Release Notes for UCC 5G PCF, Release 2026.02.0

Contents

Ultra Cloud Core – Policy Control Function, Release 2026.02.0 3
New software features 3
Changes in behavior 4
Resolved issues 4
Open issues 4
Compatibility 4
Supported software packages 4
Related resources 7
Legal information 7

Ultra Cloud Core – Policy Control Function, Release 2026.02.0

This Release Notes identifies changes and issues related to the release of Ultra Cloud Core Policy Control Function (PCF).

The key highlights of this release include:

- **PCF Sy Interface enhancements**: PCF now supports the Supported-Features and SN-Request-Type AVPs, enabling improved session management and robust handling of abort use cases on the Sy interface.
- **SCP Integration (Model-D)**: Added support for the 3GPP Rel.16 indirect communication model (Model-D) with delegated discovery, enabling the Service Communication Proxy (SCP) to mediate. signaling between SMF-PCF and BSF-PCF.

For more information about PCF, see the Related resources section.

Release lifecycle milestones

This table provides EoL milestones for Cisco UCC PCF software:

Table 1. EoL milestone information for Ultra Cloud Core – Policy Control Function

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

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

Table 2. New software features for UCC PCF, Release 2026.02.0

Product impact	Feature	Description
Software reliability	Service Communication Proxy (SCP) Model-D for	In 3GPP Release 16 Model-D with delegated discovery, the Service Communication Proxy (SCP) performs discovery and routing on behalf of network functions. The SMF sends requests to the SCP, which discovers

Product impact	Feature	Description
	Indirect Node Communication	and forwards them to the PCF, where the PCF acts as a producer processing request received via the SCP. When the PCF needs to interact with the BSF, it acts as a consumer, sending requests to the SCP, which then discovers the appropriate BSF via the NRF and forwards the requests.
Software reliability	Sy Interface AVP support and enhancements	This feature improves session management and handles abort use cases on the Sy interface by updating the Policy Control Function (PCF). The PCF now supports the Supported-Features and SN-Request-Type AVPs. These additions enable the system to negotiate features and accurately process request types within incoming Spending-Status-Notification-Request (SNR) messages, ensuring more robust control over subscriber spending status reporting.

Changes in behavior

There are no behavior changes introduced 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 introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 3. Resolved issues for Product Name, Release, 2026.02.0

Bug ID	Description
CSCwt09602	Unexpected creation of br-controller-scdb pod after PCF July-25 FCS upgrade

Open issues

There are no open bugs in this specific software release.

Compatibility

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

Table 4. Compatibility information for Ultra Cloud Core - Policy Control Function, Release 2026.02.0

Product	Supported Release
Ultra Cloud Core SMI	2026.02.1.07
Ultra Cloud CDL	2.2.0

Supported software packages

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

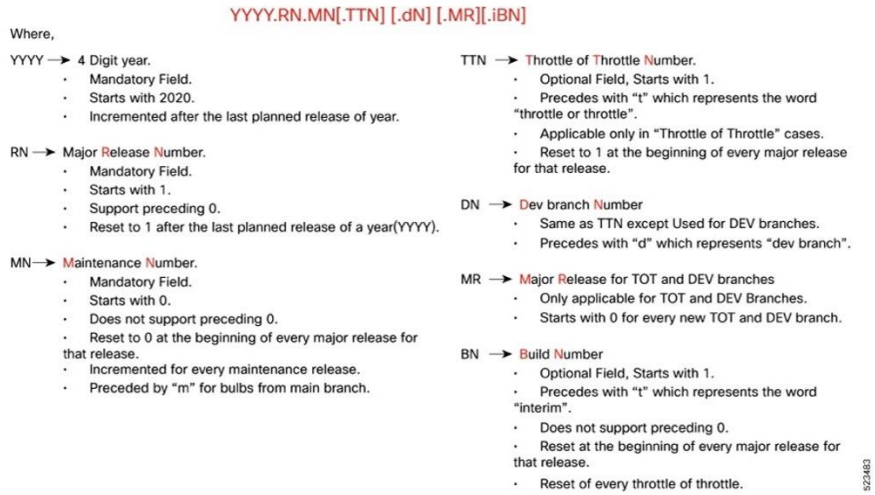
Table 5. Software packages for Ultra Cloud Core – Policy Control Function, Release 2026.02.0

Software package	Description	Release
pcf.2026.02.0.SPA.tgz	The PCF offline release signature package. This package contains the PCF deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.02.0
ncs-6.4.8.2-cisco-pcf-nc-1.1.2026.02.0.tar.SPA.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	6.4.8.2
ncs-6.1.14-cisco-pcf-nc-1.1.2026.02.0.tar.SPA.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	6.1.14

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**



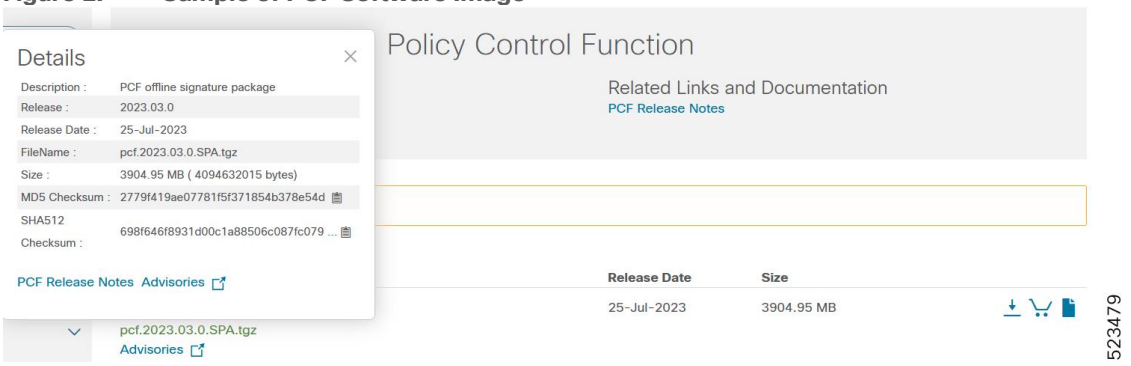
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

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 PCF 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. 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 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 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

PCF 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

This table provides key resources and links to the support information and essential documentation for PCF and SMI.

Table 7. Related resources and additional information

Resource	Link
PCF documentation	Policy Control Function
SMI documentation	Subscriber Microservices Infrastructure
Service request and additional information	Cisco Support

Legal information