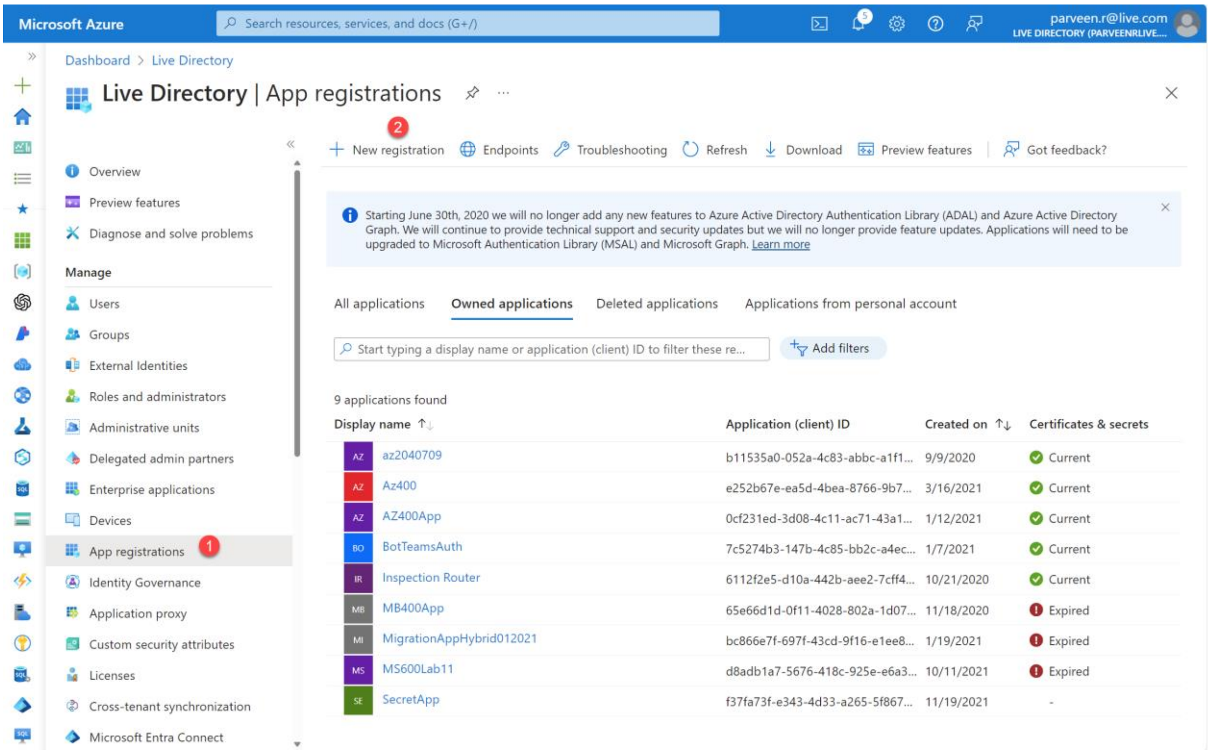
Open App Registration in Entra ID:

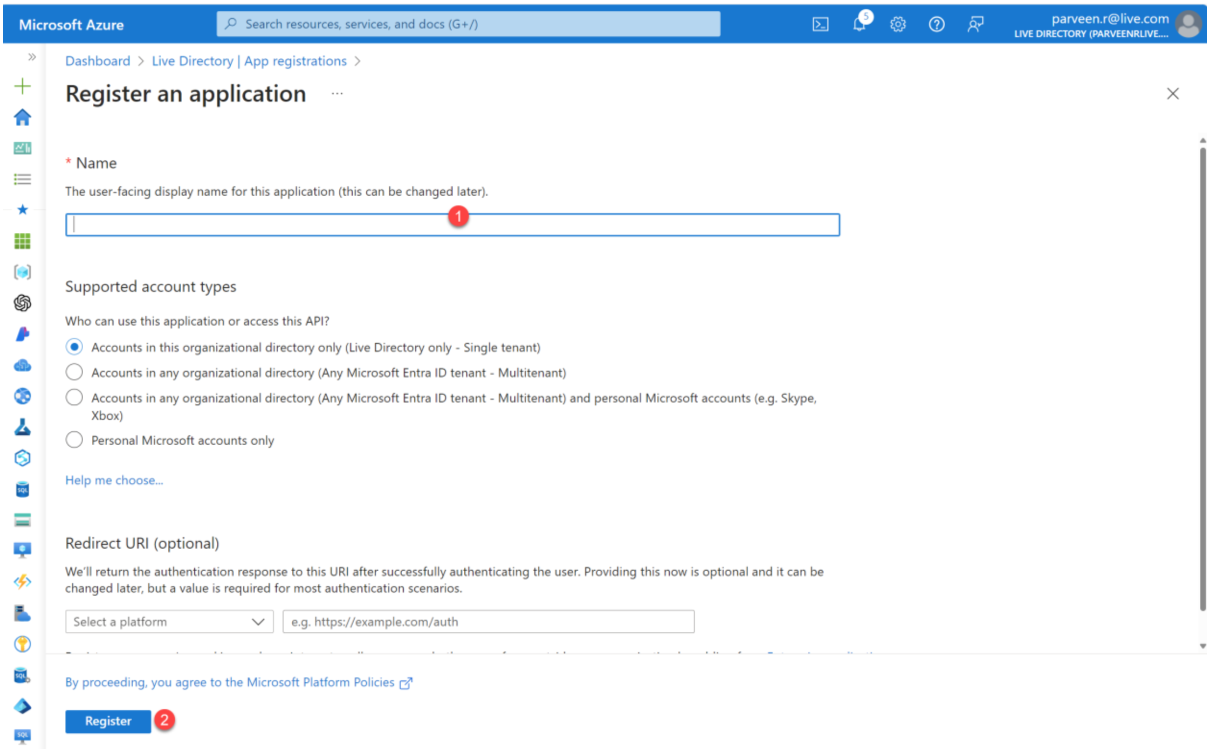


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded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

9 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
AZ az2040709	b11535a0-052a-4c83-abbc-a1f1...	9/9/2020	✓ Current
AZ Az400	e252b67e-ea5d-4bea-8766-9b7...	3/16/2021	✓ Current
AZ AZ400App	0cf231ed-3d08-4c11-ac71-43a1...	1/12/2021	✓ Current
BO BotTeamsAuth	7c5274b3-147b-4c85-bb2c-a4ec...	1/7/2021	✓ Current
IR Inspection Router	6112f2e5-d10a-442b-aee2-7cff4...	10/21/2020	✓ Current
MB MB400App	65e66d1d-0f11-4028-802a-1d07...	11/18/2020	! Expired
MI MigrationAppHybrid012021	bc866e7f-697f-43cd-9f16-e1ee8...	1/19/2021	! Expired
MS MS600Lab11	d8adb1a7-5676-418c-925e-e6a3...	10/11/2021	! Expired
SE SecretApp	f37fa73f-e343-4d33-a265-5f867...	11/19/2021	-

Put the name of the App:


Microsoft Azure
Search resources, services, and docs (G+/)
parveen.r@live.com
LIVE DIRECTORY (PARVEENRLIVE....
Dashboard > Live Directory | App registrations >
1
Select a platform
e.g. https://example.com/auth
Register
2

Register an application

* Name

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

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Live 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

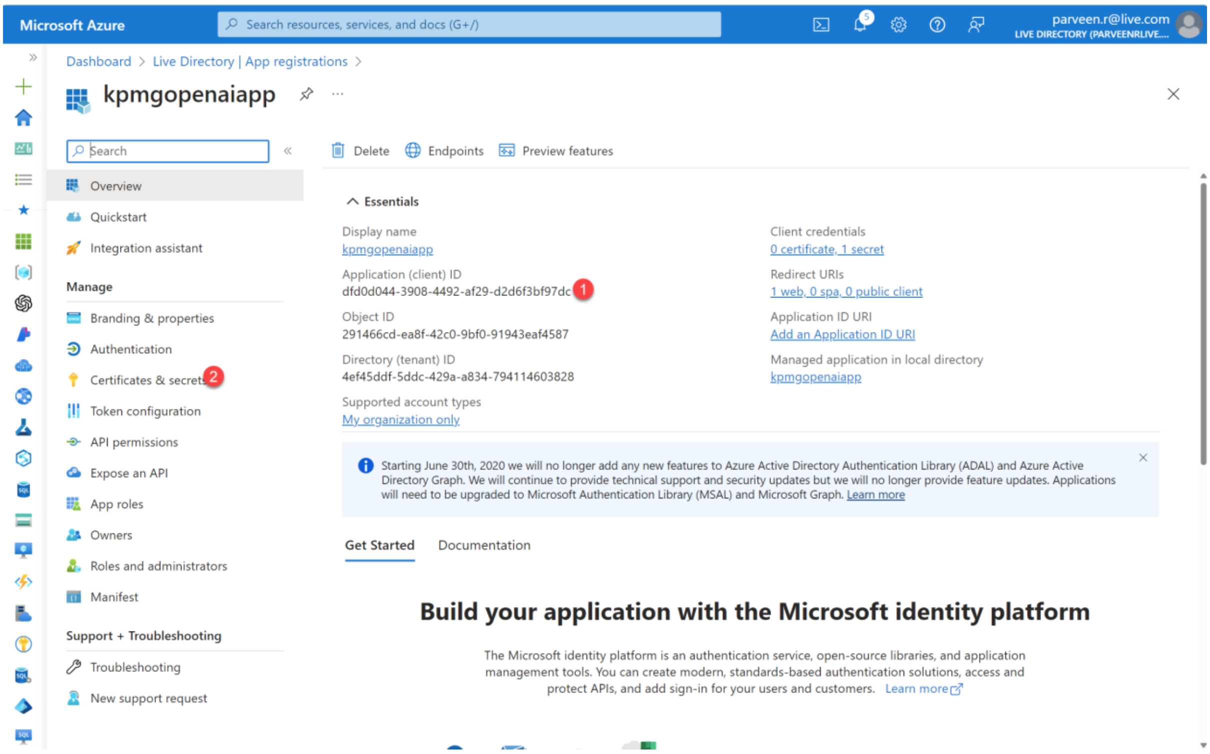
Help me choose...

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.

By proceeding, you agree to the Microsoft Platform Policies

Open the newly Registered App:



Display name
kpmgopenaiapp

Application (client) ID
dfd0d044-3908-4492-af29-d2d6f3bf97dc

Object ID
291466cd-ea8f-42c0-9bf0-91943eaf4587

Directory (tenant) ID
4ef45ddf-5ddc-429a-a834-794114603828

Supported account types
My organization only

Client credentials
0 certificate, 1 secret

Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
kpmgopenaiapp

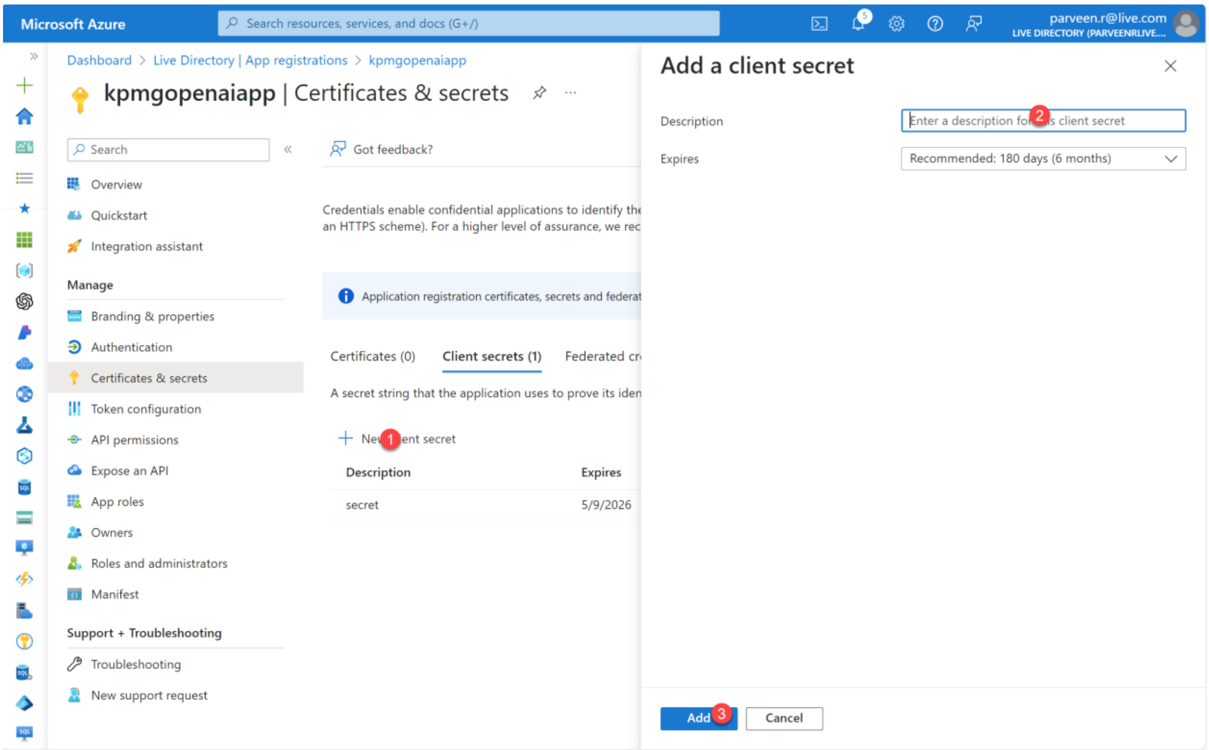
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded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

Copy Client ID

Create Secret



Credentials enable confidential applications to identify the
an HTTPS scheme). For a higher level of assurance, we rec

Application registration certificates, secrets and federat

A secret string that the application uses to prove its iden

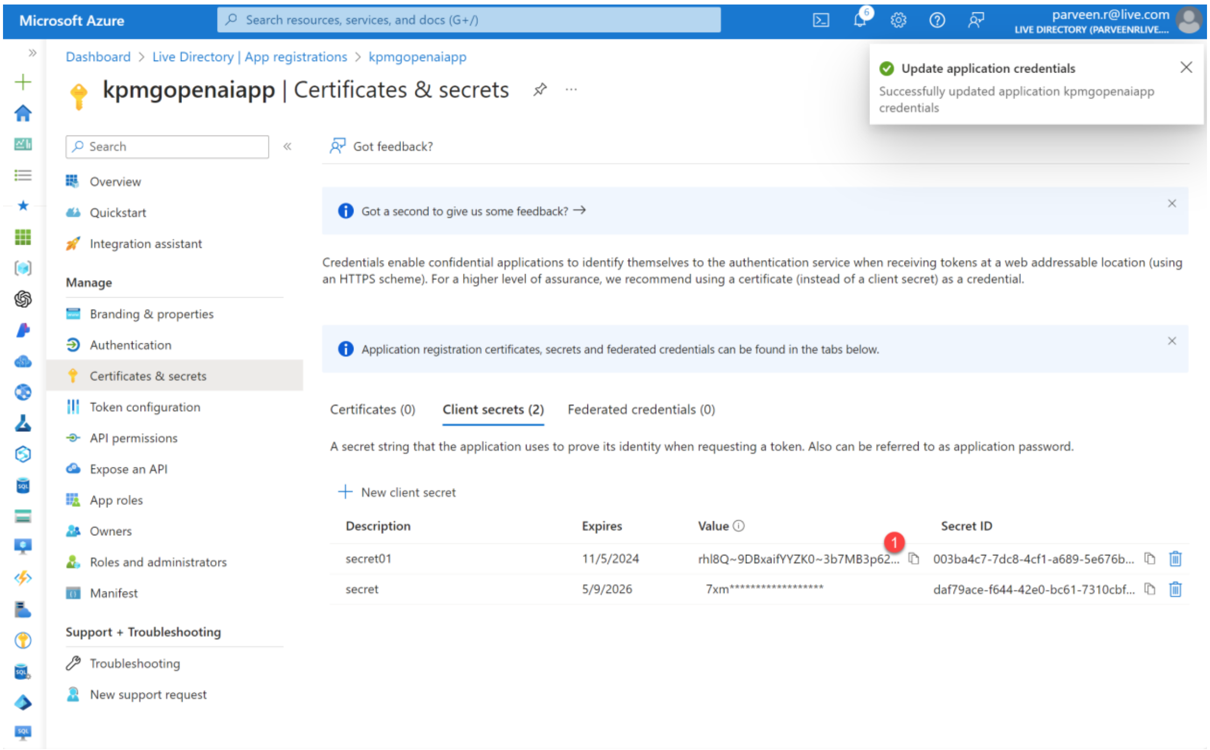
Description	Expires
secret	5/9/2026

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 180 days (6 months)

Copy the secret Value:



kpmgopenaiapp | Certificates & secrets

Update application credentials

Successfully updated application kpmgopenaiapp credentials

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

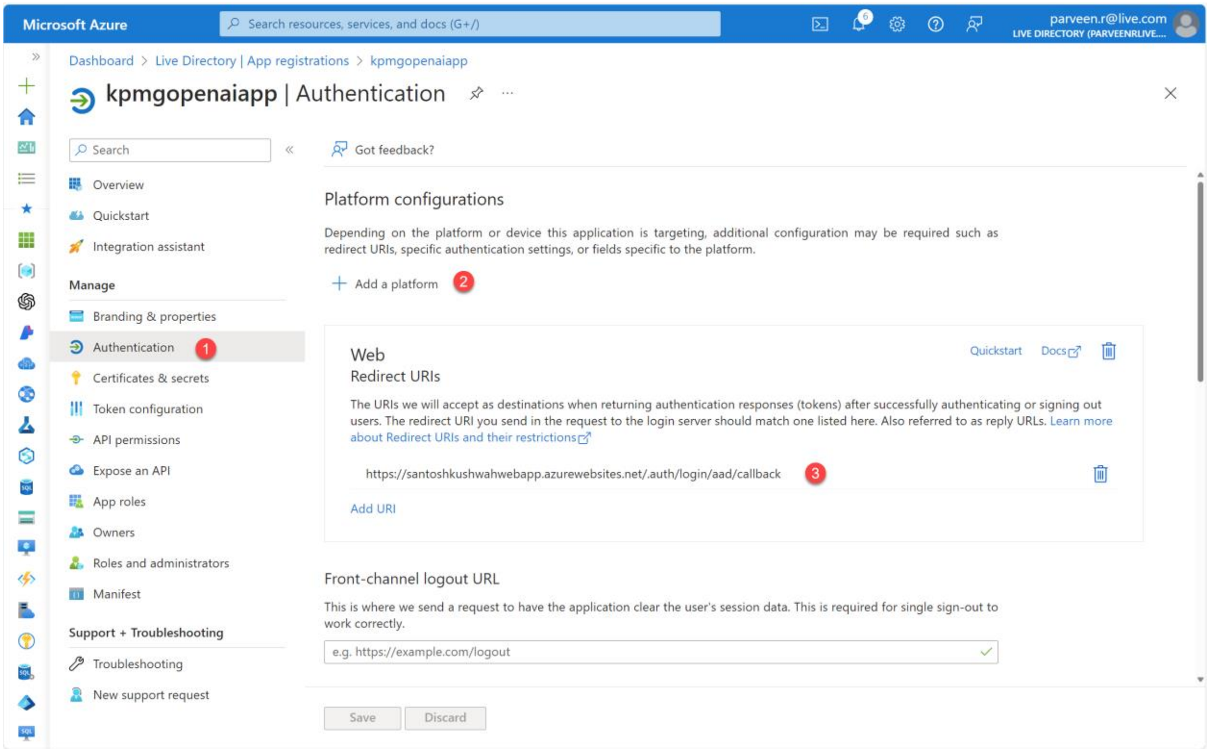
Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | **Client secrets (2)** | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
secret01	11/5/2024	rhl8Q~9DBxaifYYZK0~3b7MB3p62...	003ba4c7-7dc8-4cf1-a689-5e676b...
secret	5/9/2026	7xm*****************	daf79ace-f644-42e0-bc61-7310cbf...



kpmgopenaiapp | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://santoshkushwahwebapp.azurewebsites.net/.auth/login/aad/callback

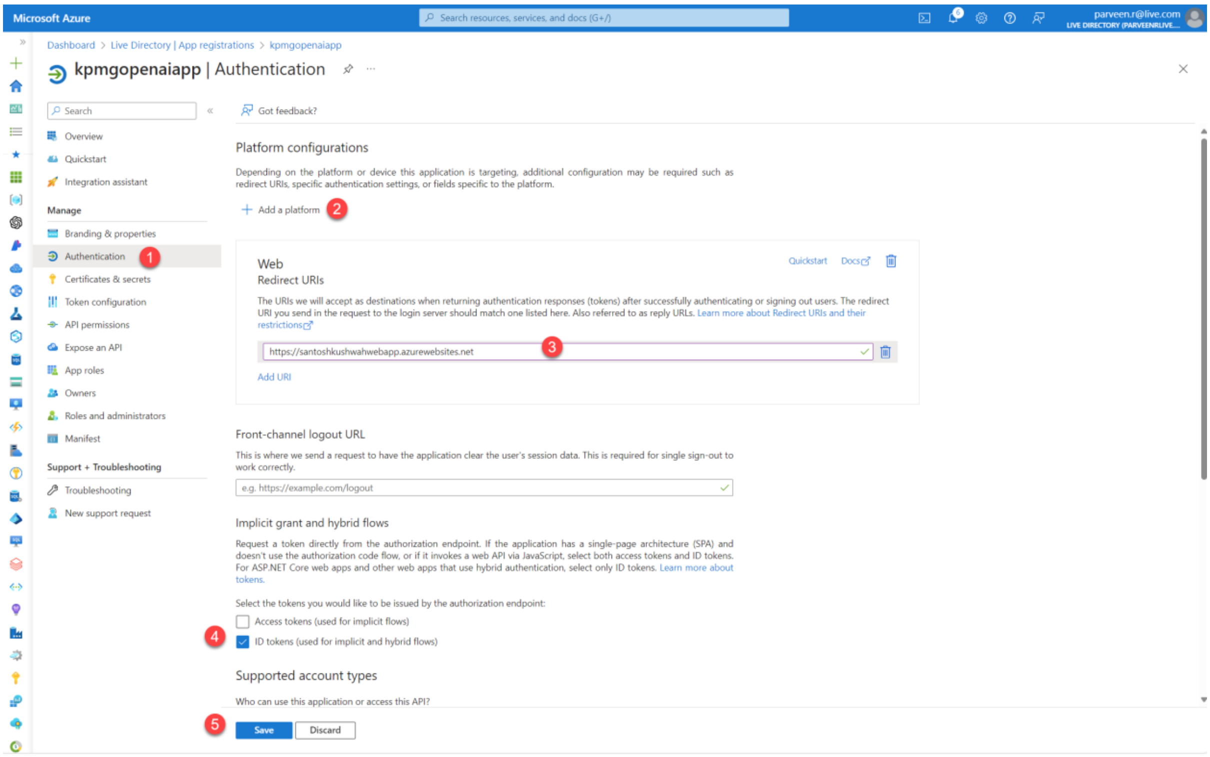
Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Update the url with your own url followed by:



kpmgopenaiapp | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://santoshkushwahwebapp.azurewebsites.net

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

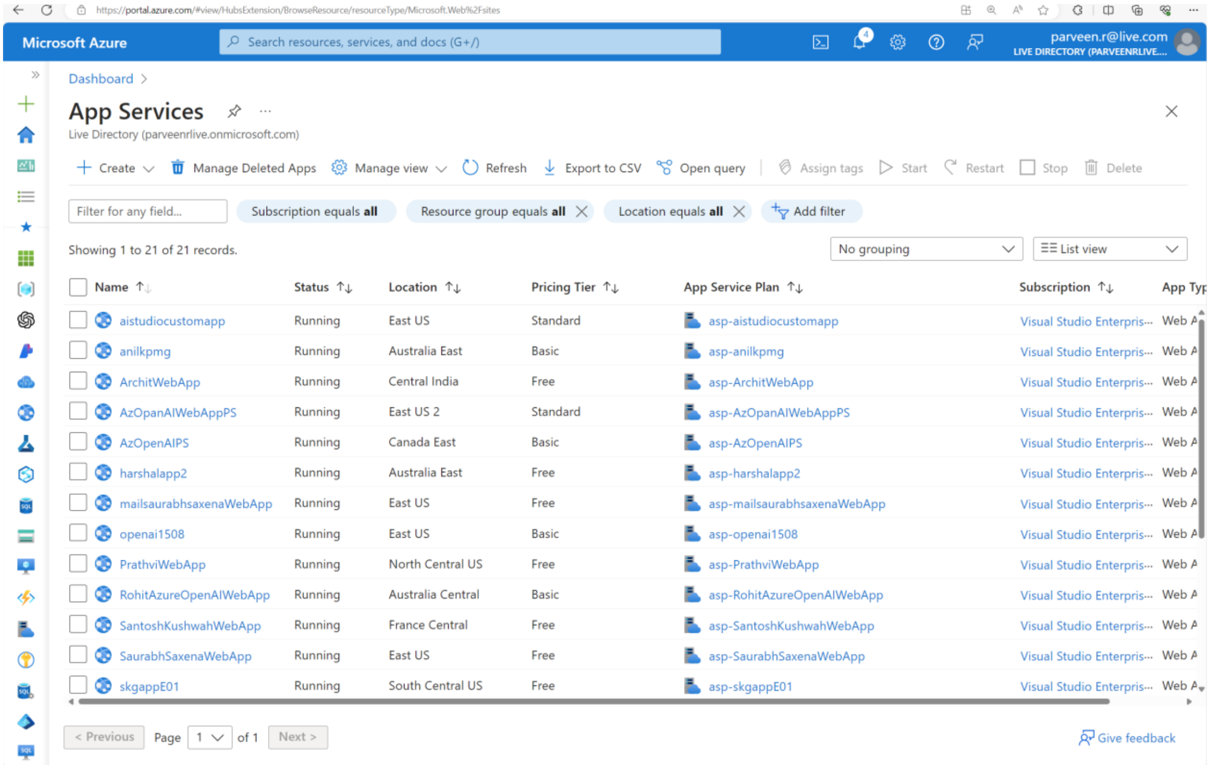
Supported account types

Who can use this application or access this API?

Save Discard

Go back to your App Service:

Open your App:



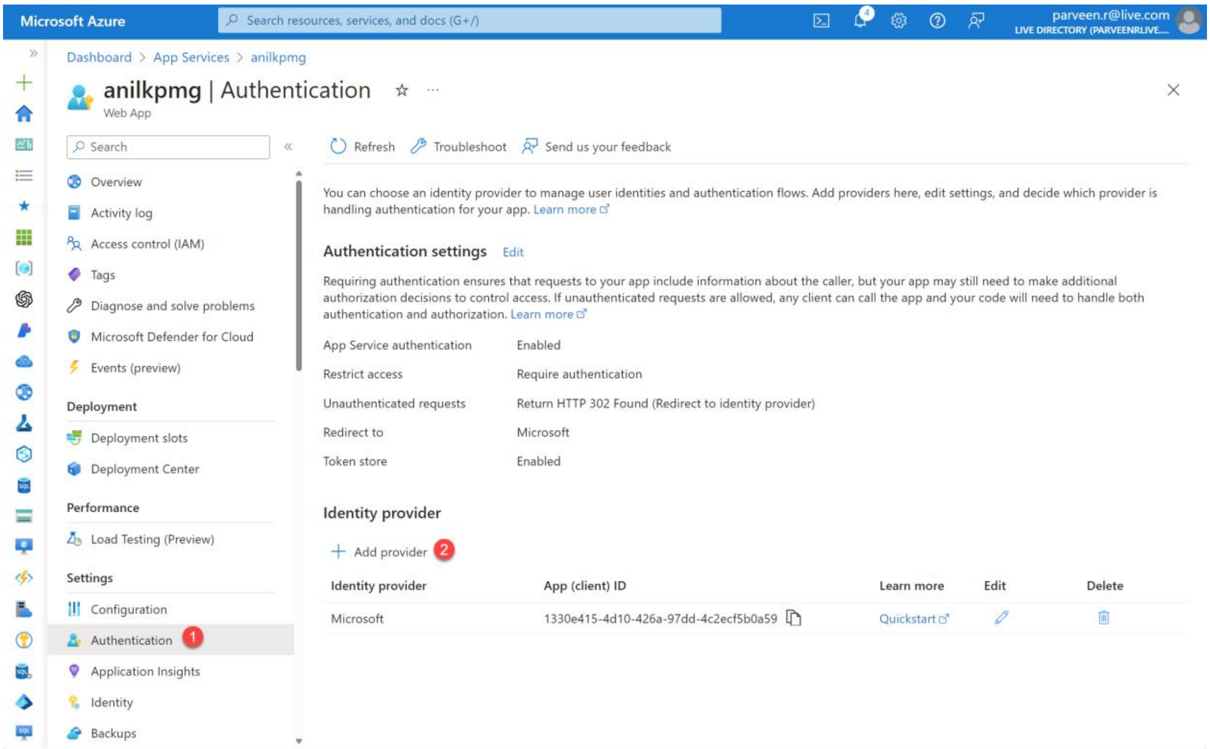
App Services

Live Directory (parveenrlive.onmicrosoft.com)

Showing 1 to 21 of 21 records.

Name	Status	Location	Pricing Tier	App Service Plan	Subscription	App Typ
aistudiocustomapp	Running	East US	Standard	asp-aistudiocustomapp	Visual Studio Enterpris...	Web A
anilkpmg	Running	Australia East	Basic	asp-anilkpmg	Visual Studio Enterpris...	Web A
ArchitWebApp	Running	Central India	Free	asp-ArchitWebApp	Visual Studio Enterpris...	Web A
AzOpanAIWebAppPS	Running	East US 2	Standard	asp-AzOpanAIWebAppPS	Visual Studio Enterpris...	Web A
AzOpenAIPS	Running	Canada East	Basic	asp-AzOpenAIPS	Visual Studio Enterpris...	Web A
harshalapp2	Running	Australia East	Free	asp-harshalapp2	Visual Studio Enterpris...	Web A
mailsaurabhsaxenaWebApp	Running	East US	Free	asp-mailsaurabhsaxenaWebApp	Visual Studio Enterpris...	Web A
openai1508	Running	East US	Basic	asp-openai1508	Visual Studio Enterpris...	Web A
PrathviWebApp	Running	North Central US	Free	asp-PrathviWebApp	Visual Studio Enterpris...	Web A
RohitAzureOpenAIWebApp	Running	Australia Central	Basic	asp-RohitAzureOpenAIWebApp	Visual Studio Enterpris...	Web A
SantoshKushwahWebApp	Running	France Central	Free	asp-SantoshKushwahWebApp	Visual Studio Enterpris...	Web A
SaurabhSaxenaWebApp	Running	East US	Free	asp-SaurabhSaxenaWebApp	Visual Studio Enterpris...	Web A
skgappE01	Running	South Central US	Free	asp-skgappE01	Visual Studio Enterpris...	Web A

Click on Authentication:



anilkpmg | Authentication

Web App

You can choose an identity provider to manage user identities and authentication flows. Add providers here, edit settings, and decide which provider is handling authentication for your app. Learn more

Authentication settings Edit

Requiring authentication ensures that requests to your app include information about the caller, but your app may still need to make additional authorization decisions to control access. If unauthenticated requests are allowed, any client can call the app and your code will need to handle both authentication and authorization. Learn more

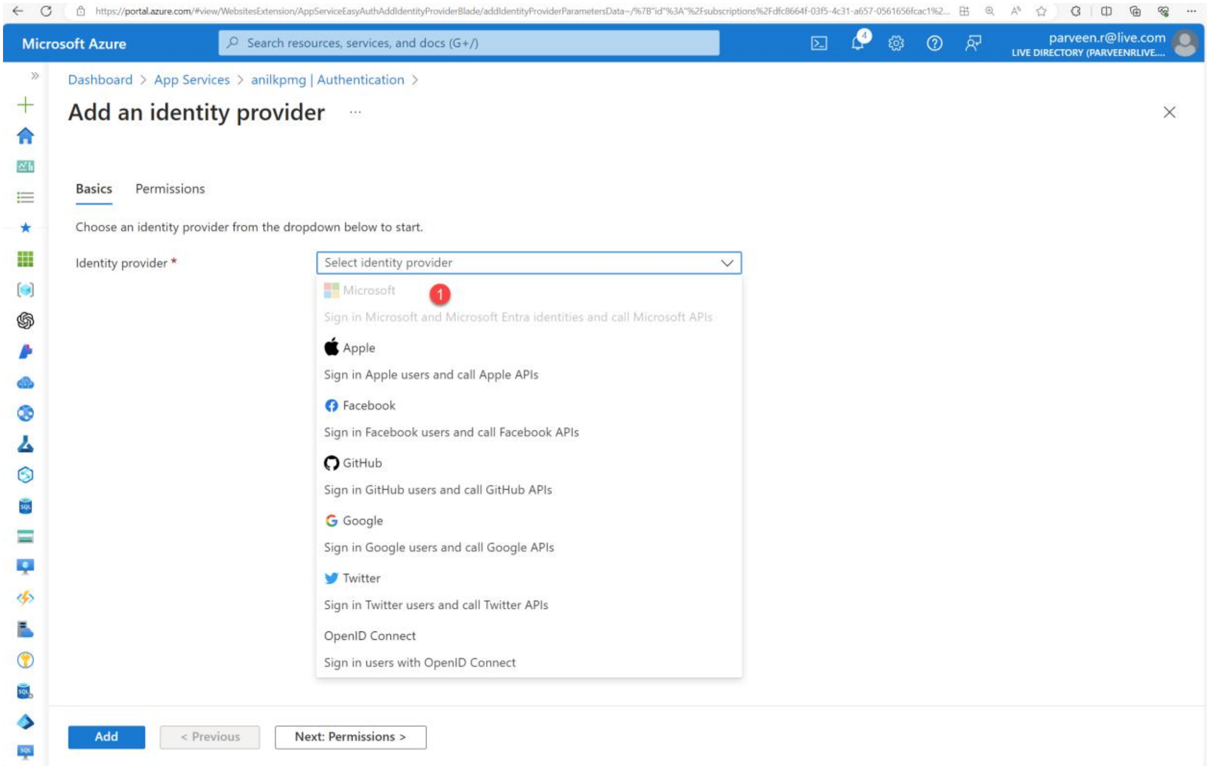
App Service authentication	Enabled
Restrict access	Require authentication
Unauthenticated requests	Return HTTP 302 Found (Redirect to identity provider)
Redirect to	Microsoft
Token store	Enabled

Identity provider

+ Add provider 2

Identity provider	App (client) ID	Learn more	Edit	Delete
Microsoft	1330e415-4d10-426a-97dd-4c2ecf5b0a59	Quickstart		

Select Microsoft as Provider:


https://portal.azure.com/#view/WebsitesExtension/AppServiceEasyAuthAddIdentityProviderBlade/addIdentityProviderParametersData~/%7B"id"%3A"%2Fsubscriptions%2Fdfc8664f-03f5-4c31-a657-0561656fcac1%2...
Microsoft Azure
Search resources, services, and docs (G+/)
parveen.r@live.com
LIVE DIRECTORY (PARVEENRLIVE....
Dashboard > App Services > anilkpmg | Authentication >
Basics
Permissions
1
Add
< Previous
Next: Permissions >

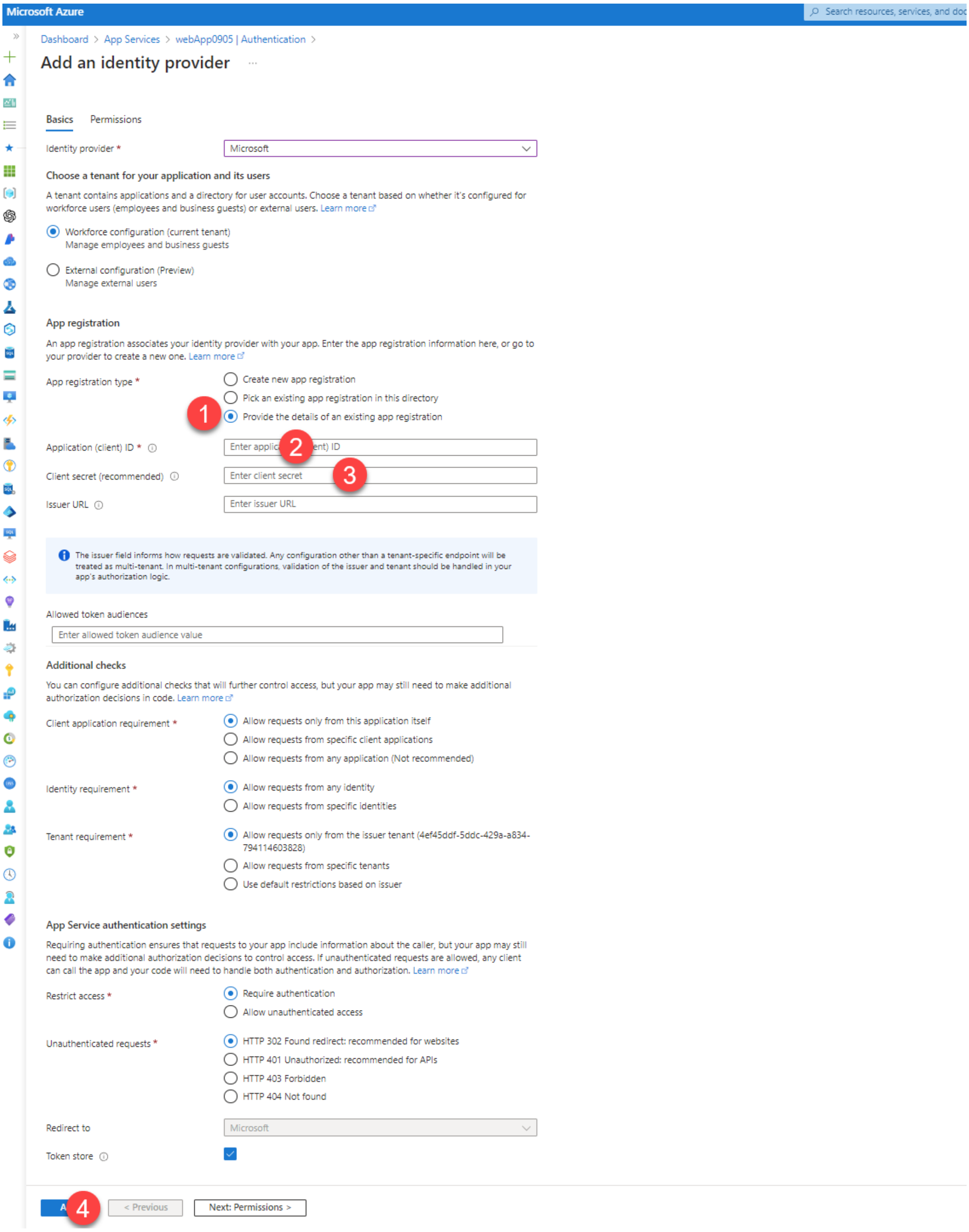
Add an identity provider

Choose an identity provider from the dropdown below to start.

Identity provider * Select identity provider

- Microsoft
  Sign in Microsoft and Microsoft Entra identities and call Microsoft APIs
- Apple
  Sign in Apple users and call Apple APIs
- Facebook
  Sign in Facebook users and call Facebook APIs
- GitHub
  Sign in GitHub users and call GitHub APIs
- Google
  Sign in Google users and call Google APIs
- Twitter
  Sign in Twitter users and call Twitter APIs
- OpenID Connect
  Sign in users with OpenID Connect

Add the values copied in previous step:



Dashboard > App Services > webApp0905 | Authentication >

Add an identity provider ...

Basics Permissions

Identity provider * Microsoft

Choose a tenant for your application and its users

A tenant contains applications and a directory for user accounts. Choose a tenant based on whether it's configured for workforce users (employees and business guests) or external users. Learn more

● Workforce configuration (current tenant)
Manage employees and business guests

○ External configuration (Preview)
Manage external users

App registration

An app registration associates your identity provider with your app. Enter the app registration information here, or go to your provider to create a new one. Learn more

App registration type *
○ Create new app registration
○ Pick an existing app registration in this directory
● Provide the details of an existing app registration

Application (client) ID * Enter applic ent) ID

Client secret (recommended) Enter client secret

Issuer URL Enter issuer URL

The issuer field informs how requests are validated. Any configuration other than a tenant-specific endpoint will be treated as multi-tenant. In multi-tenant configurations, validation of the issuer and tenant should be handled in your app's authorization logic.

Allowed token audiences

Enter allowed token audience value

Additional checks

You can configure additional checks that will further control access, but your app may still need to make additional authorization decisions in code. Learn more

Client application requirement *
● Allow requests only from this application itself
○ Allow requests from specific client applications
○ Allow requests from any application (Not recommended)

Identity requirement *
● Allow requests from any identity
○ Allow requests from specific identities

Tenant requirement *
● Allow requests only from the issuer tenant (4ef45ddf-5ddc-429a-a834-794114603828)
○ Allow requests from specific tenants
○ Use default restrictions based on issuer

App Service authentication settings

Requiring authentication ensures that requests to your app include information about the caller, but your app may still need to make additional authorization decisions to control access. If unauthenticated requests are allowed, any client can call the app and your code will need to handle both authentication and authorization. Learn more

Restrict access *
● Require authentication
○ Allow unauthenticated access

Unauthenticated requests *
● HTTP 302 Found redirect: recommended for websites
○ HTTP 401 Unauthorized: recommended for APIs
○ HTTP 403 Forbidden
○ HTTP 404 Not found

Redirect to Microsoft

Token store ☑

A < Previous Next: Permissions >