# Release Notes for UCC 5G PCF,Release 2025.03.0

# Contents

Ultra Cloud Core – Policy Control Function, Release 2025.03.0 .......... 3
New software features .......... 3
Changes in behavior .......... 5
Resolved issues .......... 5
Open issues .......... 5
Compatibility .......... 5
Supported software packages .......... 5
Related resources .......... 7
Legal information .......... 8

# Ultra Cloud Core - Policy Control Function, Release 2025.03.0

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:

- Enhanced security and reliability: Introduced mongoDB authentication for database security. Ensures robust end-to-end security for MongoDB databases used in PCF.
- Improved analytics and diagnostics: Enhanced the API router and unified API KPI counters for accurate issue identification and diagnostic capabilities.
- Scalability and performance: Support for multiple arbiters in SCDB mongoDB replica sets within Kubernetes clusters improves the flexibility and scalability.
- Enhanced operational efficiency: Introduced support for sharing Admin Database (DB) replica sets across PCF clusters, ensuring seamless functionality of distributed tasks such as CRD import/export.

For more information on the 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, Release 2025.03.0

| Milestone | Date |
| --- | --- |
| First Customer Ship (FCS) | 14-Aug-2025 |
| End of Life (EoL) | 14-Aug-2025 |
| End of Software Maintenance (EoSM) | 12-Feb-2027 |
| End of Vulnerability and Security Support (EoVSS) | 12-Feb-2027 |
| Last Date of Support (LDoS) | 29-Feb-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 2025.03.0

| Product impact | Feature | Description |
|---|---|---|
| Software reliability | MongoDB authentication for database security | The MongoDB authentication feature ensures robust end-to-end authentication and security for the MongoDB database used by the PCF. The authentication is qualified through CLI.<br><br>MongoDB serves as an administrative database supporting critical functionalities such as Custom Reference Data (CRD) and Policy tracing, and also for inbuilt Subscriber Profile Repository (SPR) and Balance databases, enhancing operational efficiency.<br><br>Command introduced:<br><br>**db global-settings db-user-name <*MongoDB-username*> password <*password*>**: Enables database authentication.<br><br>**Default setting:** Disabled – Configuration Required to Enable |
| API Experience | Enhancement to API router and unified API KPI counters | In PCF, the KPI counters are enhanced for various operations of UnifiedApi and ApiRouter calls. These operations include:<br><br>• Total count of API Request received<br>• Number of ingress API requests responded with http response code<br>• Success message count of given API type and request type<br>• Total milliseconds of successful API request processed by API type and request type<br>• Total count of getEntry/setKeys/updateKeys/ removeKeys/isDuplicateKey Request received and result type for ApiRouter calls<br><br>The KPI data can help in identifying and diagnosing issues with API calls and routing.<br><br>**Default Setting:** Enabled – Always on |
| Software reliability | Support for multiple arbiters in SCDB | This feature allows the deployment of multiple arbiters within the SCDB (Subscriber and Policy Database) MongoDB replica set on a Kubernetes cluster namespace.<br><br>Previously, the SCDB replica set only supported a single arbiter. This update allows for more flexible MongoDB replica set configurations, including support for setups with and without database authentication.<br><br>**Default Setting**: Disabled – Configuration Required to Enable |
| Software reliability | Shared admin DB support for PCF clusters | This feature supports the validation of the PCF with Admin Database (DB) replica sets that are created in the PCF namespace |

| Product impact | Feature | Description |
|---|---|---|
| | | and configured for sharing across clusters.<br><br>This allows the Admin DB to be effectively shared and accessed from different clusters, ensuring that functionalities like CRD import/export work correctly in this distributed setup.<br><br>**Default Setting**: Disabled – Configuration Required to Enable |

## Changes in behavior

There is no behavior changes introduced in this release.

## Resolved issues

There are no resolved bugs in this specific software release.

## 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 3.** Compatibility information for Ultra Cloud Core – Policy Control Function, Release 2025.03.0

| Product | Supported Release |
|---|---|
| Ultra Cloud Core SMI | 2025.03.1.10 |
| Ultra Cloud CDL | 1.12.2 |

## Supported software packages

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

**Table 4.** Software packages for Ultra Cloud Core – Policy Control Function, Release 2025.03.0

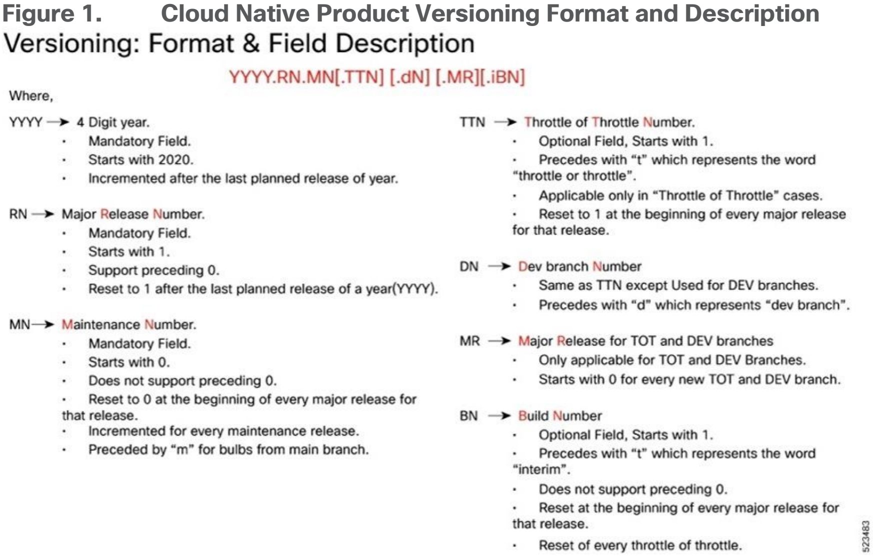
| Software package | Description | Release |
|---|---|---|
| pcf-2025.03.0.SPA.tgz | The PCF offline release signature package. This package contains the PCF deployment software, NED package, as well as the release signature, certificate, and verification information. | 2025.03.0 |
| ncs-6.4.5-cisco-pcf-nc-1.1.tar.gz | The NETCONF NED package. This package includes all the yang files that are used for NF configuration. | 6.4.5 |

| Software package | Description | Release |
|---|---|---|
| ncs-6.1.14-cisco-pcf-nc-1.1.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 5.** Checksum Calculations per 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 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 6.** 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