GoDocs®

SINGLE SIGN-ON

Client Configuration

Microsoft Entra ID

Embed the GoDocs document order process directly in our LOS to create a fully integrated client experience and access the GoDocs Platform by leveraging direct integration with Third Party Identitiy Providers and Automated User Provisioning.

Date: **July. 15, 2025**

Document Version: **1.2**

Table of Contents

Version History

Version	Changes	Date
V1.0	Initial Document Release	October 31, 2024
V1.1	Updates to step-by-step instructions for Token type setup	April 4, 2025
V1.2	Support for OKTA IDPs	July 15, 2025

Confidentiality Notice

This document contains confidential and proprietary information belonging to GoDocs. The information is intended only for the use of the individual or entity to which it is addressed. Any unauthorized disclosure, copying, distribution, or use of the contents is strictly prohibited. If you have received this document in error, please notify the sender immediately and delete it from your system.

Instructions for OpenId Connect setup for IDP configuration Azure AD (Microsoft Entra Id):

Setup Configurations for IDP:

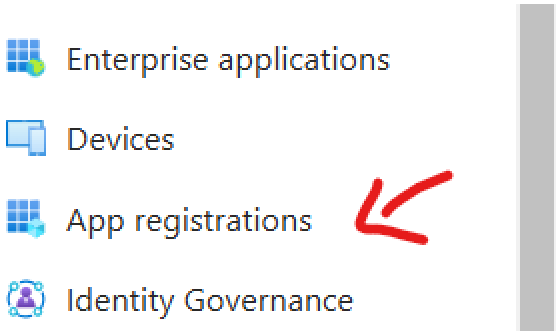
1. Create an app registration in your Azure AD (Microsoft Entra Id) tenant

2. Add GoDocs Oauth2 Authentication Response endpoint to the Authentication Tab as a Redirect Uri
    a. https://godocstestb2c.b2clogin.com/godocstestb2c.onmicrosoft.com/oauth2/authresp
    b. Select Access Token and ID Token

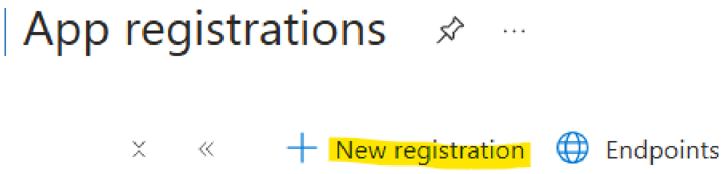
3. In the Token Configuration tab add these claims to response token:
    a. email
    b. family_name
    c. given_name
    d. preferred_username

Step-by-step instructions:

1. In your Azure AD (Microsoft Entra Id) Tenant Navigate "App registrations" Menu option.



2. Click the "+ New registration" button

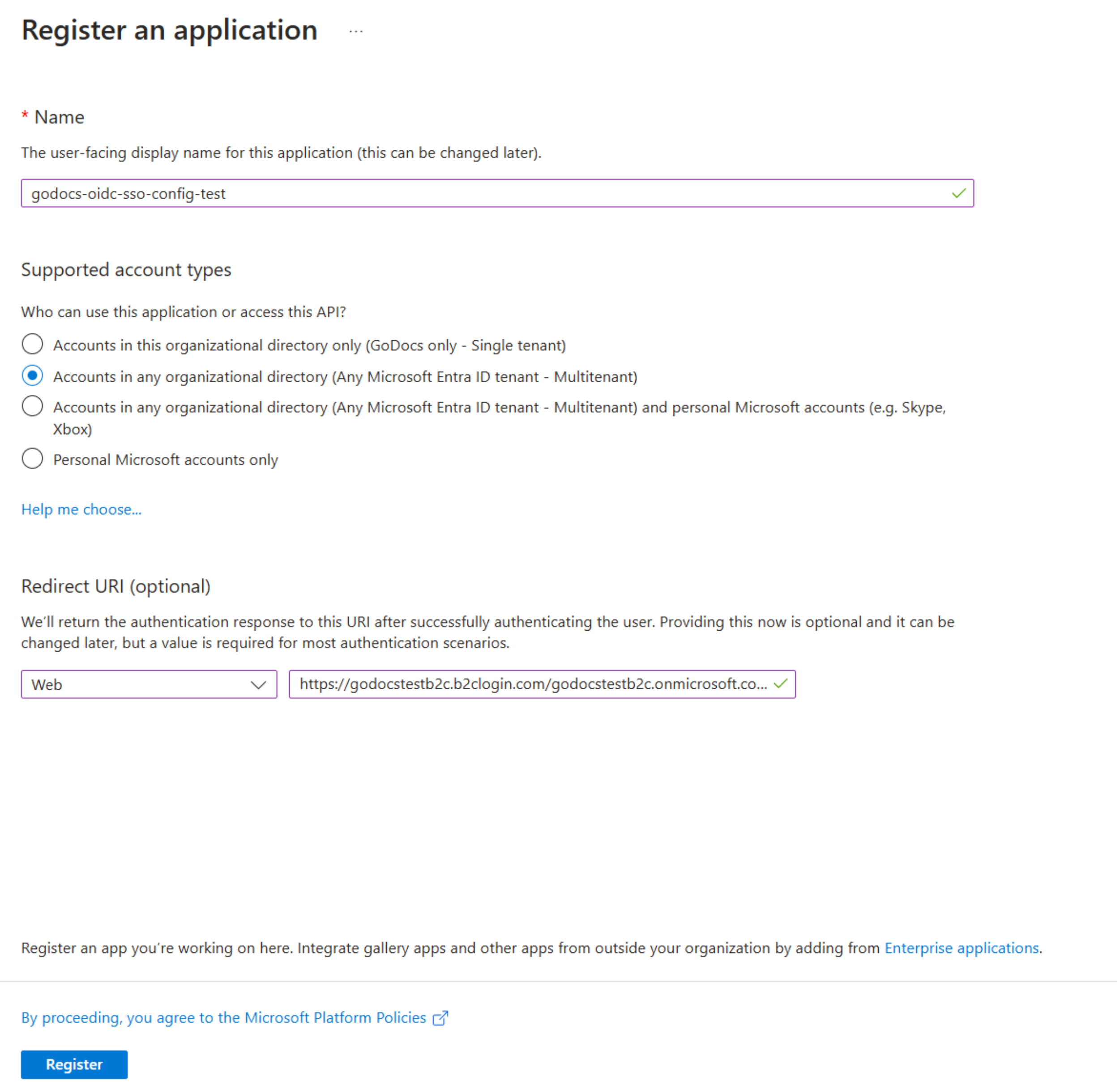


3. Enter a name for the app registration (anything you would like to call it or follow any naming convention your company follows. We do not see this name)

4. Select the "Support Account Types" depending on your company users

5. In Redirect Uri section
    a. Change the drop down to "Web"
    b. In the textbox paste in the URL:
        i. https://godocstestb2c.b2clogin.com/godocstestb2c.onmicrosoft.com/oauth2/authresp
        ii. Note: This is our testing tenant URL. We will have a production tenant URL we will send you when ready to go live.

6. Click the "Register" Button



Register an application ···

* Name

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

godocs-oidc-sso-config-test ✓

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (GoDocs 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.

Web ⌄ https://godocstestb2c.b2clogin.com/godocstestb2c.onmicrosoft.co... ✓

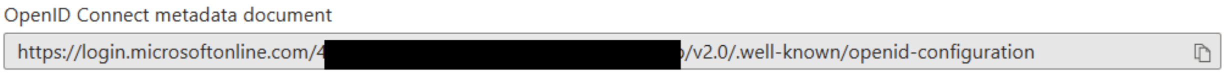
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

7\.

8. Navigate over to your "App registrations" Menu Option

9. Next, Click the "Endpoints" button and panel will open on the right with many different endpoint URLs. Look for the "OpenID Connect metadata document" save that for later.
    a. Make sure your OpenID Connect Metadata document URL has your Azure AD (Entra) Tenant Id in it. The ID should be represented as a Guid



OpenID Connect metadata document

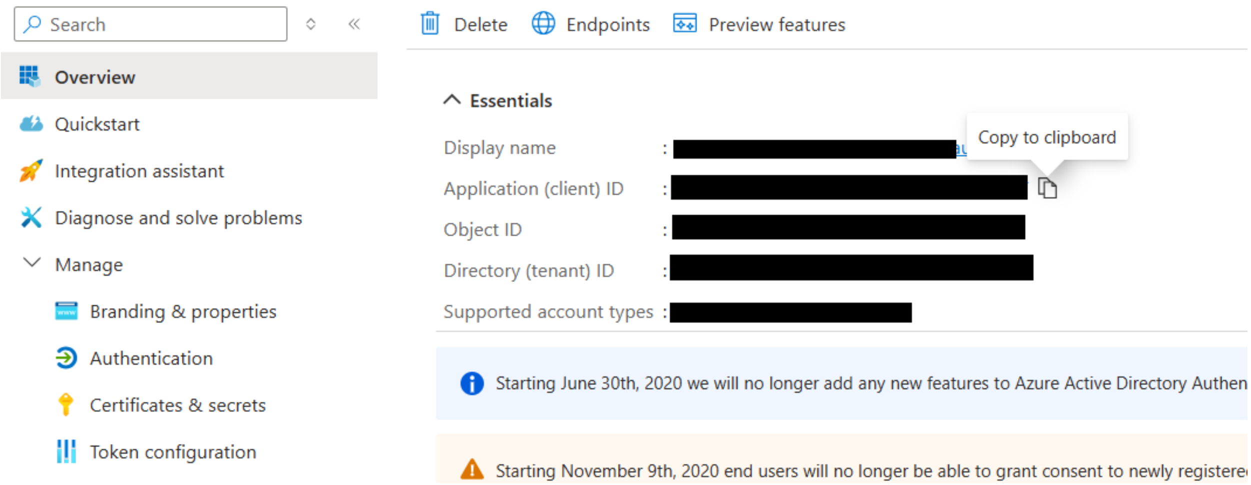
https://login.microsoftonline.com/4[redacted]/v2.0/.well-known/openid-configuration

    b.

10. Look for the new app registration you created for the sso configuration

11. Copy the "Application (client) ID" save that for later.

12. Copy the "Directory (tenant) ID" save that for later.



Display name : [redacted]

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : [redacted]

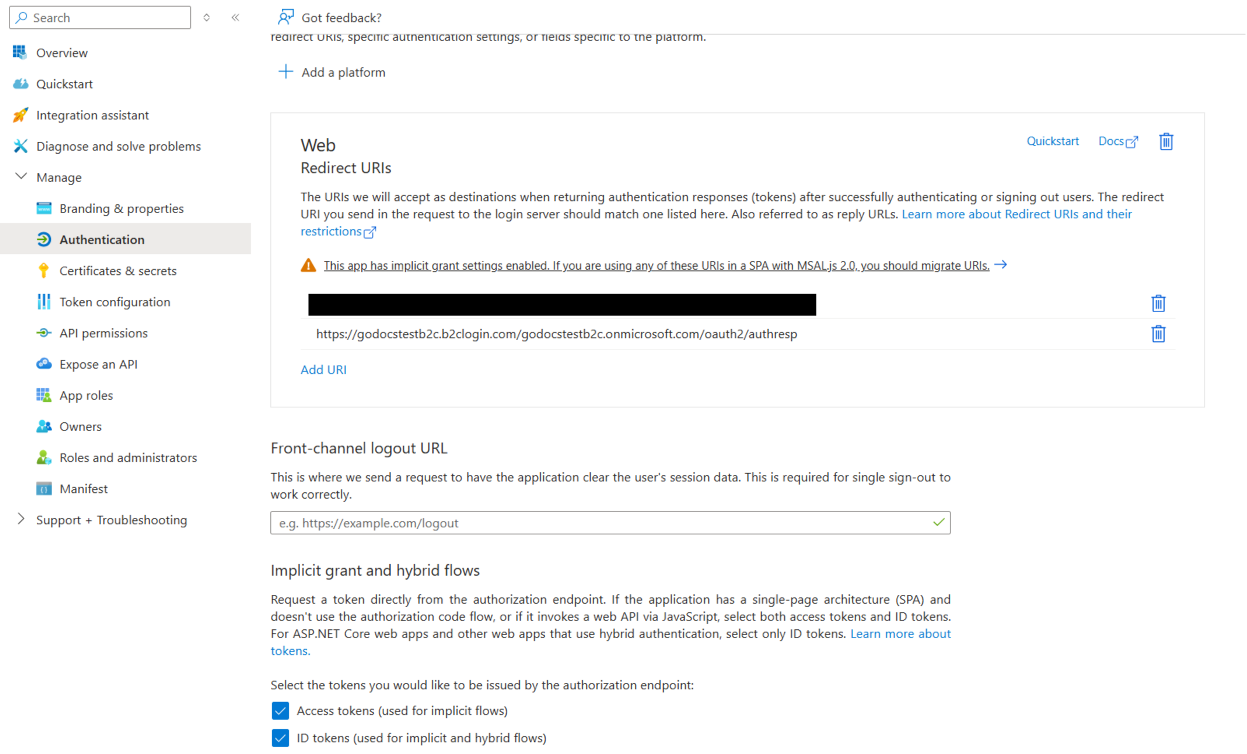
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authen

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registere

13.

14. Navigate to "Authentication" Menu option under "Manage"

15. Ensure the Redirect Uri is configured to:
    a. https://godocstestb2c.b2clogin.com/godocstestb2c.onmicrosoft.com/oauth2/authresp
    b. In the "Implicit grant and hybrid flows" section:
        i. Check both selections
        ii. If you do not want to use both you can just select "ID tokens" (Please let us know which you choose if not both we will configure accordingly)



redirect URIs, specific authentication settings, or fields specific to the 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

This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

[redacted]

https://godocstestb2c.b2clogin.com/godocstestb2c.onmicrosoft.com/oauth2/authresp

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)

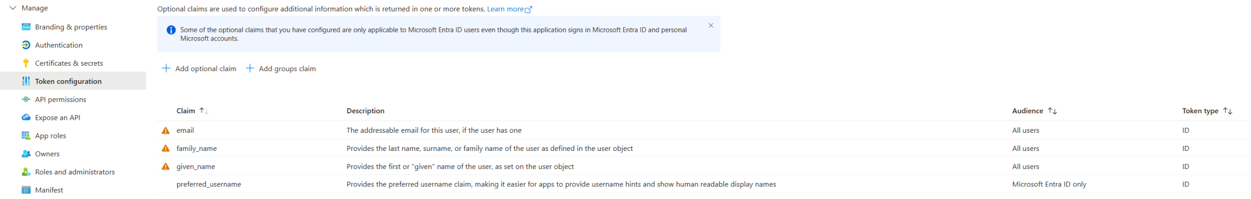
☑ ID tokens (used for implicit and hybrid flows)

c.

16. Navigate to the “Token configuration” menu option under “Manage”

17. Click the “+ Add optional claim” button
    a. Select “ID” radio button for “Token type”
    b. Add claims:
        i. email
        ii. family_name
        iii. given_name
        iv. preferred_username

18.



Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Some of the optional claims that you have configured are only applicable to Microsoft Entra ID users even though this application signs in Microsoft Entra ID and personal Microsoft accounts.

Claim	Description	Audience	Token type
email	The addressable email for this user, if the user has one	All users	ID
family_name	Provides the last name, surname, or family name of the user as defined in the user object	All users	ID
given_name	Provides the first or "given" name of the user, as set on the user object	All users	ID
preferred_username	Provides the preferred username claim, making it easier for apps to provide username hints and show human readable display names	Microsoft Entra ID only	ID

19. That’s it. Send GoDocs the “OpenId Connect metadata document” uri, “tenant id” and “client id” you saved earlier and specify whether you chose a specific token type (if you didn’t select both Access Tokens and ID tokens).