Ultra Cloud Core 5G Policy Control Function, Release 2023.02 - Release Change Reference

First Published: 2023-04-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PREFACE

CHAPTER 1

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document is a part of the Ultra Cloud Core 5G Policy Control Function documentation set.

For information about available documentation, see the Ultra Cloud Core 5G Policy Control Function Documentation Map for this release at Cisco.com.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	**Description**
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the applicable chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.

CHAPTER 1

UCC 5G PCF- Release Change Reference

Features and Changes Quick Reference

Features	Default	Release Introduced / Modified
Dynamic QoS Flow-based Application Detection and Control (ADC) Support, on page 2	Enabled	2023.02.0
Serviceability KPIs Diagnostics Implementation, on page 5	Enabled - Always-on	2023.02.0
Software Upgrade using Site Isolation Procedure, on page 3	Enabled - Always-on	2023.02.0
Support for OAUTH2 on PCF, on page 4	Disabled – Configuration required to enable	2023.02.0
Utilization of SMI Labels in the Network Policy, on page 6	Enabled - Always-on	2023.02.0
Release 16 Baseline Compliance, on page 7	Enabled - Always-on	2023.02.0

Dynamic QoS Flow-based Application Detection and Control (ADC) Support

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide*

Revision history

Table 2: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

For providing the bandwidth allocation dynamically, the PCF interacts with the SMF (N7) and LDAP to provide the ADC policy on subscriber application detection. The ADC feature applies the detection and enforcement policy actions for the specified application.

PCF verifies the support feature (suppFeat) attributes received in the N7_CREATE request from the SMF to check if the SMF supports ADC. The PCF also checks for ADC support validation among PCF feature lists and sends an LDAP query to validate the ADC support per subscriber. If all the validations are successful, PCF includes ADC in the support feature (suppFeat) of the N7_CREATE response.

PCF subscribes to SMF for the following events:

- APP_STA (Application Start)—Installs the application enforcement rules for the dedicated bearer for the detected application flows.
- APP_STO (Application Stop)—Uninstalls the application enforcement rules on the dedicated bearer for the detected application flows.

For the installed predefined rules, SMF reports the information about the detected application traffic to PCF, and PCF provides the corresponding ADC enforcement rules.

The SMF notifies the application start and detects the application flow with the following information:

- Application ID
- Instance ID
- SDF

Table 3: Enforcement Rules for Application Flows Detected

With SDF Deduced	Without SDF Deduced
• PCF creates unique Application Enforcement rule name using application ID and Instance ID. • The SMF verifies that the application ID-instance ID pair only experiences one trigger of the application detection notification. • PCF responds with the Derived rule from the CRD without any Application ID. • Application Stop event—PCF maps to the corresponding PCC rule using appId + instanceId and delete the corresponding enforcement rule.	• If the UPF can't deduce the SDF, Application Start only contains the application ID. • The SMF doesn't send any SDFs, the PCF responds without using a pccRule and logs the same information in the KPI.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Dynamic QoS Flow-based Application Detection and Control (ADC) Support chapter.

Software Upgrade using Site Isolation Procedure

Feature Summary and Revision History

Summary Data

Table 4: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide*

Revision History

Table 5: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

The PCF supports the base images of all containers from the Ubuntu and Mongo versions, which got updated from 20.04 to 18.04 for the Ubuntu version and from 4.4 to the 4.0 version for Mongo containers. The Software Upgrade using Site Isolation Procedure requires the site isolation and a method of procedures for execution during the maintenance window considering the upgrade path. The in-service updates aren't supported because there's no upgrade from Mongo 4.0 to 4.4 version.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Software Upgrade using Site Isolation Procedure chapter.

Support for OAUTH2 on PCF

Feature Summary and Revision History

Summary Data

Table 6: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide* • *UCC 5G PCF CLI Reference*

Revision History

Table 7: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

The PCF supports the OAuth2, which is an authorization protocol and NOT an authentication protocol. The Network Function Repository (NRF) is the designated OAuth2 Authorization Server. The OAuth2 provides the client to the NRF and includes the OAuth2 Access Token validation for the SBI requests from consumer NFs.

The OAuth2 feature needs to enable or disable globally for all SBA interfaces and allows the subscribers to access to a set of resources. For example:

- Remote APIs
- User data

Following the "Client Credentials" authorization, the NRF provides the Nnrf_AccessToken service for OAuth2 authorization. The OAuth2 uses Access Tokens, and the Access Token provides the authorization to access resources on behalf of the end user. However, the JSON Web Token (JWT) format needs to used in some contexts. The OAuth2 enables token issuers to include data in the token itself. For security reasons, the Access Tokens may have an expiration date.

Note There’s no specific format for Access Tokens.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Support for OAUTH2 on PCF chapter.

For more information, refer to the UCC 5G PCF CLI Reference > Mobile Policy Services Repository Commands on PCF chapter.

Serviceability KPIs Diagnostics Implementation

Feature Summary and Revision History

Summary Data

Table 8: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide*

Revision History

Table 9: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

The Cisco Policy Control Function (PCF) doesn’t offer capabilities for viewing the messages packet counters at each critical application component. The PCF uses a Key Performance Indicators (KPIs) diagnostics utility to compute and determine the systems behavioral status at a specified time interval. The diagnostics utility also collects the counters from the component and helps to limiting down the issue to a particular area. The utility computes the appropriate KPI counters by querying the prometheus server.

The services to check the counters:

- Rest-endpoint
- Engine
- CDL

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Serviceability KPIs Diagnostics Implementation chapter.

For more information, refer to the UCC 5G PCF CLI Reference > PCF System KPI Diagnostics chapter.

Utilization of SMI Labels in the Network Policy

Feature Summary and Revision History

Summary Data

Table 10: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide*

Revision History

Table 11: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

The Subscriber Microservices Infrastructure (SMI) or Cloud Native Deployment Platform (CNDP) uses the network policy usage on the Kubernetes cluster. The Utilized network policies in the Common Execution Environment (CEE) namespace block the incoming traffic from the PCF namespace. The REST endpoint provides the SMI label in the network policy for accessing CEE services. PCF manages the changes in application pods to communicate with the CEE services. The PCF REST endpoint also needs access to the Prometheus high-resolution service to collect the CPU load data.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Utilization of SMI Labels in the Network Policy chapter.

Release 16 Baseline Compliance

Feature Summary and Revision History

Summary Data

Table 12: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	• *UCC 5G PCF Configuration and Administration Guide* • *UCC 5G PCF API Reference*

Revision History

Table 13: Revision History

Revision Details	Release
First introduced.	2023.02.0

Feature Description

This release introduces new attribute "eps Cause" and Out Of Credit Information over N7.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > Policy Control Request Triggers Over N7 chapter.

For more information, refer to the UCC 5G PCF Configuration and Administration Guide > RAN-NAS Release Cause chapter.

For more information, refer to the UCC 5G PCF API Reference > Nnrf_NFDiscovery chapter.

For more information, refer to the UCC 5G PCF API Reference > Nnrf_NFManagement chapter.