scope.kz — super_admin

scope.kz
May 30, 2026

CONTENTS

Руководство super_admin (ИБ / владелец)

> Обновлено: **2026-05-30**
> Роль: **super_admin** — полный контроль single-tenant установки scope.kz.

Ваша зона ответственности

- Управление пользователями и ролями
- Выдача и отзыв доступа (grants) с режимами учётных данных
- Одобрение JIT-запросов (Access Requests)
- Просмотр audit, recordings, активных сессий
- Политики сессий, LDAP, retention, AI-настройки
- **Implicit connect** ко всем серверам без отдельного grant

См. RBAC-матрицу.

---

1. Вход и безопасность

1. Откройте **https://scope.kzSMARTPANTS_PRESERVED_71SMARTPANTS_PRESERVED_72 → Login (email + password).**

Экран входа

2. **Пройдите 2FA (TOTP) — обязательно для всех ролей.**
3. **В Profile:**
   - **смените пароль при первом входе;**
   - **включите/проверьте 2FA;**
   - **при работе с AD/RDP reuse mode — сохраните domain credential (session vault).**

Profile — domain passwords

---

2. Dashboard

Путь: Dashboard (/)

- **Обзор системы, Quick Connect к серверам.**
- **Доступен только admin и super_admin.**

Dashboard super_admin

---

3. Серверы (fleet)

Путь: Servers (`/servers`)

Действие	Как
Добавить сервер	**Add server → hostname, protocol (RDP/SSH/VNC), credentials**
Редактировать	**Карточка → Edit**
Удалить	**Delete (осторожно — audit сохраняется)**
Connect	**Connect — работает без grant (service account или vaulted по умолчанию)**

Servers — fleet и Discover domain

Discover domain — импорт компьютеров из AD:

Discover domain computers
host_kind (RDP): `ad_member`, `standalone_windows`, `workstation` — влияет на доступные credential modes. См. credential-modes.md.

---

4. Пользователи и grants

Путь: Users (`/users`) — только super_admin (admin перенаправляется на Servers).

СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ

1. **Add user → email, имя, роль (`user` / `admin` / `super_admin`).**
2. **Пользователь получает invite / временный пароль (зависит от настройки).**

ВЫДАЧА ДОСТУПА (GRANT)

Users UI

1. **Users → выберите пользователя → Grant access.**
2. **Выберите сервер(ы), срок действия (optional expiry).**
3. **Credential mode:**
   - `reuse_console_password` **— для AD member (пользователь должен сохранить domain password в Profile);**
   - `vaulted` **— пароль на permission; опционально auto-provision local user (Windows/Linux);**
   - `service_account` **— учётная запись с карточки сервера.**
4. **can_write — для SFTP: разрешить upload/delete/rename.**

Grant access (с карточки сервера)

ОТЗЫВ

Revoke на permission — при auto-provision выполняется best-effort disable локального пользователя.

> **Только super_admin может POST/DELETE** `/permissions`**. Admin видит список grants через API, но UI grant — у super_admin.**

---

5. Access Requests (JIT)

Путь: Access Requests (`/access-requests` **)**

- **Badge показывает число pending запросов (только у super_admin).**
- **Approve — создаёт permission с параметрами из запроса.**
- **Deny — отклонение с комментарием.**
- **Истёкшие запросы закрывает reaper → audit** `access_request.expire`**.**

Access Requests

> **Admin не может approve/deny — только super_admin (отличие от старого design-doc).**

---

6. Active Sessions

Путь: Active Sessions (`/active-sessions`)

- **Список всех активных RDP/SSH сессий.**
- **Disconnect — принудительное завершение (audit `session.disconnect`).**

---

7. Audit Logs

Путь: Audit Logs (`/audit`)

- **Фильтры: user, action, severity, дата.**
- **Export CSV.**
- **Просмотр screenshots, удаление screenshot/recording (audit `screenshot.delete`, `recording.delete`).**

Коды событий: audit-events.md.

---

8. Recordings

Путь: Recordings (`/recordings`)

- **Просмотр записанных сессий (если включено в policy).**

---

9. Alerts

Путь: Alerts (`/alerts`)

- **Правила на audit-события (например `ssh.command` severity ≥ warning).**
- **Test notification → `alert.test`.**

---

10. Settings

Путь: Settings (`/settings`)

Раздел	Назначение
Session policy	Idle timeout, max session duration
Terminal themes	SSH xterm themes
LDAP	Read/test (super_admin only)
Retention	Audit/recording retention, danger zone
AI assistant	Конфигурация (super_admin only)

---

11. SFTP

Путь: SFTP (`/sftp`)

- **Dual-pane файловый менеджер между серверами.**
- **Операции логируются: `sftp.file_*`, `sftp.transfer`.**

---

12. Типовые сценарии

НОВЫЙ СОТРУДНИК → ДОСТУП К ОДНОМУ LINUX-СЕРВЕРУ

1. **Users → Add user (role `user`).**
2. **Grant → server, mode `vaulted`, target username, пароль или auto-provision.**
3. **Сотрудник: login → Servers → Connect → Term/SFTP.**

ВРЕМЕННЫЙ ДОСТУП БЕЗ ПОСТОЯННОГО GRANT

1. **Пользователь создаёт Access Request.**
2. **super_admin: Access Requests → Approve.**
3. **По expiry reaper отзывает или permission истекает.**

ИНЦИДЕНТ: ПОДОЗРИТЕЛЬНАЯ SSH-КОМАНДА

1. **Alerts или Audit → filter `ssh.command`, severity warning/critical.**
2. **Active Sessions → disconnect при необходимости.**
3. **Revoke permission.**

Связанные how-to

- **Выдать доступ пользователю**
- **Одобрить JIT-запрос**
- **Добавить сервер**
- **Discover domain**
- **Connect RDP/SSH**