# Release Notes for UCC 5G UPF, Release 2026.02.h1

## Ultra Cloud Core - User Plane Function, Release 2026.02.h1

This Release Notes identifies changes and issues related to the release of 5G User Plane Function (UPF).

The key highlights of this release include:

**Optimized resource utilization and improved network efficiency:** This release increases software reliability by allowing to negotiate per-peer PFCP compression at N4 and Sx interfaces allowing CUPS and Converged Core (SMF and cnSGWc) to co-exist on the same UPF.

For more information on UPF, see the Related resources section.

### Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC UPF software:

**Table 1.** EoL milestone information for UCC UPF, Release 2026.02.h1

| Milestone | Date |
|---|---|
| First Customer Ship (FCS) | 23-Apr-2026 |
| End of Life (EoL) | 23-Apr-2026 |
| End of Software Maintenance (EoSM) | 22-Oct-2027 |
| End of Vulnerability and Security Support (EoVSS) | 22-Oct-2027 |
| Last Date of Support (LDoS) | 31-Oct-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

There is no new software features in this release.

## Changes in behavior

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

**Table 2.** Behavior changes for UCC UPF, Release 2026.02.h1

| Description | Behavior changes |
|---|---|
| ConfD Schema Compatibility Handling [CSCwo47013] | **Previous Behavior:** During ConfD upgrades, version incompatibilities with persisted schema files could lead to initialization failures and repeated confdmgr crashes; as there was no CLI utility available to clear this data, it was necessary to manually remove the contents of the /mnt/hd-raid/meta/confd directory during the upgrade process to ensure system stability.<br><br>**New Behavior:** A new CLI command, **clear confdmgr confd all**, has been introduced to clear all persistent ConfD data, which facilitates a clean reinitialization and prevents initialization failures during upgrades. |

| Description | Behavior changes |
|---|---|
| | For more information on the method of procedure, refer to the Upgrade the confD version. |

## 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 3.** Resolved issues for UCC UPF, Release 2026.02.h1

| Bug ID | Description |
|---|---|
| CSCwm14072 | Bulkstat CLI getting stuck with performance driven schema. |
| CSCws23012 | CALEA calls; wrong value in Timestamp FractionPart for X3. |
| CSCwt49018 | UPF sending Tariff time reporting as future date start time as future and end time as current. |
| CSCwt59091 | BGP process restart causes missing default route entries in VRF and stale entries in MPLS FTN table. |
| CSCwt95669 | Gy URR Usage Report sent more frequently at incorrect interval after N:M UP switchover. |
| CSCwu44945 | UPF is incorrectly checksum with 0x0000 which is invalid per RFC 2460. |

## 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 4.** Open issues for UCC UPF, Release 2026.02.h1

| Bug ID | Description |
|---|---|
| CSCws50373 | sessmgr restart observed on UPF, memory allocation failed. |
| CSCwt70285 | UPF Sends HTTP 302 Redirect After QER Gate Status Set to CLOSED. |
| CSCwt93390 | Seeing npumgr error logs ares_npumgr_vl_api_create_loopback_instance_t_callback. |

## Known issues

This section describes the known issue that may occur during the upgrade of the UPF image.

## Install 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.

**Upgrade the confD version**

This section explains upgrading third-party software. Upgrade the confD software to ensure system compatibility and performance.

**Note**: During the 2026.02.0 release, the confD software is upgraded to 8.6 version.

**Prerequisites:**

- Ensure you have appropriate permissions to perform this upgrade.
- Back up all necessary data and configurations to avoid permanent loss during file deletion.
- The ConfD configuration must be removed before running the **clear confdmgr confd all** CLI command.

Perform these steps to upgrade the confD version on the system.

- Enter the debug shell using debug shell command.
- Navigate to the confD directory.
- Run the command: cd /mnt/hd-raid/meta/confd/ to access the directory.
- Remove existing files with the command; rm -rf *

  -or-

  Run the StarOS CLI command **clear confdmgr confd all** to clear the same confD contents.

  **Note**: The /mnt/hd-raid/meta/confd directory will be empty. After clearing, confD can be started again as required. This clear cli should be used only during ConfD upgrade scenarios and not on each reload or reboot.

All files and subdirectories are deleted, preparing the system for a fresh installation. To preserve data across the Method of Procedure, users with ConfD configured must contact their Cisco accounts representative.

## Compatibility

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

**Table 5.** Compatibility information for UCC UPF, Release 2026.02.h1

| Product | Supported Release |
|---|---|
| ADC Plugin | 2.74.gh2.2788 |

| Product | Supported Release |
|---|---|
| RCM | 2026.02.0 |
| Ultra Cloud Core SMI | 2026.02.1.07 |
| Ultra Cloud SMF and cnSGWc | 2026.02.0 |

## Supported software packages

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

**Table 6.** Software packages for UCC UPF, Release 2026.02.h1

| Software Package | Description | Release |
|---|---|---|
| companion-vpc-2026.02.h1.zip.SPA.tar.gz | Contains files pertaining to VPC, including SNMP MIBs, RADIUS dictionaries, ORBEM clients, etc. These files pertain to both trusted and non-trusted build variants. The VPC companion package also includes the release signature file, a verification script, the x.509 certificate, and a README file containing information on how to use the script to validate the certificate. | 2026.02.h1 (21.28.mh39.100730) |
| qvpc-si-2026.02.h1.bin.SPA.tar.gz | The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.<br>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build. | 2026.02.h1 (21.28.mh39.100730) |
| qvpc-si-2026.02.h1.qcow2.zip.SPA.tar.gz | The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.<br>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build. | 2026.02.h1 (21.28.mh39.100730) |
| NED Package | The NETCONF NED package. This package includes all the yang files that are used for NF configuration. | ncs-6.4.8.2-cisco-staros-cli-5.58 |
| NSO | Note that NSO is used for the NED file creation. | 6.4.8 |

Use this link to download the NED package associated with the software.

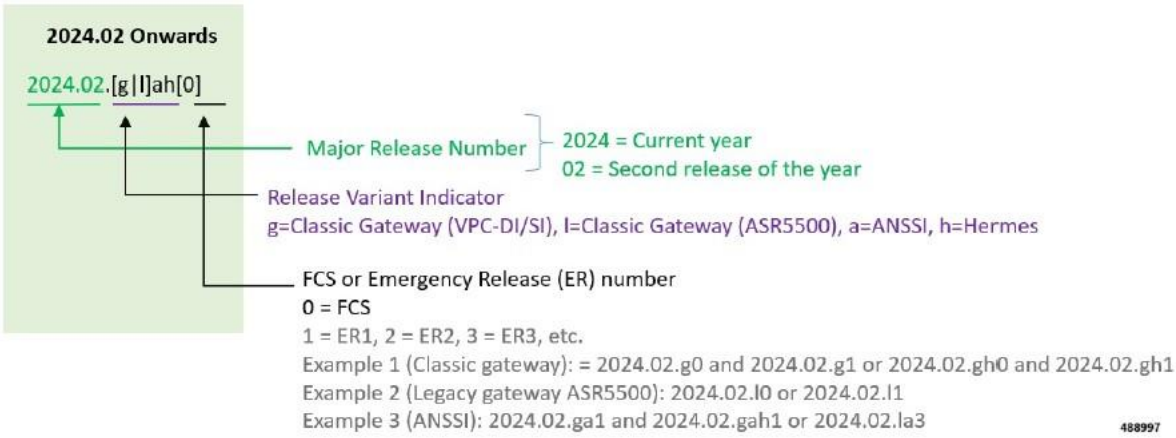
## StarOS version numbering system

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

**Note:** Starting 2024.01.0 release (January 2024), Cisco is transitioning to a new release versioning scheme. The release version is based on the current year and product. Refer to the figure for more details.

During the transition phase, some file names will reflect the new versioning whereas others will refer to the 21.28.x- based naming convention. With the next release, StarOS-related packages will be completely migrated to the new versioning scheme.

**Figure 1. StarOS version numbering system format**

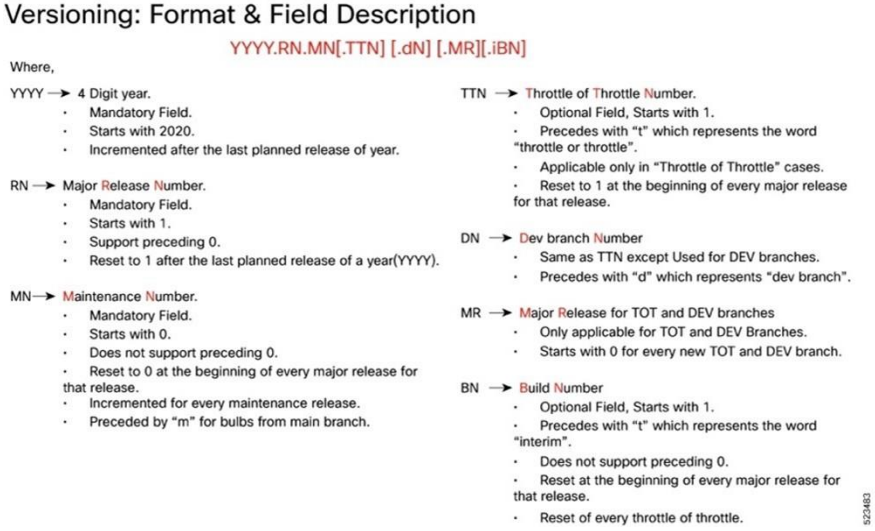



For any clarification, contact your Cisco account representative.

## 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 2. Cloud native product versioning format and description**



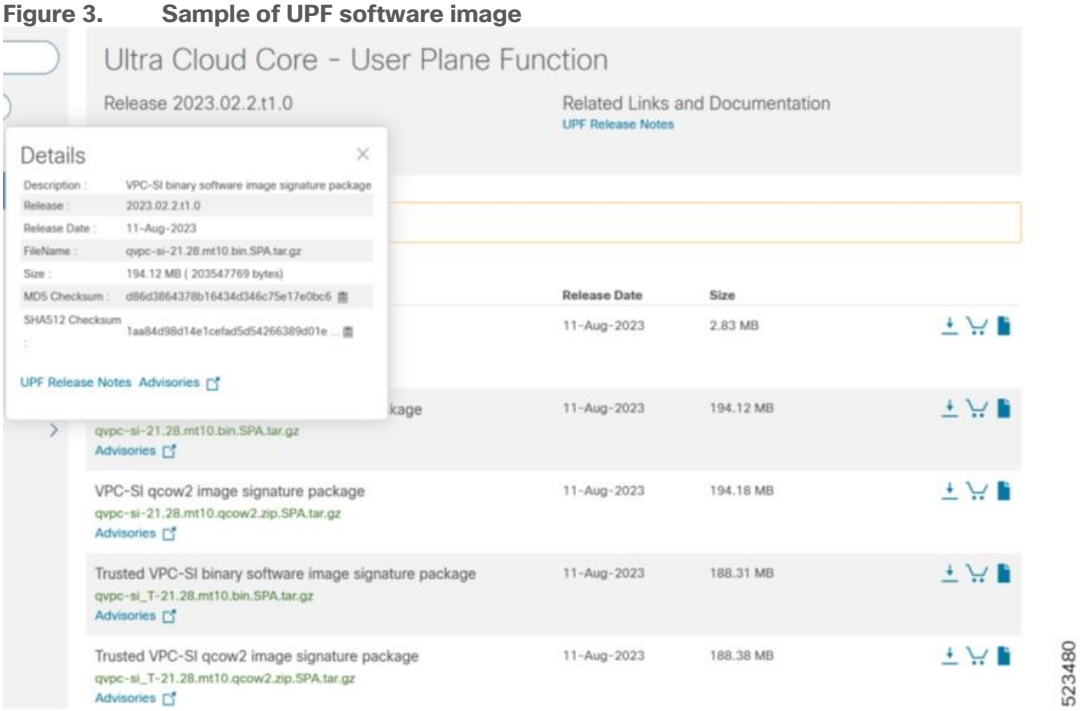

The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

## 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 3. Sample of UPF 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 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:<br>`> certutil.exe -hashfile <filename.extension> SHA512` |
| Apple MAC | Open a terminal window and type the following command:<br>`$ shasum -a 512 <filename.extension>` |
| Linux | Open a terminal window and type the following command:<br>`$ sha512sum <filename.extension>`<br>OR<br>`$ shasum -a 512 <filename.extension>` |
| **Note:** <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

UPF 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

**Table 8.** Related resources and additional information

| Resources | Link |
|---|---|
| UPF documentation | User Plane Function |
| Ultra Cloud Core Subscriber Microservices Infrastructure | Subscriber Microservices Infrastructure |
| Ultra Cloud Core Session Management Function | Session Management Function |
| Ultra Cloud Core Serving Gateway Function | Ultra Cloud Core Serving Gateway Function |
| Service Request and Additional information | Cisco Support |

## Legal information