Release Notes for UCC 5G cnSGWc, Release 2026.01.3

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Ultra Cloud Core – Serving Gateway Function, Release 2026.01.3 3
New software features 3
Changes in behavior 3
Resolved issues 3
Open issues 3
Compatibility 4
Supported software packages 4
Related resources 6
Legal information 6

© 2026 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core - Serving Gateway Function, Release 2026.01.3

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

Release lifecycle milestones

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

Table 1. EoL milestone information for UCC cnSGWc, Release 2026.01.3

Milestone	Date
First Customer Ship (FCS)	30-Jan-2026
End of Life (EoL)	30-Jan-2026
End of Software Maintenance (EoSM)	31-July-2027
End of Vulnerability and Security Support (EoVSS)	31-July-2027
Last Date of Support (LDoS)	31-July-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

There are no behavior changes in this specific software release.

Resolved issues

There are no resolved bugs in this specific software release.

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.

Table 2. Open issues for UCC cnSGWc, Release 2026.01.3

Bug ID	Description
CSCwt78846	cnSGW not sending sx-delete-req to UPF after SLA timer expired leading to stale session.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt66198	Session Reports are missed by cnSGW due to UPF sending session report on stale SEID.
CSCwt67446	cnSGW not reporting User location changes in CDR for an EBI of subscriber with Multiple default bearers (same QCI and same APN).

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 UCC cnSGWc, Release 2026.01.3

Product	Supported Release
Ultra Cloud Core SMI	2026.01.1.08
Ultra Cloud CDL	2.1
Ultra Cloud Core UPF	2026.01.0
Ultra Cloud cnSGWc	2026.01.3

Supported software packages

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

Table 4. Software packages for UCC cnSGWc, Release 2026.01.3

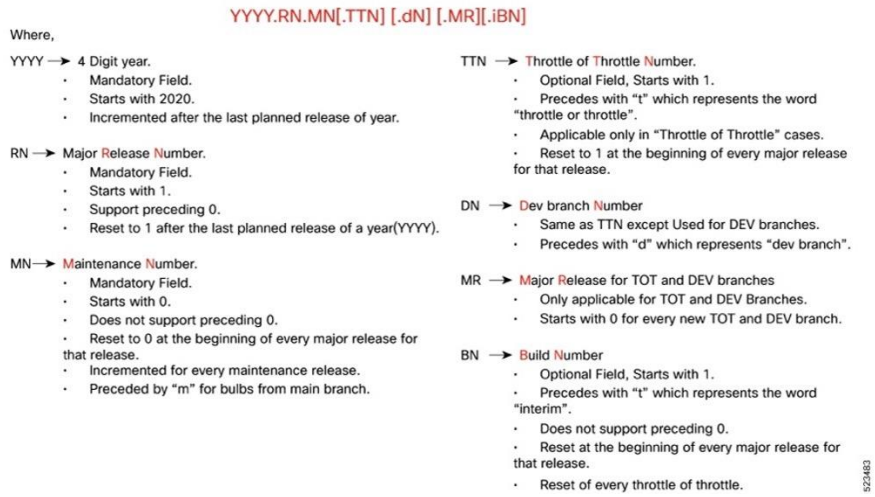
Software Package	Description	Release
ccg-2026.01.3.SPA.tgz	The offline release signature package. This package contains the deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.01.3
ncs-6.4.8.2-ccg-nc-1.1.2026.01.3.tar.SPA.tgz	The NETCONF 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.	6.4.8.2
ncs-6.1.14-ccg-nc-1.1.2026.01.3.tar.SPA.tgz		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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Figure 1. Cloud native product versioning format and description



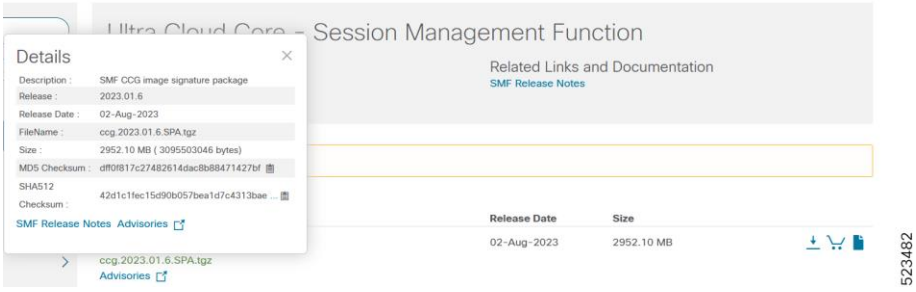
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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



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:

© 2026 Cisco and/or its affiliates. All rights reserved.

Operating System	SHA512 checksum calculation command examples
	`> 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
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.

© 2026 Cisco Systems, Inc. All rights reserved.