???????????? ?????????????? ?? ?????? OpenID ??? Google

Ця інструкція описує налаштування **єдиного входу (SSO)** до **VMware Cloud Director Tenant Portal** через **OpenID Connect (OIDC)** з використанням **Google Cloud** як Identity Provider. Підтримується централізована автентифікація та **MFA** з боку Google.

? ????????? ??????

- Адміністративний доступ до **Google Cloud Console**.
- Адміністративний доступ до **Cloud Director Tenant Portal**.
- Домен Cloud Director доданий до **Authorized domains** у Google Cloud.
- VMware Cloud Director **10.5+** (OIDC підтримується нативно).

? ????? ????????????

1) Google Cloud Console

1. Перейдіть у Google Cloud Console: https://console.cloud.google.com/
2. Відкрийте меню **APIs & Services**.

2) ????????? ???????

1. У верхній панелі відкрийте список проєктів.
2. Створіть новий проєкт:
   - **Name:** `VMware Cloud Director`
   - Натисніть **Create**.

3) OAuth Consent Screen

1. В меню зліва відкрийте **OAuth consent screen**.
2. **User Type:** `Internal`.
3. Заповніть обов’язкові поля:
   - **App name:** `VMware Cloud Director`
   - **User support email:** email адміністратора
   - **Authorized domains:** домен Cloud Director (наприклад `eurocloud.datagroup.ua`)
   - **Developer contact email:** email адміністратора
4. Збережіть і продовжуйте.
5. Додайте scopes:
   - `openid`
   - `https://www.googleapis.com/auth/userinfo.email`
   - `https://www.googleapis.com/auth/userinfo.profile`

6. Збережіть зміни.

4) ????????? OAuth Client ID

1. Перейдіть у **Credentials**.
2. **Create Credentials → OAuth client ID**
3. Тип застосунку: **Web application**
4. Заповніть:
   - **Name:** домен Cloud Director (наприклад `eurocloud.datagroup.ua`)
   - **Authorized JavaScript origins:**

     ```
     https://eurocloud.datagroup.ua
     ```

   - **Authorized redirect URIs:**

     ```
     https://eurocloud.datagroup.ua/login/oauth?service=tenant:testorg
     ```

     ⚠ `testorg` — це **Organization ID**, а не назва.
5. Натисніть **Create**.
6. Збережіть **Client ID** та **Client Secret**.

5) ????????????? VMware Cloud Director (Tenant)

1. Увійдіть у **Tenant Portal**.
2. Перейдіть:

   ```
   Administration → Identity Providers → OIDC
   ```

3. Натисніть **Configure**.
4. Вкажіть:
   - **Client ID:** з Google Cloud
   - **Client Secret:** з Google Cloud
   - **Configuration Discovery:** `Enabled`
   - **Well-known configuration endpoint:**

     ```
     https://accounts.google.com/.well-known/openid-configuration
     ```

5. Інші параметри залиште за замовчуванням.
6. **Subject claim:** `email`
7. Увімкніть **Automatic Key Refresh**:
   - Refresh interval: `1 hour`
   - Policy: `Expire After`
   - Expiration: `24 hours`
8. Збережіть конфігурацію.

6) ?????? ?????????????

Cloud Director **не створює користувачів автоматично** — їх потрібно імпортувати.

1. Перейдіть:

   ```
   Administration → Access Control → Users
   ```

2. Натисніть **Import Users**.
3. Source: **OPENID**
4. Вкажіть email користувачів (точно такий самий, як у Google).
5. Призначте роль (наприклад `Organization Administrator`).
6. Збережіть.

? ?????????

1. Вийдіть з Tenant Portal.
2. На сторінці входу оберіть **Login with OpenID**.
3. Вас має перенаправити на Google.
4. Після MFA — автоматичний вхід у Cloud Director.

? ????????

- MFA повністю контролюється **Google**, не Cloud Director.
- Один OIDC-провайдер можна використовувати для кількох org (з різними redirect URI).
- Redirect URI чутливий до **org ID** — помилка тут часто дає 401/redirect mismatch.

Версія #4
az створив 30 січня 2026 08:29:15
az оновив 30 січня 2026 08:58:46