



1. Перейдіть до розділу **Attributes & Claims** і натисніть **Edit**.
2. Додайте новий твердження (claim):

- **Roles** — джерело: user.assignedroles
- **UserName** — джерело: user.mail

3. Додайте груповий твердження **Groups**:

- Оберіть **All groups**, джерело — **Group ID**
- Увімкніть **Customize the name of the group claim** та введіть ім'я Groups.

4. Збережіть зміни.

#### 4) ?????????????? ?????????? Azure AD ? vCloud Director

1. Увійдіть назад у **vCloud Director SAML Configuration**.
2. Відкрийте **Edit**, перейдіть на вкладку **Identity Provider**.
3. Активуйте перемикач для увімкнення **SAML Identity Provider**.
4. Завантажте **Federation Metadata XML** файл, який ви завантажили з Azure AD (розділ **SAML Signing Certificate** → **Federation Metadata XML**).
5. Натисніть **SAVE** для збереження конфігурації.

#### 5) ?????? ?????????????? ?? ????? ? vCloud Director

Після успішного налаштування SAML:

1. У меню vCloud Director перейдіть у **Users** або **Groups**.
2. Натисніть **Import Users** або **Import Groups**.
3. Введіть електронні адреси користувачів так, як вони визначені в Azure AD.  
Для груп — використовуйте **Group ID**, а не назву чи email.
4. Оберіть рівень доступу (ролі) для кожного — і збережіть.

#### 6) ????????????

Відкрийте приватне/інкогніто вікно браузера та перейдіть до URL vCloud Director. При спробі входу оберіть SSO через Azure — ви повинні бути переадресовані на портал **Azure AD** для автентифікації.

#### ? ?????????? ????????

- Імена атрибутів чутливі до регістру (case-sensitive).
- Переконайтеся, що у Azure AD додані саме ті користувачі/групи, які вам потрібні для доступу.

- Після внесення змін до SAML конфігурації може знадобитися кілька хвилин на поширення змін.

---

Версія #2

az створив 29 січня 2026 08:08:06

az оновив 30 січня 2026 08:58:58