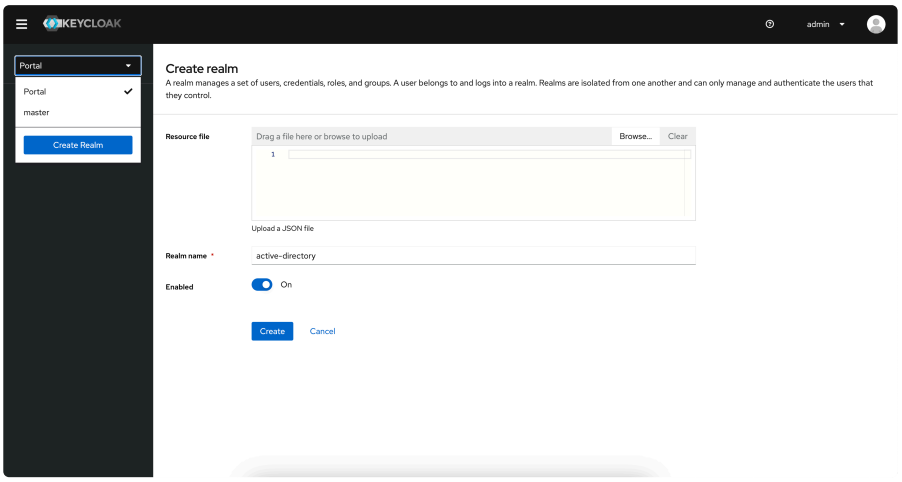
Подключение Active Directory через Keycloak и синхронизация пользователей

ОС Windows 10 не позволяет создавать Active Directory. Если у вас установлена ОС Windows 10, то рекомендуется использовать Windows Server на виртуальной машине для создания Active Directory.

1. Создание нового realm

При первой регистрации в Keycloak в нем существует только master-область, поэтому нужно создать новую область для дальнейших действий. Для этого:

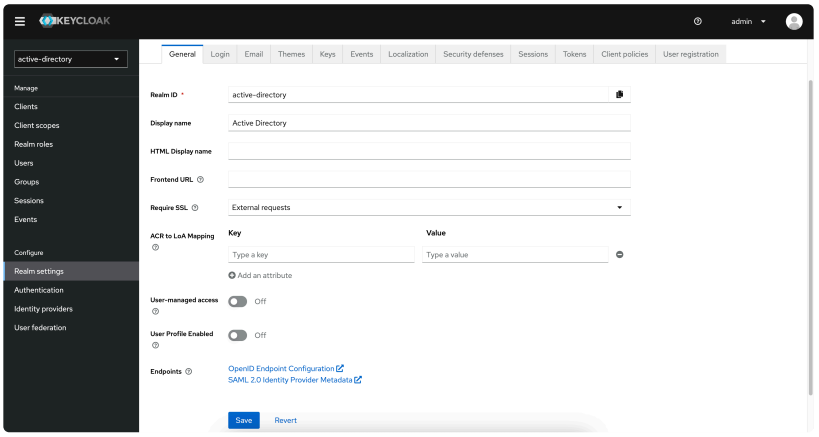
1. В верхнем левом углу нажмите **Add realm**.
2. Введите произвольное название, например, "active-directory" и нажмите **Create**.



3. Слева в панели выберите **Realm Settings** и заполните параметры нового realm:

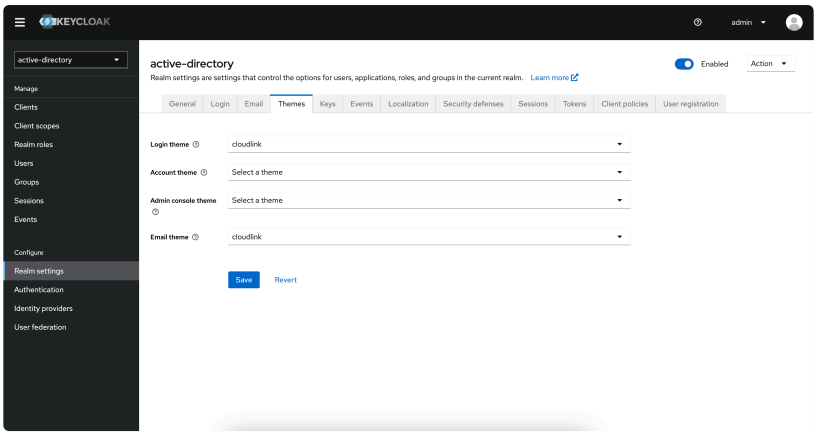
   a. На вкладке **General** введите:

   - **Display name — Active Directory**.



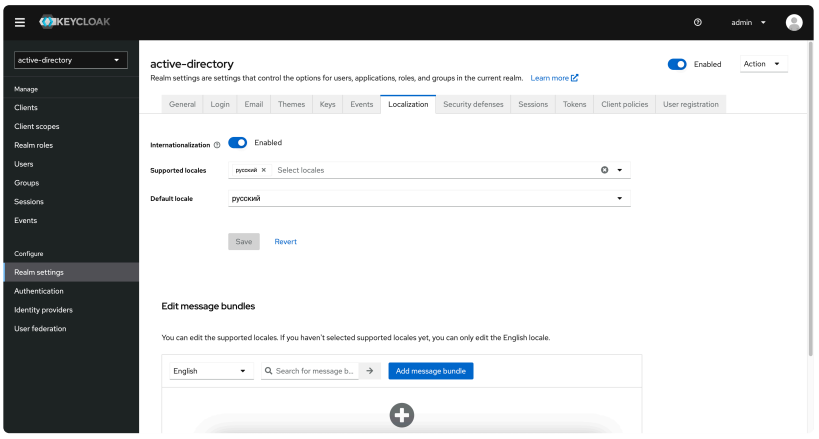
   b. На вкладке **Themes** введите:

- **Login theme** — cloudlink.
- **Email theme** — cloudlink.



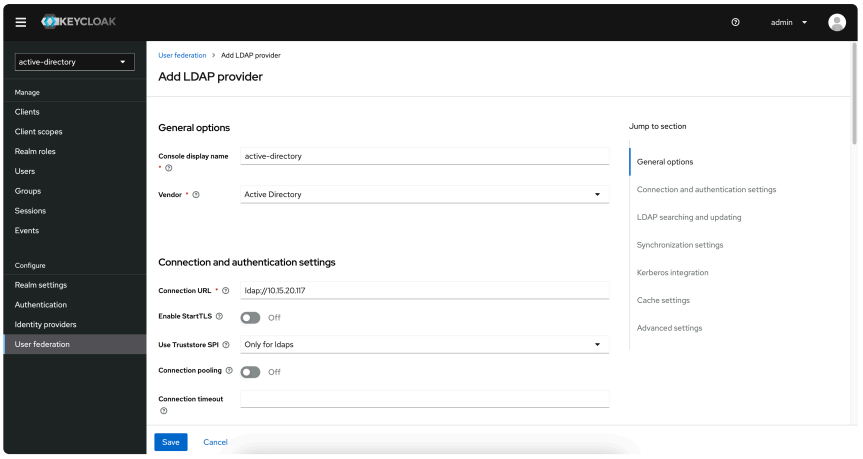
c. На вкладке **Localization** введите:

- **Internationalization** — Enabled
- **Supported locales** — русский.
- **Default locale** — русский.

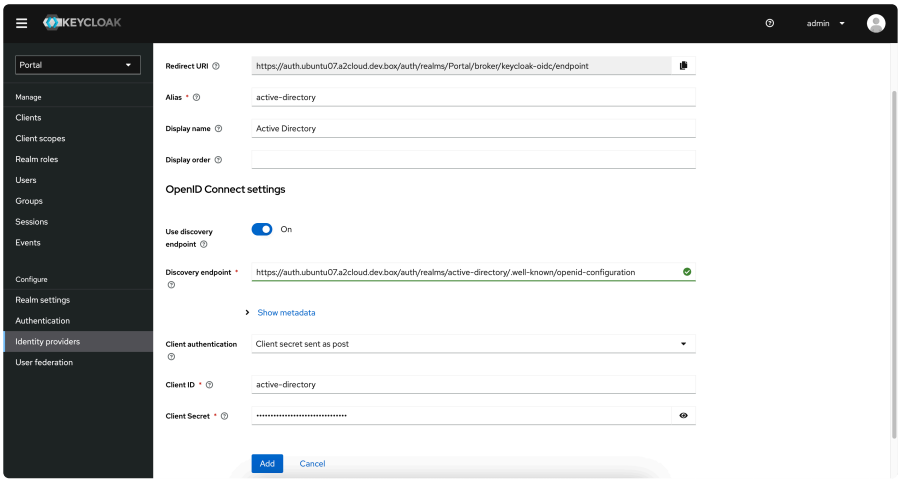


4. Нажмите **Save**.
5. Скопируйте ссылку на **OpenID Endpoint Configuration**, она пригодится для дальнейшей настройки. Пример: https://auth.example.com/auth/realms/active-directory/.well-known/openid-configuration
6. В панели слева выберите **User federation** и нажмите **Add LDAP Provider**.
7. Укажите следующие параметры для федерации пользователей:
   - **Console display name** — active-directory
   - **Vendor** — Active Directory
   - **Connection URL** — ldap://<active-directory-ip-or-dns>
   - **Bind type** — simple
   - **Bind DN** — CN=dadmin,CN=Users,DC=test,DC=ad
   - **Bind credentials** — <password>

- **Edit mode** — READ_ONLY
- **Users DN** — CN=Users,DC=test,DC=ad
- **Trust email** — On



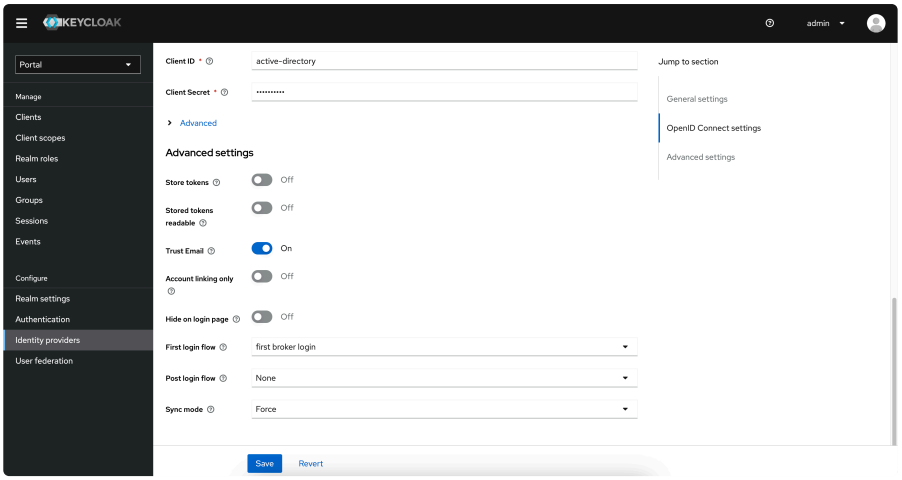
8. Завершите настройку, нажав **Save**.
9. После ввода параметров проверьте подключение с помощью **Test connection** и **Test authentication**.
10. По завершении настройки нажмите **Sync all users** и убедитесь в отсутствии ошибок.
11. Переключитесь на **realm "Portal"** и добавьте новый Identity provider с параметрами:
    - **Type** — Keycloak OpenID Connect
    - **Alias** — active-directory
    - **Display name** — Active Directory
    - **Discovery endpoint** — введите сохранённую ранее ссылку на **OpenID Endpoint Configuration**
    - **Client ID** — active-directory
    - **Client Secret** — введите сохранённый ранее **Client secret**.
12. Сохраните изменения.



13. Повторно откройте настройки подключения и установите:

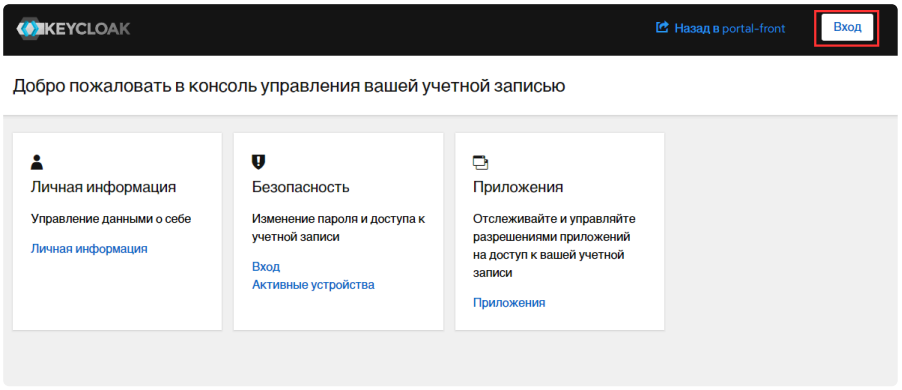
- **Trust Email** — On
- **Sync mode** — Force

14. Нажмите **Save**.



2. Проверка синхронизации Keycloak с Active Directory

1. В интерфейсе Keycloak в левой панели управления нажмите **Clients**. Нажмите на URL-адрес консоли: В **Keycloak Account Manager** в правом верхнем углу нажмите **Вход**.



2. В появившемся окне введите учетные данные любого пользователя из Active Directory.
3. После успешной аутентификации вы попадете в аккаунт созданного пользователя и увидите его профиль.