GIGACLOUD

Налаштування 2FA для VMware Cloud Director

Посібник адміністратора

версія 2.3 4_2023

+380 44 233 7170
www.gigacloud.ua

Зміст

Призначення 2FA (двофакторної автентифікації) 3
Авторизація у Google Cloud 4
Налаштування Open ID Connect у VCD 11
Налаштування смартфону з ОС Android 16

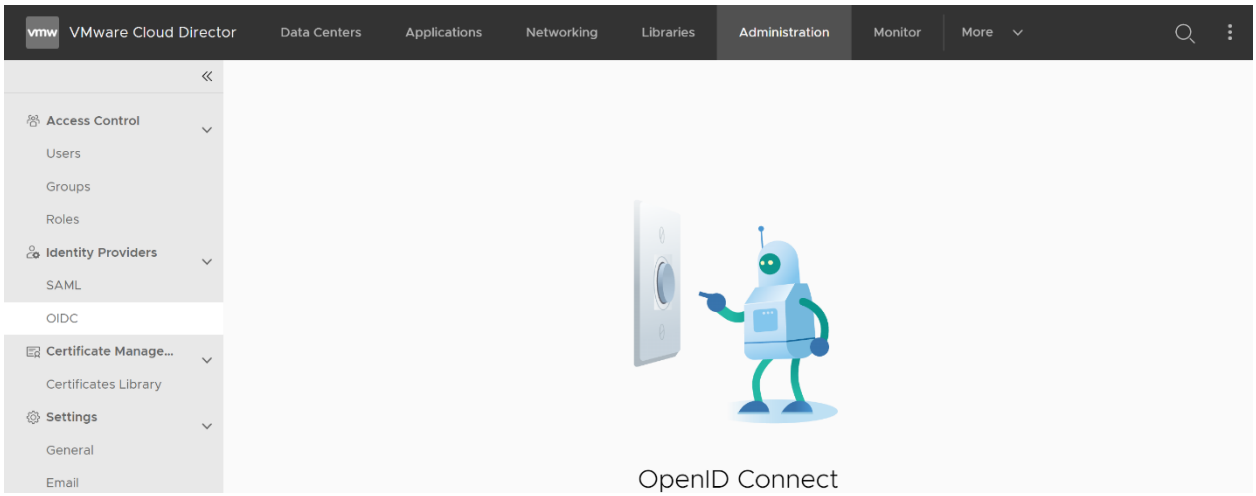
Призначення 2FA (двофакторної автентифікації)

Автентифікація – це процес проходження перевірки автентичності особи для її доступу до комп'ютерної системи або онлайн-сервісу з обліковим записом користувача. Зазвичай, використовують наступні основні фактори автентифікації:

- фактор знання (пароль або PIN-код);
- фактор володіння (мобільний пристрій або посвідчення особи);
- фактор властивості (відбиток пальця/сітківки ока або голос);
- фактори розташування та/або часу.

2FA (двофакторна автентифікація) передбачає використання вашою системою безпеки одночасно двох факторів із наведеного вище переліку. Внаслідок система отримує додатковий рівень безпеки, окрім вашого пароля або PIN-коду (переважно використовується одноразовий код підтвердження через SMS-повідомлення). Для додаткового захисту від зламу зловмисниками, цей згенерований програмою для автентифікації код має короткий термін дії (найчастіше 20 або 30 секунд).

В інтерфейсі VMware Cloud Director (починаючи з версії 10.3) для 2FA за допомогою Open ID Connect додано підтримку OAuth – протоколу авторизації, що дає змогу видати обраному сервісу (застосунку) права на доступ до ресурсів користувача на іншому сервісі.



Технології OAuth звільняють вас від необхідності щоразу довіряти застосунку свої логін і пароль, а також надають змогу видавати сервісу обмежений набір прав (а не всі одразу). Двофакторна автентифікація забезпечує додатковий рівень захисту для вашої інфраструктури у хмарі, оберігаючи конфіденційні дані від потенційних кібератак.

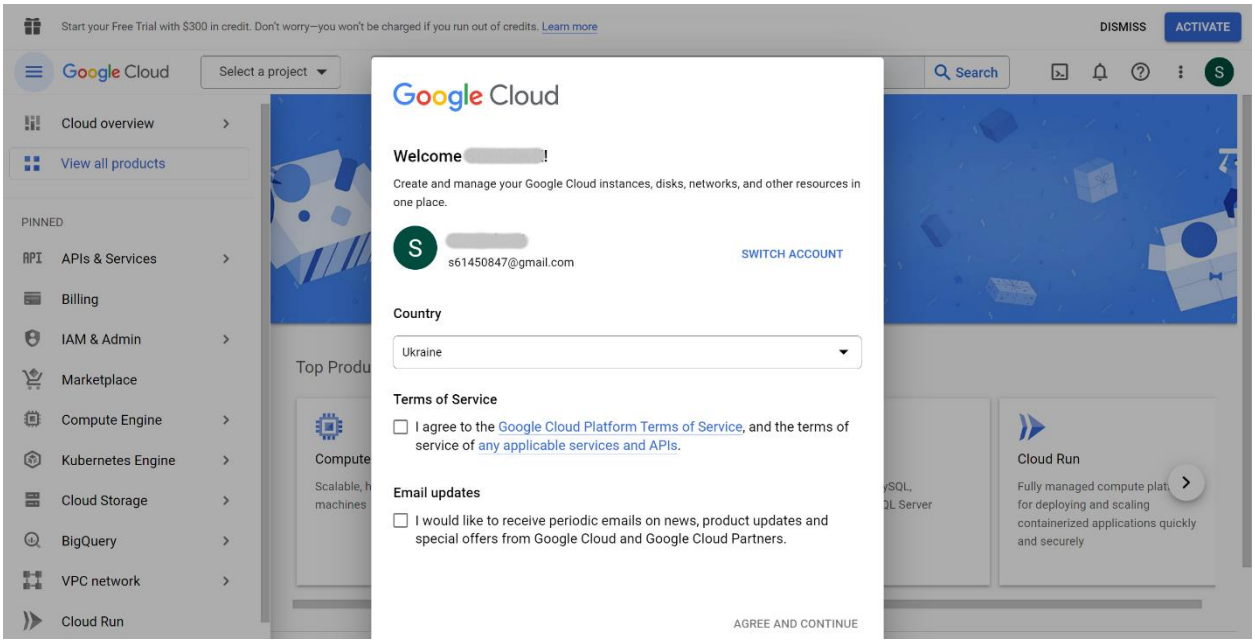
Цей документ («Посібник адміністратора») містить демонстраційний приклад послідовності з трьох етапів налаштувань 2FA:

- OAuth client ID (авторизація у Google Cloud із вашим обліковим записом);
- OIDC (Open ID Connect у розділі «Identity Providers» панелі керування Cloud Director v.10.3);
- акаунту Google у панелі керування смартфону із ОС Android.

Всі наведені нижче зображення є лише демонстраційним прикладом для ознайомлення. Вигляд веб-сторінок і значення параметрів у полях налаштувань – будуть іншими для ваших проектів.

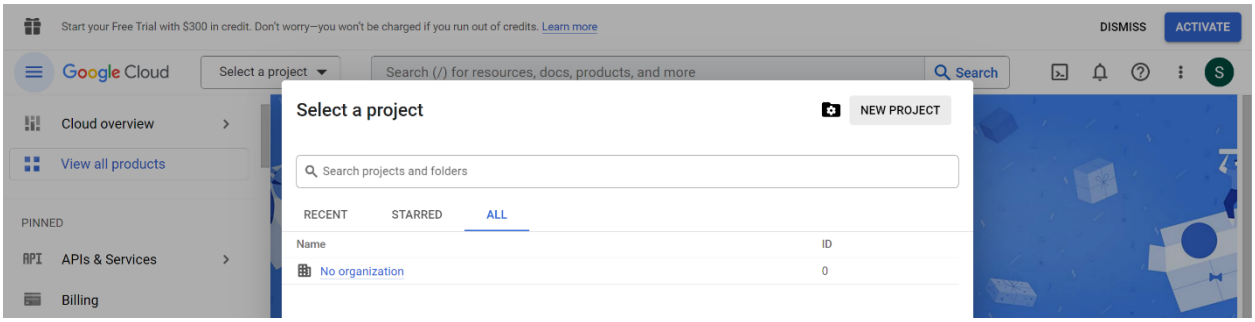
Авторизація у Google Cloud

Користуючись браузером, перейдіть до консолі Google Cloud.

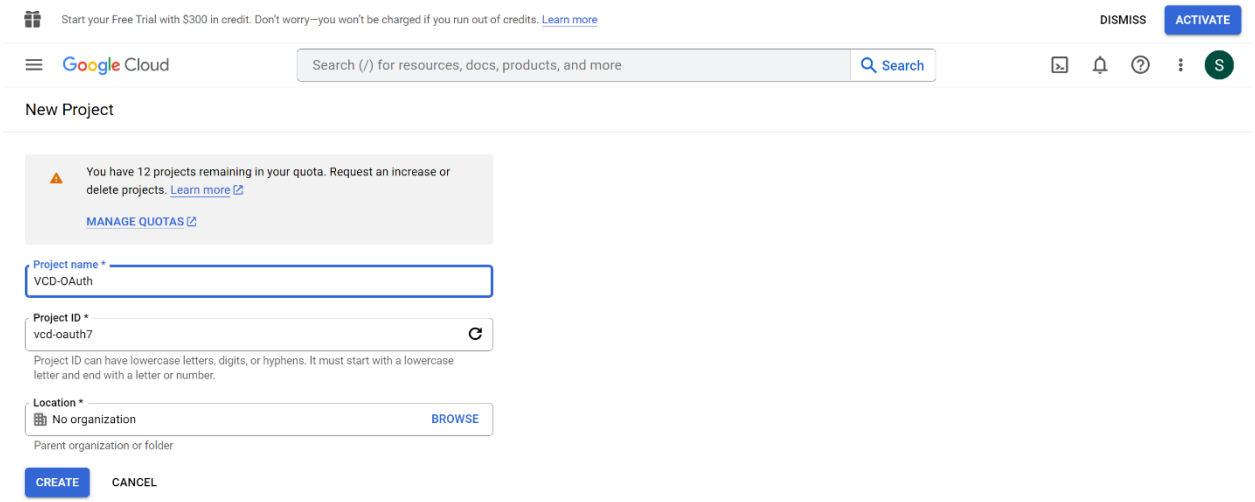


Прийміть умови використання сервісу (встановіть позначку ☑ у рядку «**Terms of Service**» екранної форми), натисніть екранний напис «AGREE AND CONTINUE» для продовження.

Натисніть екранний напис «Select a project» у верхній частині екрану та створіть новий проект (натисніть екранний напис «NEW PROJECT»):

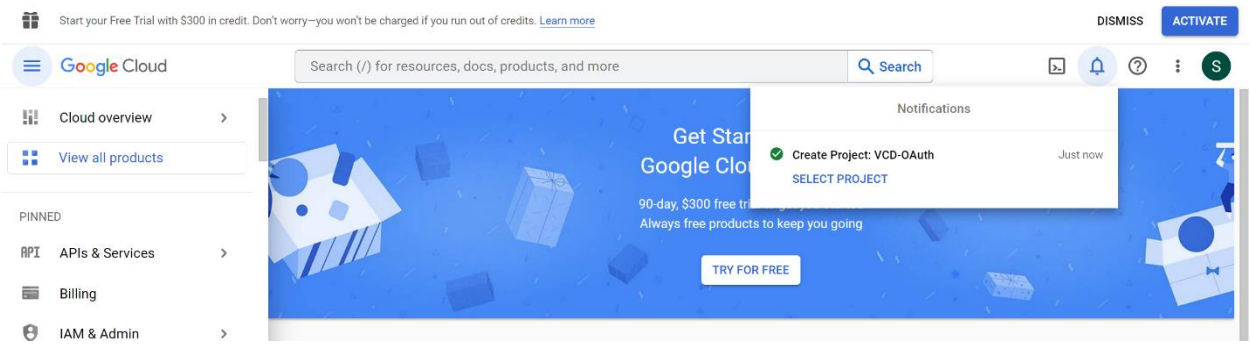


Визначте для нового проекту назву у полі «Project name» (у даному прикладі VCD-OAuth) та ідентифікатор у полі «Project ID» (малими літерами з цифрою чи літерою наприкінці):

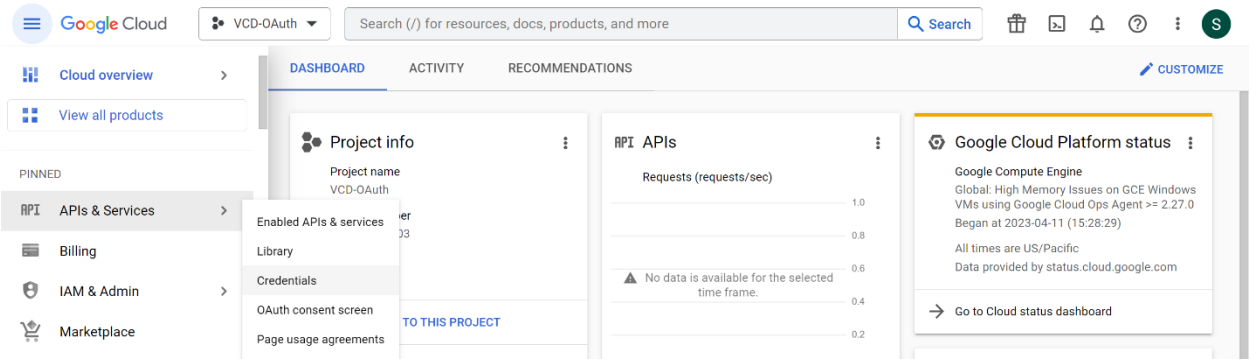


Натисніть екранну кнопку «CREATE» для продовження.

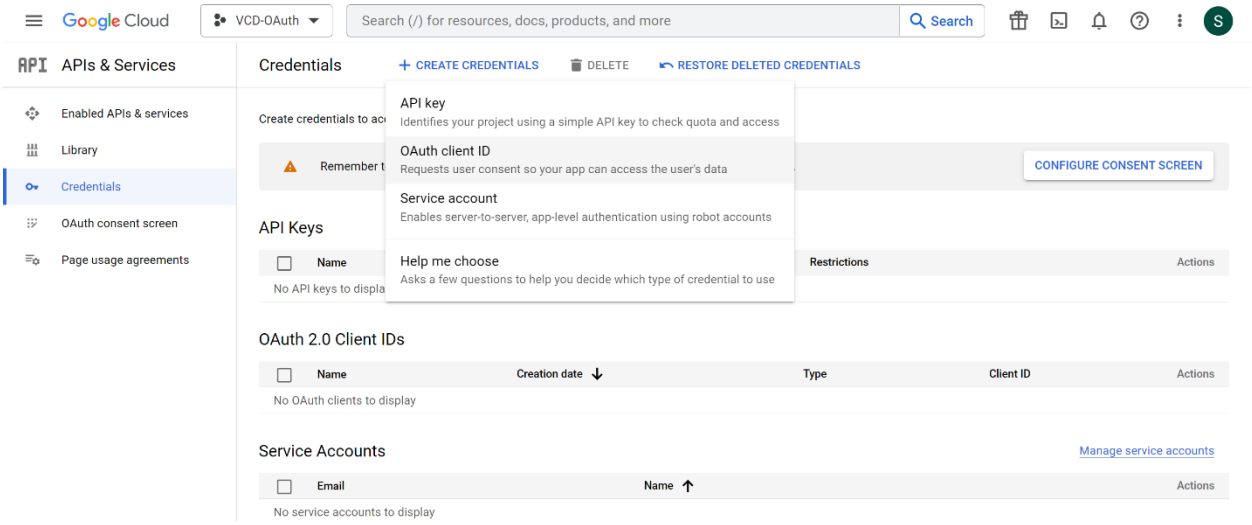
Пересвідчіться, що проект створено та оберіть його:



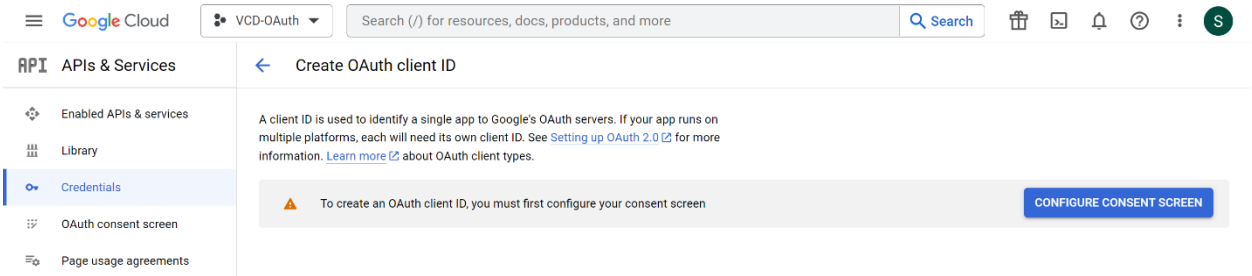
Перейдіть до розділу меню консолі «APIs & Services –> Credentials»:



Натисніть екранний напис «+ CREATE CREDENTIALS», потім оберіть створення ідентифікатора «OAuth client ID»:

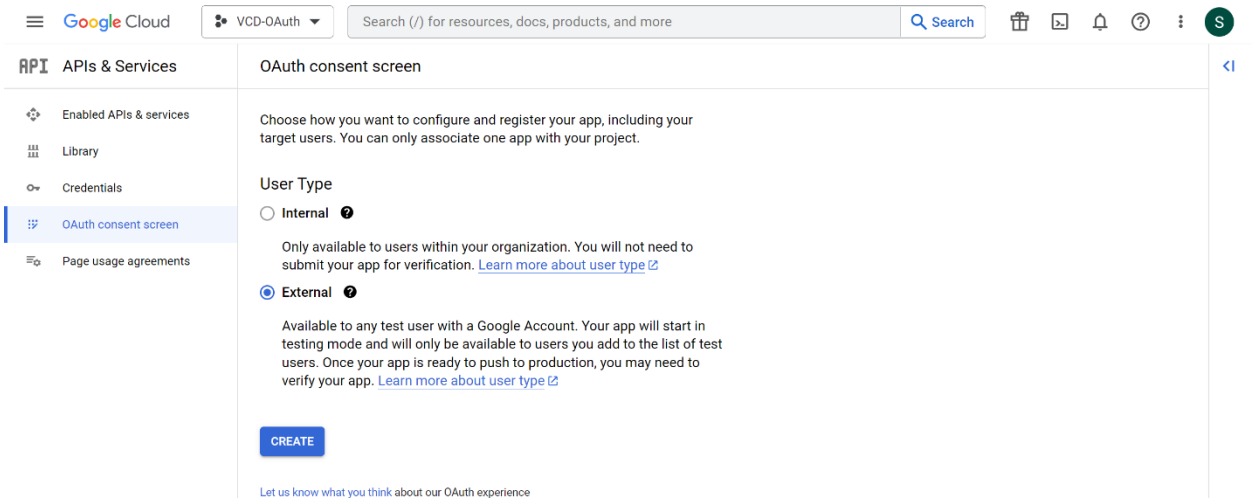


Натисніть напис «CONFIGURE CONSENT SCREEN» у новому вікні – для визначення користувача застосунку/сервісу, до ресурсів якого будуть видаватися права на доступ:

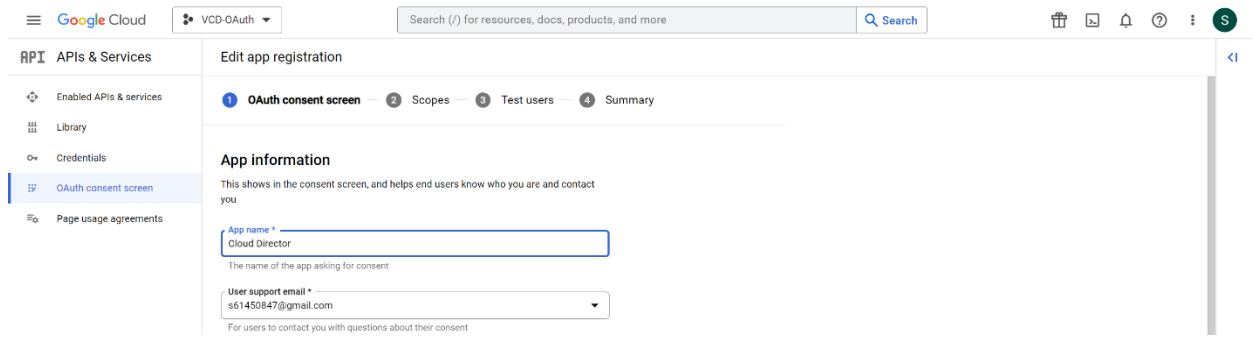


Після переходу до наступного розділу меню «OAuth consent screen», оберіть режим конфігурації та реєстрації застосунку, тип користувачів.

Встановіть позначку «**External**» у меню «User Type»:



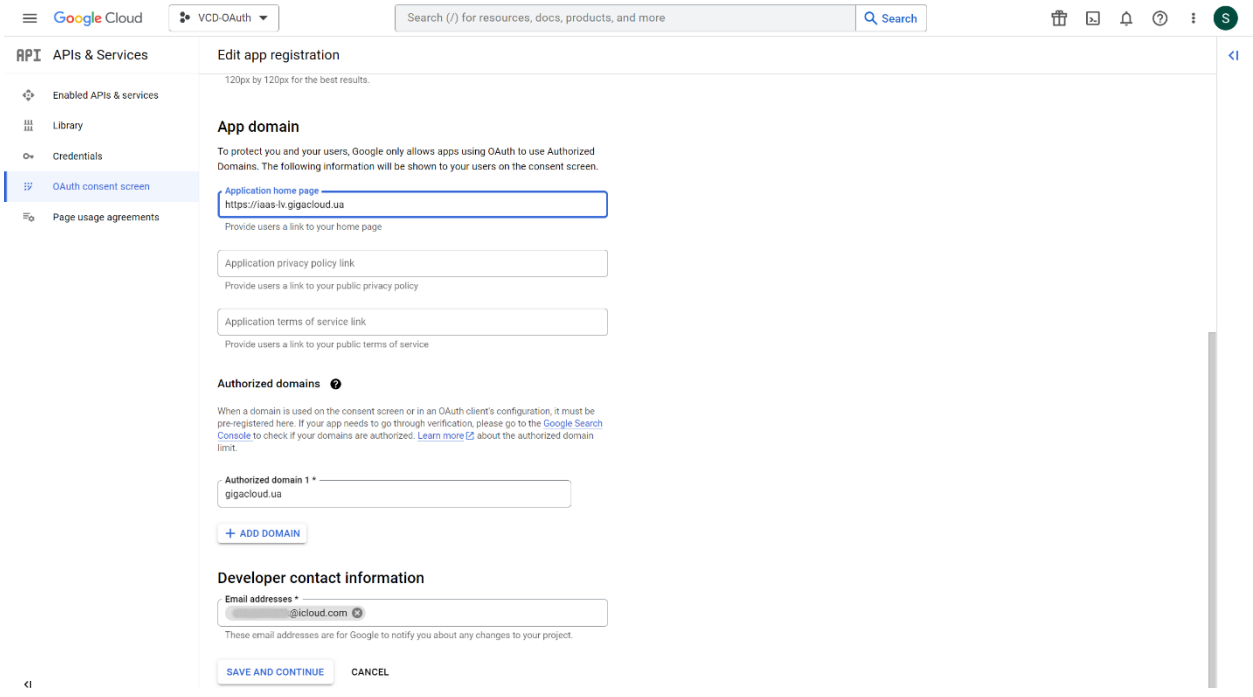
Натисніть кнопку «CREATE» для продовження, заповніть обов'язкові поля форми:



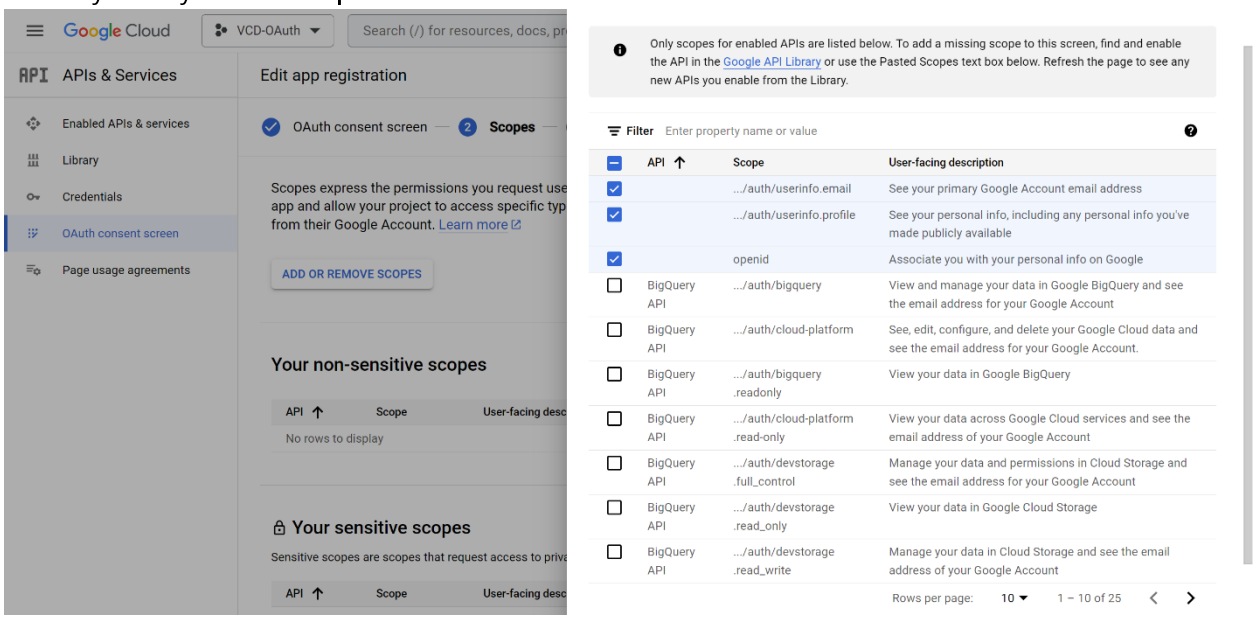
У розділі «App domain» вкажіть URL сторінки входу до VCD (відповідно до кластеру):

- https://iaas-at2.gigacloud.ua/ – кластер AT2 у Польщі;
- https://iaas-bm2.gigacloud.ua/ – кластер BM2;
- https://iaas-lv.gigacloud.ua/ – кластер Львів;
- https://iaas.gigacloud.ua/ – кластер GC/BM/PL

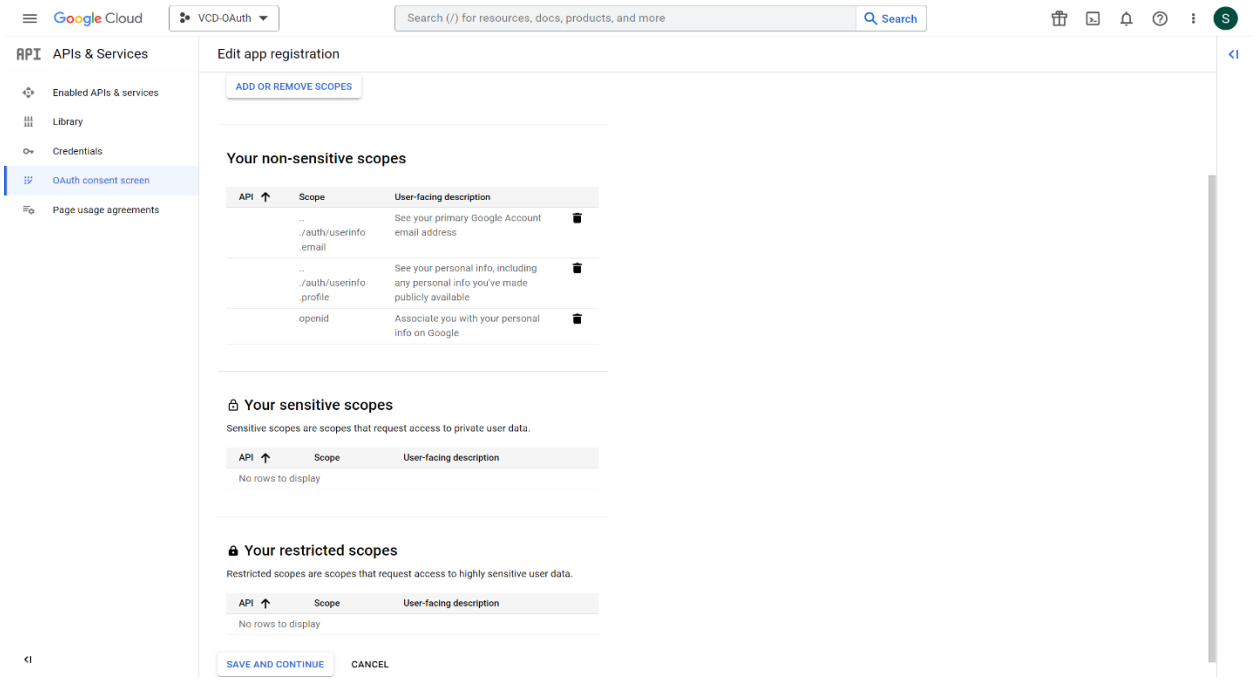
Завершіть заповнення форми. У полі «Authorized domain 1» вкажіть gigacloud.ua та натисніть кнопку «SAVE AND CONTINUE»:



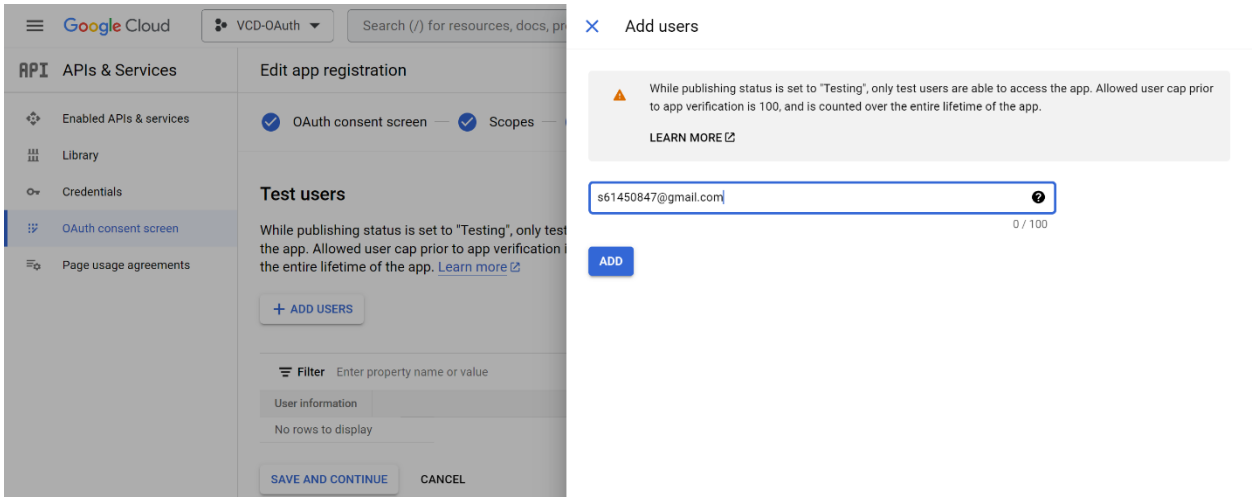
У наступному вікні «**Scopes**» натисніть напис «ADD OR REMOVE SCOPES»:



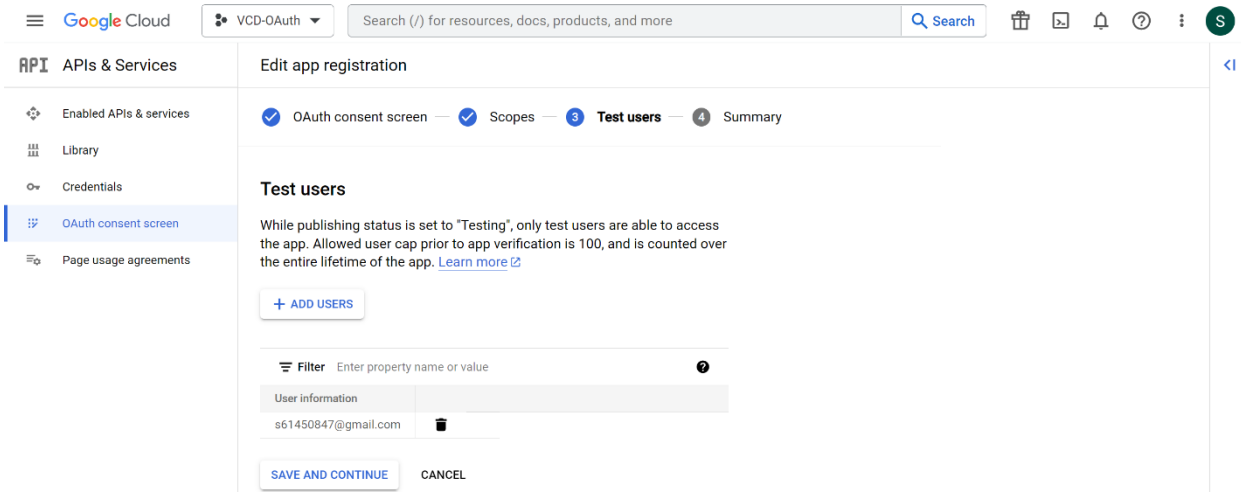
Встановіть позначки активації ☑видимості обраних даних вашого акаунту в Google.



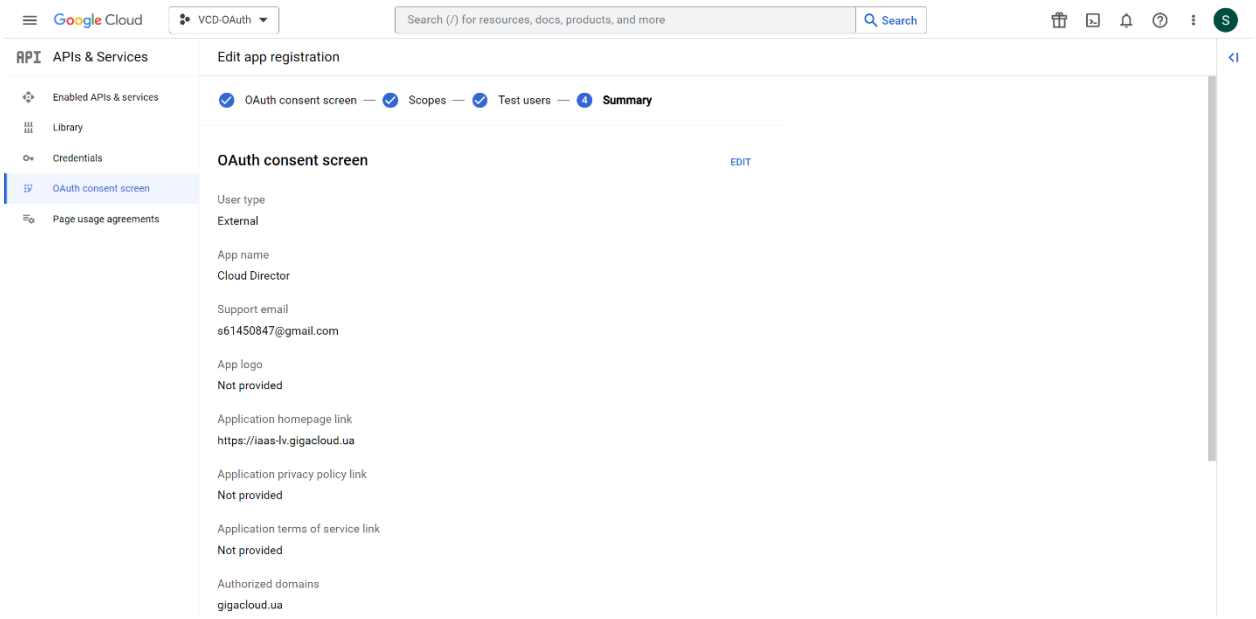
Натисніть кнопку «SAVE AND CONTINUE» для переходу до наступного вікна «**Test Users**». Додайте власну e-mail адресу, натисніть напис «ADD»:



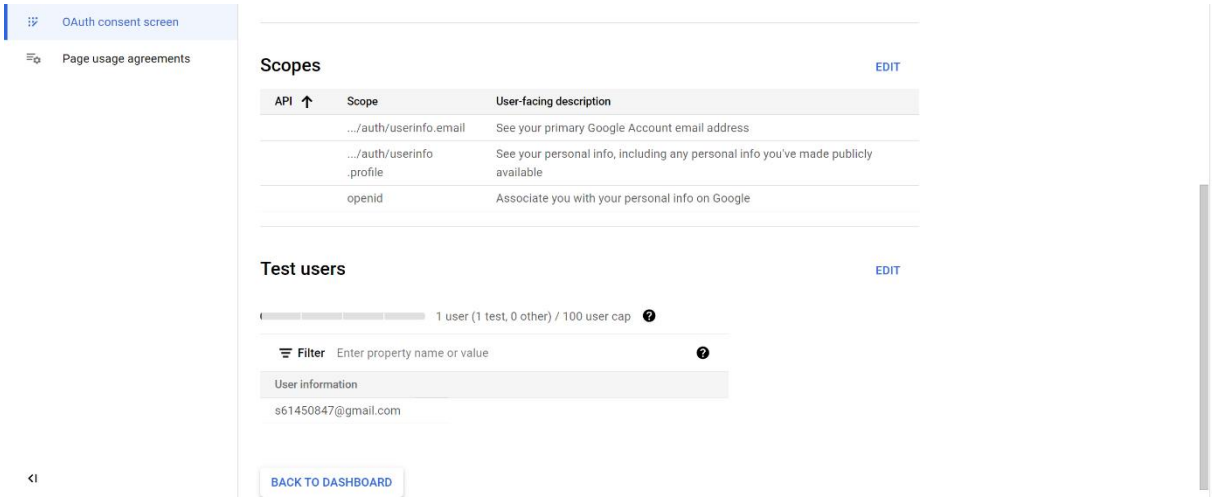
Пересвідчіться, що користувача «Test User» успішно додано:



Натисніть кнопку «SAVE AND CONTINUE» для переходу до наступного вікна «**Summary**».

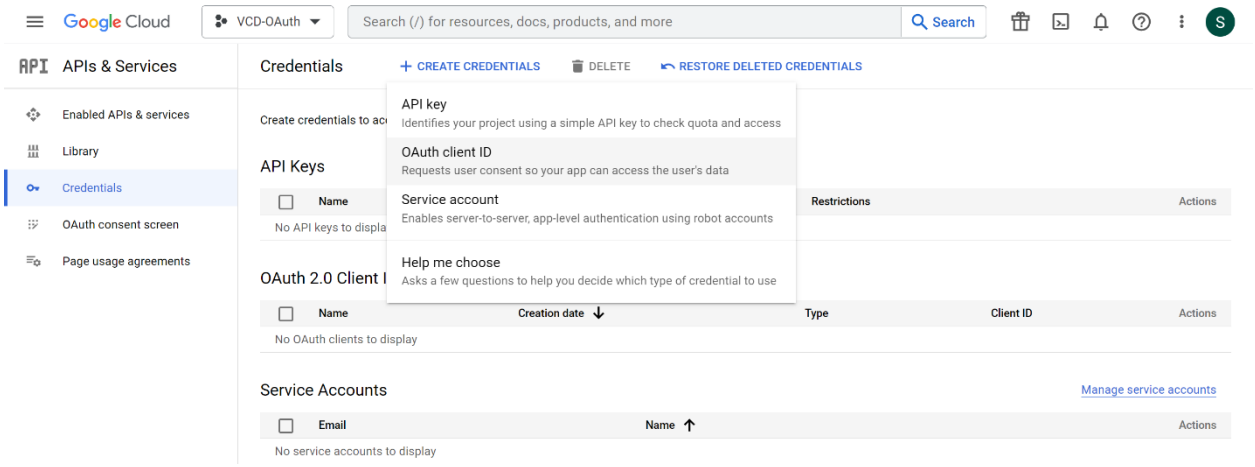


Перегляньте встановлені параметри (у разі необхідності є можливість їх редагувати після натискання написів «EDIT» у відповідних розділах вікна).

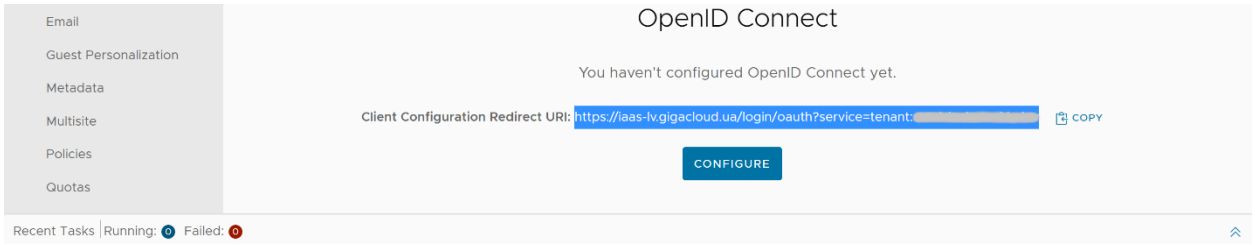


Після завершення, натисніть кнопку «BACK TO DASHBOARD» для повернення до розділу меню консолі «APIs & Services –-> Credentials».

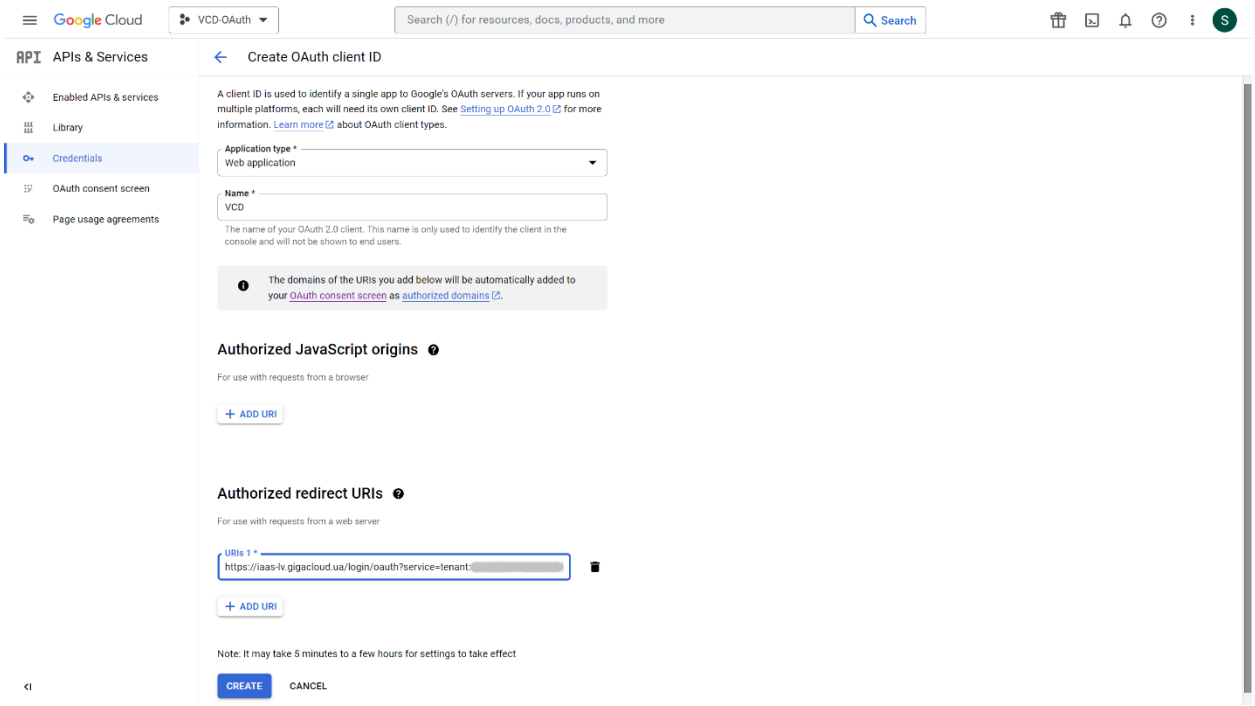
Натисніть екранний напис «+ CREATE CREDENTIALS» та оберіть створення ідентифікатора «OAuth client ID»:



Заповніть обов'язкові поля форми «Create OAuth client ID».
Значення параметрів у полі URLs 1 розділу «Authorized redirect URLs» залежить від кластеру, де розміщені VDC вашої Організації. Отримайте це значення, перейшовши до вікна інтерфейсу VMware Cloud Director «Administration –> Identity Providers –> OIDC». Натисніть екранний напис «COPY»:

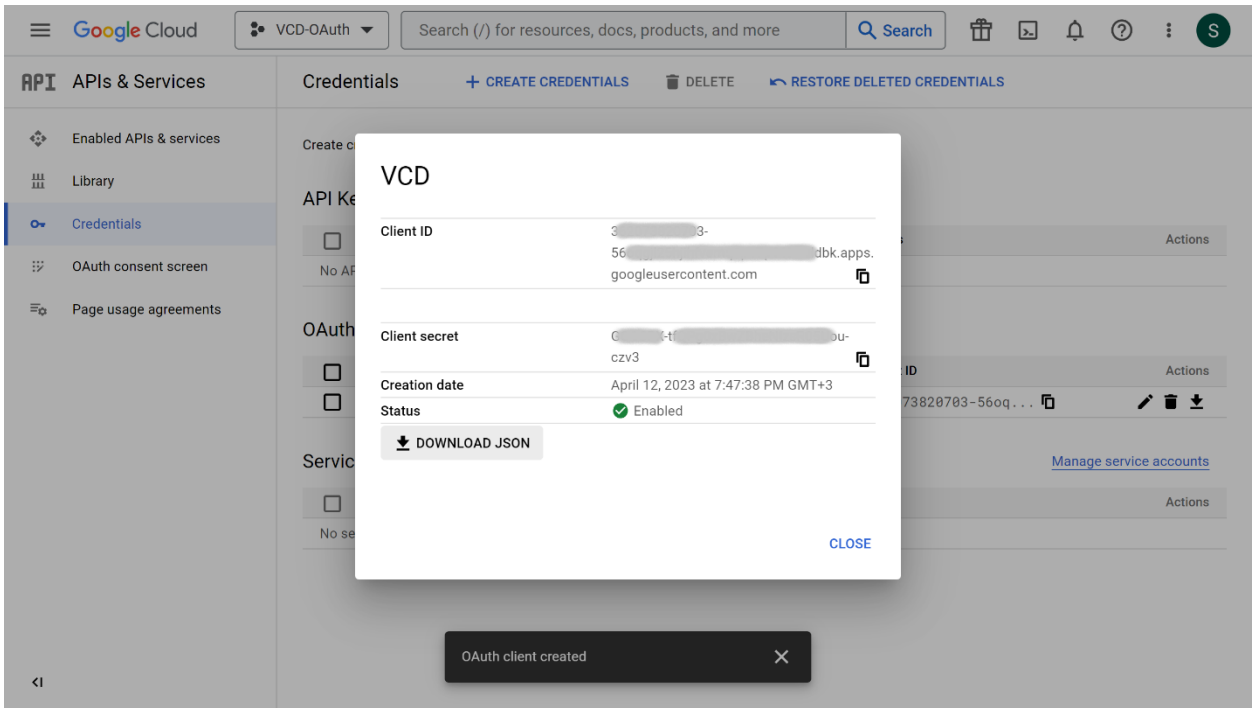


Поверніться до вікна форми «Create OAuth client ID» та вставте отримане значення параметру з буферу до поля «URLs 1» розділу «Authorized redirect URLs»:



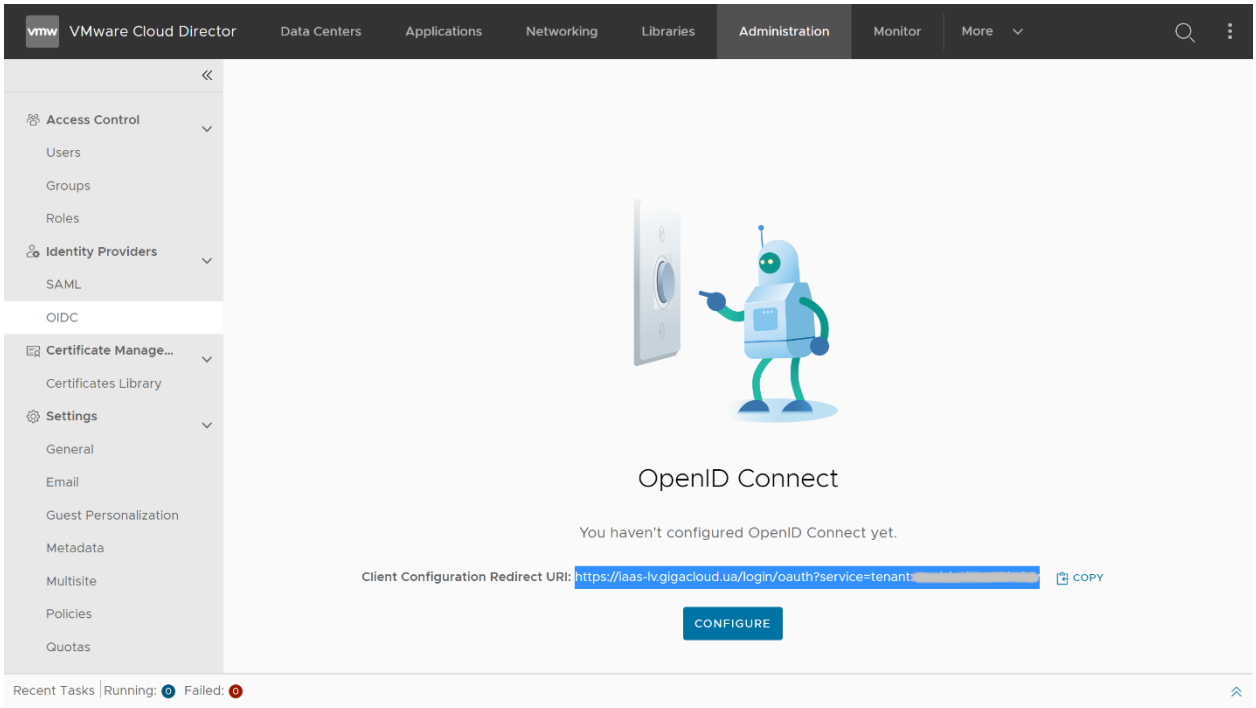
Натисніть кнопку «CREATE».

Після переходу до наступного вікна «**OAuth client created**» збережіть для подальшого використання значення текстових параметрів **Client ID** та **Client secret**, завантажте файл формату **JSON**:



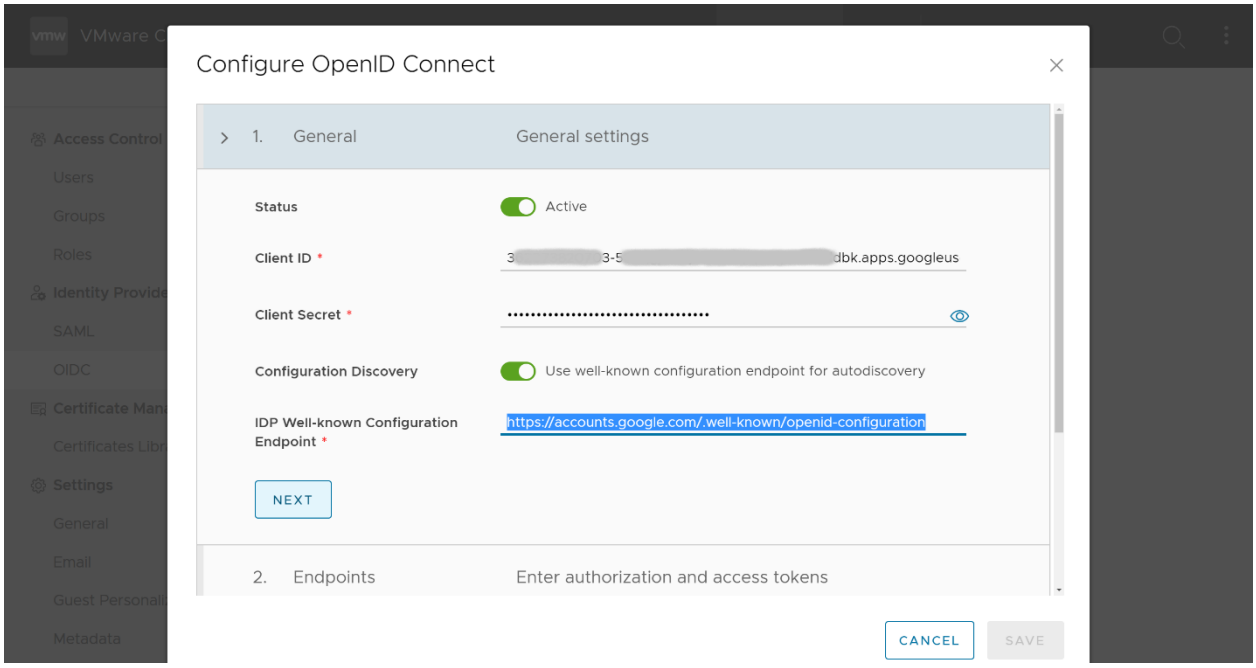
Налаштування Open ID Connect у VCD

Перейдіть до вікна інтерфейсу VCD «**Administration –> Identity Providers –> OIDC**»:



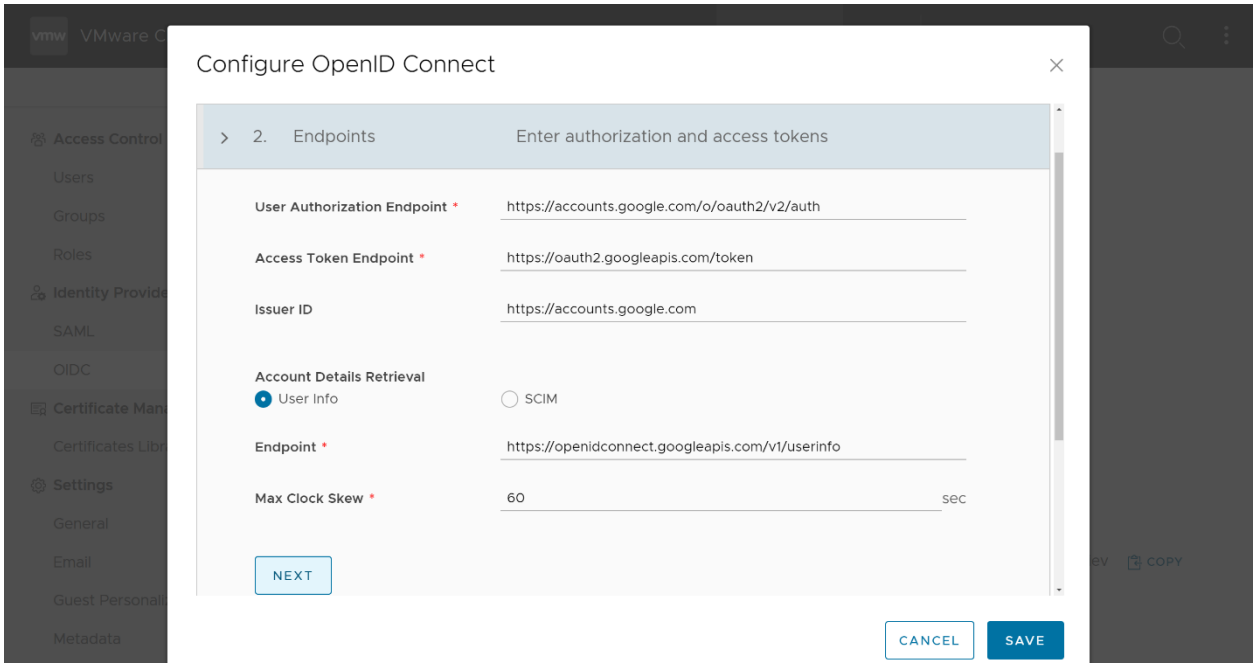
Для отримання до буферу значення «Client Configuration Redirect URL» з метою налаштувань ідентифікатора «OAuth client ID» (див. попередній розділ) – натисніть екранний напис «COPY».

Для початку налаштувань Open ID Connect у VCD натисніть екранний напис «CONFIGURE». Вставте у відповідних полях першого вікна «General» екранної форми «Configure Open ID Connect» значення текстових параметрів **Client ID** та **Client secret**, що були вами збережені раніше (див. попередній розділ).



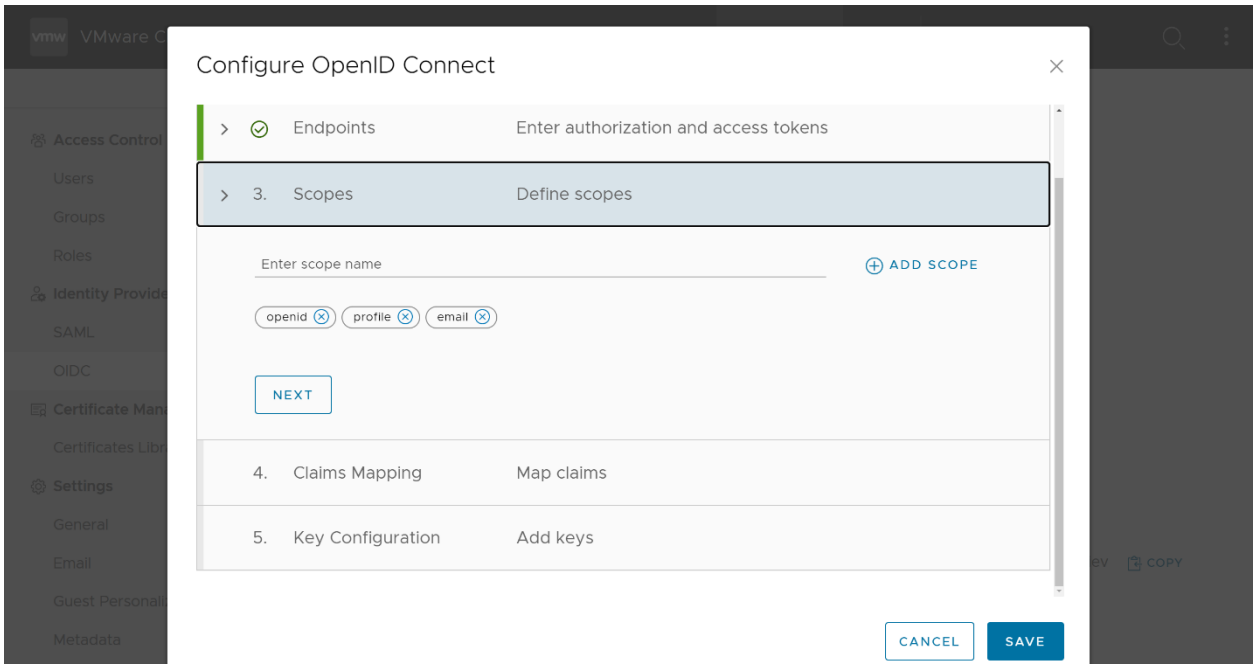
Вкажіть значення https://accounts.google.com/.well-known/openid-configuration у полі параметру «**IDP Well-known Configuration Endpoint**» і натисніть екранну кнопку «NEXT».

Після переходу до другого вікна «Endpoints» екранної форми «Configure Open ID Connect» змінювати початкові значення параметрів не потрібно:



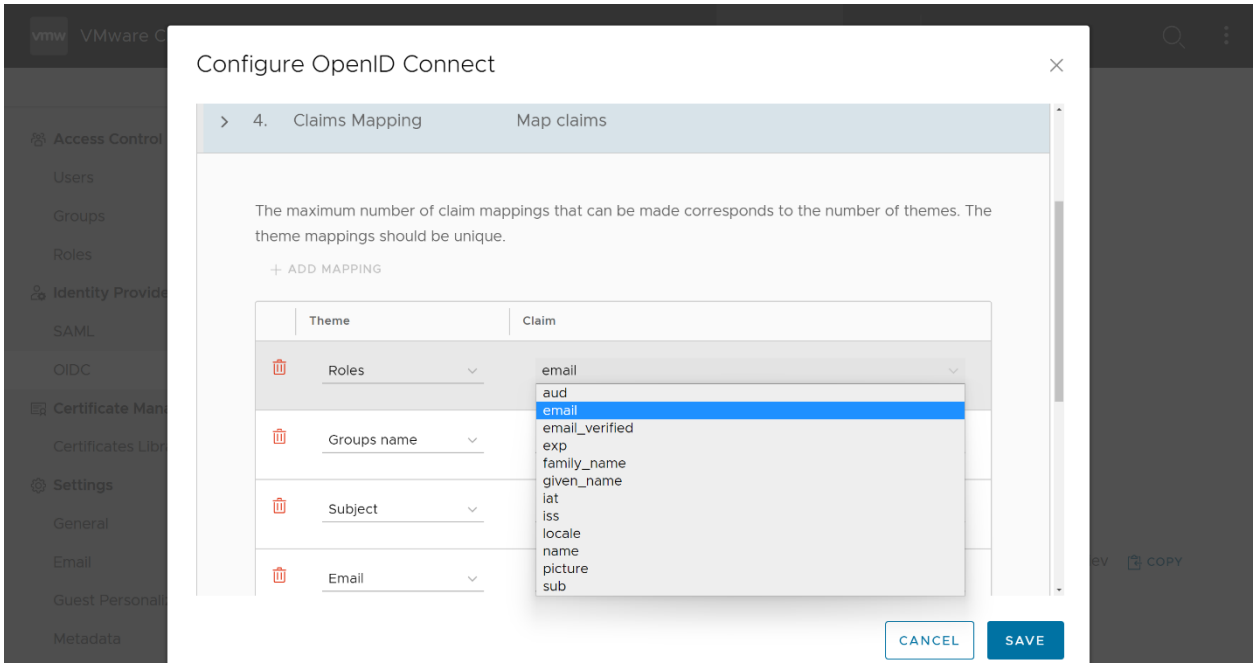
Натисніть екранну кнопку «NEXT».

Змінювати початкові значення параметрів після переходу до третього вікна «Scopes» також не потрібно, натисніть знову екранну кнопку «NEXT».



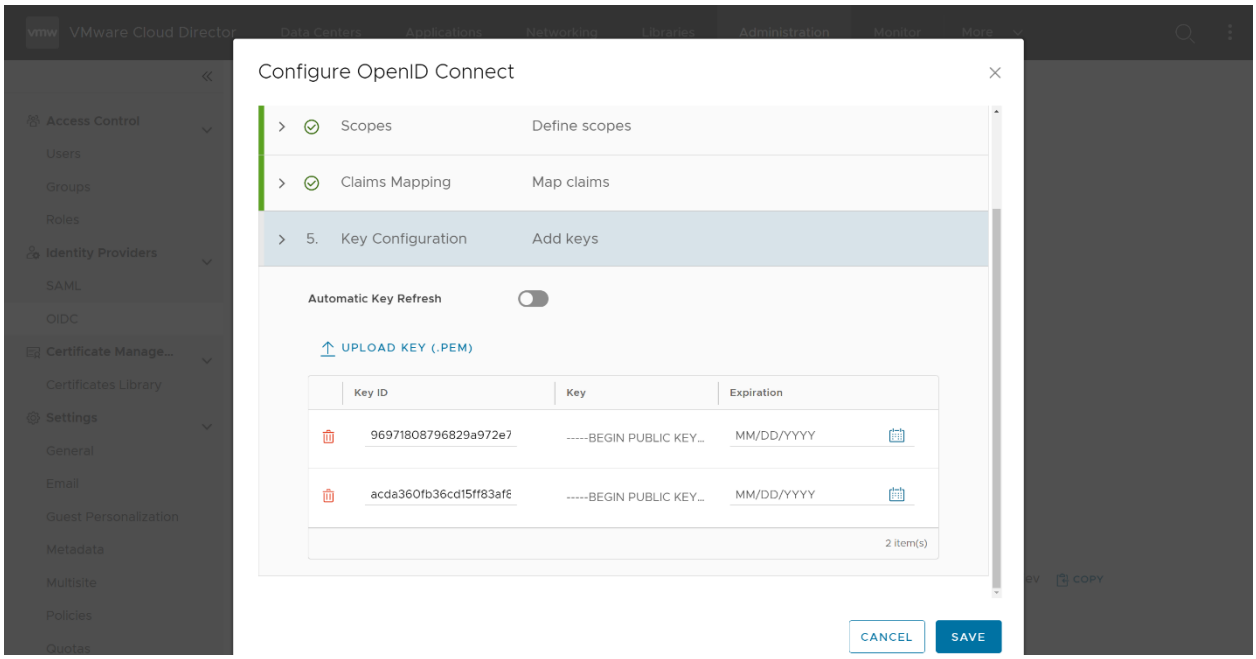
У наступному, четвертому вікні «Claims Mapping» екранної форми «Configure Open ID Connect» натисніть напис «**+ ADD MAPPING**» і додайте два нових рядки до таблиці:

Theme: **Roles** Claim: **email**
Groups name **email**



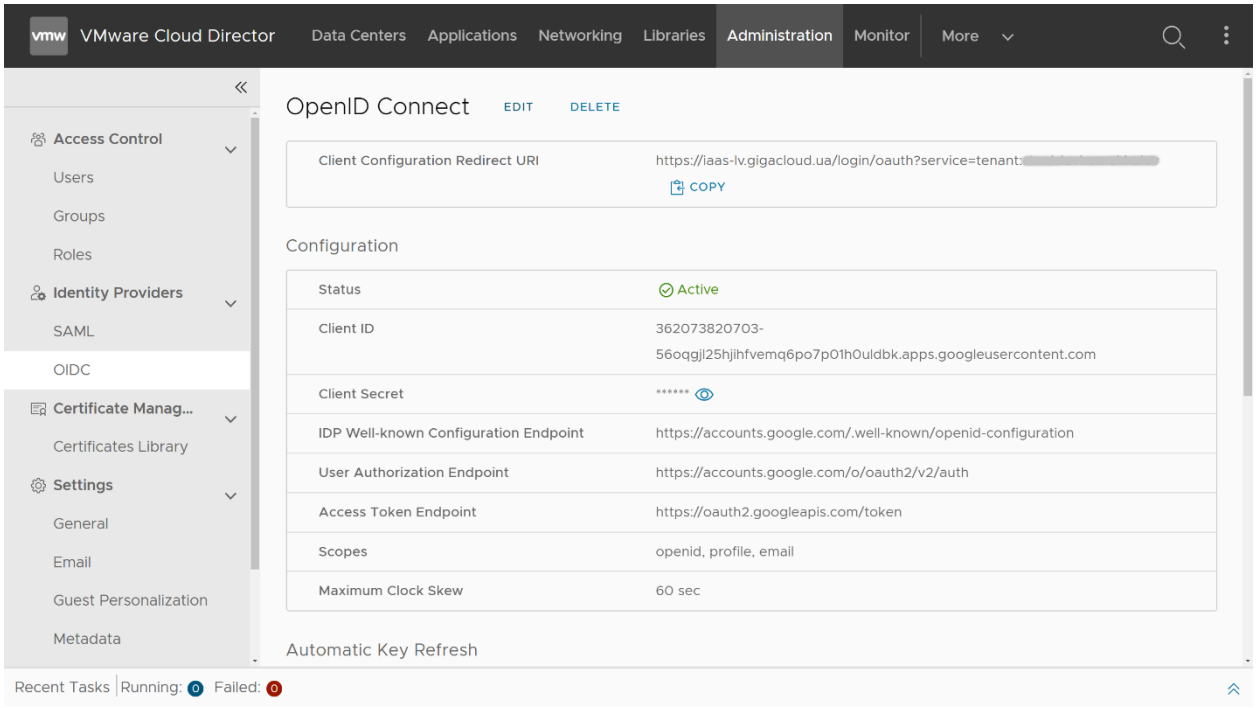
У рядку таблиці з параметром Theme: **Subject** змініть початкове значення Claim: **email** (див. зображення вище). Натисніть екранну кнопку «NEXT».

У наступному, п'ятому вікні «Key Configuration» змінювати початкові значення параметрів не потрібно:

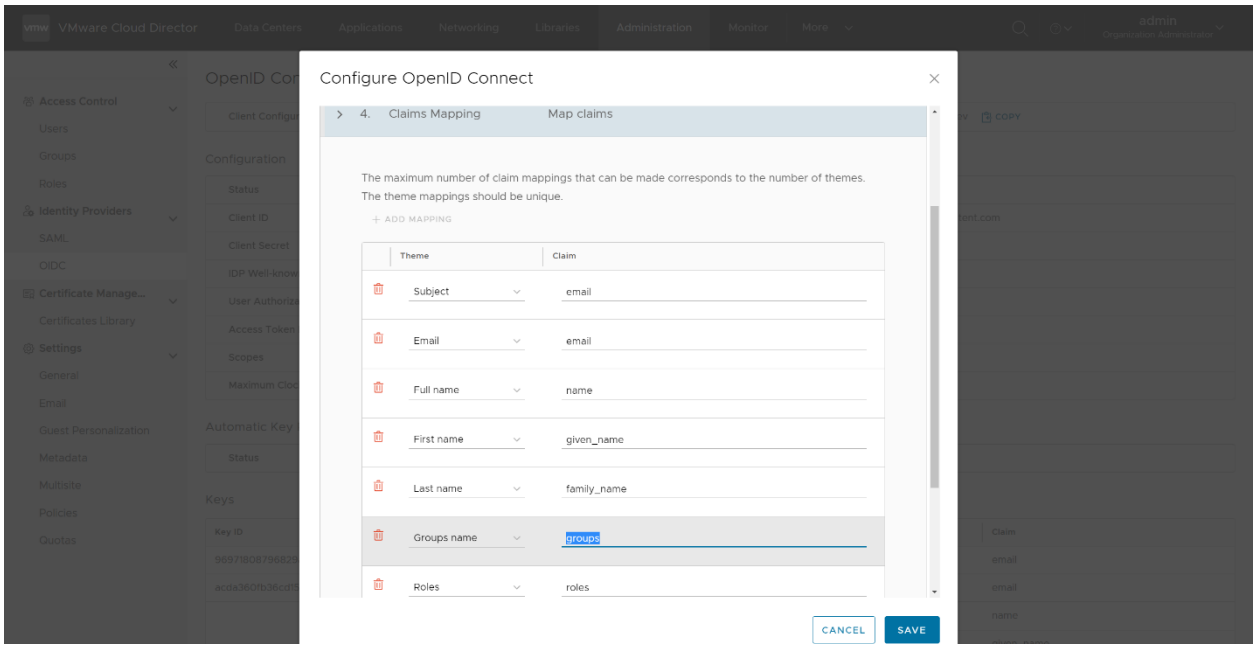


Натисніть екранну кнопку «SAVE».

Пересвідчіться в активному статусі Open ID Connect у вікні конфігурації:



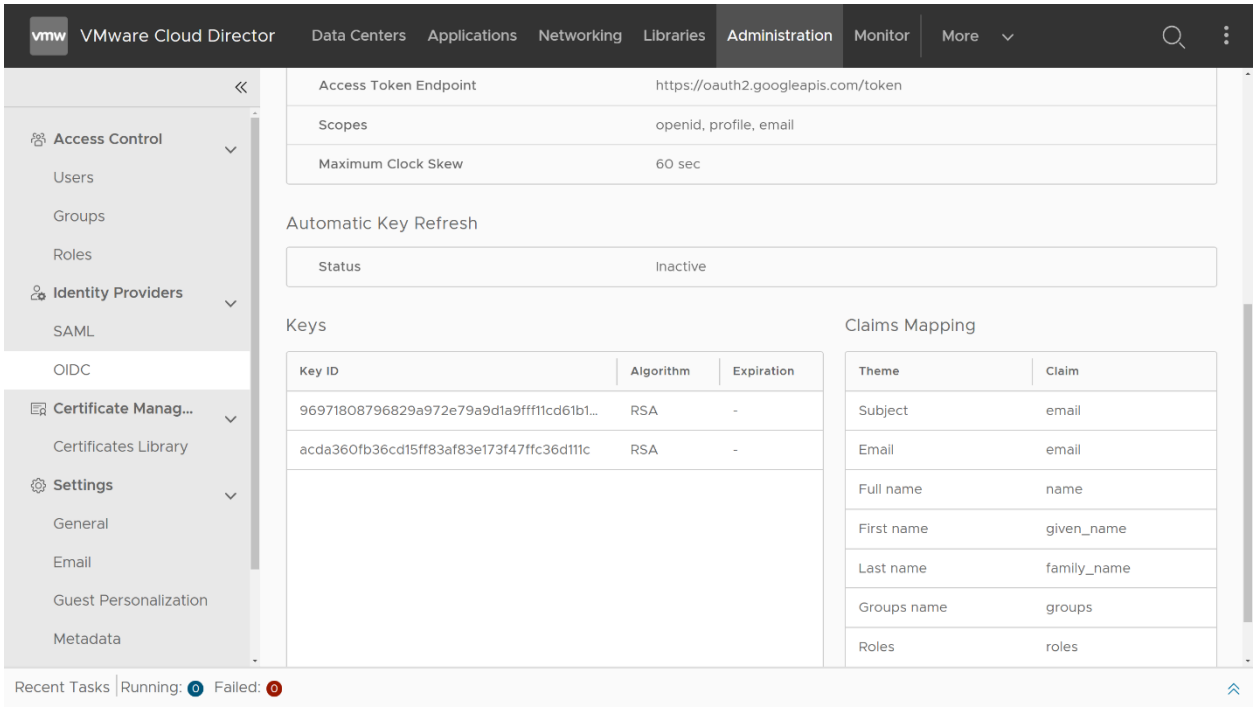
Натисніть екранний напис «EDIT» та зробіть зміни налаштувань параметрів у четвертому вікні «Claims Mapping».



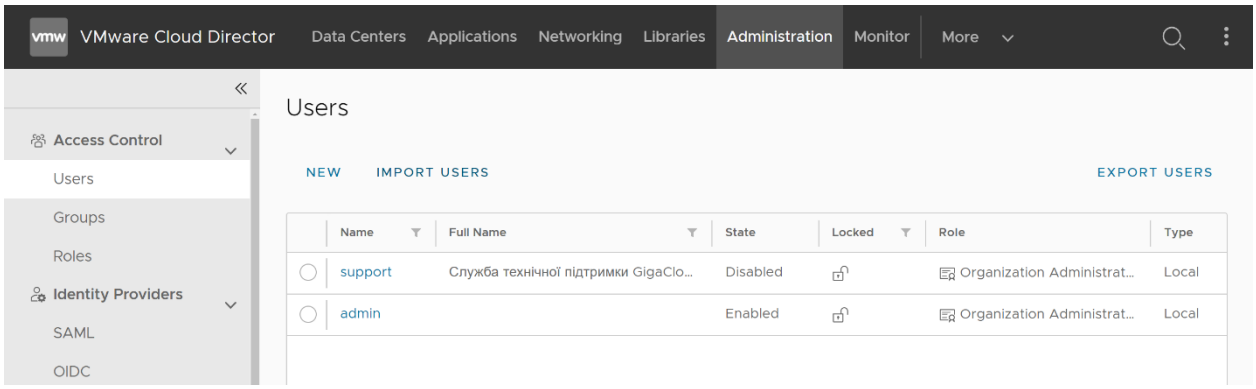
У рядку таблиці з параметром Theme: **Roles** змініть значення Claim: **roles**
У рядку з параметром Theme: **Groups name** змініть значення Claim: **groups**
(див. зображення вище).

Натисніть екранну кнопку «SAVE» для збереження виконаних змін конфігурації Open ID Connect.

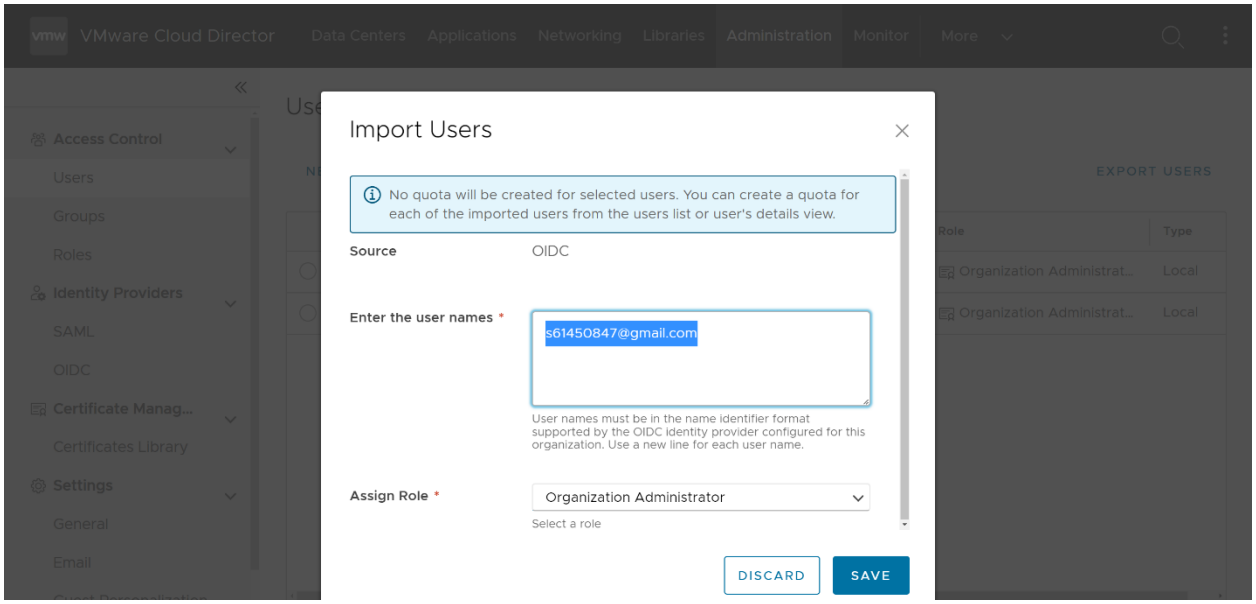
Пересвідчіться, що зміни відображаються в розділі «Claims Mapping» вікна конфігурації.



Перейдіть до вікна інтерфейсу VCD «Administration –> Access Control –> Users»:

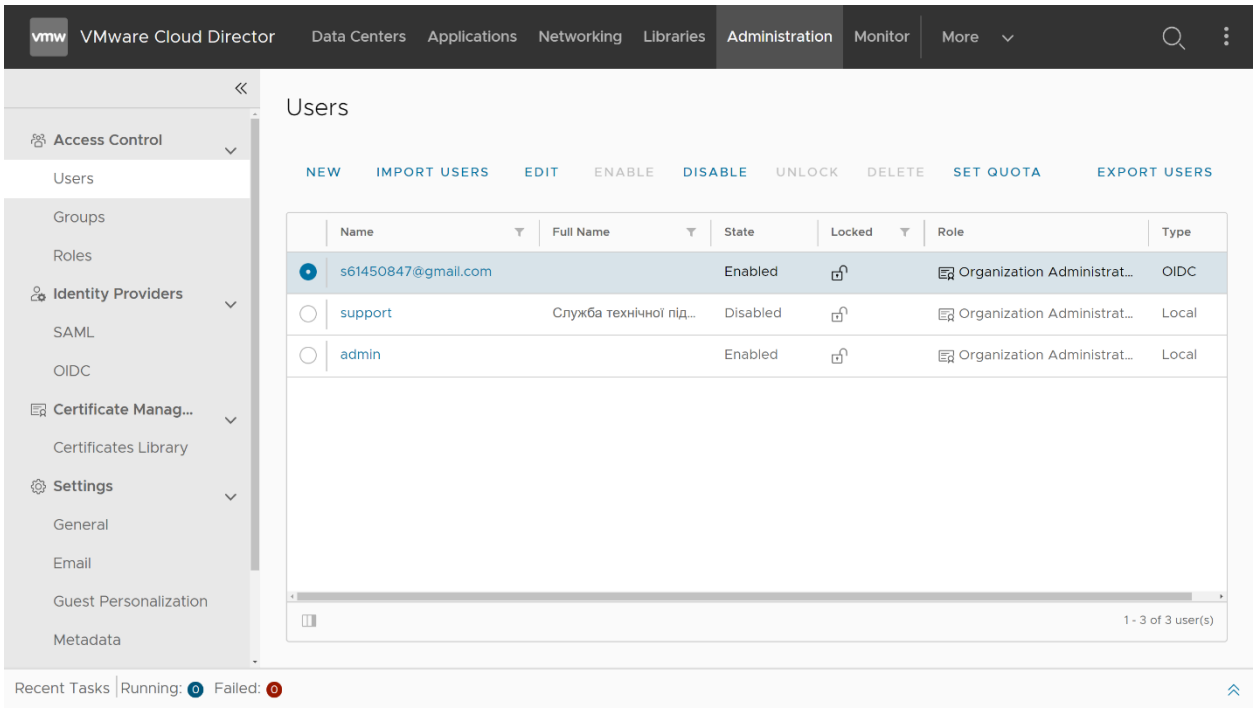


Натисніть екранний напис «IMPORT USERS», додайте e-mail та роль:



Натисніть екранну кнопку «SAVE» для збереження виконаних змін.

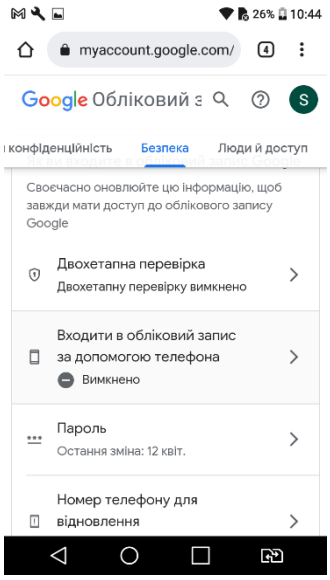
Пересвідчіться, що користувача з роллю «Organization Administrator» успішно додано:

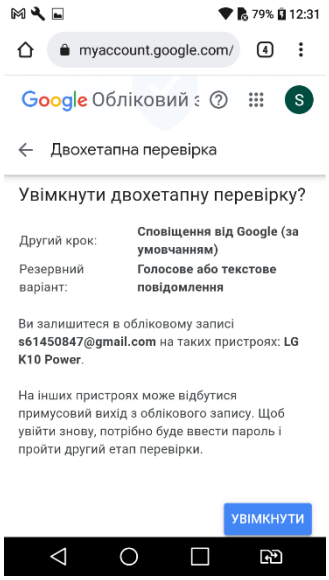


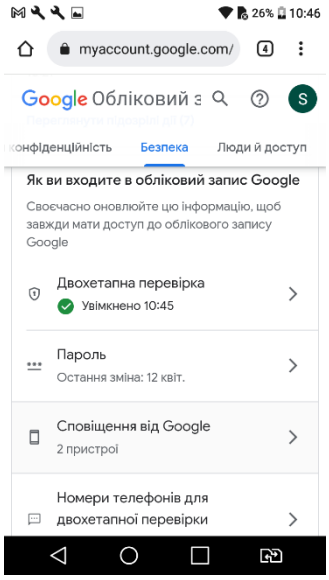
Налаштування смартфону з ОС Android

Перейдіть до вікна налаштувань системи на смартфоні з ОС Android, оберіть розділ меню налаштування «Безпека» вашого акаунту Google.

Увімкніть режим двоетапної перевірки на смартфоні:





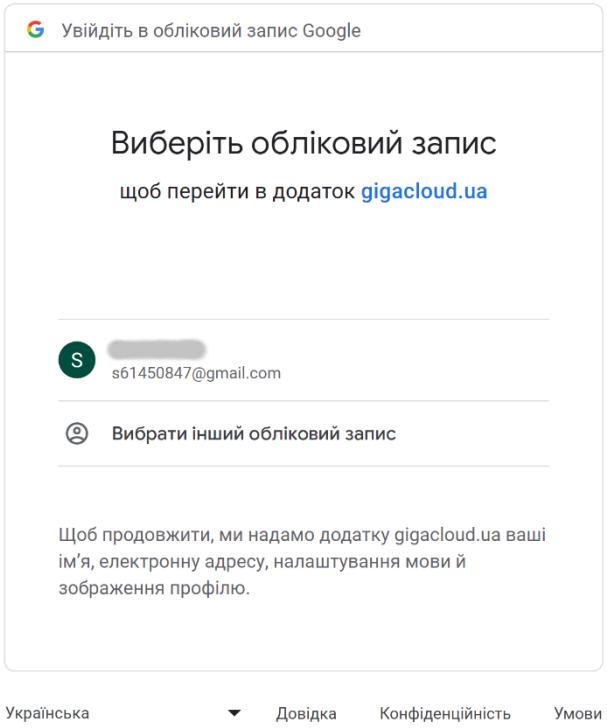


Користуючись браузером, виконайте спробу входу до інтерфейсу VMware Cloud Director: https://iaas-lv.gigacloud.ua/tenant/s**********v у наведеному демонстраційному прикладі для кластеру LV провайдера GigaCloud (ваше значення URL буде іншим).

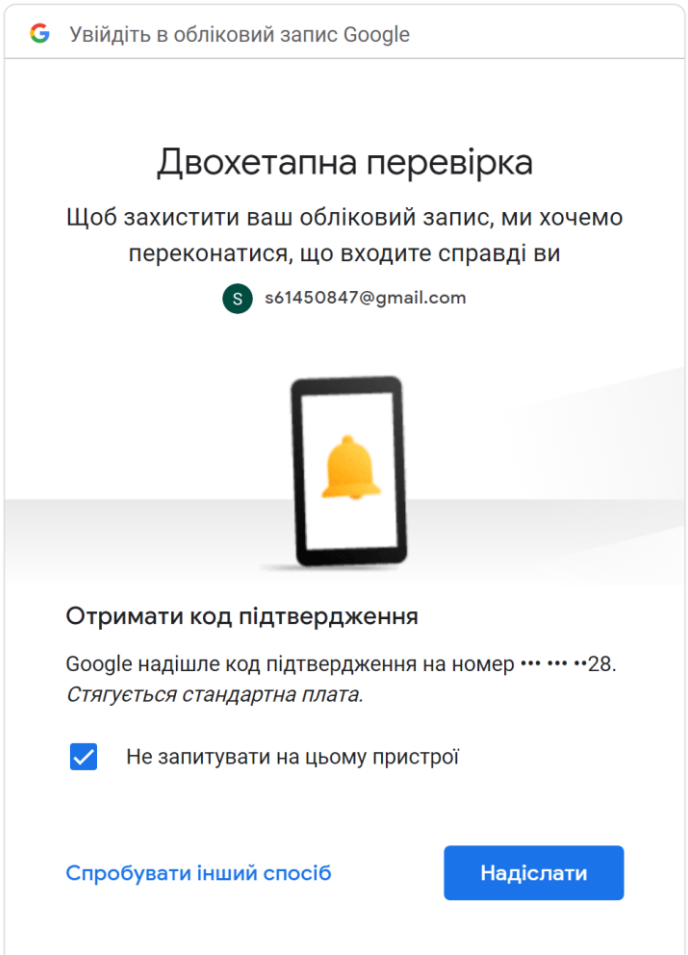
Відповідно виконаним раніше налаштуванням, спочатку відбудеться перенаправлення на сторінку входу до акаунту Google, з метою:

- перевірки та підтвердження вашої особи;
- видачі сервісу **gigacloud.ua** прав на доступ до частини ваших даних (ім'я, e-mail адреса, налаштування мови та ін., згідно виконаних вами раніше налаштувань).

Зображення у браузері вашого ПК буде подібним до наведеного нижче:

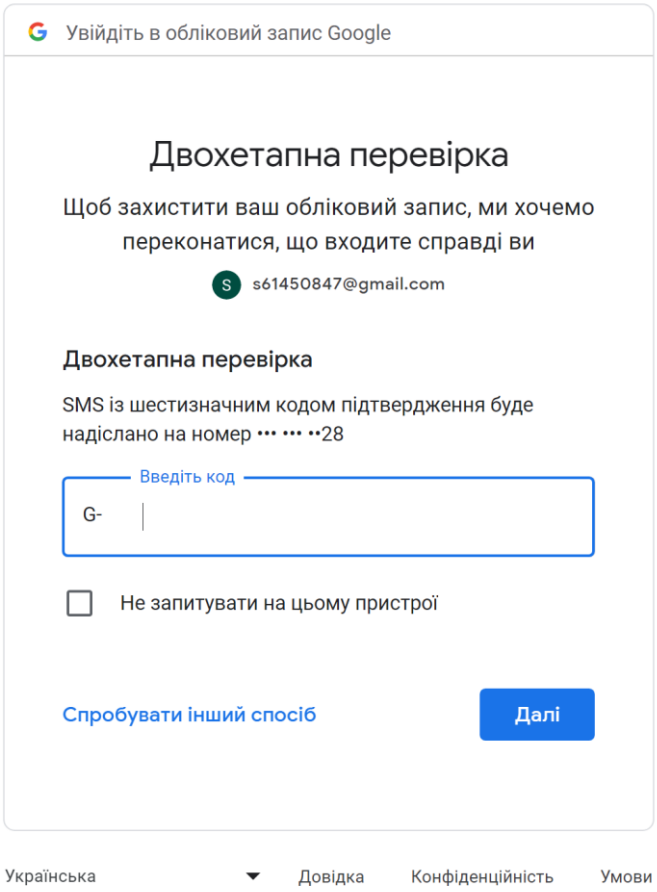


Після входу до облікового запису Google (акаунту, використання якого додано до налаштувань 2FA), ви отримаєте повідомлення на ПК:

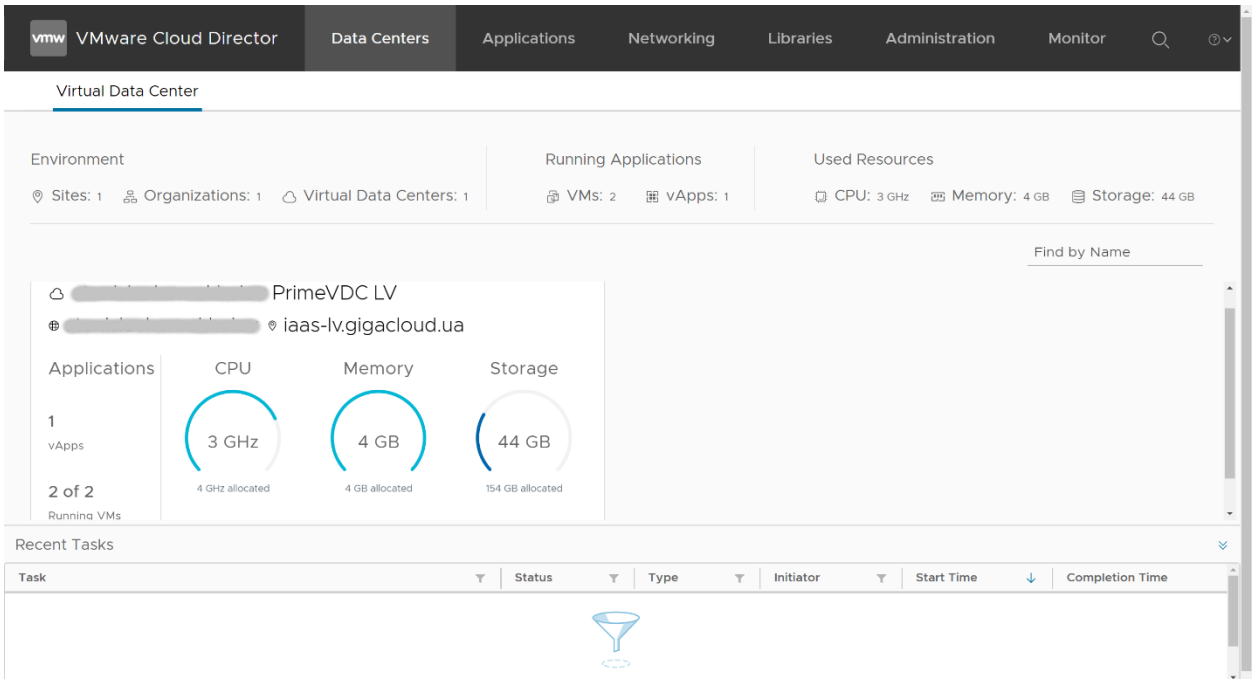


Натисніть екранну кнопку «Надіслати».

На ваш смартфон буде відправлено СМС у форматі: G- 678234 (наприклад), де 6 цифр є кодом підтвердження.



Вкажіть цей код для автентифікації вашої особи на ПК та входу до VCD, натисніть екранну кнопку «Далі». Відповідно виконаним раніше налаштуванням, відбудеться перенаправлення та вхід до VCD, тобто успішне завершення процедури 2FA.



У разі необхідності, звертайтесь до фахівців СТП провайдера за консультацією та користуйтесь послугою Gigacloud Admin.