Release Notes for UCC 5G PCF, Release 2026.01.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Ultra Cloud Core – Policy Control Function, Release 2026.01.0 3
New software features 3
Changes in behavior 4
Resolved issues 4
Open issues 4
Compatibility 5
Supported software packages 5
Related resources 7
Legal information 7

© 2026 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core – Policy Control Function, Release 2026.01.0

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:

- **Configurable pod Anti-affinity for Policy Engine pods**: Operators can now choose between strict and relaxed anti-affinity modes for Policy Engine pods.
- **PCF-based QoS boost validity timers**: PCF supports time-bound and priority-based QoS boost profile for subscribers.
- **Database monitoring dashboard**: You can optionally deploy a dedicated Grafana-based monitoring dashboard for key data stores such as MongoDB replica sets.

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)	30-Jan-2026
End of Life (EoL)	30-Jan-2026
End of Software Maintenance (EoSM)	31-July-2027
End of Vulnerability and Security Support (EoVSS)	31-July-2027
Last Date of Support (LDoS)	31-July-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 2026.01.0

Product impact	Feature	Description
Software Reliability	Configurable pod anti-affinity for policy	This feature supports configurable anti-affinity for Policy Engine pods, allowing operators to choose between strict and relaxed modes. This

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	engine pods	enhancement improves pod placement efficiency and resource utilization, especially in environments with limited nodes or high CPU density, while preserving high availability as the default behavior.
Software Reliability	PCF-based QoS boost validity timers	This enhancement introduces support for time-bound and priority-based QoS boost profiles for subscribers, enabling dynamic control of APN-level AMBR and 5QI through configured validity timers. Operators can provision multiple QoS schedules per subscriber, each with explicit start and end times, allowing temporary QoS uplift and automatic reversion to the previously active profile upon expiry. The PCF evaluates configured schedules and applies the appropriate QoS profile to active and newly established sessions, ensuring deterministic behavior across Gx and N7 interfaces.
Ease of use	Deploy database monitoring dashboard	You can enable or disable the deployment of a specific DB Monitoring dashboard (Grafana JSON) by setting a configuration value. As a result, the dashboard is deployed only when needed, which optimizes resource usage and provides critical insights into database health and usage. The Database Monitoring Dashboard provides dedicated monitoring capabilities for key PCF data stores, such as MongoDB replica sets. Command Introduced: t**esting enable-optional-dashboards** [**true**| **false**].

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, 2026.01.0

Bug ID	Description
CSCws21069	PCF Oct feature TCPDump functionality not working for ldap pod
CSCws21074	PCF Oct feature TCPDump functionality cleanup flag not working as expected
CSCws68184	PCF: Mongo upgrade from our current version 7.0.14 to 7.0.28

Open issues

There are no open bugs in this specific software release.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 2026.01.0

Product	Supported Release
Ultra Cloud Core SMI	2026.01.1.08
Ultra Cloud CDL	2.1

Supported software packages

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

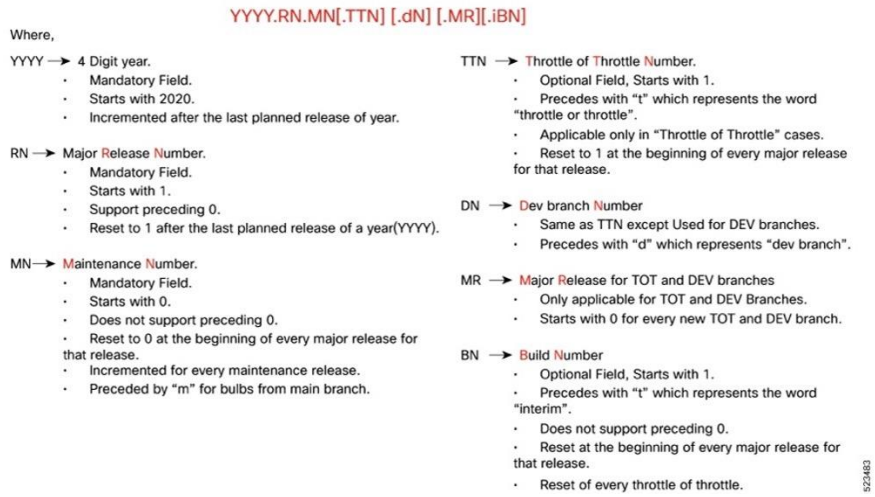
Table 5. Software packages for Ultra Cloud Core – Policy Control Function, Release 2026.01.0

Software package	Description	Release
pcf.2026.01.0.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.	2026.01.0
ncs-6.4.8.2-cisco-pcf-nc-1.1.2026.01.0.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-1.1.2026.01.0.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**



© 2026 Cisco and/or its affiliates. All rights reserved.

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).	

© 2026 Cisco and/or its affiliates. All rights reserved.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.