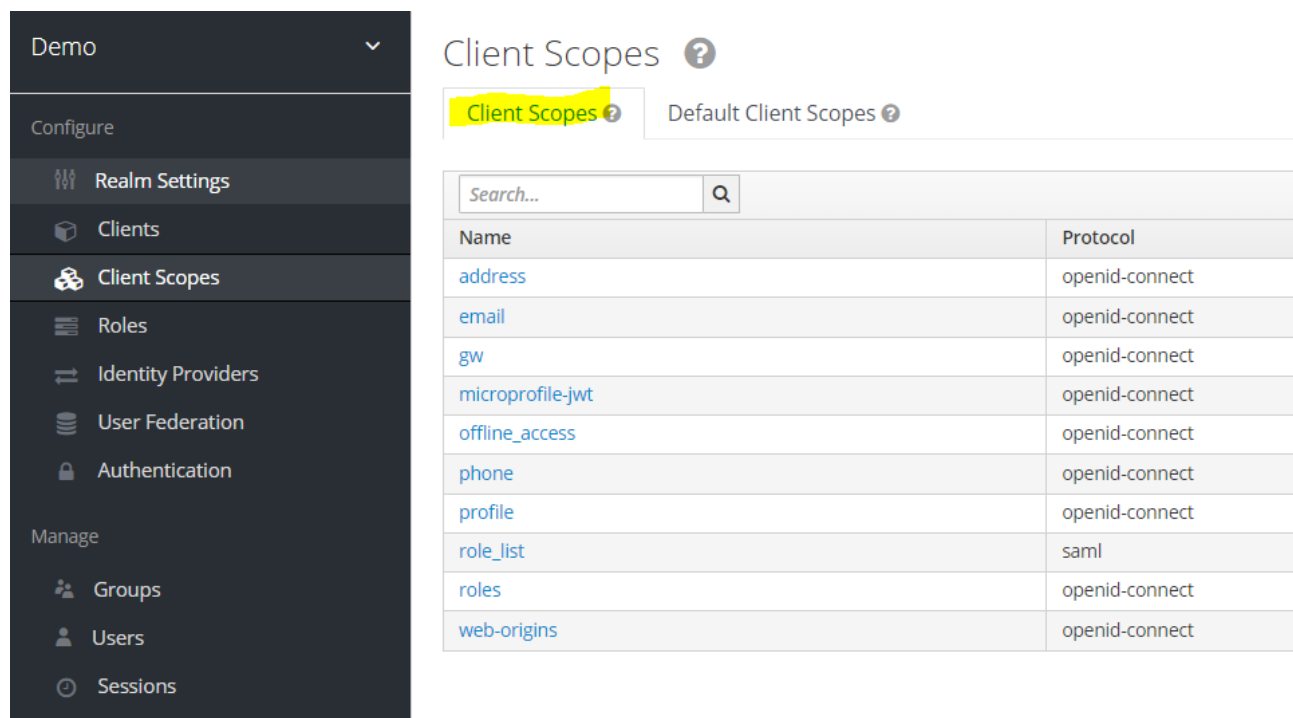


Score. Варианты конфигурации

Score – сущность, позволяющая разграничивать доступ. В keycloak используется преимущественно score на уровне realm и затем он задается как клиентский score на уровне клиента.

Client scopes

Клиентские scores определяются изначально на уровне Realm.



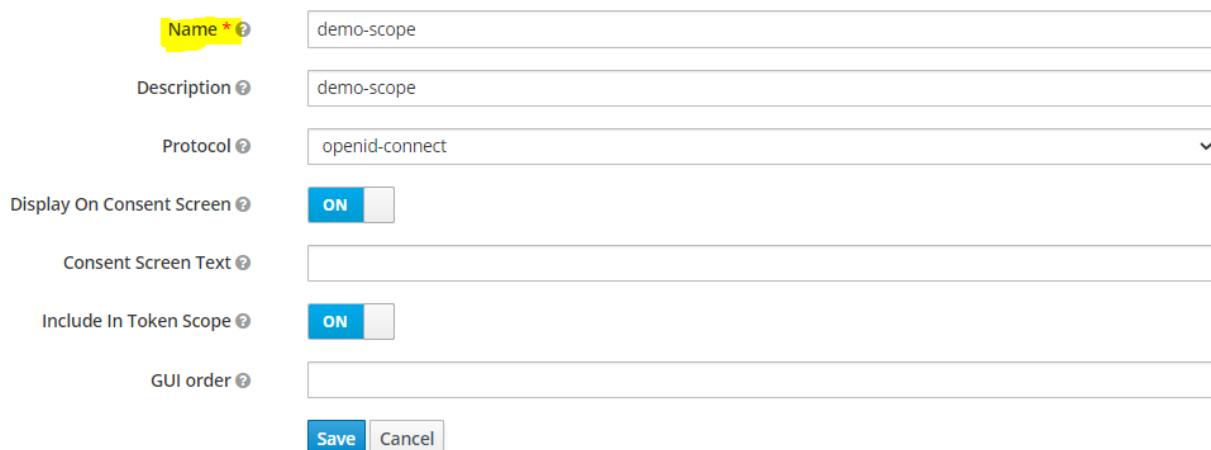
The screenshot shows the Keycloak Admin Console interface. On the left is a dark sidebar with a navigation menu. The 'Client Scopes' option is highlighted. The main content area is titled 'Client Scopes' and contains a search bar and a table of default client scopes.

Name	Protocol
address	openid-connect
email	openid-connect
gw	openid-connect
microprofile-jwt	openid-connect
offline_access	openid-connect
phone	openid-connect
profile	openid-connect
role_list	saml
roles	openid-connect
web-origins	openid-connect

При создании score достаточно задать наименование и тип протокола:

[Client Scopes](#) > Add client scope

Add client scope



The screenshot shows the 'Add client scope' form. It contains the following fields and controls:

- Name ***: Text input with value 'demo-scope'.
- Description**: Text input with value 'demo-scope'.
- Protocol**: Dropdown menu with value 'openid-connect'.
- Display On Consent Screen**: Toggle switch set to 'ON'.
- Consent Screen Text**: Text input.
- Include In Token Scope**: Toggle switch set to 'ON'.
- GUI order**: Text input.
- Save** and **Cancel** buttons at the bottom.

Client score после создания может быть указан, как дефолтный, тогда он будет добавляться в score каждого нового создаваемого client по умолчанию. Либо как опциональный, и тогда его потребуется явно указывать в запросе для получения.

Default Client Scopes ?

Client Scopes ?

Default Client Scopes ?

Default Client Scopes ?

Available Client Scopes ?

gw

Add selected »

Assigned Default Client Scopes ?

email
profile
role_list
roles
web-origins

« Remove selected

Optional Client Scopes ?

Available Client Scopes ?

gw

Add selected »

Assigned Optional Client Scopes ?

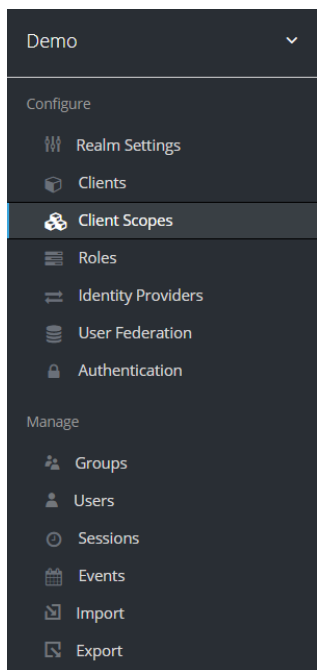
address
microprofile-jwt
offline_access
phone

« Remove selected

Для отдельно каждого клиента score может быть изменен:

The screenshot shows the Keycloak Admin Console interface. On the left is a dark sidebar with a menu. The top of the sidebar has a 'Demo' dropdown. Below it is a 'Configure' section with links to 'Realm Settings', 'Clients' (highlighted), 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. The bottom of the sidebar is a 'Manage' section with links to 'Groups', 'Users', 'Sessions', 'Events', and 'Import'. The main content area has a breadcrumb 'Clients > client-app' and a title 'Client-app' with a trash icon. Below the title is a horizontal tab bar with 'Settings', 'Credentials', 'Roles', 'Client Scopes' (highlighted), 'Mappers', 'Scope', 'Revocation', 'Sessions', 'Offline Access', and 'Clustering'. Under the 'Client Scopes' tab, there are two sub-tabs: 'Setup' (active) and 'Evaluate'. The 'Setup' sub-tab contains three panels: 'Default Client Scopes', 'Available Client Scopes', and 'Assigned Default Client Scopes'. The 'Available Client Scopes' panel lists 'gw' and 'web-origins', with 'web-origins' highlighted in yellow. Below this list is an 'Add selected »' button. The 'Assigned Default Client Scopes' panel lists 'email', 'profile', and 'roles', with a « Remove selected button. Below these are two more panels for 'Optional Client Scopes', which also show 'gw' and 'web-origins' in the 'Available Client Scopes' list and 'address', 'microprofile-jwt', 'offline_access', and 'phone' in the 'Assigned Optional Client Scopes' list.

Client score позволяет связать используемый протокол, клиента и другой параметр, например, через mapper:



Client Scopes > phone > Mappers > Create Protocol Mappers

Create Protocol Mapper

Protocol openid-connect

Name

Mapper Type User Realm Role

Realm Role prefix

Multivalued ☒

Token Claim Name

Claim JSON Type Select One...

Add to ID token ☒

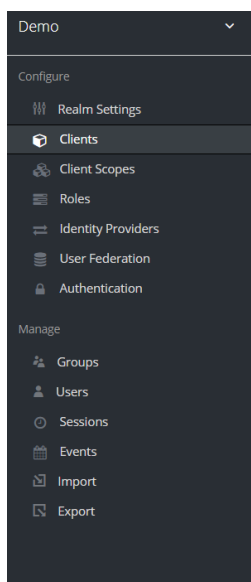
Add to access token ☒

Add to userinfo ☒

Role scope mappings

Также под scope в keycloak может подразумеваться набор доступных ролей на клиенте. При выключении флага о передаче всего доступного scope, можно избирательно настроить необходимый scope, который складывается из ролей на уровне Realm и из ролей clients, зарегистрированных в Keycloak.

При создании токена доступа OIDC или SAML набор ролей пользователя становится набором «разрешений» внутри токена. Приложения используют эти «разрешения» для принятия решений о доступе к ресурсам, контролируемым приложением. Keycloak подписывает токены доступа цифровой подписью, и приложения повторно используют их для вызова защищенных REST-сервисов. Однако существует риск кражи токена. Злоумышленник может получить токен и использовать «разрешения» для взлома. Чтобы предотвратить эту ситуацию, рекомендуется явно задавать набор ролей. Область scope ограничивает роли, объявленные внутри токена доступа. Когда клиент запрашивает проверку подлинности пользователя, токен доступа, который они получают затем, содержит только ограниченный настроенный набор ролей, которые явно указаны в scope клиента. В результате вы ограничиваете разрешения каждого отдельного токена доступа вместо того, чтобы предоставлять клиенту доступ ко всем разрешениям пользователей.



Clients > client-app

Client-app

Settings Credentials Roles Client Scopes Mappers **Scope** Revocation Sessions Offline Access

Service Account Roles Permissions

client-app Scope Mappings

Full Scope Allowed

☒ OFF

Realm Roles

Available Roles

offline_access
role
uma_authorization

Add selected >

Assigned Roles

<< Remove selected

Effective Roles

Client Roles

Available Roles

gateway

Add selected >

Assigned Roles

<< Remove selected

Effective Roles