

Roles. Варианты конфигурации

Роли и группы имеют схожую цель, которая заключается в предоставлении пользователям доступа и разрешений. Группы - это набор пользователей, к которым вы применяете роли и атрибуты. Роли определяют конкретные разрешения приложений и контроль доступа. Роль обычно применяется к одному типу пользователей. Например, организация может включать роли администратора, пользователя, менеджера и сотрудника. Приложение может назначить разрешения для роли, а затем назначить нескольким пользователям эту роль, чтобы пользователи имели одинаковый доступ и разрешения.

Roles

Существует глобальное пространство имен для ролей (Roles на уровне Realms),

Role Name	Composite	Description	Actions	
offline_access	False	\${role_offline-access}	Edit	Delete
role	True		Edit	Delete
uma_authorization	False	\${role_uma_authorization}	Edit	Delete

Для создания роли на уровне всего пространства, выполните:

- Нажмите кнопку Добавить роль.
- Введите Имя роли.
- Введите описание.
- Нажмите кнопку Сохранить.

Roles > Add Role

Add Role

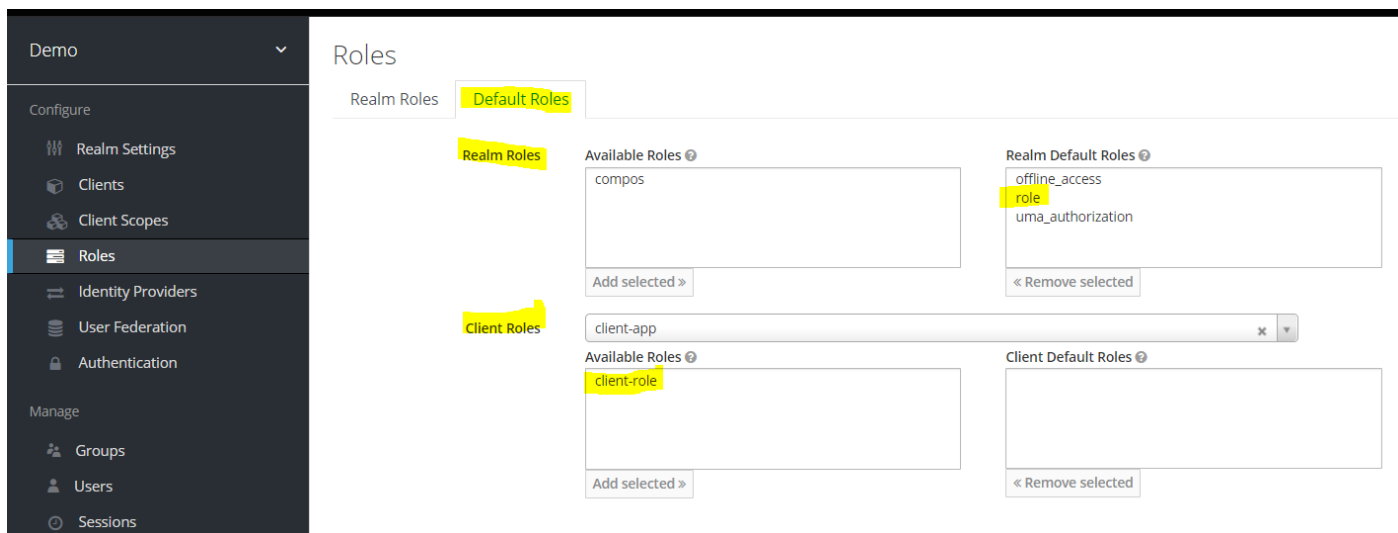
* Role Name

Description

Save Cancel

Поле описания можно локализовать, указав переменную подстановки со строками `${var-name}`. Локализованное значение настраивается для темы в файлах свойств тем.

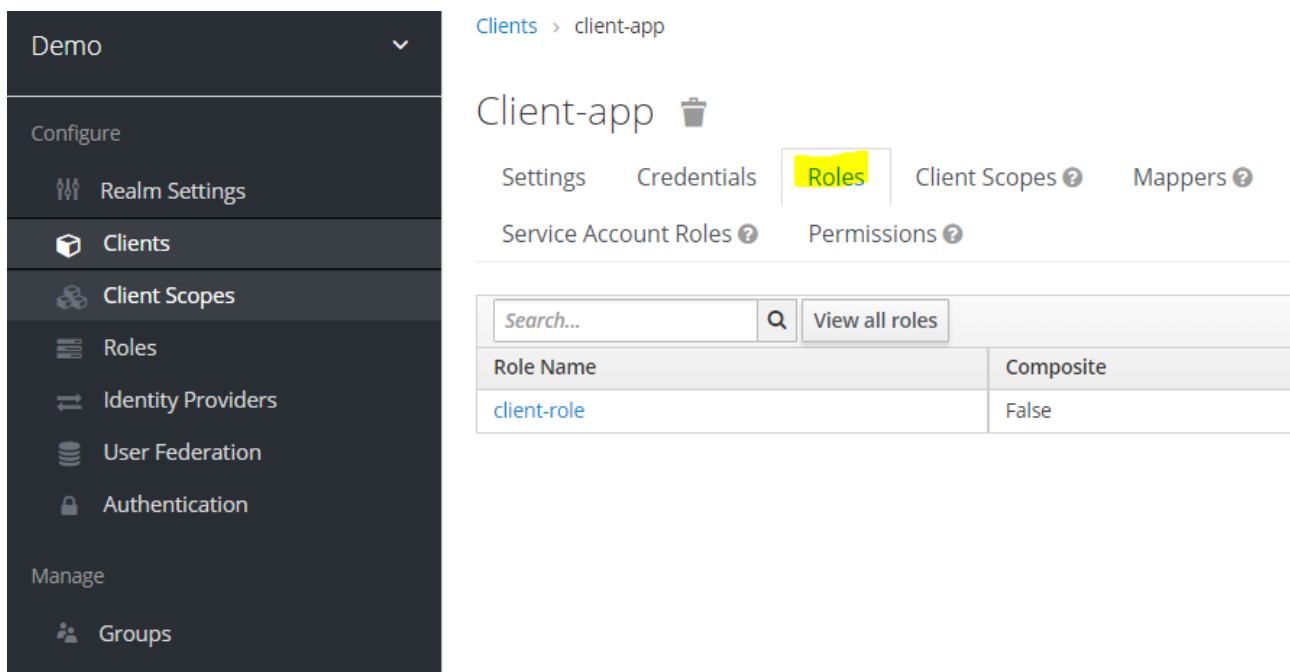
Роли можно устанавливать как дефолтные.



Используйте роли по умолчанию для автоматического назначения ролей пользователей через настройки в mappers при создании или импорте пользователя с помощью провайдера IDP.

Client roles

И каждый клиент также имеет свое собственное выделенное пространство имен, в котором могут быть определены роли.



Преобразование роли в композитную (сложную)

Любая роль уровня Realm или клиента может стать составной ролью.

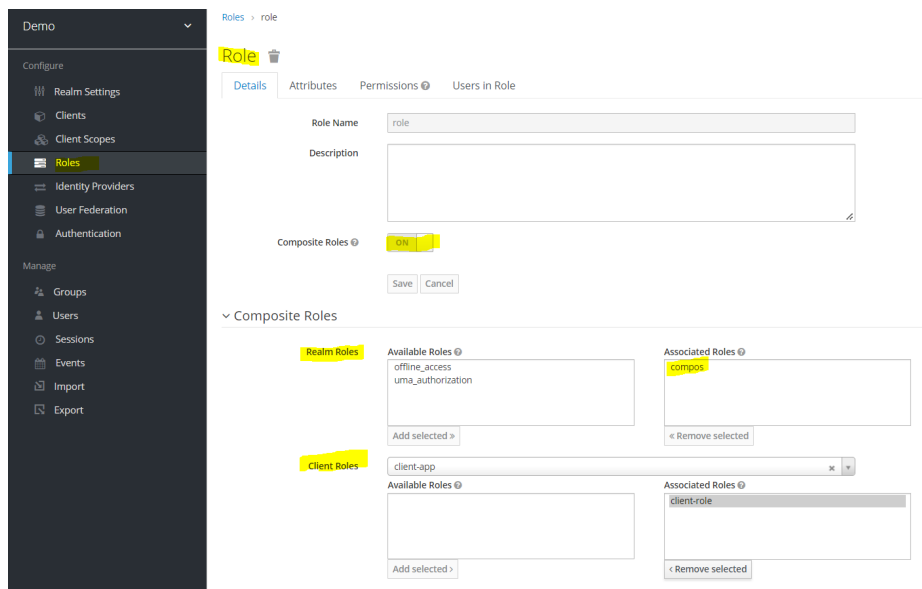
Составная роль - это роль, с которой связана одна или несколько дополнительных ролей. Когда составная роль сопоставляется пользователю, пользователь получает роли, связанные с составной ролью. Это наследование является рекурсивным, поэтому пользователи также наследуют любой состав композитов. Однако мы рекомендуем не злоупотреблять составными ролями.

Настройка композитной роли

Выберите пункт Роли в меню.

Щелкните роль, которую вы хотите преобразовать.

Переключите составные роли в положение ВКЛ.



Role scope mappings

Также под scope в keycloak может подразумеваться набор доступных ролей на клиенте. При выключении флага о передаче всего доступного scope на клиенте, 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.

