First Customer Ship (FCS)	31-Jul-2025
End of Life (EoL)	31-Jul-2025
End of Software Maintenance (EoSM)	29-Jan-2027
End of Vulnerability and Security Support (EoVSS)	29-Jan-2027
Last Date of Support (LDoS)	31-Jan-2028

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.

New software features

There are no new software features in this specific software release.

Changes in behavior

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

Table 2. Behavior changes for Ultra Cloud Core - Session Management Function, Release 2025.03.2

Description	Behavior changes
EPSFB - DLDR collision - invalid_rat_type for DLDR getting pegged.	Previous Behavior: In the July-25 build, DLDR (Downlink Data Report) handling during EPS-FB (EPS Fallback) led to an increase in the Invalid-RAT-Type KPI. This was a change from the July-24 build's behaviour. New Behavior: The system's behaviour for DLDR during EPS-FB has been reverted to that of the July-24 build. DLDR will now be ignored if EPS-FB is in progress, resolving the Invalid-RAT-Type KPI increase.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#).

Table 3. Resolved issues for Ultra Cloud Core - Session Management Function, Release 2025.03.2

Bug ID	Description
CSCwr63968	VSMF sending EBI 0, resulting in Handover failure.
CSCwr68259	VSMF not sending mapped slice information to UE.
CSCwr69644	VSMF is not sending hoPreparationIndication during 4G to 5G HO.
CSCwr72442	SMF-restart seen with AMF sending complete in s11create.
CSCwr35761 CSCwr72478	SMF-REDCAP - Lower-compliance - RATTTYPE sent empty in 4G to 5G for REDCAP.
CSCwr75437	EPSFB - DLDR collision - invalid_rat_type for DLDR getting pegged.
CSCwr77014	SMF sending 404 - Retrieve and N1N2failurenotification collision.
CSCwr77921	SMF fails to process the addition of pccrule belonging to default flow with packetFilterUsage true post N2 failure.
CSCwr83436	SMF-Service restart when 5ql missing in policy create response.

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#). To search for a documented Cisco product issue, type in the browser: <bug_number> site:[cisco.com](#)

Table 4. Open issues for Ultra Cloud Core - Session Management Function, Release 2025.03.2

Bug ID	Description
CSCwr97192	PDU session establishment getting failed because of EBI assignment failure with NF-Set based subscription feature enabled.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC SMF software.

Table 5. Compatibility information for Ultra Cloud Core - Session Management Function, Release 2025.03.2

Product	Supported Release
Ultra Cloud Core SMI	2025.03.1.10
Ultra Cloud CDL	1.12.2
Ultra Cloud Core UPF	2025.02.0
Ultra Cloud cnSGWc	2025.03.2

Supported software packages

This section provides information about the release packages associated with UCC SMF software.

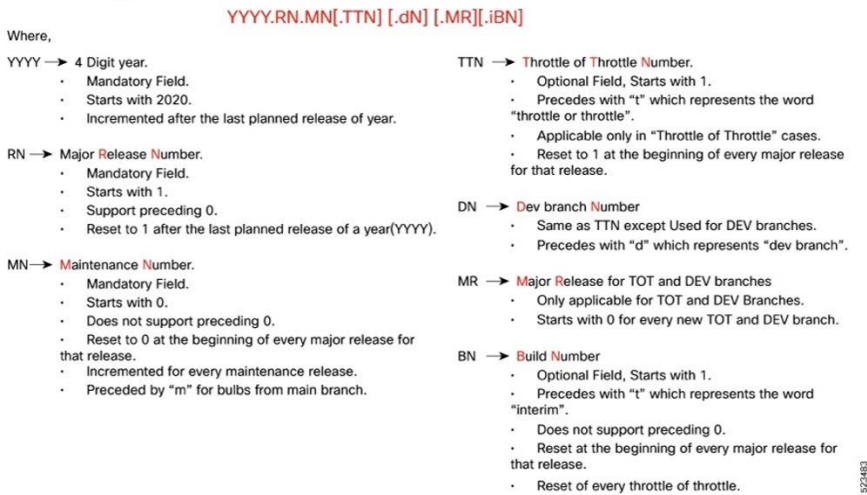
Table 6. Software packages for Ultra Cloud Core – Session Management Function, Release 2025.03.2

Software Package	Description	Release
ccg-2025.03.2.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.	2025.03.2
ncs-6.4.5-ccg-nc-2025.03.2.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	6.4.5
ncs-6.1.14-ccg-nc-2025.03.2.tar.gz	Note that NSO is used for the NED file creation.	6.1.14

Cloud native product version numbering system

The show helm list command displays detailed information about the version of the cloud native product currently deployed.

Figure 1. Cloud native product versioning format and description
Versioning: Format & Field Description



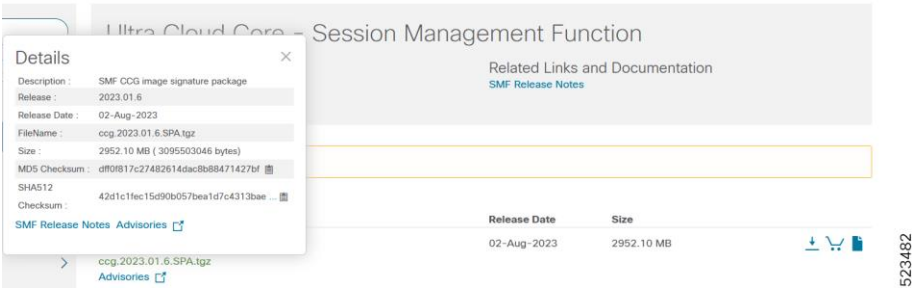
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

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.

Figure 2. Sample of converged core gateway software image



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 the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 7. 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>> 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>
Note: <filename> is the name of the file. <extension> is the file type 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 not to 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.

Related resources

This table provides key resources and links to the support information and essential documentation for SMF and other Ultra Cloud Core (UCC) products.

Table 8. Related resources and additional information

Resource	Link
SMF documentation	Session Management Function
cnSGWc documentation	Serving Gateway Function
SMI documentation	Subscriber Microservices Infrastructure
UPF documentation	User Plane Function
Service request and additional information	Cisco Support

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.