



Release Notes for UCC 5G AMF, Release 2026.01.0



Contents

- Ultra Cloud Core – Access and Mobility Management Function, Release 2026.01.0 3
- New software features 3
- Changes in behavior 4
- Resolved issues 4
- Open issues..... 4
- Compatibility..... 5
- Supported software packages 5
- Related resources..... 7
- Legal information 7

Ultra Cloud Core - Access and Mobility Management Function, Release 2026.01.0

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

The key highlights of this release include:

- **AMF performance enhancements:** Enhances performance for event processing.
- **UE location reporting to SMF via AMF event subscription:** Enables the SMF to directly subscribe to the AMF for UE location information.
- **Public Warning System (PWS) Inter Working Functionality (IWF):** Simplifies public warning system operations by consolidating functionality and offering flexible, protocol-based configuration options within the AMF.

For more information on the AMF software product, 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 2026.01.0

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

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

Table 2. New software features for UCC AMF, Release 2026.01.0

Product impact	Feature	Description
Software Reliability	Performance enhancements for AMF	This feature enhances the event processing and offers new configuration options to optimize resource allocation.
Upgrade	UE location reporting to SMF through AMF event subscription	AMF handles event subscriptions requests coming from SMF for location reporting. With this implementation, the SMF directly subscribes to the AMF for location information.

Product impact	Feature	Description
Upgrade	PWS-IWF functionality	<p>This feature enables the AMF to process the SBc interface messages using the SBc Application Protocol (SBc-AP), allowing direct communication with the CBC. The PWS-IWF functionality is now integrated within the AMF, removing the requirement for a separate PWS-IWF node. This streamlines the network architecture and reduces processing overhead.</p> <p>Command introduced:</p> <ul style="list-style-type: none"> amf-services amf_services_name pws-enabled interface [Sbi][SBc]– The interface option SBc is used to enable the PWS-IWF functionality via CBC over SBc-AP protocol. The default value of the interface is Sbi where PWS messages are handled via CBCF over N50 interface. <p>Runtime change in the interface value is not supported and hence requires ops center shut and start.</p> <ul style="list-style-type: none"> amf-services amf_services_name pws-enabled interface SBc custom-enabled– The custom option is only applicable for SBc interface which allows AMF to process custom requirements – such as conversion of TAC and handling of warning area list IE. <p>Default Setting: Disabled – Configuration Required</p>

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 Ultra Cloud Core – Access and Mobility Management Function, Release 2026.01.0

Bug ID	Description
CSCws41393	proto-ep pod failure for PWS restart and failure indication in bulk call
CSCws92825	Few Cause codes(#7, #31, #27) to be added for context transfer failure and authentication failure errors for allowing UE to move to EPS
CSCws94421	AMF is not using the ulnas cnt from the most recent security mode command when multiple smc happens during registration request

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 4. Open issues for Ultra Cloud Core – Access and Mobility Management Function, Release 2026.01.0

Bug ID	Description
CSCwt02824	minor service pod memory leak observed during longevity run

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 5. Compatibility information for UCC AMF, Release 2026.01.0

Product	Supported Release
Ultra Cloud Core SMI	2026.01.1.08
Ultra Cloud CDL	2.1.0

Supported software packages

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

Table 6. Software packages for UCC AMF, Release 2026.01.0

Software Package	Version
amf.2026.01.0.SPA.tgz	2026.01.0
cdl-2.1.0.i0-amf-2026.01.0.SPA.tgz	2.1.0
NED package	ncs-6.4.8.2-amf-nc-1.1.2026.01.0
NSO	6.4.8.2

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

Where,

YYYY → 4 Digit year.

- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.

- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.

- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number

- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches

- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number

- Optional Field, Starts with 1.
- Precedes with "i" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

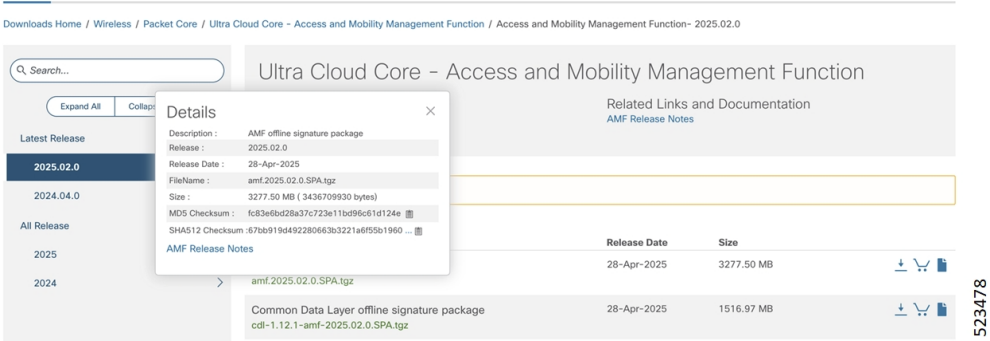
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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



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. 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.

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 8. 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.