Release Notes for UCC 5G AMF, Release 2026.04.0

Contents

Ultra Cloud Core – Access and Mobility Management Function, Release 2026.04.0 3
New software features 3
Changes in behavior 4
Resolved issues 4
Open issues 4
Compatibility 4
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 2026.04.0

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

The key highlights of this release include:

- **Automatic N2 Error Recovery**: Detects protocol errors on the N2 interface and initiates recovery actions to maintain a consistent network state and minimize service disruption.
- **Flexible Foreign PLMN Access Control**: Allows or rejects registration requests from foreign PLMNs based on GUTI or SUCI identifiers, with wildcard support for unknown PLMNs
- **Precedence-Based SUPI Policy Selection**: Matches IMSI-based SUPI against MCC, MNC, and optional MSIN ranges to assign operator policies, with precedence evaluation and a catch-all rule for unmatched subscribers.

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 2026.04.0

Milestone	Date
First Customer Ship (FCS)	5-Nov-2026
End of Life (EoL)	5-Nov-2026
End of Software Maintenance (EoSM)	5-May-2028
End of Vulnerability and Security Support (EoVSS)	5-May-2028
Last Date of Support (LDoS)	31-May-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 2026.04.0

Product impact	Feature	Description
Software Reliability	Error indication handling on the N2 interface	AMF provides improved network reliability and service continuity, as the system automatically detects and responds to protocol errors on the N2 interface. When error indications are received from the gNB, the system initiates appropriate recovery actions to maintain consistent network state and minimize service disruption.

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

Ease of Use	Foreign PLMN GUTI and SUCI management	This feature lets you control network access by allowing or rejecting registration requests from foreign PLMNs based on GUTI or SUCI identifiers. You can configure rules to process or block these requests, including handling unknown PLMNs with wildcard entries for better flexibility. Command introduced: **amf-services foreign-plmn-mgmt-db** *db_name* **{ plmn mcc** *mcc_value* **| any | mnc {** *mnc_value* **| any } [suci { allow | reject }] [guti { allow | reject }] }**– Used to configure the PLMN entry for the foreign PLMN management database. **Default Setting**: Disabled – Configuration Required
Ease of Use	SUPI policy management	This feature enables the AMF to select an operator policy by matching an IMSI-based SUPI against an MCC, MNC, and optional MSIN range. It also supports precedence-based rule evaluation and a catch-all rule for unmatched SUPIs. Command introduced: **amf-global { fiveG-policy | subscriber-map** *map_name* **{ precedence** *precedence_number* **| supi | mcc** *mcc_number* **| mnc** *mnc_number* **| msin-first** *start_range* **| msin-last** *end_range* **| operator-policy-name** *policy_name* **} }** – Used to configure a precedence-based subscriber map that associates subscribers—matched by SUPI MCC, MNC, and MSIN range—with a specified operator policy. **Default Setting**: Disabled – Configuration Required

Changes in behavior

There are no behavior changes in this release.

Resolved issues

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

Note: This software release may contain bug fixes 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 3. Resolved issues for UCC AMF, 2026.04.0

Bug ID	Description
CSCww57465	AMF path-based ingress fails when NF HTTPRoute creates shared Gateway listener without ReferenceGrant

Open issues

There are no open issues in this release.

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.

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

Table 4. Compatibility information for UCC AMF, Release 2026.04.0

Product	Supported Release
Ultra Cloud Core SMI	2026.04.1.10
Ultra Cloud CDL	2026.04.1

Supported software packages

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

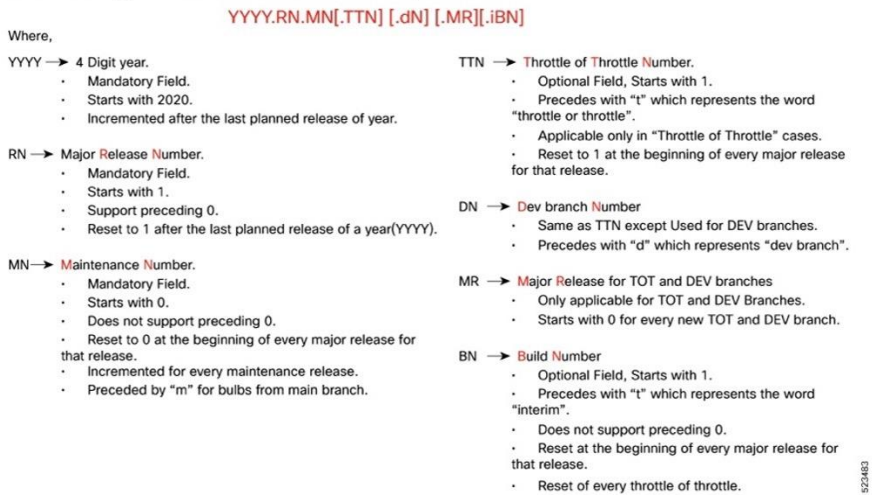
Table 5. Software packages for UCC AMF, Release 2026.04.0

Software Package	Version
amf.2026.04.0.SPA.tgz	2026.04.0
cdl-2026.04.1-amf-2026.04.0.SPA.tgz	2026.04.1
NED package	ncs-6.4.15-amf-nc-1.1.2026.04.0
NSO	6.4.15

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.

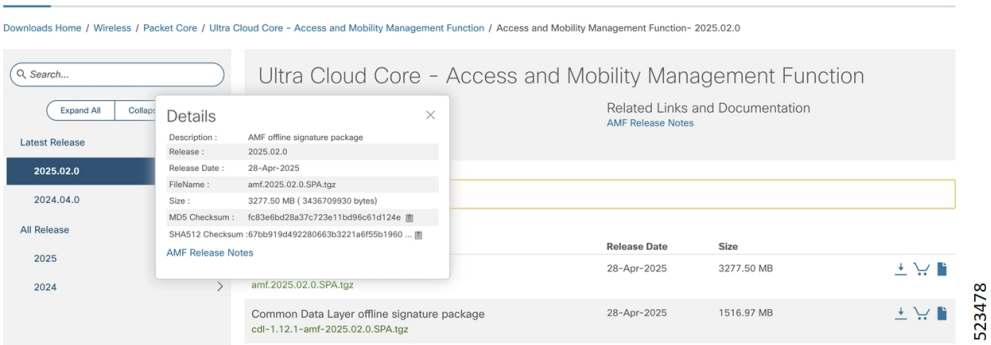
© 2026 Cisco and/or its affiliates. All rights reserved.

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 6. 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.

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.

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

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 7. 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.