Configure Azure AD for SingleSignOn with nShift IdentityProvider

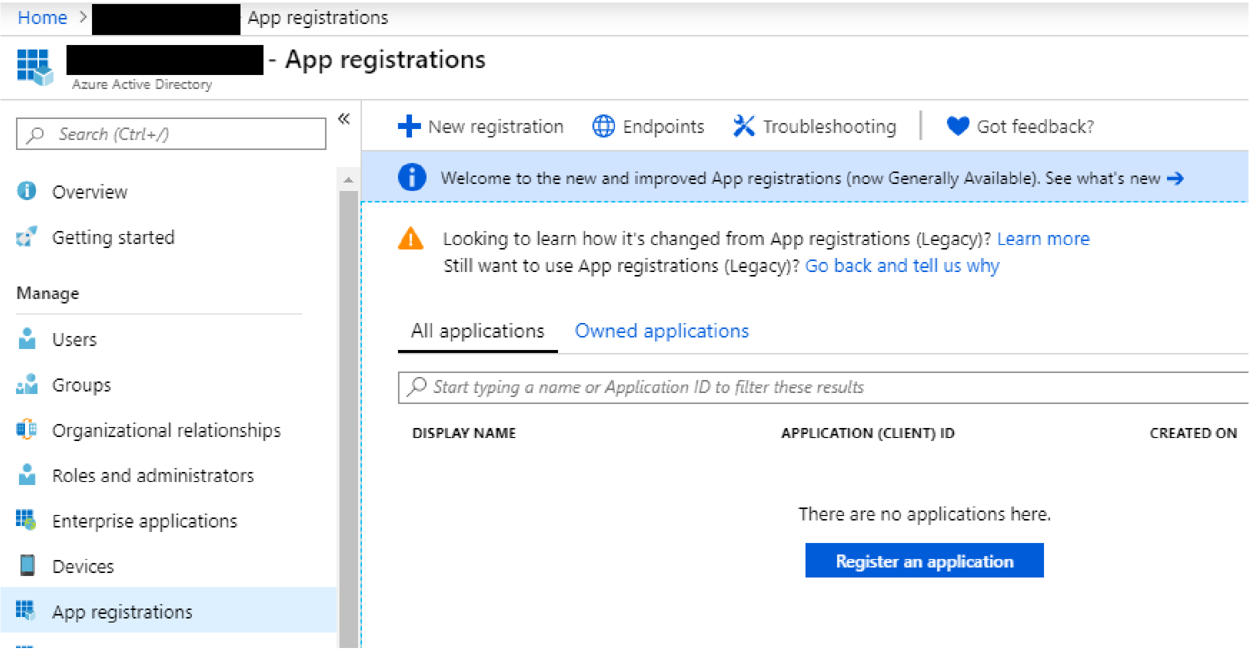
nShift

February, 2024

Part I – Configure Azure Active Directory

1. Create a new Azure Active Directory tenant

2. Click **App registrations > Register an application**.



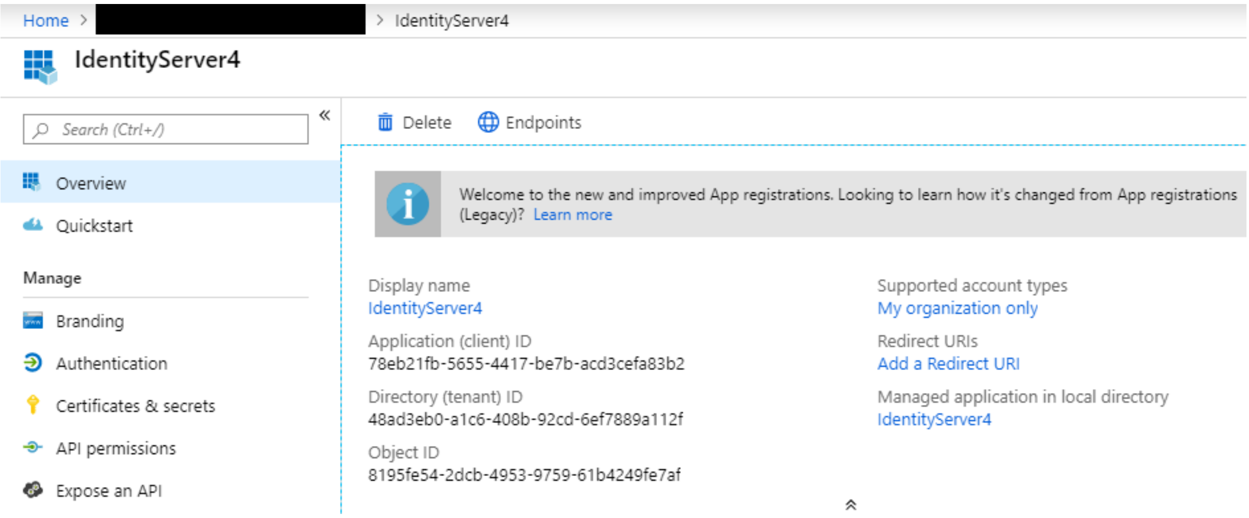
Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON

There are no applications here.

3. Make a note of your Application (client) ID and Directory (tenant) ID values. If you have set up a client secret for the newly created client ID, please make a note of that also.



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

Display name
IdentityServer4

Application (client) ID
78eb21fb-5655-4417-be7b-acd3cefa83b2

Directory (tenant) ID
48ad3eb0-a1c6-408b-92cd-6ef7889a112f

Object ID
8195fe54-2dcb-4953-9759-61b4249fe7af

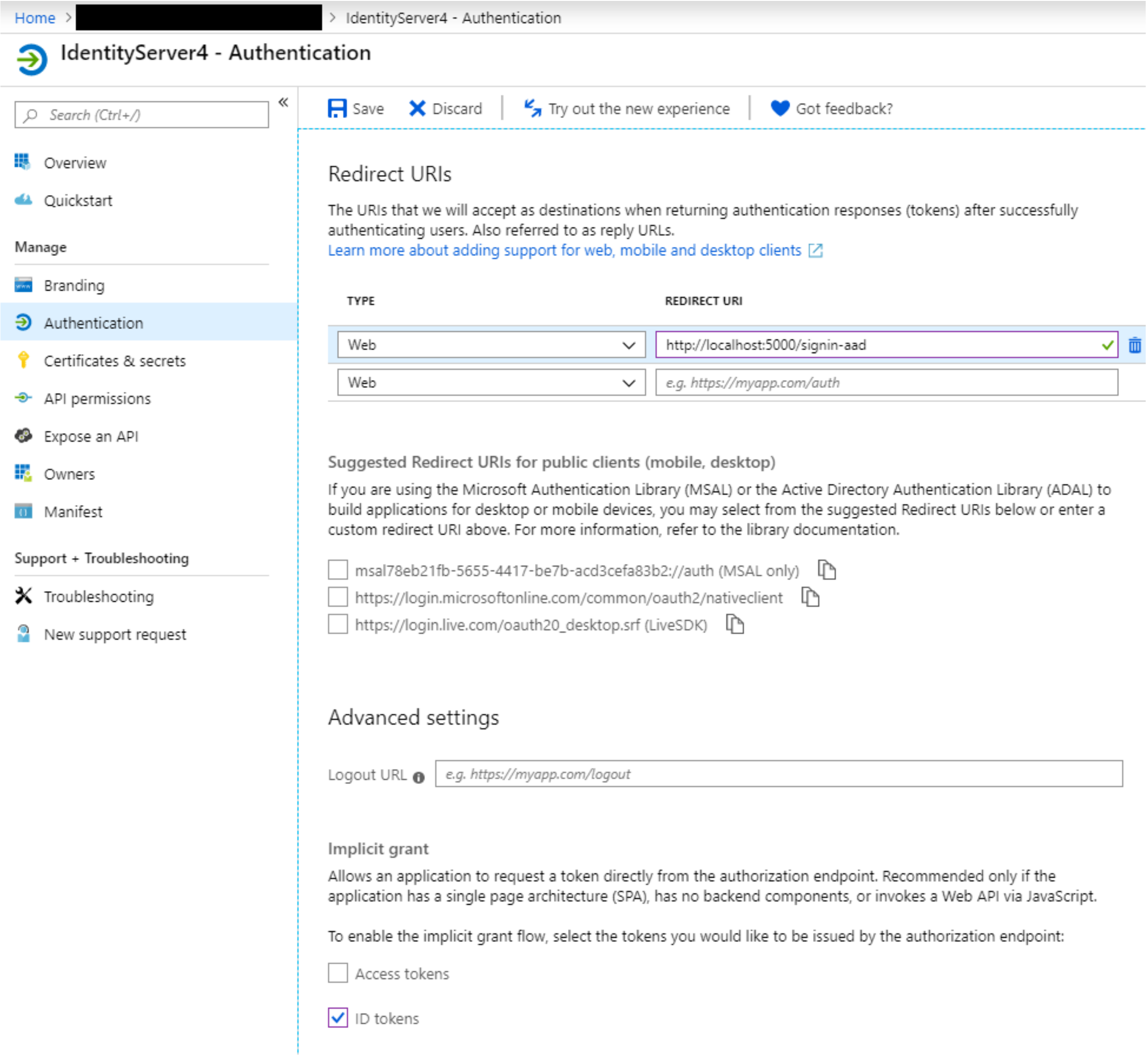
Supported account types
My organization only

Redirect URIs
Add a Redirect URI

Managed application in local directory
IdentityServer4

4. In the **Redirect URI** field enter the callback path nShift will provide. The type should be web.

5. Under **Advanced settings** fill in the **Logout URL** with the one provided by nShift.



IdentityServer4 - Authentication

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs.

Learn more about adding support for web, mobile and desktop clients

TYPE	REDIRECT URI
Web	http://localhost:5000/signin-aad
Web	e.g. https://myapp.com/auth

Suggested Redirect URIs for public clients (mobile, desktop)

If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.

- ☐ msal78eb21fb-5655-4417-be7b-acd3cefa83b2://auth (MSAL only)
- ☐ https://login.microsoftonline.com/common/oauth2/nativeclient
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)

Advanced settings

Logout URL: e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.

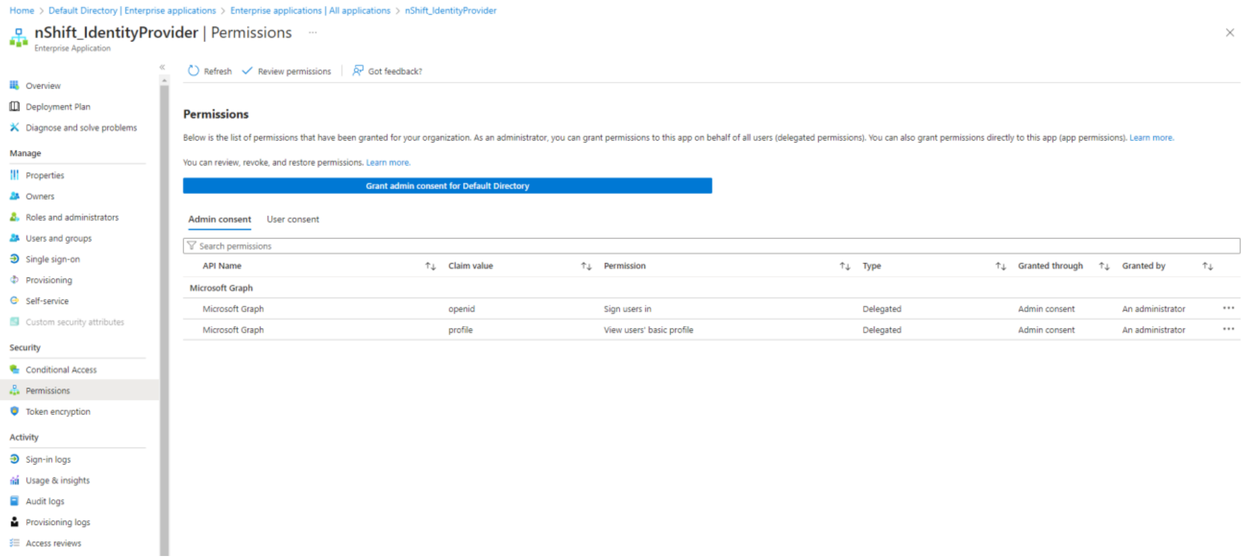
To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

- ☐ Access tokens
- ☑ ID tokens

*Note: The URLs used in the image are samples only – please use the ones provided by nShift.

6. Check the **ID tokens** checkbox

7. Configure **Permissions**. Please ensure that you have properly configured the permissions for the nShift application in Entra. Add the following permissions:



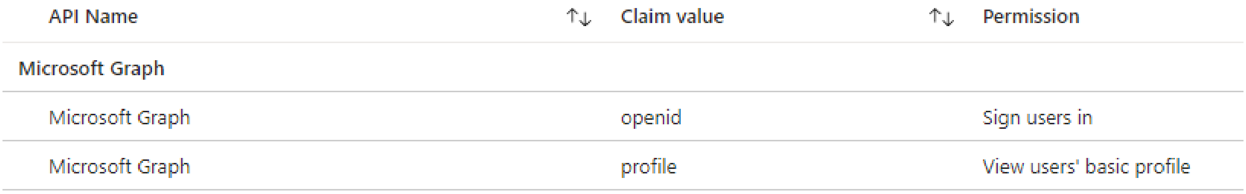
Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). Learn more.

You can review, revoke, and restore permissions. Learn more.

API Name ↑↓	Claim value ↑↓	Permission ↑↓	Type ↑↓	Granted through ↑↓	Granted by ↑↓	
Microsoft Graph						
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator	···
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator	···

Close up of the permissions:



API Name ↑↓	Claim value ↑↓	Permission
Microsoft Graph		
Microsoft Graph	openid	Sign users in
Microsoft Graph	profile	View users' basic profile

Please be prepared to provide us with a test user with access to the newly created tenant/client for troubleshooting. The user can be deleted after the setup is done.

Part II - Information provided by nShift

The redirect URI to use when configuring AAD should be:
https://account.nshiftportal.com/idp/federation/sample-name/signin

**type should be web*

The logout URL to use when configuring AAD should be:

https://account.nshiftportal.com/idp/federation/sample-name/signout

Part III - Information required by nShift

To configure our nShift IdentityProvider to allow access through your Azure AD portal we will require the TenantId, ClientId, ClientSecret(if provided) of the newly AAD registered application.

**Important note:*

To use Azure AD as an authentication provider for nShift Portal, Azure AD will need to have the same usernames as the Portal user (usernames used to log in).