Release notes for UCC Converged Policy and Charging (CPC) AAA, Release 2026.04.0

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

Contents

Ultra Cloud Core CPC, Release 2026.04.0 3
New software features 4
Changes in behavior 4
Resolved issues 4
Open issues 5
Compatibility 5
Supported software packages 5
Related resources 8
Legal information 8

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

Ultra Cloud Core CPC, Release 2026.04.0

This Release Notes identifies changes and issues related to the release of Ultra Cloud Core Converged Policy and Charging (CPC)**,** software release.

The key highlights of this release include:

- Subscriber authentication: Matches the Network-ID in the RADIUS Access-Request to the subscriber record in the SPR and validates the circuit ID (Called-Station-ID) against that record.
- Duplicate Called-Station-ID handling: Prevents duplicate circuit IDs across subscriber shards and supports subscriber lookup by circuit ID.
- Automatic site failover: Isolates RADIUS traffic at the source site when an eligible critical alert fires, then verifies that Unified API external IP is removed.
- Grafana dashboard optimization: Organizes monitoring metrics into modular dashboards to improve visibility, segregating data into functional areas such as RADIUS, node and pod resource utilization, SOAP API, and SOAP-to-CPC migration.
- Log suppression enhancements: Adds the session ID and MAC address to log statements and uses leader election to prevent duplicate scheduler execution in multi-engine mode.
- SOAP API rate limiting: Dynamically applies the configured TPS threshold and error response code to SOAP API POST requests without restarting the engine.
- Circle code KPI: Adds a circle_code label to RADIUS request and response KPIs to identify traffic by circle and help detect BNG failover.
- Component updates:
  - MongoDB upgrade to version 8.0.
  - The container image is upgraded to Ubuntu 24.04.
  - NGINX Ingress is replaced with Gateway API.

For more information about the Ultra Cloud Core CPC documentation, see the Related resources section.

Release lifecycle milestones

Table 1. EoL milestone information for CPC, Release 2026.04.0

Milestone	Date
First Customer Ship (FCS)	5-Nov-2026
End of Life (EoL)	5-Nov-2026
End of Software Maintenance (EoSM)	5-May-2028
End of Vulnerability and Security Support (EoVSS)	5-May-2028
Last Date of Support (LDoS)	31-May-2029

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

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 CPC, Release 2026.04.0

Product impact	Feature	Description
Software Reliability	Automatic Site failover	Uses eligible critical alerts to trigger remote-site failover and removal of Unified API external IP. The workflow verifies the resulting state and retains recovery data for operator-controlled restoration.
Ease of Use	Grafana dashboard optimization	Separates monitoring metrics into dashboards for RADIUS, node and pod resource utilization, SOAP API, and SOAP-to-CPC migration.
Ease of Use	Log suppression enhancements for CRD and Control Center Pods	Adds session ID and MAC address to log statements to improve traceability. Ensures that only one scheduler runs in multi-engine mode, preventing duplicate scheduler execution in the CRD, Control Center, and Policy Builder components. Suppresses high-volume warmup-subscriber RADIUS messages to reduce log file size and improve focus on critical system events.
Software Reliability	SOAP API engine rate limiting	Dynamically applies a configurable TPS threshold and error response code to SOAP API POST requests. Policy Builder changes take effect without restarting the engine.
Software Reliability	Subscriber authentication with MAC address and circuit ID	In addition to matching the subscriber Network-ID, validates the Called-Station-ID in the RADIUS Access-Request against the subscriber record in the SPR.
Software Reliability	Duplicate Called-Station-ID handling	Enforces global Called-Station-ID uniqueness across subscriber shards and supports cross-shard subscriber lookup by Called-Station-ID.
Software Reliability	Circle code label in RADIUS KPIs	Adds a circle_code label to RADIUS request and response KPIs to identify traffic by circle and help detect BNG failover.

Changes in behavior

This software release introduces no behavioral changes.

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.

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

Table 3. Resolved issues for Ultra Cloud Core CPC, Release 2026.04.0

Bug ID	Description
CSCwv36674	Adding BNG at the North and East cnAAA sites causes an AccountingProxy error in production deployments.
CSCwv39451	The radius-ep readiness check does not verify iptables rules.
CSCwv31755	The BNG IP addition script publishes a configuration even when an IP address conflicts with a CIDR entry in Policy Builder.
CSCwv31775	The script execution summary reports a gateway timeout when you add RADIUS servers, although the servers are added in the backend.
CSCwt89980	The Policy Builder and CPC Central user interfaces show a new SMI user with read-only access as an admin.
CSCwv25539	Policy Builder does not display the remaining number of attempts after a failed login.
CSCwv71167	Added support for multiple Kafka partitions and configurable Kafka log retention policies.
CSCwv99377	MongoDB connection attempts can fail because the history file cannot be opened.
CSCwv94663	The mongo replica-set-status output does not highlight the primary replica.

Open issues

There are no open issues in this 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 CPC cnAAA software.

Table 4. Compatibility information for Ultra Cloud Core CPC, Release 2026.04.0

Product	Supported release
Ultra Cloud Core SMI	2026.04.1.10
Ultra Cloud Core CDL	2.3
Unified Load Balancer (ULB)	2026.04.0.54

Supported software packages

This section provides information about the release packages associated with Ultra Cloud Core CPC, cnAAA software.

Table 5. Software packages for Ultra Cloud Core CPC, Release 2026.04.0

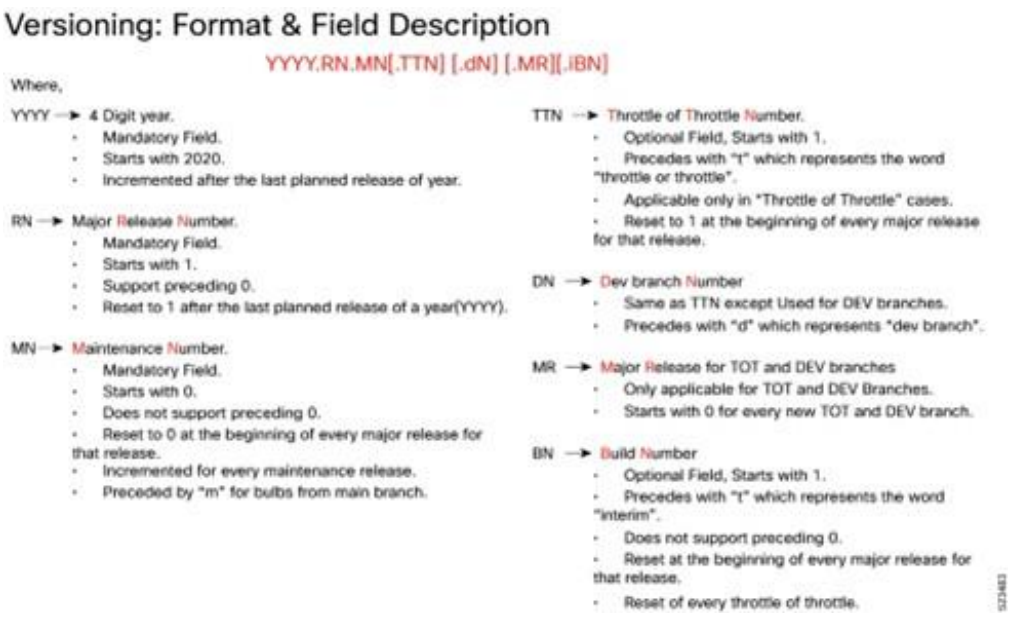
© 2026 Cisco and/or its affiliates. All rights reserved.

Software package	Description	Release
cpc.2026.04.0.SPA.tgz	The CPC offline release signature package. This package contains the CPC deployment software as well as the release signature, certificate, and verification information.	2026.04.0

Cloud native product version numbering system

The **show helm list** command displays detailed information about the version of the cloud native product currently deployed.

This is a sample for version numbering system:



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.

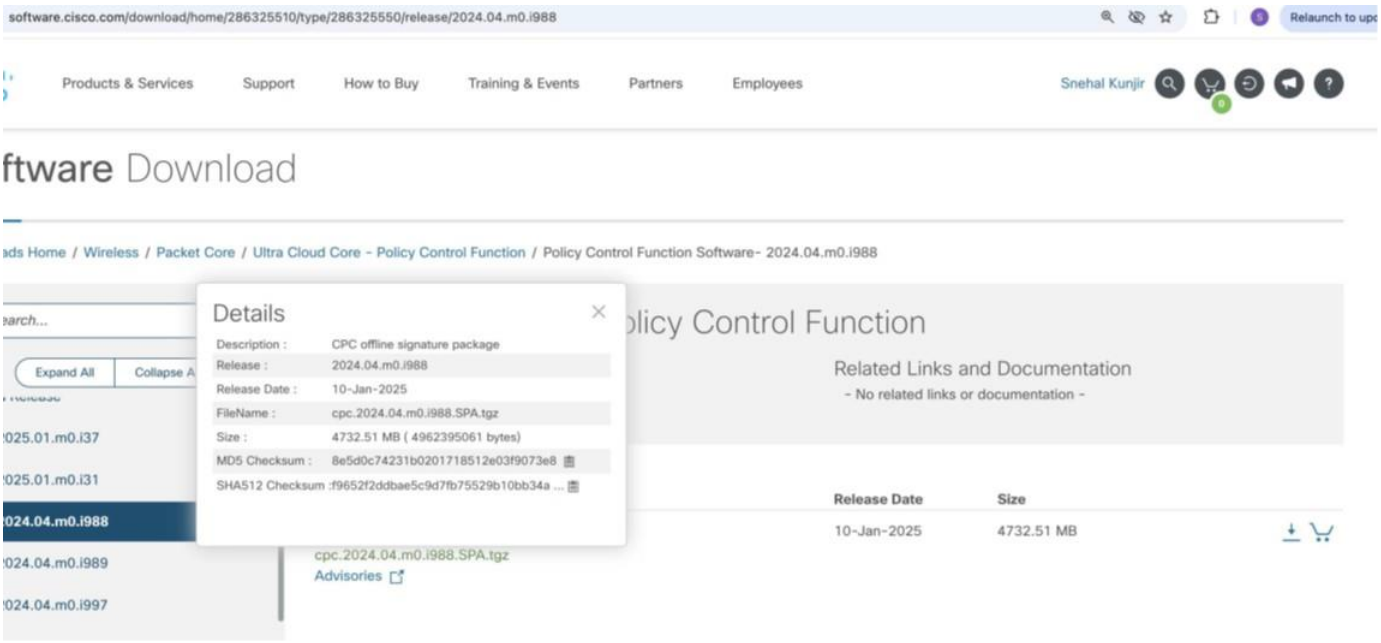
Software integrity verification

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.

This is a sample for software integrity verification.

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



At the bottom, you will find the SHA512 checksum. If you do not see the whole checksum, you can expand it by pressing " ..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches the provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the following 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*
<filename> is the name of the file. <extension> is the file type extension (for example, .zip or .tgz).	

Certificate validation

CPC software images are signed through x509 certificates. For information and instructions on how to validate the certificates, refer to the .README file packaged with the software.

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

Related resources

This table provides key resources and links to the support information and essential documentation for Ultra Cloud Core CPC AAA products.

Table 7. Related resources and additional information

Resource	Link
cnAAA documentation	Converged Policy and Charging
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.