Nine authorization guard fixes from the authz audit (Agno pull request 10270)

PRIMARY

Publisher	GitHub
Published	2026-09-22
Retrieved	2026-09-24
Cite key	github2026nine
URL	https://github.com/agno-agi/agno/pull/10270

Merged 22 September 2026 into feat/agentos-authz, 15 commits, approved by SamJupe on 22 September 2026.

The nine fixes: (1) user endpoint gating - prevent unauthorized token access to /users endpoints; (2) scope namespace reservation - reserve the agent_os namespace against privilege escalation; (3) draft preview access - correct admin privilege checking for draft configurations; (4) provider error handling - unhandled provider errors changed from 401 leaks to 403 denials with audit logging; (5) reserved principals - reject service accounts and role slugs as user IDs; (6) scope PATCH validation - full validation before persisting; (7) knowledge refresh mapping - add the missing scope mapping for the refresh endpoint; (8) role-slug provisioning - prevent JIT provisioning of subjects matching role names; (9) request-time gating - runtime checks for manually added JWT middleware.

The description emphasises authorization, guard-style fixes and the audit trail. It does not mention approval workflows, human-in-the-loop, approval binding, or Loopjacking.