User Groups & Permissions Guide

Overview

GATE implements a **role-based access control (RBAC)** model that ensures secure and organized user management. Permissions are never assigned directly to individual users. Instead, users inherit their permissions from one or more **groups**, allowing you to tailor user experiences while maintaining platform security.

Every group provides access to a specific **functional area** (such as AAA, payments, or advertising) at a defined **privilege level** (full admin, read-only admin, or reports-only). You can assign multiple groups to a single user to grant cross-functional responsibilities.

```
flowchart LR
    U[User] -->|member of| G1[Group A<br/>e.g. AAA admins]
    U -->|member of| G2[Group B<br/>e.g. Payment reports]
    G1 -->|grants| P1[Permissions on AAA]
    G2 -->|grants| P2[Permissions on Payment reports]
    P1 --> UI[GATE admin UI]
    P2 --> UI
```

> **Key Concept:** Groups are additive. A user belonging to multiple groups receives the **union** of all their permissions. This allows you to compose roles rather than creating new groups for every possible combination.

Permission Levels

Most functional areas provide three standard permission levels. Always select the lowest level that enables users to complete their tasks effectively — this follows the **principle of least privilege**.

Standard Permission Levels

Level	Indicator	Access Granted	Typical Use Cases
Admin	□□	Full CRUD operations (create, view, update, delete) on area resources	Day-to-day feature configuration and management
Read-only Admin	□□	Browse all objects in the area without modification or deletion capabilities	Auditors, trainees, support staff conducting investigations
Reports	□□	Access to dashboards, charts, and transaction listings without configuration access	Business analysts, finance teams, marketing personnel

Special Cross-Cutting Roles

Beyond the standard levels, GATE includes two important cross-cutting roles:

Role	Indicator	Access Granted
End User	•	Personal profile access, password changes, and preference settings (non-administrative)
Expert Mode	□□	Unlocks hidden "Expert Mode" toggle revealing advanced menus and **destructive operations** (bulk deletes, internal settings)

> ⚠ **Expert Mode Warning:** Only grant Expert Mode access to senior operators who understand the consequences of destructive operations.

Functional Areas

GATE organizes functionality into distinct areas, each with its own group hierarchy using the three standard permission levels where applicable.

Area	Scope
□□ **Global Administration**	Cross-cutting operations, organization-wide configuration, and platform health monitoring
□□ **AAA**	Authentication, Authorization, and Accounting — profiles, realms, clients, home servers, session logs

Area	Scope
◫ **Account**	Tenant/account configuration including plans, services, lists, parameters, and site settings
◫ **Advertisement**	Campaign management, banner configuration, segmentation rules, and advertising transaction logs
◫ **API Logs**	Platform API request history inspection for debugging and auditing purposes
◫ **Devices & Applications**	Mobile/desktop app registrations, device metadata, connection logs, and app subscriptions
◫ **Hotspot Monitoring**	Real-time access point health monitoring including reachability, uptime, coverage, and availability reports
◫ **Payments**	Payment plan management, gateway configuration, transaction processing, and refund handling
◫ **Users**	End-user account management, social login configuration, and user-level activity logs
◫ **Reports & Dashboards**	Cross-area analytics, KPI tracking, and exportable report generation
◫ **SONDA / User Experience**	Real-world user experience monitoring including latency, throughput, and client-side reachability measurements

Group Catalog

The following tables detail every built-in group shipped with GATE, organized by functional area. Group names are stable identifiers that you can search for in the group administration interface.

Global Administration

Group	Level	Description
`GATE admins`	◫ Admin	Comprehensive platform administration access for day-to-day operations across most areas
`GATE read-only admins`	◫ Read-only	Platform-wide browsing access without modification capabilities
`GATE reports`	◫ Reports	Access to dashboards, KPIs, and transaction listings across the platform

> **Usage Recommendation:** These general-purpose roles serve as excellent starting points for most operators. Combine them with area-specific groups when users require deeper access to particular modules.

AAA (Authentication, Authorization, Accounting)

Group	Level	Description
`GATE AAA admins`	Admin	Complete AAA administration including profiles, realms, clients, home servers, and accounting
`GATE AAA admins w/o Portals`	Admin	Full AAA administration **excluding** captive portal builder access
`GATE AAA admins w/o Portals RO`	Read-only	Read-only AAA administration without captive portal builder access
`GATE AAA read-only admins`	Read-only	Read-only access to the complete AAA functional area
`GATE AAA reports`	Reports	AAA accounting reports, session analytics, and traffic dashboard access
`GATE AAA user admins`	Admin	Specialized role for managing AAA **end-users only** (profiles, attributes, credentials) without infrastructure access

> **Selection Guidelines:**
>
> - Use `AAA admins` for complete AAA stack ownership
> - Use `AAA admins w/o Portals` when captive portal design is managed separately
> - Use `AAA user admins` for support desk personnel who only reset credentials or adjust user attributes
> - Use `AAA reports` for analytics roles that must not access configuration

Account Management

Group	Level	Description
`GATE account admins`	Admin	Complete account administration including plans, services, lists, parameters, and site settings

Group	Level	Description
`GATE account read-only admins`	□□ Read-only	Read-only account administration access for audit and review purposes

> □□ **Selection Guidelines:** `account admins` represents the closest equivalent to a tenant "owner" role — grant sparingly. `account read-only admins` is ideal for auditors and onboarding verification.

Advertisement Management

Group	Level	Description
`GATE advertisement admins`	□□ Admin	Complete advertisement administration including campaigns, banners, and segmentation rules
`GATE advertisement read-only admins`	□□ Read-only	Read-only advertisement administration for audit purposes
`GATE advertisement reports`	□□ Reports	Advertisement reporting and transaction access including impressions, clicks, and conversions

> □□ **Team Separation:** Assign `advertisement admins` to marketing teams, `advertisement reports` to analytics teams, and `advertisement read-only admins` to finance auditors.

API Logs

Group	Level	Description
`GATE API Logs read-only`	□□ Read-only	API request log browser access for debugging and auditing

> □□ **Usage Recommendation:** Ideal for integration teams and third-party partners who need API call troubleshooting capabilities without broader platform access.

Devices & Applications

Group	Level	Description
`GATE device admins`	□□ Admin	Device and application administration including registrations, subscriptions, and configuration

> □□ **Usage Recommendation:** Designed for mobile/desktop application operations teams responsible for registered device lifecycle management.

Hotspot Monitoring

Group	Level	Description
`GATE hotspots monitoring`	□□ Admin	Hotspot monitoring administration including monitoring profiles, thresholds, and alert configuration
`GATE hotspots monitoring read-only`	□□ Read-only	Read-only access to hotspot monitoring dashboards and availability reports

> □□ **Usage Recommendation:** Essential for network operations center (NOC) teams monitoring access point health and coverage.

Payment Management

Group	Level	Description
`GATE payment admins`	□□ Admin	Complete payments and plans administration including pricing, gateways, and plan lifecycle
`GATE payment read-only admins`	□□ Read-only	Read-only payment area access for audit and compliance
`GATE payment reports`	□□ Reports	Payment reporting and transaction access including revenue dashboards and reconciliation exports

> □□ **Selection Guidelines:** Finance teams typically need `payment reports` for reconciliation **plus** `payment read-only admins` for transaction investigation. Reserve `payment admins` for billing operations personnel only.

User Management

Group	Level	Description
`GATE users admins`	□□ Admin	User account and user log administration
`GATE users RO`	□□ Read-only	Read-only access to user lists and user activity logs
`Users`	• End user	Standard end-user role providing profile access and password change capabilities
`Users: Expert mode`	□□ Expert	Enables **Expert Mode** toggle in admin UI, unlocking advanced menus and destructive operations

> ⚠ **Expert Mode Security Notice:** Expert Mode reveals advanced and destructive operation menus (bulk accounting record deletion, low-level configuration, internal tooling). Grant `Users: Expert mode` exclusively to trained senior operators who understand operational consequences.

Reports & Dashboards

Group	Level	Description
`Report admins`	□□ Admin	Report and dashboard administration including creation, editing, and sharing of custom reports

> □□ **Usage Recommendation:** Designed for business intelligence teams responsible for building and maintaining organizational dashboards.

SONDA / User Experience

Group	Level	Description
`SONDA admins`	□□ Admin	SONDA probing and user experience measurement system administration
`SONDA reports`	□□ Reports	SONDA reporting and transaction access including latency, throughput, and reachability metrics

> **Usage Recommendation:** Essential for quality-of-experience (QoE) teams monitoring real user service perception.

Access Matrix

This visual summary shows available group combinations for each functional area and permission level. Empty cells indicate no pre-built group exists for that combination — use the closest available level or combine multiple groups.

Area	Admin	Read-only	Reports	Notes
Global	`GATE admins`	`GATE read-only admins`	`GATE reports`	Starting point for most operators
AAA	`GATE AAA admins`	`GATE AAA read-only admins`	`GATE AAA reports`	`w/o Portals` variants available
AAA (user-level)	`GATE AAA user admins`	—	—	Support/helpdesk focused
Account	`GATE account admins`	`GATE account read-only admins`	—	Tenant configuration
Advertisement	`GATE advertisement admins`	`GATE advertisement read-only admins`	`GATE advertisement reports`	Complete coverage
API logs	—	`GATE API Logs read-only`	—	Integration/debug role
Devices & apps	`GATE device admins`	—	—	Limited coverage
Hotspot monitoring	`GATE hotspots monitoring`	`GATE hotspots monitoring read-only`	—	NOC teams
Payments	`GATE payment admins`	`GATE payment read-only admins`	`GATE payment reports`	Complete coverage
Users	`GATE users admins`	`GATE users RO`	—	See also `Users` and `Users: Expert mode`
Reports & dashboards	`Report admins`	—	—	BI team role
SONDA / UX	`SONDA admins`	—	`SONDA reports`	QoE role

Common User Profiles

These ready-to-apply group combinations cover most real-world operational requirements.

??? Platform Operator (Day-to-Day Admin)

Group Assignment:

- `GATE admins`
- `GATE AAA admins`
- `GATE account admins`
- `GATE device admins`

Role Description: Handles platform configuration, service onboarding, and operational issue resolution across all areas. Expert Mode is **not** included by default.

? Helpdesk / Tier-1 Support

Group Assignment:

- `GATE read-only admins`
- `GATE AAA user admins`
- `GATE users RO`
- `GATE API Logs read-only`

Role Description: Platform browsing, user credential resets, and API log inspection without configuration modification or data deletion capabilities.

? Business Analyst / BI

Group Assignment:

- `GATE reports`
- `GATE AAA reports`
- `GATE advertisement reports`
- `GATE payment reports`
- `SONDA reports`
- `Report admins` *(optional, for dashboard creation)*

Role Description: Dashboard-focused access without configuration capabilities, eliminating accidental change risks.

? Finance / Billing

Group Assignment:

- `GATE payment read-only admins`
- `GATE payment reports`
- `GATE read-only admins` *(optional, for context)*

Role Description: Transaction reconciliation and payment configuration auditing without modification capabilities.

? Marketing Operator

Group Assignment:

- `GATE advertisement admins`
- `GATE advertisement reports`

Role Description: Campaign creation and measurement with isolated functional scope.

? Network Operations (NOC)

Group Assignment:

- `GATE hotspots monitoring`
- `GATE AAA reports`
- `SONDA reports`

Role Description: Real-time access point health monitoring with session analytics and user experience correlation capabilities.

? Senior Operator (with Destructive Tooling)

Group Assignment:

- `GATE admins`
- `GATE AAA admins`
- `Users: Expert mode`

Role Description: Standard operator capabilities enhanced with Expert Mode access. Reserve for trusted operators exclusively.

? End User (Self-Service)

Group Assignment:

- `Users`

Role Description: Personal profile and password management without administrative area access.

Best Practices

? Principle of Least Privilege

Always assign the **minimum permission level** required for job function completion. Prefer `read-only admins` over `admins` for investigation or audit roles. Choose `reports` over `read-only admins` when users only need dashboard access.

? Compose Rather Than Customize

Resist creating specialized groups for individual users. Combining two or three built-in groups typically addresses requirements while maintaining audit simplicity.

? Test in Staging Environment

Before production deployment, apply new user profiles (group combinations) to test users in non-production environments. Verify exact menu, button, and action visibility before real user rollout.

? Periodic Review Schedule

Implement quarterly group membership reviews. Revoke `admins` and Expert Mode capabilities from users who no longer require them. Former employee accounts with lingering admin access represent the most common security incident cause.

? Separation of Duties

When possible, distribute **configuration** and **audit** responsibilities among different personnel:

- Payment configuration (`payment admins`) and payment auditing (`payment read-only admins` + `payment reports`) should involve different individuals
- Campaign creation (`advertisement admins`) and advertising budget approval (via `payment reports`) should involve different individuals

? Expert Mode Access Control

Treat `Users: Expert mode` as break-glass permission due to irreversible operation access:

- Grant exclusively to named senior operators
- Document justification for each recipient
- Implement quarterly Expert Mode group membership reviews

- Remove temporary Expert Mode access immediately upon task completion

Frequently Asked Questions

Can I modify built-in groups to add or remove permissions?

While technically possible, modification is **not recommended**. Built-in groups may receive updates in future GATE releases, overwriting manual changes. Instead, create **additional** groups with required deltas and assign both to users.

Can a user belong to multiple groups simultaneously?

Yes. Group memberships are **additive** — users inherit the union of all permissions from assigned groups. This represents the recommended approach for role composition.

Which groups should new support agents receive?

Start with `GATE read-only admins` + `GATE users RO` + `GATE API Logs read-only`. Add area-specific groups as responsibilities expand.

A user sees unauthorized menus. How do I remove access?

Remove the group granting menu access. If the menu persists, verify the user is not a **superuser** — superusers bypass the group system entirely and see all menus. Downgrade to regular user status and assign appropriate groups instead.

How do I identify which group grants specific menu access?

Each admin section corresponds to a functional area (AAA, payments, advertising, etc.). Match the menu to the area using **Section 3: Functional Areas**, then select the appropriate level from **Section 5: Access Matrix**.

Can I grant access to organization subsets only?

Yes — group-granted permissions are automatically scoped to the user's organization and its sub-organizations. A user with `GATE admins` in organization "Acme" will only see and administer Acme and its children, never sibling organizations.

> **Documentation Feedback:** If you believe a group is missing, misnamed, or if use cases in this guide don't match your requirements, please submit a documentation request for review in the next release.

Revision #1
Created 2026-04-09 03:26:01 UTC by mauro@zequenze.com
Updated 2026-04-09 03:26:01 UTC by mauro@zequenze.com