Operator determined barring for packet services in AMF

Operator determined barring for packet services in AMF

Operator Determined Barring (ODB) for packet services in AMF is a network policy feature that supports the following functionalities:

- Enforces barring of all packet services for selected subscribers, except emergency services, through both dynamic UDM-triggered activation and static local configuration override.
- Supports ODB updates through UDM Data Change Notification, enabling flexible policy enforcement after subscriber data changes.
- When the UDM initiates de-registration with the reason OPERATOR_DETERMINED_BARRING, the AMF releases all active PDU sessions and detaches the subscriber.
- If the UDM returns an OPERATOR_DETERMINED_BARRING status during an initial registration request, the AMF rejects the registration attempt.
- If the UDM returns an OPERATOR_DETERMINED_BARRING status during a mobility registration with an AMF change, the AMF terminates all non-emergency PDU sessions. If an emergency PDU session is active, the subscriber is moved to the emergency-registered state; otherwise, the AMF rejects the registration request.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Operator determined barring for packet services in AMF	2026.03.0	You can block all packet services for selected users through AMF based on policy or regulatory requirements, either dynamically from UDM subscription changes or by local override, while emergency access remains unaffected. This feature gives you flexible network-level control over user packet service access.

Limitation

AMF does not support the roaming functionality for the ODB packet service.

Configure operator determined barring for packet services in AMF

Before you begin

Follow these steps to configure operator determined barring for packet services in AMF.

Procedure

Step 1 Enter the AMF configuration mode.

config

Step 2 Set the local operator determined barring packet services policy using the following command.

amf-global { call-control-policy *call_control_policy_value* **{ odbPacketServices { all-packet-services | none } } }**

Bar or allow packet services for new subscribers or establishment attempts. Choose:

- `all-packet-services`: Enables barring for all packet services for new subscriber registrations and new PDU sessions, overriding UDM settings.
- `none`: Disables all packet service barring, overriding UDM settings.

Step 3 (Optional) Define a local cause code map for ODB-related NAS rejection causes using the following command.

local-cause-code-map name *map_name*

Step 4 Configure cause code mapping for ODB using `local-cause-code-map name <map-name> odb-packet-services cause-code-5gmm <cause>`.

local-cause-code-map name *map-name* **{ odb-packet-services cause-code-5gmm { 5GS-services-not-allowed | n1-mode-not-allowed | no-suitable-cells-in-tracking-area | plmn-not-allowed | restricted-service-area | tracking-area-not-allowed }**

If no cause code map is configured then default AMF cause code is used. The default cause code is `plmn-not-allowed`.

Step 5 Save and commit the configuration.