1-10: Общие вопросы по Keycloak Admin UI

Как создать нового пользователя в Keycloak через UI и какие минимальные параметры обязательны?

Войдите в Admin UI → Users → Add user. Минимальные параметры: Username (обязательный), Email, First Name, Last Name (по желанию).

Как включить многофакторную аутентификацию (MFA) для пользователей через UI?

Войдите в Authentication → Flows → выберите Browser и добавьте OTP Form после Username Password Form.

Как настроить автоматическое удаление неактивных пользователей? **(ПОВТОРИТЬ)**

В Realm settings → User policies можно задать параметр User inactivity timeout.

Как изменить default-реалм в Keycloak? **(ПОВТОРИТЬ)**

В Admin Console настройте нужный Realm, измените параметры и убедитесь, что в конфигурации сервера указан KEYCLOAK\_DEFAULT\_REALM.

Как изменить URL-адрес для входа в административную панель?

Измените параметр adminUrl в конфигурации Keycloak.

Как добавить пользовательские атрибуты (custom attributes) к профилю пользователя?

Перейдите в Users → выберите пользователя → Attributes → Add Attribute.

Как управлять сессиями пользователей через UI? **(ПОВТОРИТЬ)**

В Sessions можно завершать активные сессии пользователей и изменять их таймауты.

Как настроить хранение логов аутентификации?

Включите Events в Realm settings → Events и настройте хранение событий.

Какие настройки политики паролей можно задать в UI?

В разделе Authentication → Password policies можно настроить длину, сложность, историю паролей и минимальное количество цифр, символов.

Как экспортировать настройки реалма через UI?

В Realm settings → Export можно сохранить текущие настройки.

11-20: OAuth2 и OpenID Connect

Как создать OAuth2-клиент в Keycloak? **(ПОВТОРИТЬ)**

В Clients → Create → укажите Client ID, выберите тип клиента (confidential/public).

Как настроить PKCE (Proof Key for Code Exchange) в Keycloak? **(ПОВТОРИТЬ)**

Включите Client authentication → OAuth 2.0 Proof Key for Code Exchange.

Какие способы аутентификации клиентов поддерживает Keycloak?

Client ID & Secret, JWT, mTLS, Public Key, OpenID Connect.

Как задать максимальное время жизни access token?

В Token settings укажите Access Token Lifespan.

Как ограничить refresh token по IP-адресу пользователя? **(ПОВТОРИТЬ)**

Можно использовать Client Policies → Conditional Policy.

Как добавить кастомные claims в ID Token?

Через Client Scopes → Mappers.

Как настроить single sign-out (SSO logout)? **(ПОВТОРИТЬ)**

Включите Front-channel Logout в настройках клиента.

Как настроить интеграцию Keycloak с Google OAuth?

Включите Identity Providers → Google → укажите Client ID и Secret.

Как принудительно обновлять Access Token через UI?

Перейдите в Sessions и выберите пользователя → Log out.

Как настроить OAuth 2.0 Introspection Endpoint? **(ПОВТОРИТЬ)**

Включите Token Introspection в настройках клиента.

21-30: Настройки групп и ролей

Как создать пользовательскую роль через UI?

В Roles → Add role.

Как назначить пользователю роль на уровне реалма?

Откройте пользователя → Role Mappings.

Как настроить иерархию ролей?

Используйте Composite roles.

Как ограничить доступ к API Keycloak на основе ролей? **(ПОВТОРИТЬ)**

Настроить Client Roles и включить Authorization Services.

Как создать группу пользователей с преднастроенными ролями?

В Groups → Create group, затем назначить роли.

Как управлять доступом к клиентам через UI?

В Clients → Authorization.

Как использовать Attribute-based Access Control (ABAC)? **(ПОВТОРИТЬ)**

Настроить User attributes и применить политики на их основе.

Как настроить Time-based Access Control (TBAC)? **(ПОВТОРИТЬ)**

Включить Policy enforcer и задать временные условия.

Как проверить, какие пользователи принадлежат группе?

Открыть Groups → Members.

Как ограничить доступ по IP-адресу через UI? **(ПОВТОРИТЬ)**

Использовать Client Policies.

31-40: Безопасность и аутентификация

Как включить Brute Force Protection?

В Realm settings → Security Defenses.

Как задать максимальное количество неудачных входов?

В Brute Force Detection настройте Failure Factor.

Как задать доверенные источники для входа? **(ПОВТОРИТЬ)**

Включите Trusted Hosts.

Как настроить поддержку WebAuthn (Passkeys)? **(ПОВТОРИТЬ)**

В Authentication → WebAuthn.

Как включить аудит безопасности? **(ПОВТОРИТЬ)**

В Events включите Admin Events.

Как привязать пользователя к конкретному устройству? **(ПОВТОРИТЬ)**

Использовать Authenticator с параметром Remember device.

Как заблокировать доступ пользователю?

Включить статус Disabled.

Как настроить требование изменения пароля при следующем входе?

Установите Temporary Password.

Как принудительно разлогинить всех пользователей?

В Sessions → Logout all.

Как ограничить время сессии пользователя?

Настроить Session Lifespan.

41-50: Расширенные настройки и интеграции

Как добавить кастомный аутентификационный поток?

В Authentication → Flows → Create Flow.

Как подключить внешний LDAP через UI?

В User Federation добавьте LDAP.

Как интегрировать Keycloak с Active Directory?

Аналогично LDAP, но укажите AD в качестве провайдера.

Как изменить темы интерфейса Keycloak?

В Realm settings → Themes.

Как настроить авторизацию через SAML 2.0?

В Identity Providers добавьте SAML.

Как включить поддержку API Gateway (например, Kong)? **(ПОВТОРИТЬ)**

Настроить OIDC-клиент для Kong.

Как использовать Keycloak для multi-tenancy?

Создать несколько реалмов.

Как мониторить Keycloak с помощью Prometheus?

Включить Metrics.

Как обновить Keycloak без потери данных? **(ИЗУЧИТЬ)**

Использовать Rolling Update.

Как включить Keycloak на Kubernetes?

Использовать Helm-чарт Keycloak.