Аудит и сессии

Аудит и сессии

Маршрут: `/access` — вкладки **Пользователи** | **Сессии** | **Аудит** сразу под заголовком (underline, как на шаблонах узлов).

На всех трёх вкладках: карточка таблицы, footer с «Всего: N» и постраничная навигация.

Пользователи

- Сводка: четыре карточки (всего / ожидают / активные / заблокированные)
- Фильтры: роль, статус, поиск
- Пагинация в footer карточки (клиентская, 25 строк по умолчанию)
- ADMIN: **Создать пользователя** (после «Сбросить»), approve/reject pending, смена роли, block/unblock, **Удалить** (подтверждение; нельзя себя и последнего активного ADMIN); индикатор «онлайн» по активным сессиям
- INFOSEC: только просмотр (кнопки создания/записи скрыты)

Аудит

- Сводка сверху: три карточки той же высоты, что на Пользователях / Сессиях
- Ниже — плитки 24ч (неудачные входы, сессии, права, **безопасность**, экспорт): клик применяет фильтр
- Фильтры: поиск + **Кто** сверху; действие / тип / период / IP и Применить / Сбросить во второй строке
- Таблица: фиксированные колонки, footer с «Всего: N» и серверная пагинация
- Фильтры действия / типа объекта: полный каталог `AuditActions` (в т.ч. топология, discovery action flow, правила регистрации агентов, шаблоны availability/web-scenario, `USER_CREATE` / `DELETE`, `DASHBOARD_CLONE`)
- Risk flags: fail, auth, security, brute_force, **lockout**, **acl**
- Флаг **security** также у: `PASSWORD_CHANGE`, `MFA_*`, `API_TOKEN_*`, `SESSION_REVOKE*`, `SIEM_FORWARD`, `LICENSE_*`, алерты ИБ; у `SETTINGS_UPDATE` — если менялись ключи `security.*`, `ldap.*` или `oidc.*`
- Вход/выход SSO: в meta событий `LOGIN_*` / `LOGOUT` — `auth_method=oidc`; при logout в IdP — `idp_logout=true`; deprovision → `USER_UPDATE` + `LOGIN_FAILURE`
- Деталь: before/after JSON
- Экспорт CSV/JSON (фиксируется как `AUDIT_EXPORT`)
- Целостность: hash-chain (`content_hash` / `prev_hash`); кнопка **Проверить цепочку** → `POST /api/v1/audit-events/verify-chain` + отчёт о разрывах (`AUDIT_CHAIN_VERIFY`)

- Смена прав (роль/статус): `USER_APPROVE` / `USER_REJECT` / `USER_UPDATE` / `USER_CREATE` / `USER_DELETE` с `SUCCESS` или `FAILURE` (403 и отказ по правилам: не pending, само-disable, само-удаление, последний активный ADMIN, неизвестный пользователь, занятый логин, `password_policy` при создании локального пользователя)
- Смена пароля: `PASSWORD_CHANGE` с `SUCCESS` или `FAILURE` (`bad_current_password`, `policy_rejected`, `ldap_local_password`)
- MFA enable/disable/rotate backup: успех и отказы (`bad_password`, `bad_otp`, `setup_not_started`, `mfa_not_enabled`)
- Forward в SIEM: `SIEM_FORWARD` (успех/ошибка); ручной flush `POST /api/v1/audit-events/siem-forward` (ADMIN); lab sink — siem-lab
- Из детали аудита: deep-link на сессию (`/access/sessions?session=...&view=history`)
- Шаблоны здоровья: `HEALTH_TEMPLATE_CREATE` / `UPDATE` / `DELETE`, `HEALTH_BINDING_REPLACE` / `DEACTIVATE`, `HEALTH_OVERRIDE_UPDATE` (объект `health_template` / `node_template` / `service`). Мутации — ADMIN и OPERATOR; VIEWER и INFOSEC только чтение.
- Контрагенты: `COUNTERPARTY_CREATE` / `UPDATE` / `DELETE` (объект `counterparty`). Мутации — ADMIN (с правилом ответственных); INFOSEC только чтение списка и карточки.

Не пишутся: heartbeat агентов, успешный refresh токена.

Сессии

- Сводка: пять равных карточек (активных / текущая / остальные / мульти / простой)
- Список активных сессий; **пагинация** в footer карточки таблицы
- **История**: отозванные за 7/30/90 дней (`GET /api/v1/sessions/history`)
- Карточка одной сессии: `GET /api/v1/sessions/{id}` (active или revoked)
- Бейджи в строке совпадают с карточками (точка + подпись, тот же цвет)
- Revoke одной / остальных — только ADMIN (в режиме активных)
- INFOSEC видит список без revoke

Типовые проверки ИБ

1. Пресет failed logins / SECURITY_ALERT.
2. Всплеск LOGIN_FAILURE с одного IP.
3. Сессии с new_ip / multi_ip у привилегированных учёток.
