Release Notes for UCC 5G cnSGWc, Release 2025.04.0

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Ultra Cloud Core – Serving Gateway Function, Release 2025.04.0 3
New software features 3
Changes in behavior 4
Resolved issues 4
Open issues 4
Compatibility 4
Supported software packages 4
Related resources 6
Legal information 7

© 2025 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core - Serving Gateway Function, Release 2025.04.0

This Release Notes identifies changes and issues related to the software release of Ultra Cloud Core (UCC) Serving Gateway Control Plane Function (cnSGWc).

The key highlights of this release include:

- Custom3 CDR file format support: Introduces support for the custom3 file format for SGW Charging Data Records (CDRs), enhancing flexibility in CDR storage and management, with automatic, secure SFTP transfer to external storage and new CLI tools for management and troubleshooting.

For more information about Ultra Cloud Core – Serving Gateway Function, see the Related resources section.

Release lifecycle milestones

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

Table 1. EoL milestone information for Ultra Cloud Core – Serving Gateway Function, Release 2025.04.0

Milestone	Date
First Customer Ship (FCS)	31-Oct-2025
End of Life (EoL)	31-Oct-2025
End of Software Maintenance (EoSM)	01-May-2027
End of Vulnerability and Security Support (EoVSS)	01-May-2027
Last Date of Support (LDoS)	30-Apr-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

This section provides a brief description of the new software features introduced in this release.

Table 2. New software features for Ultra Cloud Core – Serving Gateway Function, Release 2025.04.0

Product impact	Feature	Description
Software Reliability	IPv6 support for cnSGWc	This release supports the deployment and configuration of cnSGWc on IPv6 network through SMI.
Hardware Reliability	Supermicro server validation	cnSGWc has been tested and validated for deployment on the Supermicro server.
Software Reliability	Custom3 CDR storage and reliable transfer	This feature adds support for the custom3 file format for SGW Charging Data Records (CDRs), giving operators more flexibility in how they store and manage CDRs. In addition to the existing custom1 and custom5 formats, operators can configure the system to use custom3 through a CLI setting

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		under the gtpp-profile. To improve operational reliability, the system can automatically transfer these custom3 CDR files to external storage servers using encrypted SFTP, with built-in failover support to handle any connection issues. New CLI commands make it easier for operators to view, manage, and troubleshoot CDR files in the custom3 format.

Changes in behavior

There are no behavior changes in this specific software release.

Resolved issues

There are no resolved bugs in this specific software release.

Open issues

There are no open bugs in this specific software release.

Compatibility

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

Table 3. Compatibility information for Ultra Cloud Core - Serving Gateway Function, Release 2025.04.0

Product	Supported Release
Ultra Cloud Core SMI	2025.04.1.15
Ultra Cloud CDL	1.12.3
Ultra Cloud Core UPF	2025.04.0.i5
Ultra Cloud cnSGWc	2025.04.0

Supported software packages

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

Table 4. Software packages for Ultra Cloud Core - Serving Gateway Function, Release 2025.04.0

Software Package	Description	Release
ccg-2025.04.0.SPA.tgz	The offline release signature package. This package contains the deployment software, NED package, as well as the release signature, certificate, and verification information.	2025.04.0

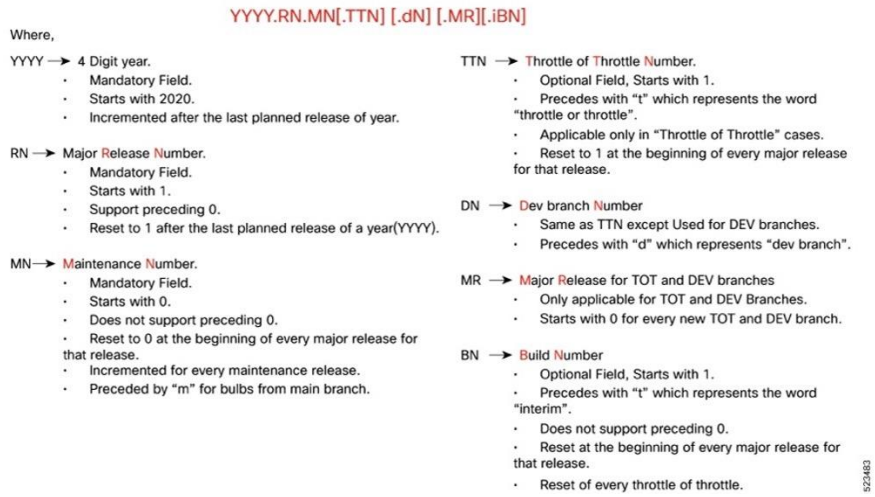
© 2025 Cisco and/or its affiliates. All rights reserved.

Software Package	Description	Release
ncs-6.4.8-ccg-nc-2025.04.0.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.	6.4.8.1
ncs-6.1.14-ccg-nc-2025.04.0.tar.gz		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



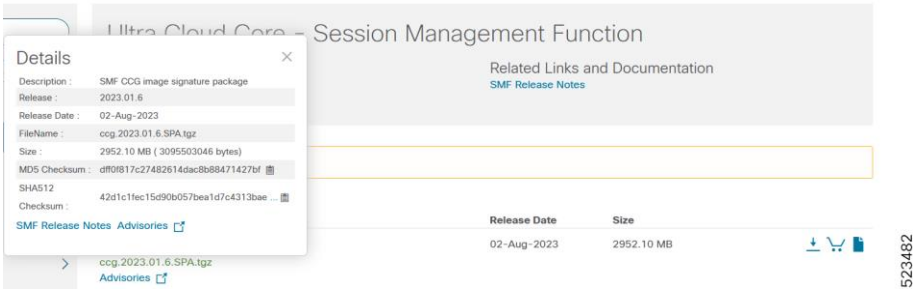
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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



© 2025 Cisco and/or its affiliates. All rights reserved.

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 5. 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>`

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 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

The software images are signed via x509 certificates. For information and instructions on how to validate the certificates, refer to the README file packaged with the software

Related resources

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

Table 6. Related resources and additional information

Resource	Link
cnSGWc documentation	Serving Gateway Function
SMF documentation	Session Management Function
SMI documentation	Subscriber Microservices Infrastructure

© 2025 Cisco and/or its affiliates. All rights reserved.

Resource	Link
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.