Роли и права доступа

AgentOps использует RBAC с пятью ролями. Права проверяются на API; меню UI скрывает недоступные разделы. Если страница открыта, но действие запрещено — будет **403 Forbidden**.

Иерархия

```
super_admin (5) → admin (4) → security_analyst (3) → developer (2) → viewer (1)
```

Роль	Кто обычно	Зона ответственности
Viewer	Аудитор, наблюдатель	Только обзор и чтение аудита
Developer	Инженер ML / агентов	Агенты, сценарии, чтение политик
Security Analyst	Аналитик SOC	Аудит (экспорт), аномалии, HITL, политики (чтение)
Admin	Админ тенанта	Пользователи, политики CRUD, агенты, HITL
Super Admin	Оператор платформы	Все тенанты, provisioning

Матрица возможностей (смысл для оператора)

Раздел	Viewer	Developer	Security Analyst	Admin	Super Admin
Dashboard	✔	✔	✔	✔	✔
Agents / Workflows / Cost / Marketplace	ограничено*	✔	по UI*	✔	✔
Policies (чтение)	—	✔	✔	✔	✔
Policies (создание/правка)	—	—	—	✔	✔
Audit (чтение)	✔	✔	✔	✔	✔
Audit (экспорт)	—	—	✔	✔	✔
Anomalies / Discovery / Guard ML / HITL	—	—	✔	✔	✔
Users	—	—	—	✔	✔
Settings	✔	✔	✔	✔	✔

*В интерфейсе часть пунктов меню может быть видна шире, чем разрешает API. Источник истины — ответ API (403). При сомнении запросите у Admin повышение роли.

Изоляция тенантов

- Пользователь видит только ресурсы своего `tenant_id`.
- **Super Admin** может работать кросс-тенантно; для UI часто нужно вручную указать tenant API key в **Settings**.
- Назначить роль выше своей нельзя; `super_admin` назначает только другой Super Admin.

Смена роли

После изменения роли администратором **выйдите и войдите снова**, чтобы обновился JWT.