

Lock It Down:

Using Azure Entra for .NET APIs and SPAs

By Shawn Wildermuth



@shawnwildermuth



Who Am I?



- **Microsoft MVP**
- **Docker Captain**
- **Instructor**
- **Consultant**

<https://wildermuth.com>
<https://twainfilms.com>
<https://shawnl.ink/yt>



@shawnwildermuth

In This Talk



- Azure AD – Now Azure Entra
- Enabling OpenID in ASP.NET Core
- Enabling OpenID in JavaScript



@shawnwildermuth



What is Azure Entra ID?

- Identity Management
 - (Was Azure AD)
 - Can manage APIs and Apps too
 - Single-sign on
 - Typically B2B or OnPrem
 - Integration across ecosystems
 - .NET
 - JavaScript/TypeScript
 - Etc.



@shawnwildermuth



Microsoft Entra product family

Establish Zero Trust access controls



Microsoft Entra ID
P1

Secure access for your employees



Microsoft Entra
Private Access



Microsoft Entra
Internet Access



Microsoft Entra ID
Governance



Microsoft Entra ID
ID Protection



Microsoft Entra Verified ID
Premium

Secure access for customers/partners



Microsoft Entra
External ID

Secure access in any cloud



Microsoft Entra
Permissions Management



Microsoft Entra
Workload ID



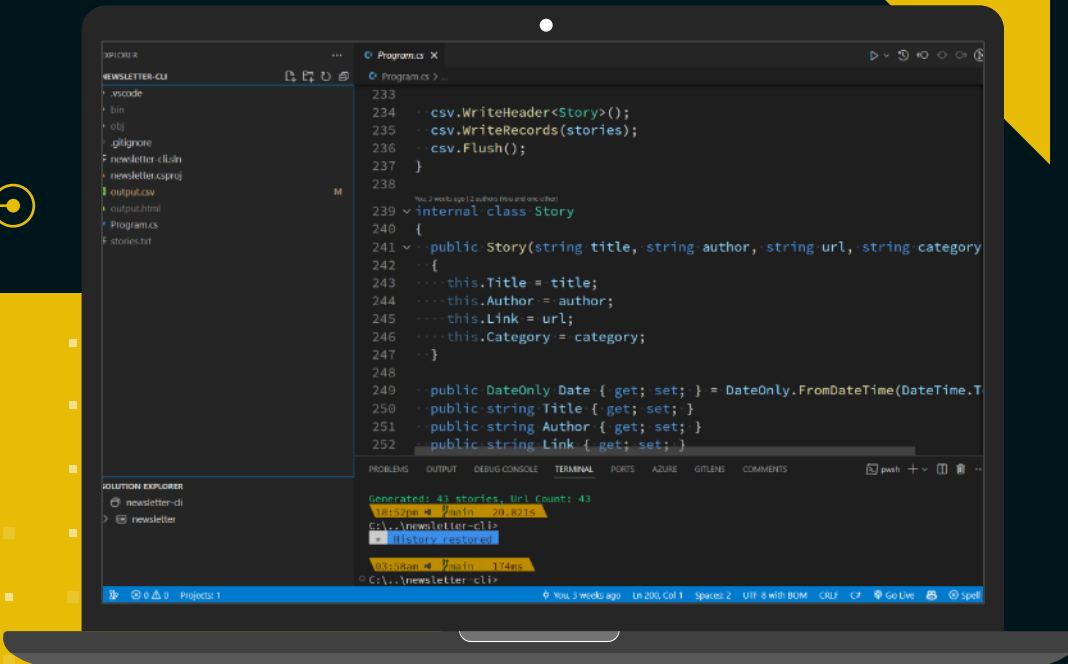
Microsoft Copilot for Security



Azure and Entra

- Azure Hosting?
 - Not required
 - Similar to Auth0/Okta
 - Solutions for enterprise and B2C





> Demo

Registering in Azure



@shawnwildermuth

[Home](#) >

Default Directory | Overview ...



Add ▾



Manage tenants



What's new



Preview features



Got feedback? ▾



Overview



Preview features



Diagnose and solve problems



Manage



Users



Groups



External Identities



Roles and administrators



Administrative units

Delegated admin
partners

Enterprise applications



Devices



App registrations



Identity Governance

Overview

Monitoring

Properties

Recommendations

Setup guides



Basic information

Name	Default Directory	Users	3
Tenant ID	<div></div>	Groups	1
Primary domain	shawnwildermuth.onmicrosoft.com	Applications	6
License	Microsoft Entra ID Free	Devices	1

Alerts



Service Change to Microsoft Entra Connect

We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.



Upcoming MFA Server deprecation

Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.



[Home](#) > [Default Directory](#)

Default Directory | App registrations

[New registration](#)[Endpoints](#)[Troubleshoot](#)[Refresh](#)[Download](#)[Preview features](#)[Got feedback?](#)[Overview](#)[Preview features](#)[Diagnose and solve problems](#)[Manage](#)[Users](#)[Groups](#)[External Identities](#)[Roles and administrators](#)[Administrative units](#)[Delegated admin partners](#)[Enterprise applications](#)[Devices](#)[App registrations](#)[Health](#)

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

[All applications](#)[Owned applications](#)[Deleted applications](#)[Applications from personal account](#)

x

[Add filters](#)

We didn't find your item. Try searching in All Applications.

[View all applications in the directory](#)



Register an application



* Name

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

ShoeMoney ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ 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.

Single-page application (SPA) ▾

http://localhost:5173 ✓

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](#)

Register



Shoe Money Tonight



Search



Delete



Endpoints



Preview features



Overview



Quickstart



Integration assistant



Diagnose and solve problems



Manage



Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles



Owners



Roles and administrators



Manifest



Support + Troubleshooting



New support request

Essentials

Display name : [Shoe Money Tonight](#)

Application (client) ID : ef17c6c1-3671-4e0c-ad45-da026b924e77

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [0 web, 1 spa, 0 public client](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in I... : [ShoeMoney](#)



Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)



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](#)



Get Started

Documentation

[Microsoft identity platform](#)

[Code samples](#)

[Help and Support](#)

[Authentication scenarios](#)

[Microsoft Graph](#)

[Glossary](#)

[Authentication libraries](#)





ShoeMoney | Branding & properties



Search

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties**
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting
 - New support request

Name *	Shoe Money Tonight
Logo	
Upload new logo	<input type="text" value="shoe-money-logo.png"/>
Home page URL	<input type="text" value="e.g. https://example.com"/>
Terms of service URL	<input type="text" value="e.g. https://example.com/termsofservice"/>
Privacy statement URL	<input type="text" value="e.g. https://example.com/privacystatement"/>
Service management reference	<input type="text"/>
Internal notes	<div>Add information relevant to the management of this application.</div>
Publisher domain	<div><div></div><div><input type="text"/></div><div>Update domain</div></div> <div>The application's consent screen will show 'Unverified'. Learn more about publisher domain</div>

Publisher verification

Save Discard

Shoe Money Tonight | Expose an API

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- ▼ Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest
- ▼ Support + Troubleshooting

New support request

Got feedback?

Application ID URI [Add](#)

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires a API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'Ap type. [Go to App roles](#).

Add a scope

Scopes	Who can consent	Admin consent display ...
No scopes have been defined		

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consen this API.

Add a client application

Client Id	Scopes
No client applications have been authorized	

Add a scope

You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI *

api://ef17c6c1-3671-4e0c-ad45-da026b924e77

Shoe Money Tonight | Expose an API

Search

- Got feedback?
- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest
- Support + Troubleshooting
- New support request

Application ID URI :

api://shoemoneyapi

Edit

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires a API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'A type. [Go to App roles](#).

+ Add a scope

Scopes	Who can consent	Admin consent display ...
No scopes have been defined		

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consen this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Add a scope

Scope name * ⓘ

theapi

api://shoemoneyapi/theapi

Who can consent? ⓘ

Admins and users

Admins only

Admin consent display name * ⓘ

e.g. Read user files

Admin consent description * ⓘ

e.g. Allows the app to read the signed-in user's files.

User consent display name ⓘ

e.g. Read your files

User consent description ⓘ

e.g. Allows the app to read your files.

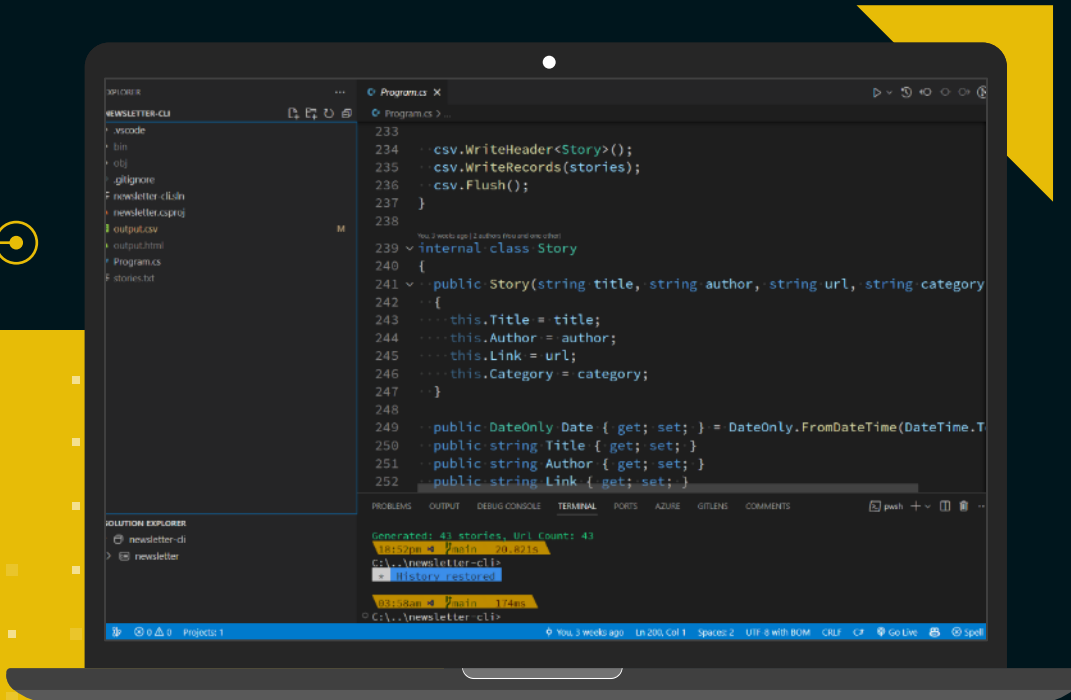
State ⓘ

Enabled

Disabled

Add scope

Cancel



> Demo

Adding Identity



@shawnwildermuth

> 15

> Questions?



@shawnwildermuth

Links



- **Azure Entra:** <https://shawnl.ink/entra>
- **More About Me:** <https://wildermuth.com>
- **My Films:** <https://twainfilms.com>
- **Follow me:** @shawnwildermuth



@shawnwildermuth



THANK YOU

Shawn Wildermuth