Release Notes for UCC 5G PCF, Release 2025.04.0

Contents

Ultra Cloud Core – Policy Control Function, Release 2025.04.0

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:

- Cross-Site session handling for distributed PCF: Improved service continuity and reliability during site failovers, load balancing, or dynamic routing.
- Periodic backup option for Ops Center, PB and CRD: Reduces manual workload and risk of configuration loss.
- Serviceability enhancements: Simplifies troubleshooting and diagnostics of network issues in application pods.

For more information about PC, 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)	31-Oct-2025
End of Life (EoL)	31-Oct-2025
End of Software Maintenance (EoSM)	01-May-2027
End of Vulnerability and Security Support (EoVSS)	01-May-2027
Last Date of Support (LDoS)	30-Apr-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 Ultra Cloud Core – Policy Control Function, Release 2025.04.0

Product impact	Feature	Description
Ease of use	Cross-Site session handling for distributed	The feature enables PCF nodes to process Rx session-related messages for sessions created at other sites. When the system is configured to

Product impact	Feature	Description
	PCF	accept Diameter messages with unknown destination hostnames, session processing continues during site failovers, load balancing, or dynamic routing scenarios.
Ease of setup	Auto-backup of PB, CRD and Ops Center configurations	This feature allows for automated backups of PB, CRD, and Ops Center configurations through customizable schedules and on-demand triggers. It consolidates backup processes, replacing manual tasks with automation, thereby enhancing operational efficiency.
Ease of use	TCP Dump Functionality for Enhanced Serviceability	You can now easily troubleshoot network issues in critical application pods using the tcpdump functionality, while ensuring minimal impact on system performance and efficient management of captured TCP dump files. **Command introduced: pcf-system tcpdump** { capture | clear } – Used to capture the network traffic using tcpdump command in specified pod. **Default Setting**: Disabled – Configuration Required

Changes in behavior

There is 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. 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 – Policy Control Function, Release 2025.04.0

Bug ID	Description	Product Found
CSCwr39806	N7 update failure from SMF with unsuccessful QoS value due to missing ARP parameters.	pcf

Open issues

This table provides open bugs in this specific software release.

Table 4. Open issues for Ultra Cloud Core – Policy Control Function, Release 2025.04.0

Bug ID	Description	Product Found
CSCwr88736	PCF-NED: Error while package reload with PCF NED for 6.4.8.1/6.1.14	pcf

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 5. Compatibility information for Ultra Cloud Core – Policy Control Function, Release 2025.04.0

Product	Supported Release
Ultra Cloud Core SMI	2025.04.1.15
Ultra Cloud CDL	1.12.3

Supported software packages

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

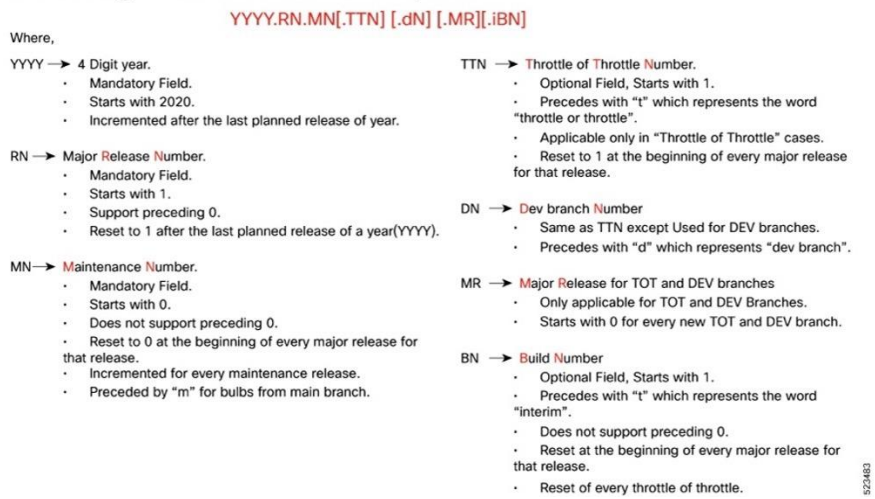
Table 6. Software packages for Ultra Cloud Core – Policy Control Function, Release 2025.04.0

Software package	Description	Release
pcf.2025.04.0.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.	2025.04.0
ncs-6.4.8.1-cisco-pcf-nc-1.1.2025.04.0.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	6.4.8.1
ncs-6.1.14-cisco-pcf-nc-1.1.2025.04.0.tar.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**



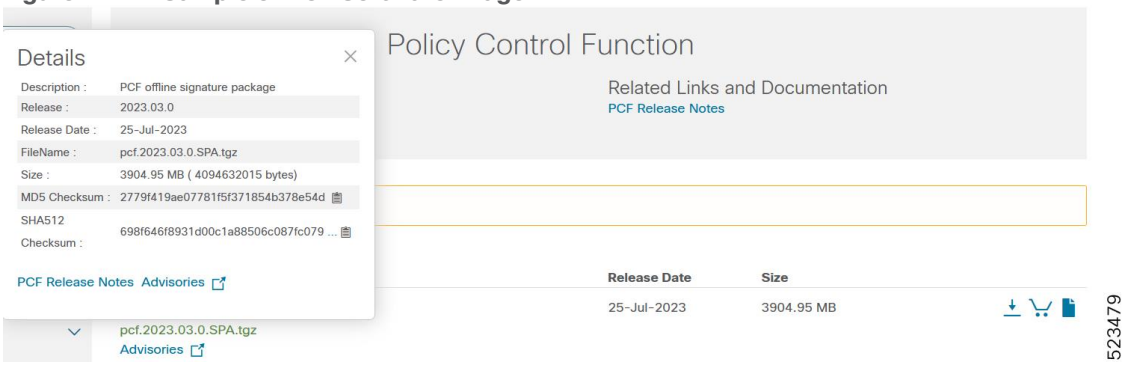
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 7. 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 8. 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