Release Notes for UCC 5G AMF, Release 2026.03.5

Contents

Ultra Cloud Core – Access and Mobility Management Function, Release 2026.03.5 3
New software features 3
Changes in behavior 3
Resolved issues 4
Open issues 4
Compatibility 5
Supported software packages 5
Related resources 7
Legal information 7

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

Ultra Cloud Core - Access and Mobility Management Function, Release 2026.03.5

This Release Notes identifies changes and issues related to the Access and Mobility Management Function (AMF).

For more information on the AMF software, see the Related resources section.

Release Lifecycle Milestones

This table provides EoL milestones for Cisco Ultra Cloud Core – Access and Mobility Management Function software:

Table 1. EoL milestone information for UCC AMF, Release 2026.03.5

Milestone	Date
First Customer Ship (FCS)	23-July-2026
End of Life (EoL)	23-July-2026
End of Software Maintenance (EoSM)	31-Jan-2028
End of Vulnerability and Security Support (EoVSS)	31-Jan-2028
Last Date of Support (LDoS)	31-Jan-2029

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 UCC AMF, Release 2026.03.5

Product impact	Feature	Description
Software Reliability	Xn-C TNL address discovery	Enables the AMF to relay NGAP RAN configuration transfer requests and responses between NG-RAN nodes to support Xn-C address discovery.

Changes in behavior

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

Table 3. Behavior changes for Ultra Cloud Core – Access and Mobility Management Function, Release 2026.03.5

Description	Behavior changes
Subscriber information tracking and reporting	**Previous behavior**: AMF supports individual subscriber lookups and subscriber listings but does not filter bulk results by UE registration state. **New behavior**: AMF now supports state-based subscriber lookups. Individual lookups continue to return subscriber details regardless of UE state.

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

Description	Behavior changes
	Commands: • show subscriber supi <supi-val> – Displays details for the specified UE, regardless of its state. • show subscriber supi all – Lists all registered and idle UEs. • show subscriber guti all – Lists all deregistered UEs.

Resolved issues

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

Note: This software release may contain resolved 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. Resolved issues for UCC AMF, Release 2026.03.5

Bug ID	Description
CSCwx44497	UECM deregistration request is sent before UnSubscribe request during purge timer expiry
CSCwx69971	AMF send ICSR instead of PDUSessionResourceSetupRequest for 2nd PDU
CSCwx77859	AMF didn't send FRCN during HO from 4G to 5G when HandoverNotify & registration comes together
CSCwx77878	AMF deletes the user after receiving DeregistrationNotification with a former callback URL
CSCwx79218	AMF overwrites MME-provided EPS NAS algorithm selection with locally configured algorithm

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 5. Open issues for UCC AMF, Release 2026.03.5

Bug ID	Description
CSCwv64244	T-AMF is not gracefully handling the collision of N2HO and registration procedure during SCTP Pod resiliency scenario

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

Compatibility

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

Table 6. Compatibility information for UCC AMF, Release 2026.03.5

Product	Supported Release
Ultra Cloud Core SMI	2026.03.1.08
Ultra Cloud CDL	2.3.0

Supported software packages

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

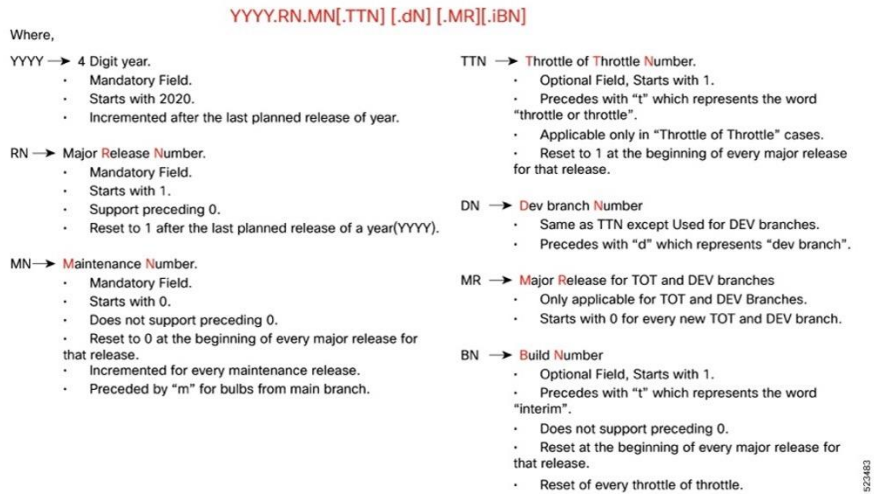
Table 7. Software packages for UCC AMF, Release 2026.03.5

Software Package	Version
amf.2026.03.5.SPA.tgz	2026.03.5
cdl-2.3.0-amf-2026.03.5.SPA.tgz	2.3.0
NED package	ncs-6.4.8.3-amf-nc-1.1.2026.03.5
NSO	6.4.8.3

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

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

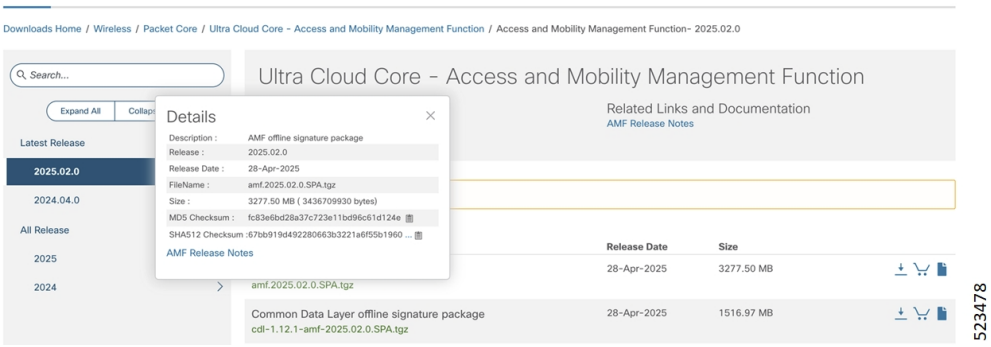
releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

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 AMF 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 8. SHA512 checksum calculation commands by 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>

<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.

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

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

AMF 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

The following table provides key resources and links to the essential documentation and support information for the Ultra Cloud Core AMF and Subscriber Microservices Infrastructure (SMI).

Table 9. Related resources and additional information

Resource	Link
AMF documentation	Access and Mobility Management Function
SMI documentation	Subscriber Microservices Infrastructure
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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

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 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.