Release Notes for the Ultra Cloud Core Access and Mobility Management Function Version 2023.04.0

First Published: 2023-10-18

Ultra Cloud Core Access and Mobility Management Function

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Oct-2023
End of Life	EoL	31-Oct-2023
End of Software Maintenance	EoSM	30-Apr-2025
End of Vulnerability and Security Support	EoVSS	30-Apr-2025
Last Date of Support	LDoS	30-Apr-2026

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.

Release Package Version Information

Software Packages	Version
amf.2023.04.0.SPA.tgz	2023.04.0
cdl-1.11.5-amf-2023.04.0.SPA.tgz	1.11.5
NED package	ncs-6.1-amf-nc-2023.04.0
NSO	6.1.3

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 6 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2023.04.1
Ultra Cloud CDL	1.11.5

For information on the Ultra Cloud Core SMI release, refer to the SMI documents available at:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/series.html

What's New in this Release

New in Documentation

This version of Release Notes includes a new section titled **What's New in this Release** comprising of all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.01.0, the RCR document will be deprecated.

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
Enhancements to AMF Statistics	Updated the statistics used in AMF service for all inbound and outbound messages/procedures. Introduced new statistics to track the N14 failure request and response messages. **Default Setting**: Not Applicable
Monitor Subscriber	AMF supports the monsub to capture the N1/N2/N8/N11/N12/N15/N20/N22/N26 interface level messages. **Default Setting**: Disabled – Configuration Required
Network Slicing Support	AMF allows the slice selection and reallocation during the UE registration. **Default Setting**: Disabled – Configuration Required
Service Area Restriction	AMF supports the service area restriction for the UE to enforce restrictions on the services that UE can access based on location and tracking area codes. **Default Setting**: Disabled – Configuration Required

Behavior Changes

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

Feature	Description
Enhancement to the Context Release Command Sent to gNB and SMF	**Previous Behavior:** When a user equipment (UE) initiates the establishment of new UE-associated logical NG-connection while there is already an existing connection within the AMF, then AMF does not send the UE Context Release Command to gNB. **New Behavior:** When a user equipment (UE) initiates the setup of a new UE-associated logical NG-connection while there is already an existing connection within the AMF, then: • "UE Context Release Command" is sent to the gNB to release the existing context associated with UE. • PDU session modify is sent to SMF for the available PDU in AMF with status as deactivated.

Related Documentation

For the complete list of documentation available for this release, see:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-access-mobility-management-function/products-installation-and-configuration-guides-list.html

Installation and Upgrade Notes

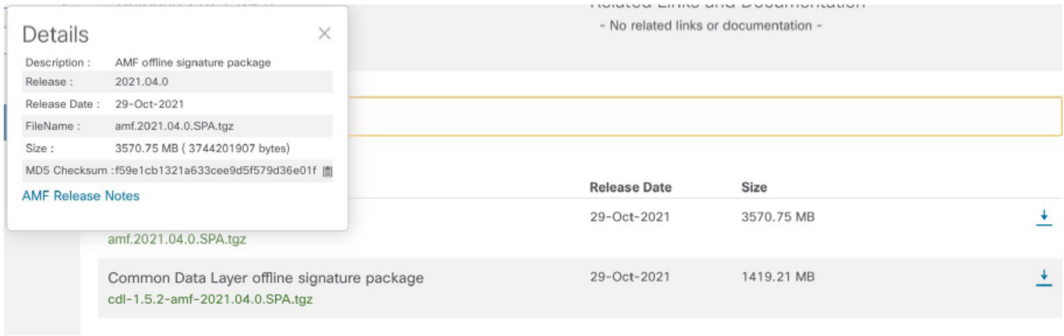
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Note ETCD v3.5.x does not support in-service downgrade to 3.4.x. If you are downgrading from 2023.04.0 builds to previous releases, perform system mode shutdown before downgrade.

Software Integrity Verification

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.



Details

Description : AMF offline signature package
Release : 2021.04.0
Release Date : 29-Oct-2021
FileName : amf.2021.04.0.SPA.tgz
Size : 3570.75 MB (3744201907 bytes)
MD5 Checksum :f59e1cb1321a633cee9d5f579d36e01f

AMF Release Notes

- No related links or documentation -

	Release Date	Size
amf.2021.04.0.SPA.tgz	29-Oct-2021	3570.75 MB
Common Data Layer offline signature package cdl-1.5.2-amf-2021.04.0.SPA.tgz	29-Oct-2021	1419.21 MB

523478

At the bottom, you will find the SHA512 checksum. If you do not see the whole checksum, you can expand it by pressing "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the table below.

Table 1: 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 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 to not 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.

Open Bugs for this Release

The following table lists the open bugs in this specific software release.

Note This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release is available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwh87733	service pods go routine increase trend observed for N26 Connected HO

Resolved Bugs for this Release

The following table lists the resolved bugs in this specific software release.

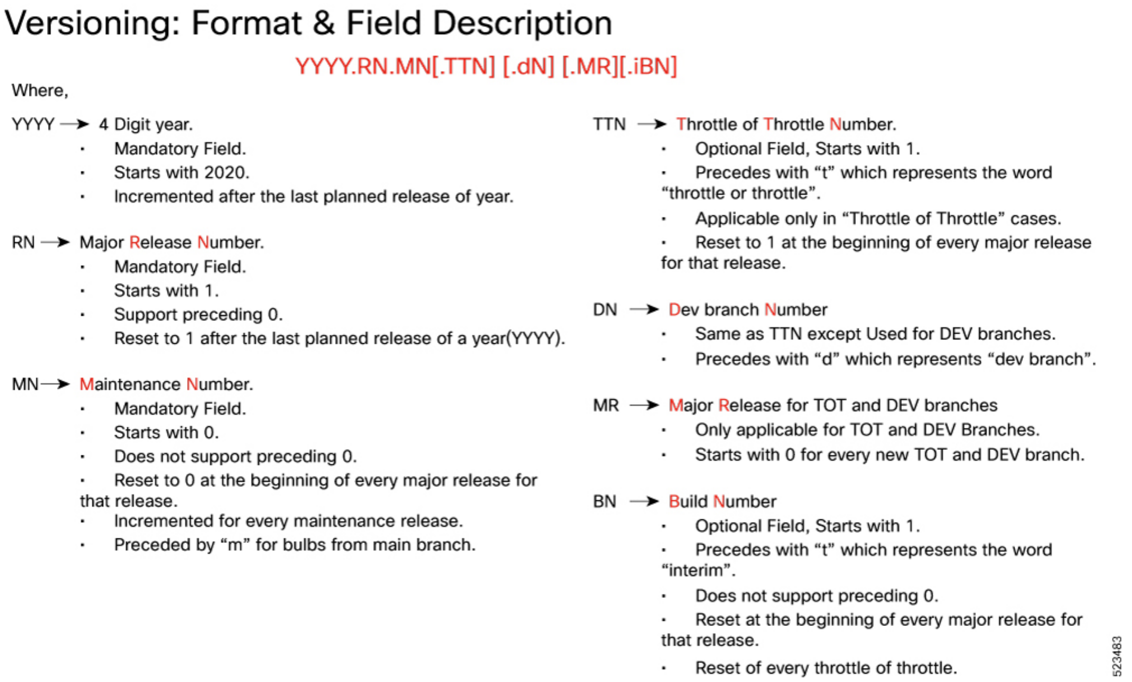
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwe69418	PDCP integrity check failure for RRC Reconfiguration Complete during HO 5G to 4G after HO Command	No
CSCwf48354	No PDUSession modify with upCnxState DEACTIVATED sent to SMF after UEContextReleaseRequest	Yes
CSCwf69143	NGAP response not received from AMF after node 1 power off	No
CSCwf79433	Call model not recovered after sync successful for rolling upgrade from CM to AMF	No
CSCwf93938	AMF upgrade from i138 April to i137 july, call model impacted	No

Operator Notes

Cloud Native Product Version Numbering System

The show helm list command displays detailed information about the version of the cloud native product currently deployed.



Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

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 "t" 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.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
amf.<version>.SPA.tgz	The offline release signature package. This package contains the AMF deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-amf-<version>.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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.