Hướng dẫn triển khai xác thực với Microsoft Entra ID (OIDC) trên Ubuntu

1. Giới thiệu

Tài liệu này hướng dẫn cách triển khai một ứng dụng web Node.js trên Ubuntu, tích hợp xác thực người dùng với Microsoft Entra ID (Azure AD) sử dụng giao thức OpenID Connect (OIDC).

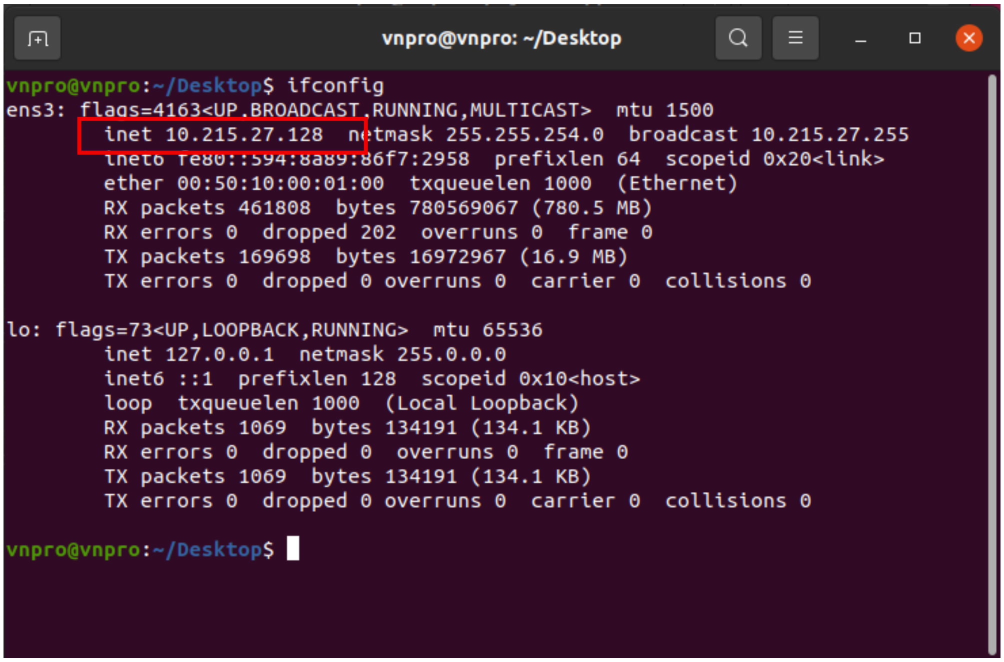
2. Yêu cầu

- Ubuntu Server hoặc Desktop
- Node.js và npm
- Tài khoản Azure (Entra ID)

3. Các bước thực hiện

3.1. Kiểm tra IP public trên

Trên linux kiểm tra ip, đây sẽ là url_ID khai báo để chuyển hướng khi xác thực thành công trên Azure



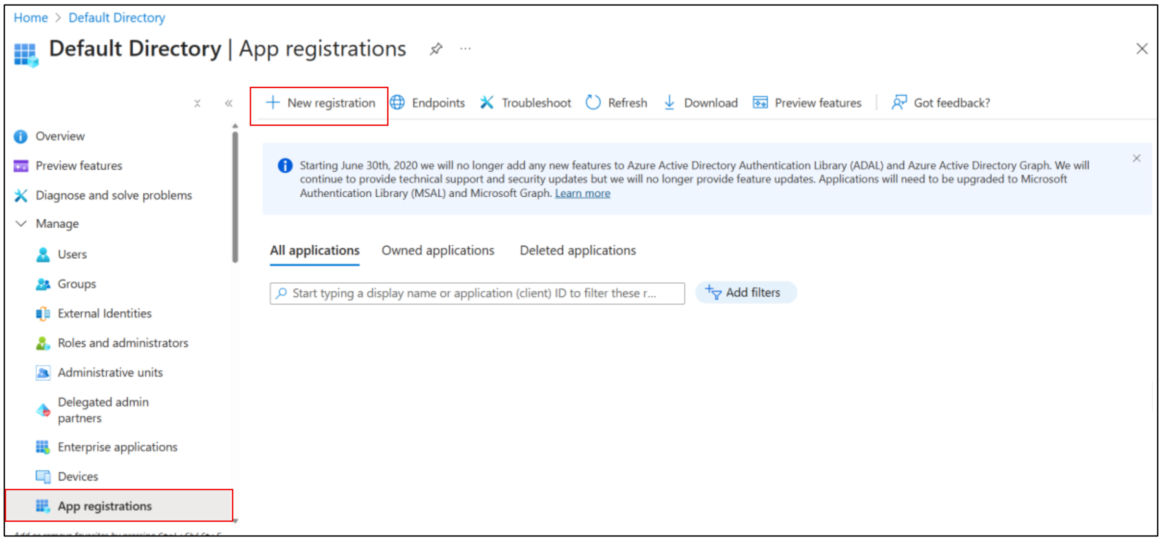
```
vnpro@vnpro:~/Desktop$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.215.27.128  netmask 255.255.254.0  broadcast 10.215.27.255
        inet6 fe80::594:8a89:86f7:2958  prefixlen 64  scopeid 0x20<link>
        ether 00:50:10:00:01:00  txqueuelen 1000  (Ethernet)
        RX packets 461808  bytes 780569067 (780.5 MB)
        RX errors 0  dropped 202  overruns 0  frame 0
        TX packets 169698  bytes 16972967 (16.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1069  bytes 134191 (134.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1069  bytes 134191 (134.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vnpro@vnpro:~/Desktop$ 
```

3.1. Tạo ứng dụng trong Azure (App Registration)

1. Đăng nhập Azure Portal: https://portal.azure.com
2. Vào *Azure Active Directory → App registrations → New registration*

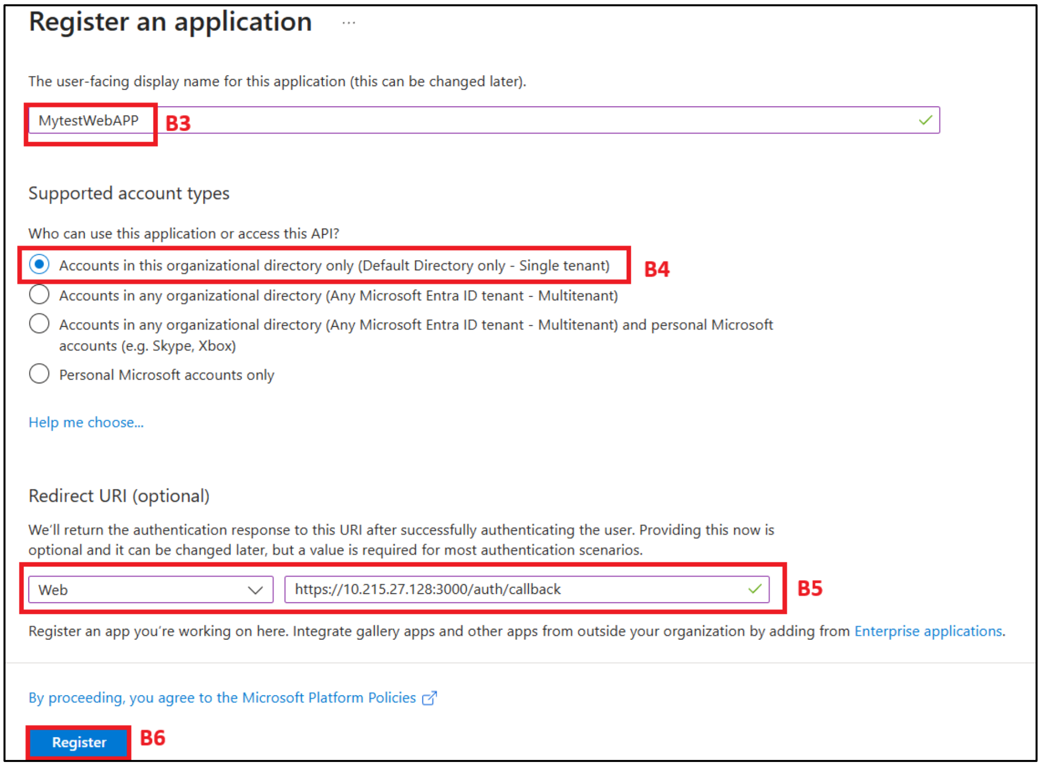


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

3. Nhập tên ứng dụng, ví dụ: MytestWebAPP

4.Support account type chọn: *Accounts in this organizational directory only (Default Directory only - Single tenant)*
5. Ở Redirect URI chọn *Web* và nhập tạm thời:

https://10.215.27.128:3000/auth/callback
6. Nhấn Register.



Register an application ...

The user-facing display name for this application (this can be changed later).

MytestWebAPP ✓ B3

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant) B4
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://10.215.27.128:3000/auth/callback ✓ B5

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

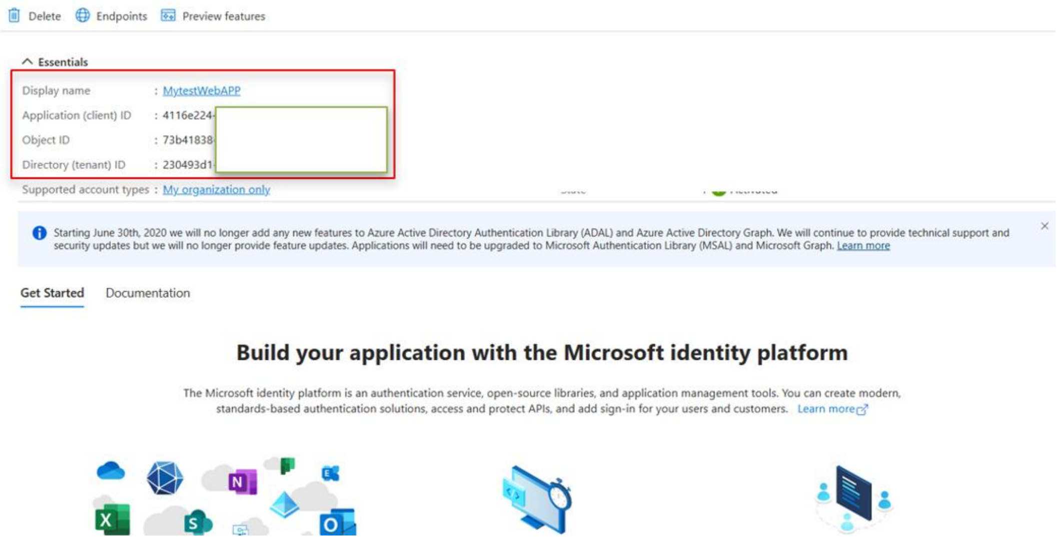
By proceeding, you agree to the Microsoft Platform Policies

B6

3.2. Lấy thông tin cấu hình

- Application (client) ID: trong mục Overview
- Directory (tenant) ID: trong mục Overview
- Tạo Client Secret: Certificates & secrets → New client secret

Lưu giá trị Client Secret ngay sau khi tạo.



Essentials

Display name : MytestWebAPP
Application (client) ID : 4116e224-[redacted]
Object ID : 73b41838
Directory (tenant) ID : 230493d1
Supported account types : My organization only

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

3.3. Tạo ứng dụng Node.js

Chạy các lệnh sau:

```
mkdir myentraapp && cd myentraapp
npm init -y
npm install express express-session passport passport-azure-ad
```

3.4. Tạo file app.js

Tạo file app.js với nội dung sau (đổi các giá trị <client-id>, <tenant-id>, <client-secret>):

```
const express = require('express');
const session = require('express-session');
const passport = require('passport');
const OIDCStrategy = require('passport-azure-ad').OIDCStrategy;
const https = require('https');
const fs = require('fs');
const app = express();
const config = {
  identityMetadata: https://login.microsoftonline.com/<tenant-id>/v2.0/.well-known/openid-configuration,
  clientID: '<client-id>',
  clientSecret: '<client-secret>',
  redirectUrl: ' https://10.215.27.128:3000/auth/callback’,
  responseType: 'code',
  responseMode: 'query',
  scope: ['openid', 'profile', 'email']
};
```

```
passport.use(new OIDCStrategy(config, (iss, sub, profile, accessToken, refreshToken, done) => {
  return done(null, profile);
}));
app.use(session({ secret: 'secret', resave: false, saveUninitialized: true }));
app.use(passport.initialize());
app.use(passport.session());
passport.serializeUser((user, done) => done(null, user));
passport.deserializeUser((obj, done) => done(null, obj));
app.get('/login', passport.authenticate('azuread-openidconnect', { failureRedirect: '/' }));
app.get('/auth/callback', passport.authenticate('azuread-openidconnect', { failureRedirect: '/' }),
  (req, res) => res.send(Hello ${req.user.displayName})
);
app.get('/', (req, res) => res.send('<a href="/login">Login with Entra ID</a>'));
// Tạo HTTPS server
const httpsOptions = {
  key: fs.readFileSync('./certs/server.key'),
  cert: fs.readFileSync('./certs/server.cert')
};
https.createServer(httpsOptions, app).listen(3000, () => {
  console.log('App running on https://10.215.27.128:3000 ');
});
```

3.5. Tạo chứng chỉ tự ký

Trên ubuntu:

```
mkdir certs
cd certs
```

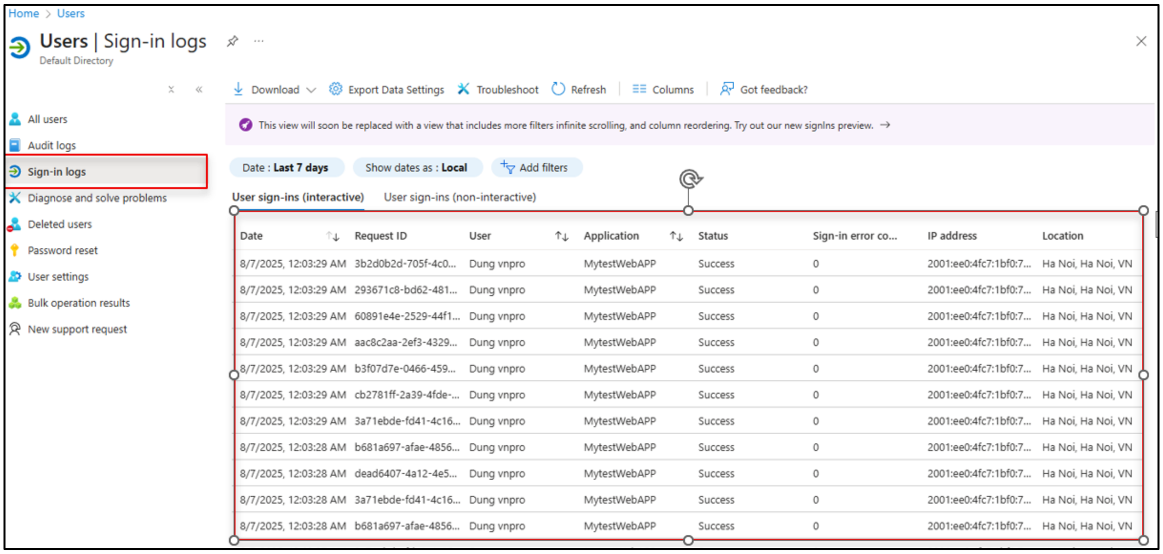
openssl req -nodes -new -x509 -keyout server.key -out server.cert -days 365

Common Name (CN) nhập: localhost

4. Kiểm tra kết quả

Trường hợp cho phép đăng nhập

➔ Mở URL trong trình duyệt → Nhấn Login with Entra ID → Đăng nhập bằng tài khoản Microsoft. Trên Azure vào user➔Sign-in logs

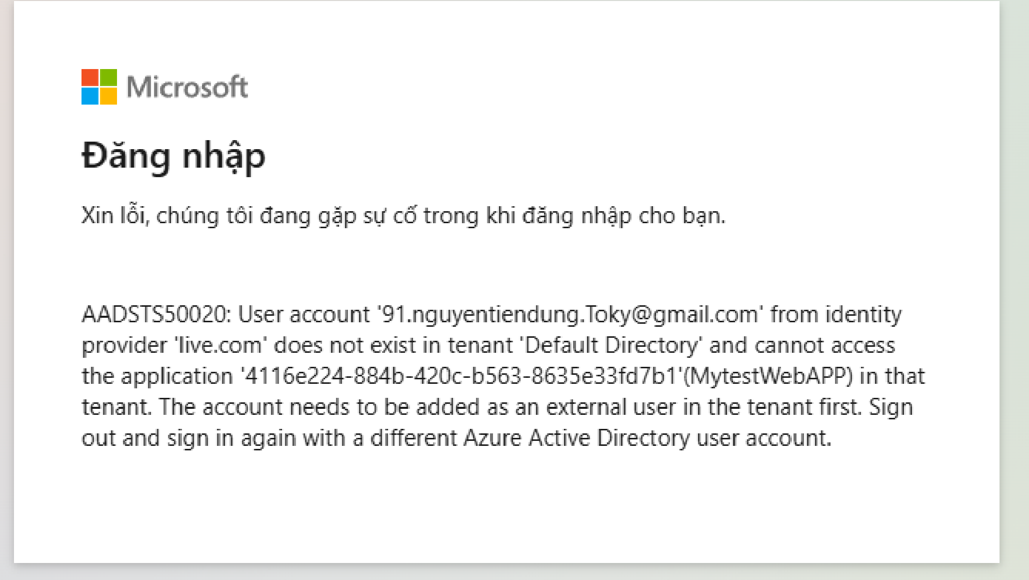


This view will soon be replaced with a view that includes more filters infinite scrolling, and column reordering. Try out our new signIns preview. →

Date	Request ID	User	Application	Status	Sign-in error co...	IP address	Location
8/7/2025, 12:03:29 AM	3b2d0b2d-705f-4c0...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	293671c8-bd62-481...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	60891e4e-2529-44f1...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	aac8c2aa-2ef3-4329...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	b3f07d7e-0466-459...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	cb2781ff-2a39-4fde-...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:29 AM	3a71ebde-fd41-4c16...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:28 AM	b681a697-afae-4856...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:28 AM	dead6407-4a12-4e5...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:28 AM	3a71ebde-fd41-4c16...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN
8/7/2025, 12:03:28 AM	b681a697-afae-4856...	Dung vnpro	MytestWebAPP	Success	0	2001:ee0:4fc7:1bf0:7...	Ha Noi, Ha Noi, VN

Trường hợp không cho phép đăng nhập:

➔Mở URL trong trình duyệt → Nhấn Login with Entra ID → Đăng nhập bằng tài khoản Microsoft không nằm trong tổ chức→ Kiểm tra báo lỗi khi đăng nhập.



Đăng nhập

Xin lỗi, chúng tôi đang gặp sự cố trong khi đăng nhập cho bạn.

AADSTS50020: User account '91.nguyentiendung.Toky@gmail.com' from identity provider 'live.com' does not exist in tenant 'Default Directory' and cannot access the application '4116e224-884b-420c-b563-8635e33fd7b1'(MytestWebAPP) in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account.