Release Notes for the Ultra Cloud Serving Gateway Control Plane Function, Version 2024.02.0

First Published: 2024-04-30

Ultra Cloud Serving Gateway Control Plane 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	30-Apr-2024
End of Life	EoL	30-Apr-2024
End of Software Maintenance	EoSM	29-Oct-2025
End of Vulnerability and Security Support	EoVSS	31-Oct-2025
Last Date of Support	LDoS	31-Oct-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**
ccg-2024.02.0.SPA.tgz	2024.02.0
NED package	ncs-5.6.8-ccg-nc-2024.02.0 ncs-6.1-ccg-nc-2024.02.0
NSO	5.6.8 6.1.3

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

Note The ccg.<*version*>.SPA.tgz software package is common to both the cnSGWc and SMF 5G Network Functions (NF). The deployment and configuration procedure determines the NF deployment.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.02.1.14
Ultra Cloud CDL	1.11.7
Ultra Cloud Core UPF	2024.02.0
Ultra Cloud SMF	2024.02.0

For information on the Ultra Cloud Core products, refer to the documents for this release available at:

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/products-installation-and-configuration-guides-list.html

What's New in this Release

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
Charging Support for Converged Calls	With UPF supporting the collapsed-data path functionality, cnSGW supports charging with converged UPF (UPF + SGW-U). This support prevents affecting the Local Breakout (LBO) calls for which the carrier uses SGW-based CDRs for reporting and charging. **Default Setting**: Not Applicable

Feature	Description
Dual Stack Support for Data Plane	cnSGW-c enables the dual stack transport for Data Plane using the **dual-stack-transport { false | true }** CLI command in the UPF network profile. With this support, you can: • Configure new eNBs and UPFs with IPv6 addresses for network expansion. • Continue with the existing eNBs and UPFs with IPv4 addresses for phased migration to IPv6 addresses. **Default Setting:** Disabled – Configuration Required
Rolling Upgrade Optimization	Converged Core Gateway provides the following support: • Retry mechanism at service and protocol pods during upgrades • Configuration-based rolling upgrade enhancements This optimization helps in reduced session and Call Events Per Second (CEPS) loss during the upgrade procedure. The configurable rolling upgrade enhancements enable smooth rollout of the changes. This feature introduces the new CLI command **supported-features [app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra]** in the converged core profile. **Default Setting:** Disabled – Configuration Required
Supporting IPv6 Only eNB Insertion through Show and Clear Subscriber CLI commands	Before you add IPv6 only eNBs in a network, all UPFs in a mesh must be IPv6 enabled for successful handovers of IPv4 only eNB sessions to IPv6 only eNB sessions. In addition, all sessions must have V4V6 tunnel before inserting a V6 only eNB. To support this IPV6 only eNB insertion, cnSGW-c includes the following CLI commands: • The **show subscriber nf-service sgw data-tunnel** *data_tunnel_type* and **show subscriber count nf-service sgw data-tunnel** *data_tunnel_type* CLI commands • The **clear subscriber nf-service sgw data-tunnel** *data_tunnel_type* CLI command **Default Setting**: Not Applicable

Behavior Changes

There are no behavior changes in this release.

Related Documentation

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

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

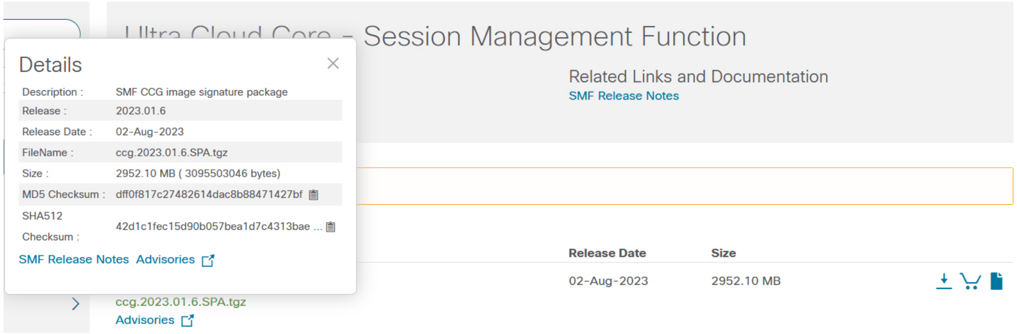
Installation and Upgrade Notes

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

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.



Ultra Cloud Core - Session Management Function

Related Links and Documentation
SMF Release Notes

Details

Description :	SMF CCG image signature package
Release :	2023.01.6
Release Date :	02-Aug-2023
FileName :	ccg.2023.01.6.SPA.tgz
Size :	2952.10 MB (3095503046 bytes)
MD5 Checksum :	dff0f817c27482614dac8b88471427bf
SHA512 Checksum :	42d1c1fec15d90b057bea1d7c4313bae ...

SMF Release Notes Advisories

	Release Date	Size
ccg.2023.01.6.SPA.tgz Advisories	02-Aug-2023	2952.10 MB

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 Table 1 and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the following table.

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`

Operating System	SHA512 checksum calculation command examples
NOTES: *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

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.

Open Bugs for this Release

The following table lists the open bug 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 are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwj66542	IntraMME, InterEnB HO failures seen during Rolling upgrade
CSCwi11657	Evaluation of sgw for HTTP/2 Rapid Reset Attack vulnerability

Resolved Bugs for this Release

The following table lists the known bug that is resolved 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.

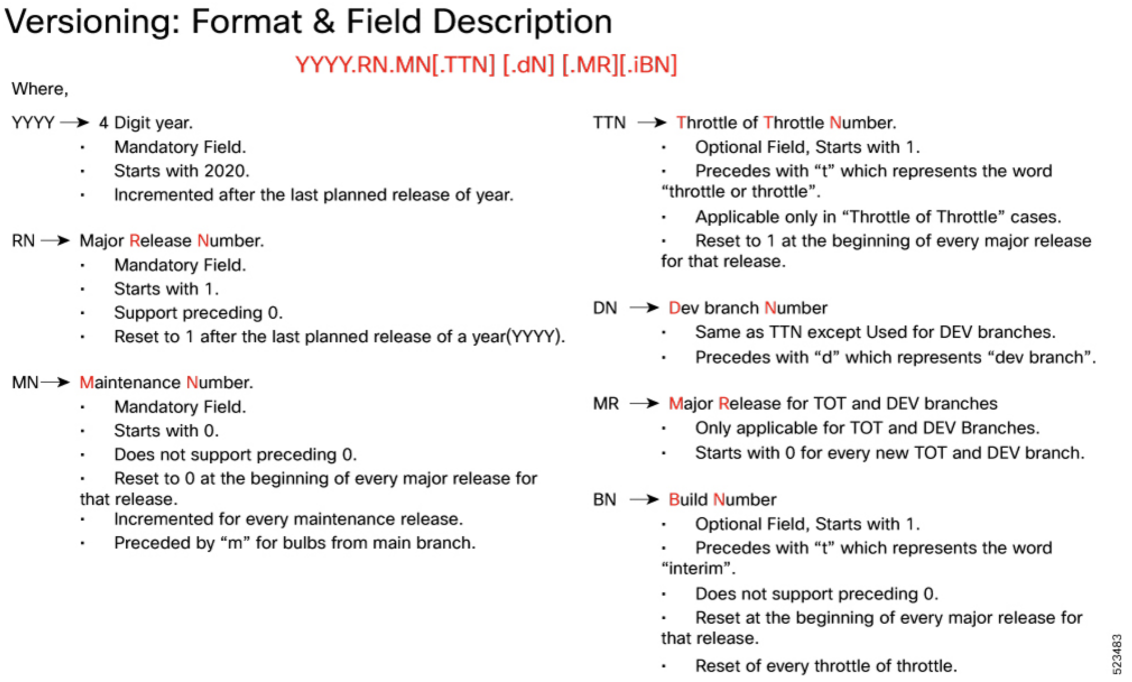
Bug ID	Headline	Behavior Change
CSCwi21692	On Converged Core (cn-ccg-smf)when trying the 4G attach User plane Selection failure Occured	No

Bug ID	Headline	Behavior Change
CSCwj31295	udp-prox is listening to all the IPs/Ports; needs to have some restrictions around it	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

This table lists provide descriptions for the packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
ccg.<version>.SPA.tgz	The offline release signature package. This package contains the deployment software as well as the release signature, certificate, and verification information.

Software Packages	Description
ncs-<nso_version>-ccg-nc-<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.

Note The ccg.<*version*>.SPA.tgz software package is common to both the cnSGWc and SMF 5G Network Functions (NF). The deployment and configuration procedure determines the NF deployment.

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.