4TWO – SINGLE SIGN ON MANUAL

This manual guides you through the process of setting up Single Sign-On (SSO) for your 4two application.

SSO has become the preferred solution for simplifying and securing user authentication across applications. By leveraging Microsoft's authentication flow, SSO streamlines the user experience by eliminating the need for additional usernames and passwords. This approach enhances security through Multi-Factor Authentication (MFA), ensuring that user accounts are protected while maintaining ease of access.

Furthermore, SSO makes the onboarding process more efficient, as employees are automatically granted access to the application through their Microsoft accounts. Access is also seamlessly revoked when a Microsoft account is deactivated during offboarding, ensuring that only active employees retain access to your systems.

This manual will guide you through setting up an Enterprise Application, followed by configuring the Application Registration. During the Application Registration process, you will configure the Authentication settings, API permissions, and the client secret. Finally, the manual concludes with instructions for registering the Enterprise Application in 4Two and testing the SSO connection.

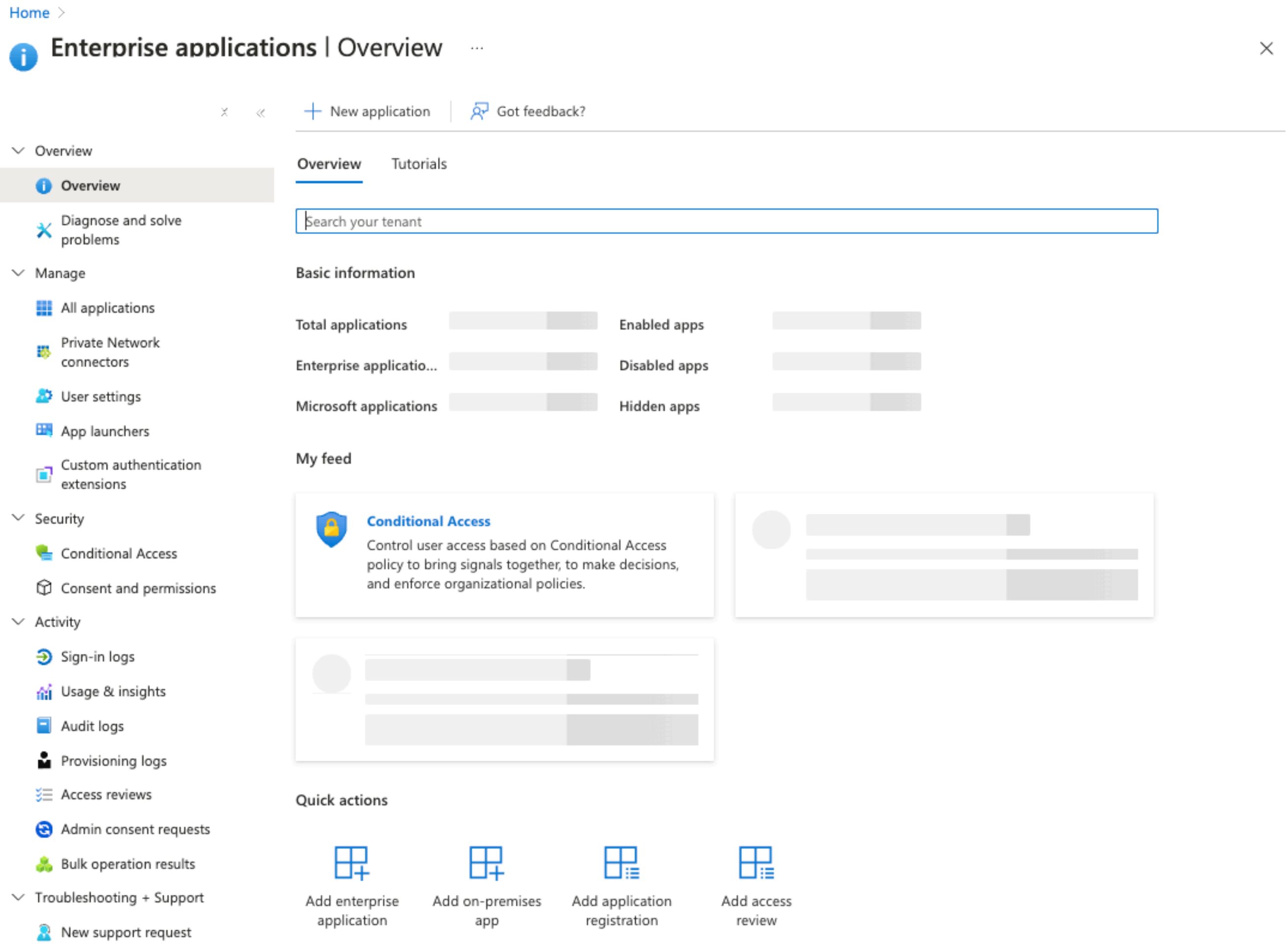
1 GO TO THE AZURE PORTAL

Go to the aure portal to access Microsoft Entra Portal.

https://portal.azure.com

2 SET UP AN ENTERPRISE APPLICATION

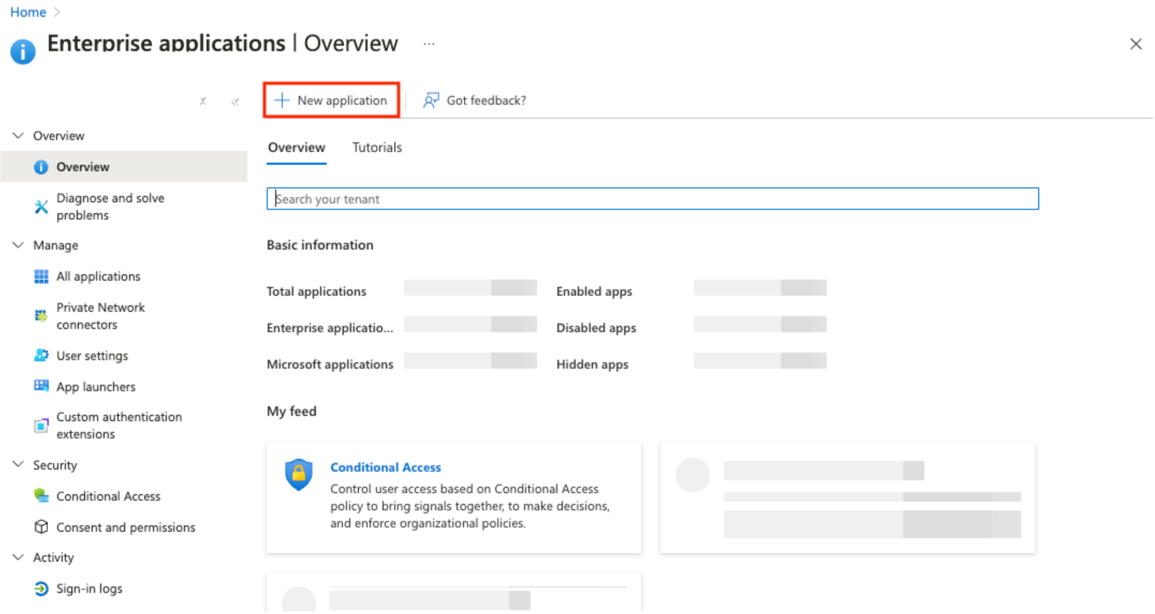
2.1 GO TO THE ENTERPRISE APPLICATIONS



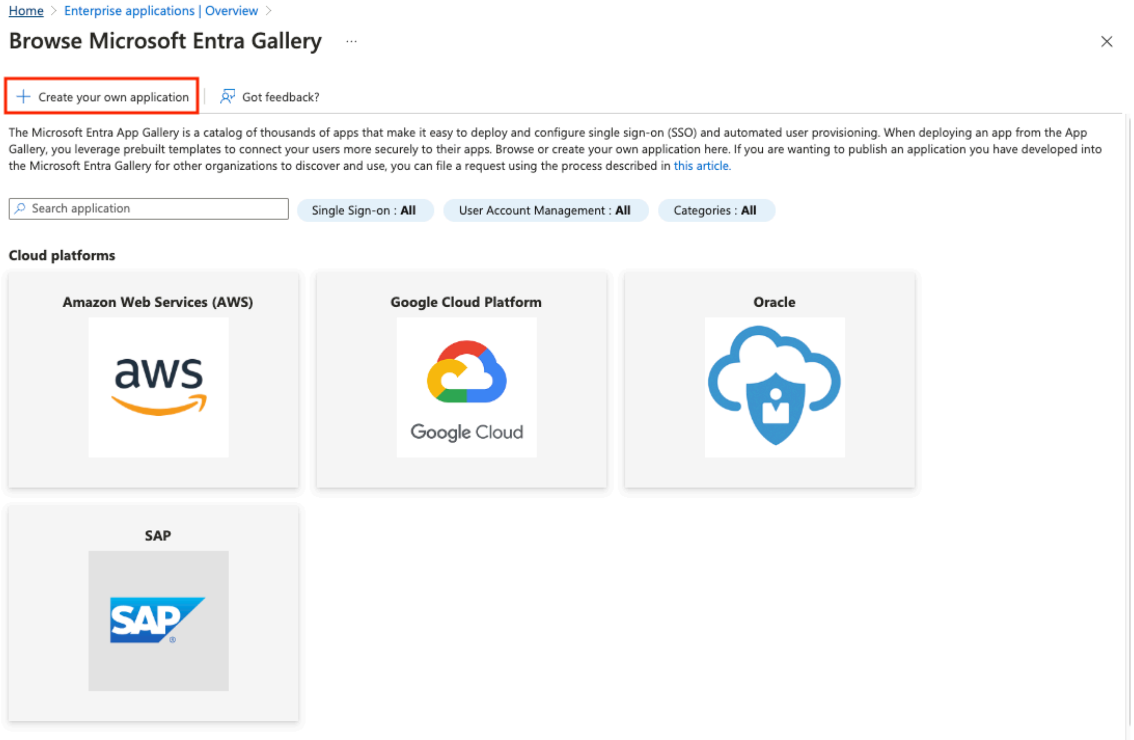
Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

2.2 Add a new application

2.2.1 Press New Application -> Create your own application

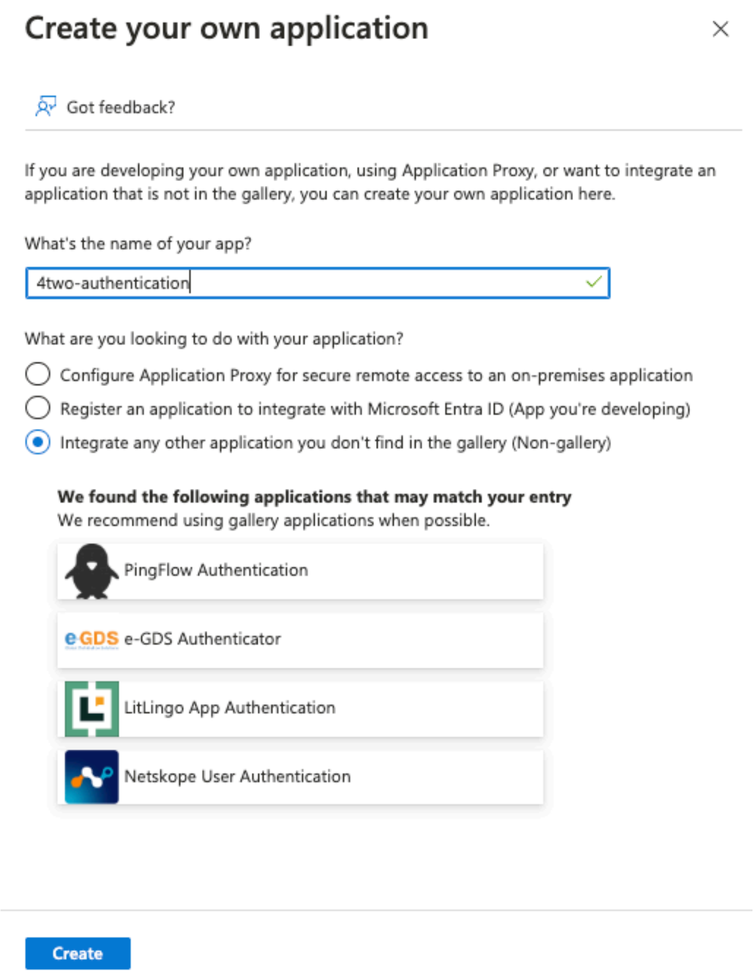


Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.


Home > Enterprise applications | Overview >
Browse Microsoft Entra Gallery ...
+ Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
aws
Google Cloud Platform
Google Cloud
Oracle
SAP

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

2.2.2 Fill in an app name and select the *Integrate any other application that you don't find in the gallery (Non-gallery)* option.



Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

4two-authentication ✓

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

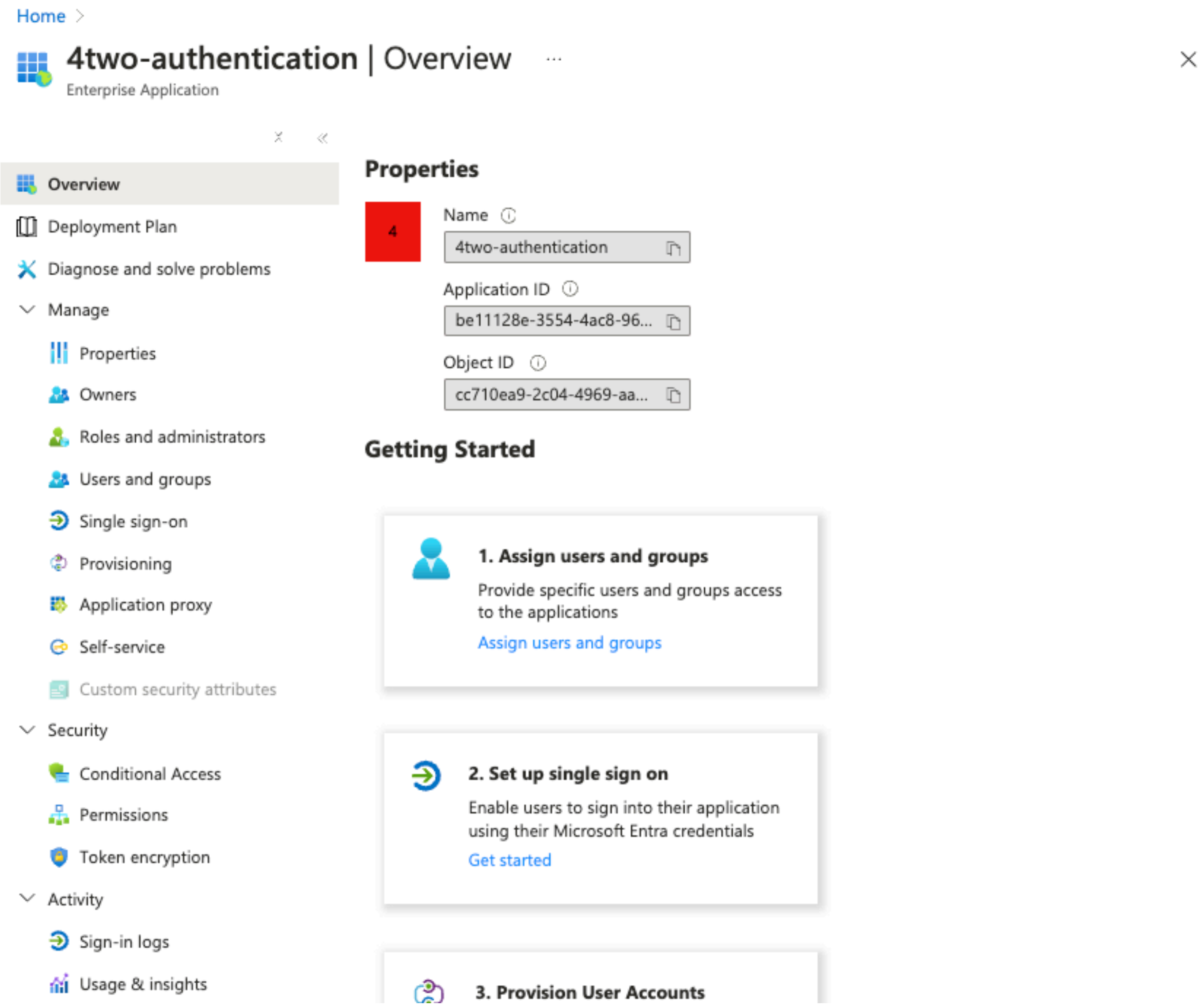
● Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry

We recommend using gallery applications when possible.

- PingFlow Authentication
- e-GDS Authenticator
- LitLingo App Authentication
- Netskope User Authentication

You have now created the Enterprise Application and corresponding Application Registration. You should be directed to the following screen:



Properties

Name: 4two-authentication

Application ID: be11128e-3554-4ac8-96...

Object ID: cc710ea9-2c04-4969-aa...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

2. Set up single sign on

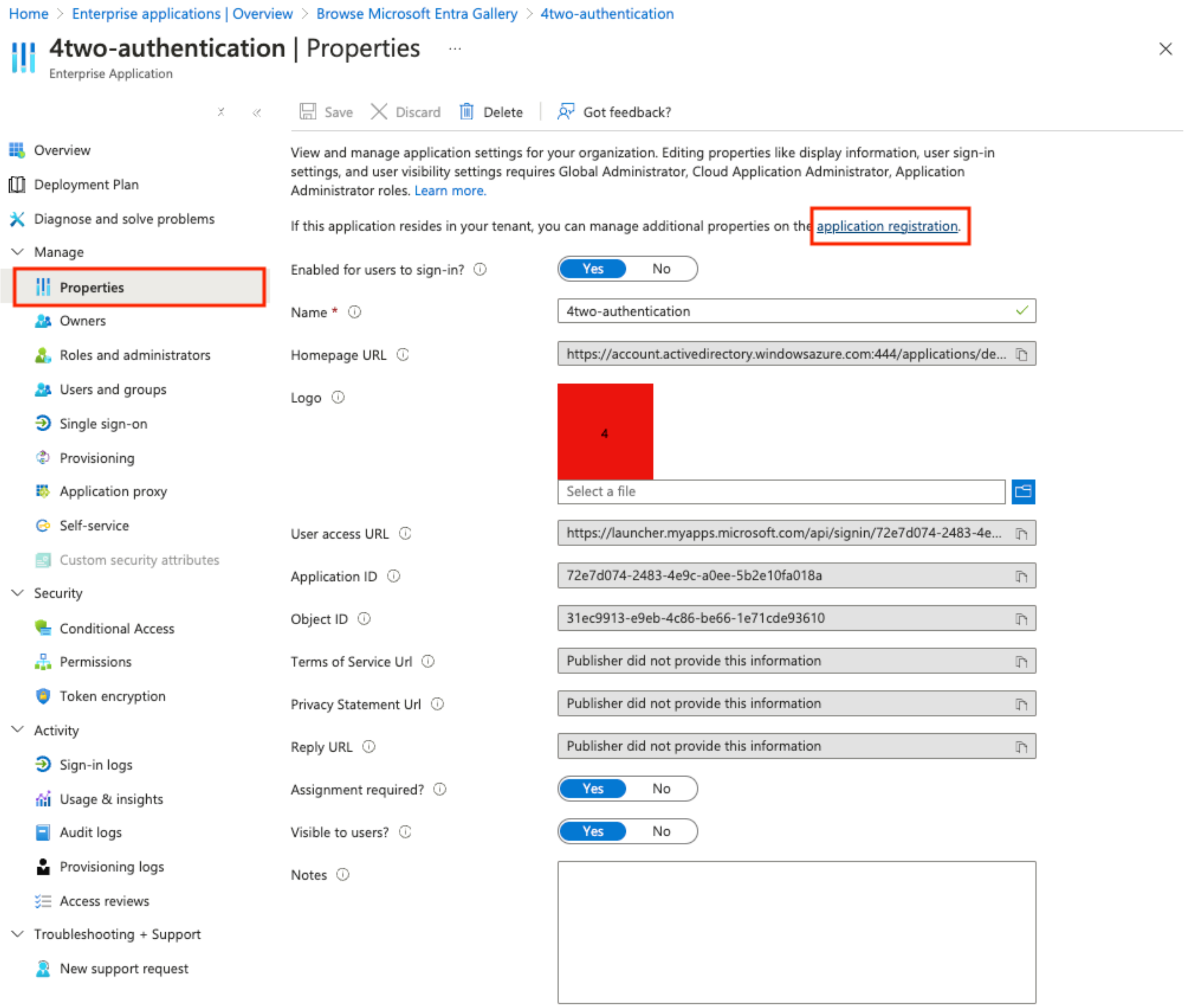
Enable users to sign into their application using their Microsoft Entra credentials

Get started

3. Provision User Accounts

3 GO TO THE APPLICATION REGISTRATION

On the Enterprise Application page, go to the *properties panel* -> then press *application registration* to go to the application registration page



View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

If this application resides in your tenant, you can manage additional properties on the application registration.

Enabled for users to sign-in?	[✓ Yes] No
Name *	4two-authentication
Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/de...
Logo	Select a file
User access URL	https://launcher.myapps.microsoft.com/api/signin/72e7d074-2483-4e...
Application ID	72e7d074-2483-4e9c-a0ee-5b2e10fa018a
Object ID	31ec9913-e9eb-4c86-be66-1e71cde93610
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply URL	Publisher did not provide this information
Assignment required?	[✓ Yes] No
Visible to users?	[✓ Yes] No
Notes	

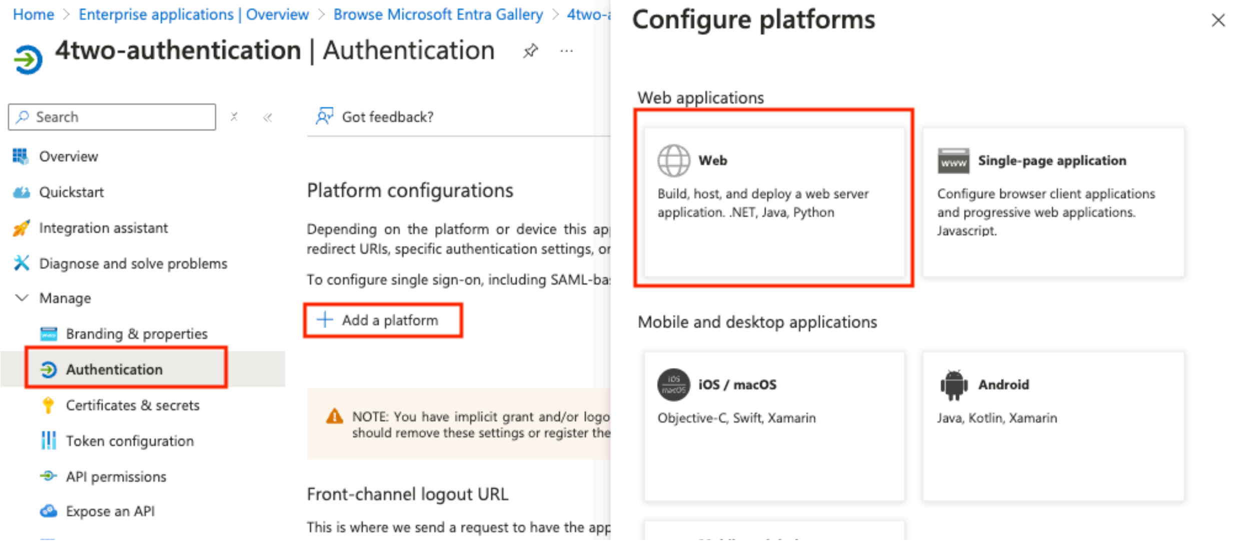
4 CONFIGURE THE APPLICATION REGISTRATION

4.1 CONFIGURE THE AUTHENTICATION SETTINGS

4.1.1 On the Application registration page, go to the *Authentication* panel

4.1.2 Click *Add a platform*

4.1.3 Choose Web



Platform configurations

Depending on the platform or device this ap redirect URIs, specific authentication settings, or

To configure single sign-on, including SAML-ba

NOTE: You have implicit grant and/or logo should remove these settings or register the

Front-channel logout URL

This is where we send a request to have the app

Web: Build, host, and deploy a web server application. .NET, Java, Python

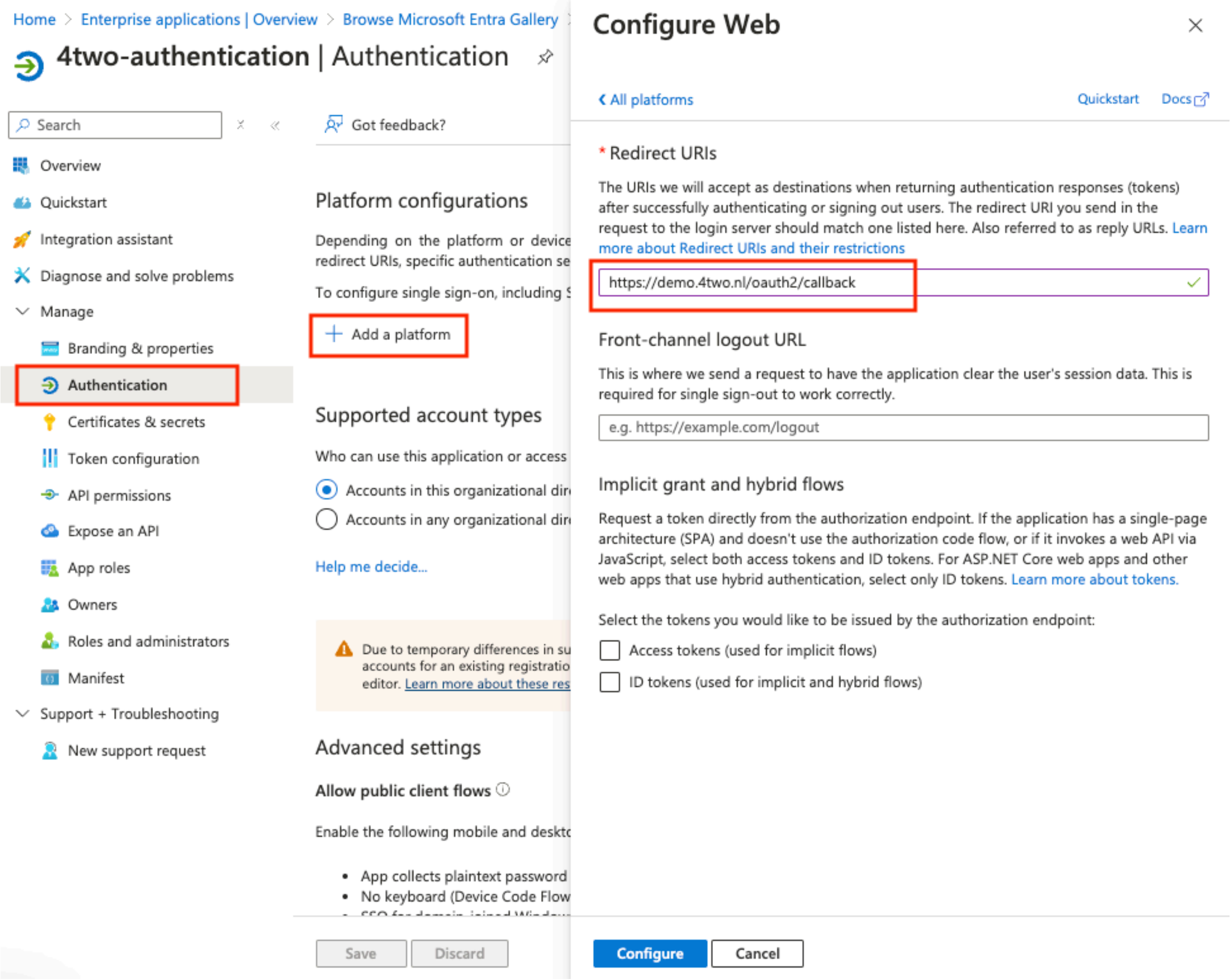
Single-page application: Configure browser client applications and progressive web applications. Javascript.

iOS / macOS: Objective-C, Swift, Xamarin

Android: Java, Kotlin, Xamarin

4.1.4 Fill in the redirect url. This should be: **https://<your-company-name>.4two.nl/oauth2/callback**

4.1.5 *Access token* and *ID token* can be unchecked.



Depending on the platform or device redirect URIs, specific authentication se

To configure single sign-on, including S

Who can use this application or access

● Accounts in this organizational dir

○ Accounts in any organizational dir

Due to temporary differences in su accounts for an existing registratio editor. Learn more about these res

Enable the following mobile and deskto

- App collects plaintext password
- No keyboard (Device Code Flow

* 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://demo.4two.nl/oauth2/callback ✓

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

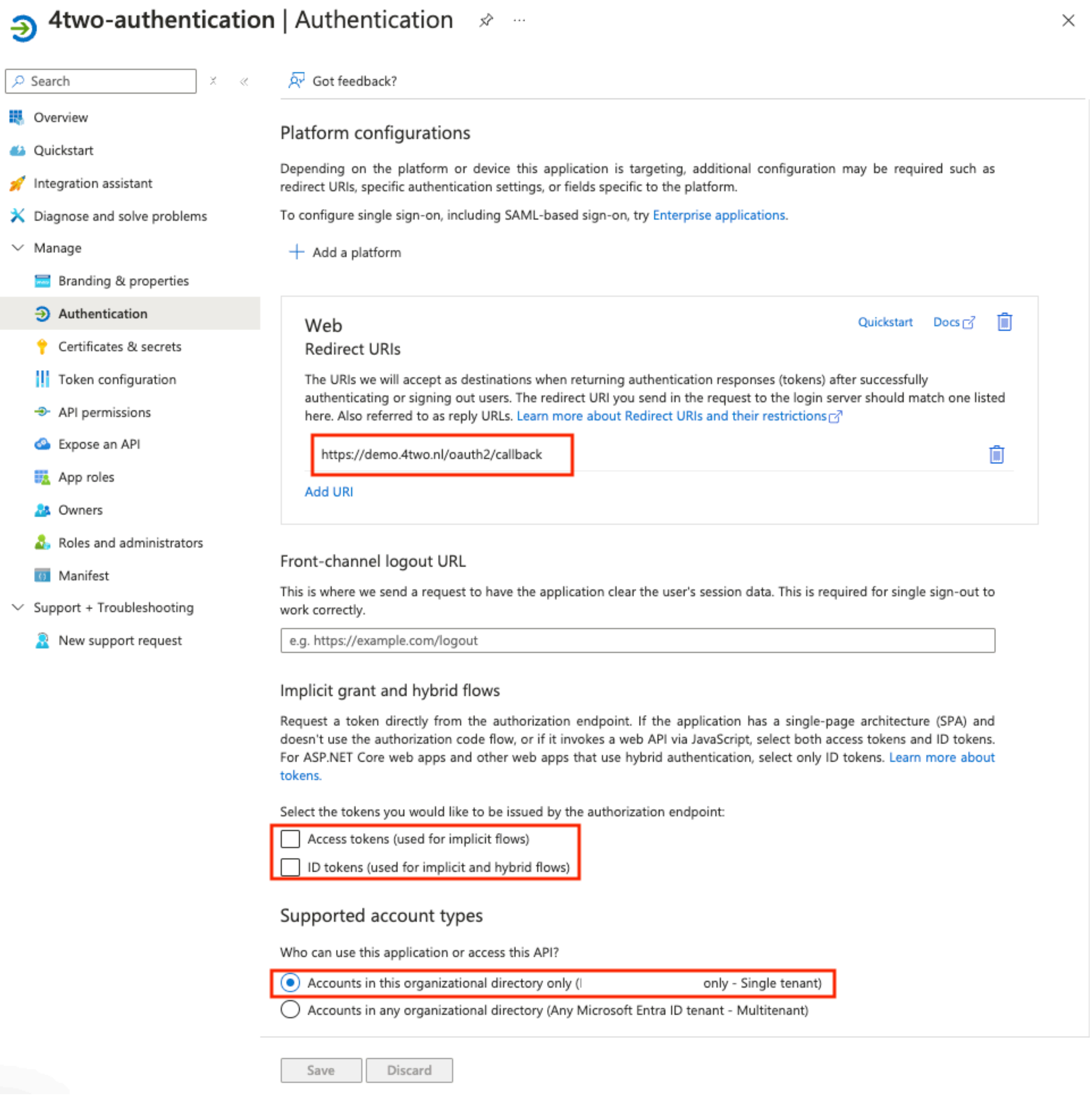
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid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

If you’ve set up the authentication settings correctly, it should look something like this.



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.

To configure single sign-on, including SAML-based sign-on, try Enterprise applications.

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://demo.4two.nl/oauth2/callback

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?

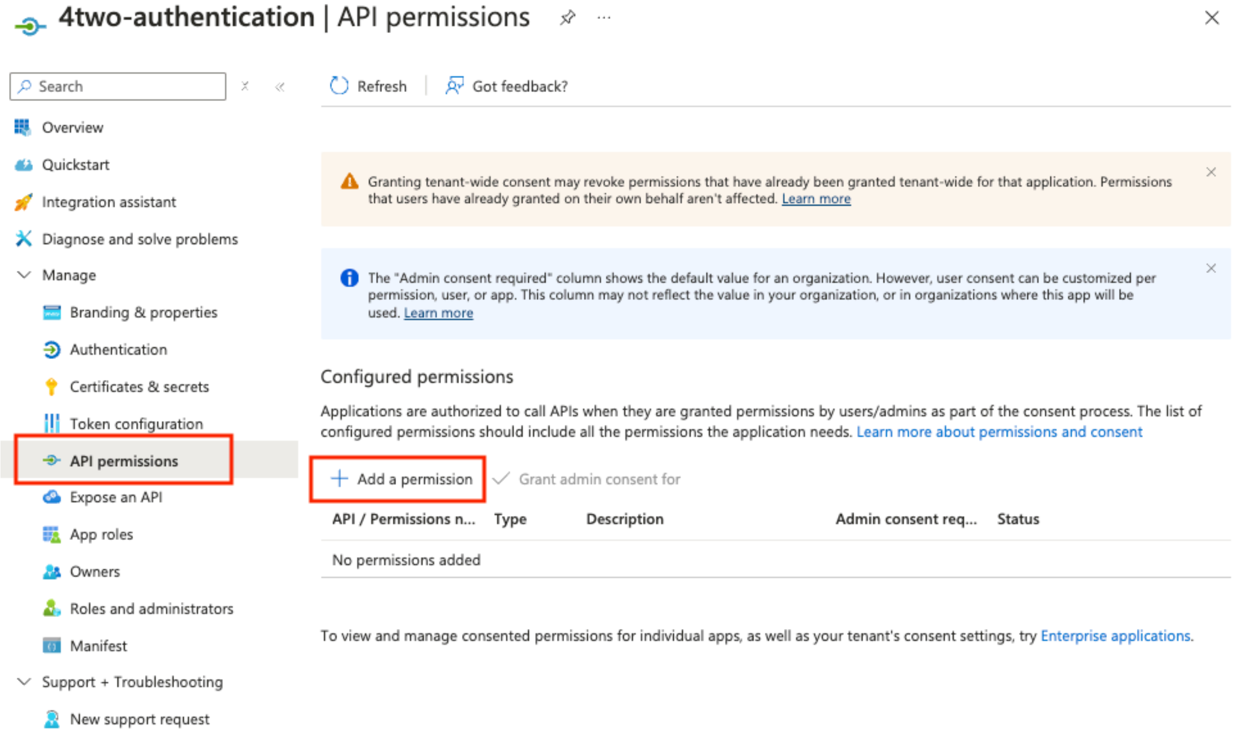
- ● Accounts in this organizational directory only (I only - Single tenant)
- ○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

4.2 CONFIGURE THE API PERMISSIONS

We need to assign permissions to the *Application Registration* for the 4Two site to access the user information of the authenticated user.

4.2.1 Go to the *API permissions panel*

4.2.2 Click *Add a permission*



Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

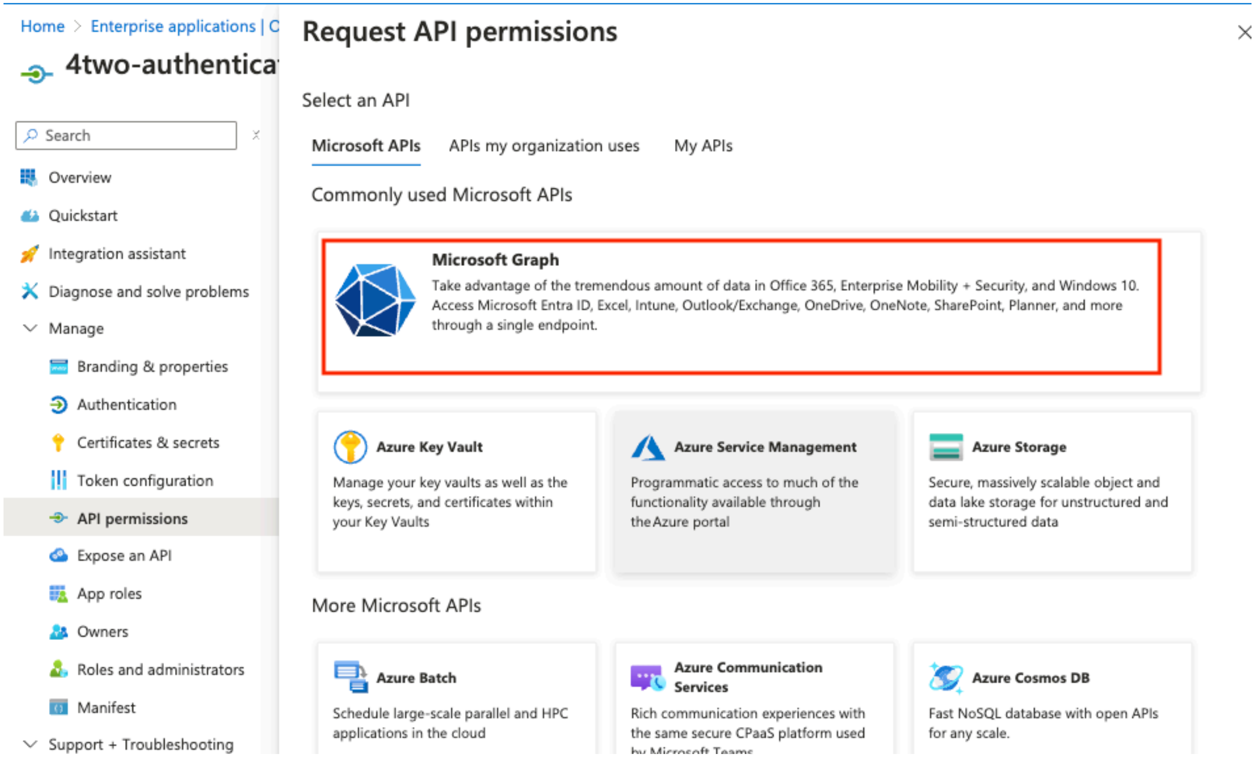
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions n...	Type	Description	Admin consent req...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

4.2.3 Select *Microsoft Graph* -> *Delegated permissions*



Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Key Vault: Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management: Programmatic access to much of the functionality available through the Azure portal

Azure Storage: Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Azure Batch: Schedule large-scale parallel and HPC applications in the cloud

Azure Communication Services: Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Cosmos DB: Fast NoSQL database with open APIs for any scale.

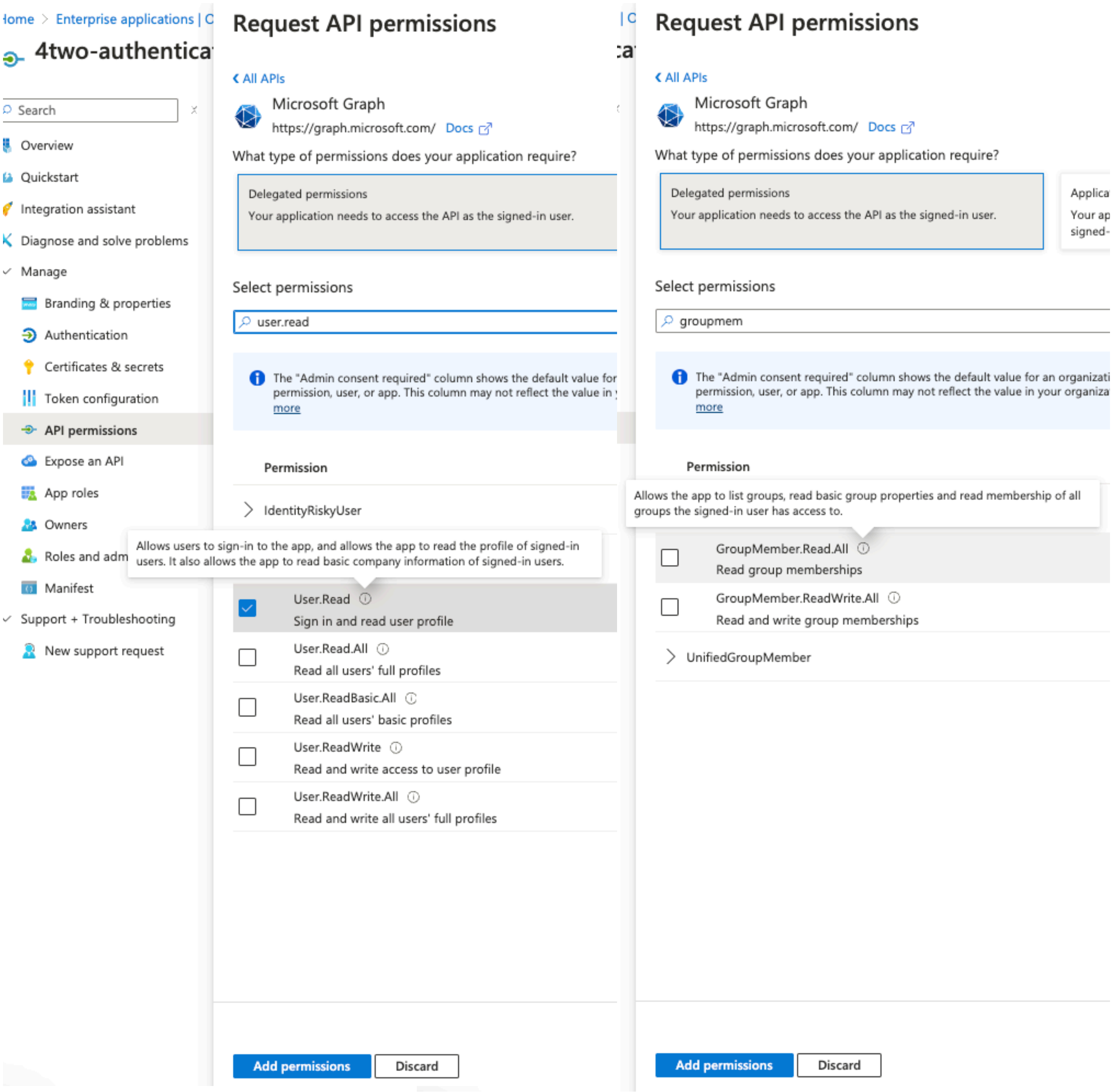
4.2.4 Search the permissions to select the following:

- User.Read

  Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

- Group.Read.All

  Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.



lome > Enterprise applications | C

4two-authentica

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 adm
  - Manifest
- Support + Troubleshooting
  - New support request

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Select permissions

user.read

The "Admin consent required" column shows the default value for permission, user, or app. This column may not reflect the value in more

Permission

> IdentityRiskyUser

Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

☑ User.Read ⓘ
Sign in and read user profile

□ User.Read.All ⓘ
Read all users' full profiles

□ User.ReadBasic.All ⓘ
Read all users' basic profiles

□ User.ReadWrite ⓘ
Read and write access to user profile

□ User.ReadWrite.All ⓘ
Read and write all users' full profiles

Add permissions Discard

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Applica
Your ap
signed-

Select permissions

groupmem

The "Admin consent required" column shows the default value for an organizati permission, user, or app. This column may not reflect the value in your organiza more

Permission

Allows the app to list groups, read basic group properties and read membership of all groups the signed-in user has access to.

□ GroupMember.Read.All ⓘ
Read group memberships

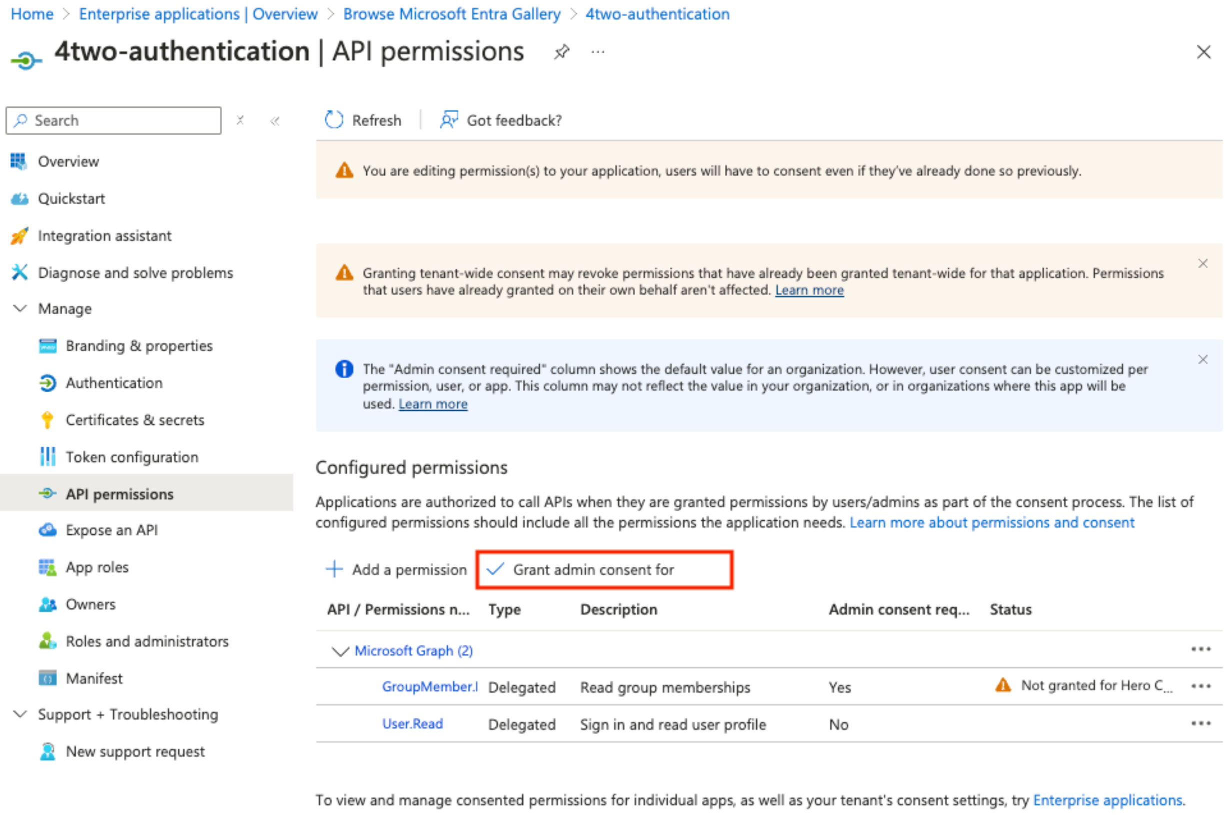
□ GroupMember.ReadWrite.All ⓘ
Read and write group memberships

> UnifiedGroupMember

Add permissions Discard

Then select *Add permissions* to finalize.

4.2.5 *Grant admin consent* for the API -> Select *Yes* for confirmation



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
GroupMember.I	Delegated	Read group memberships	Yes	Not granted for Hero C...
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

5 Generating the application credentials

You need the following information from Microsoft Entra for the 4Two site to make use of this Enterprise Application:

- ***Tenant ID***
- ***Client ID***
- ***Client Secret***

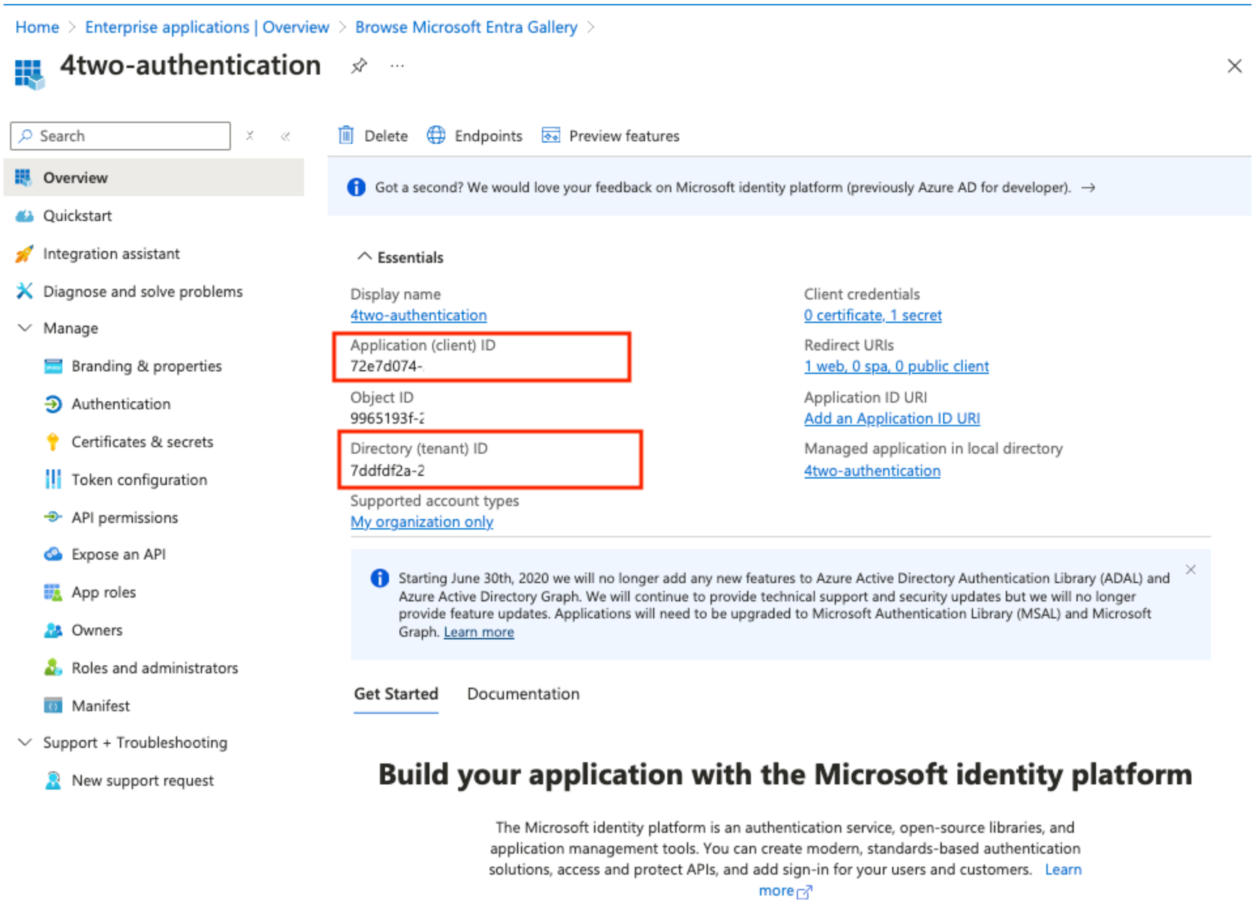
This information can be submitted in the admin panel of your 4Two site.

5.1 Getting the Client ID and and Tenant ID

5.1.1 Go to the *Overview page* of the Application Registration

5.1.2 Copy and write down the Client ID and Tenant ID

You need these values later.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name
4two-authentication

Application (client) ID
72e7d074-

Object ID
9965193f-2

Directory (tenant) ID
7ddfdf2a-2

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
4two-authentication

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

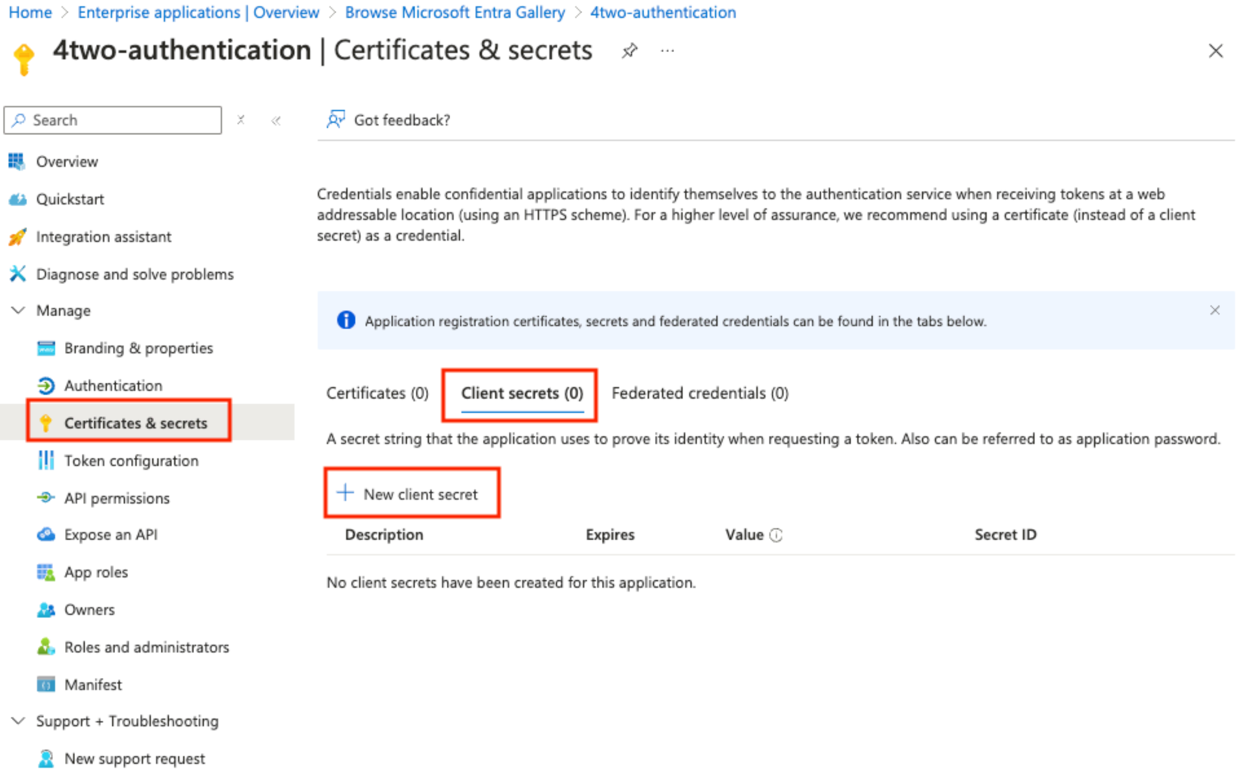
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

5.2 Generating the Client Secret

5.2.1 Go to the *Certificates & Secrets* panel

5.2.2 Select the *Client secrets* tab

5.2.3 Select *New client secret*



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.

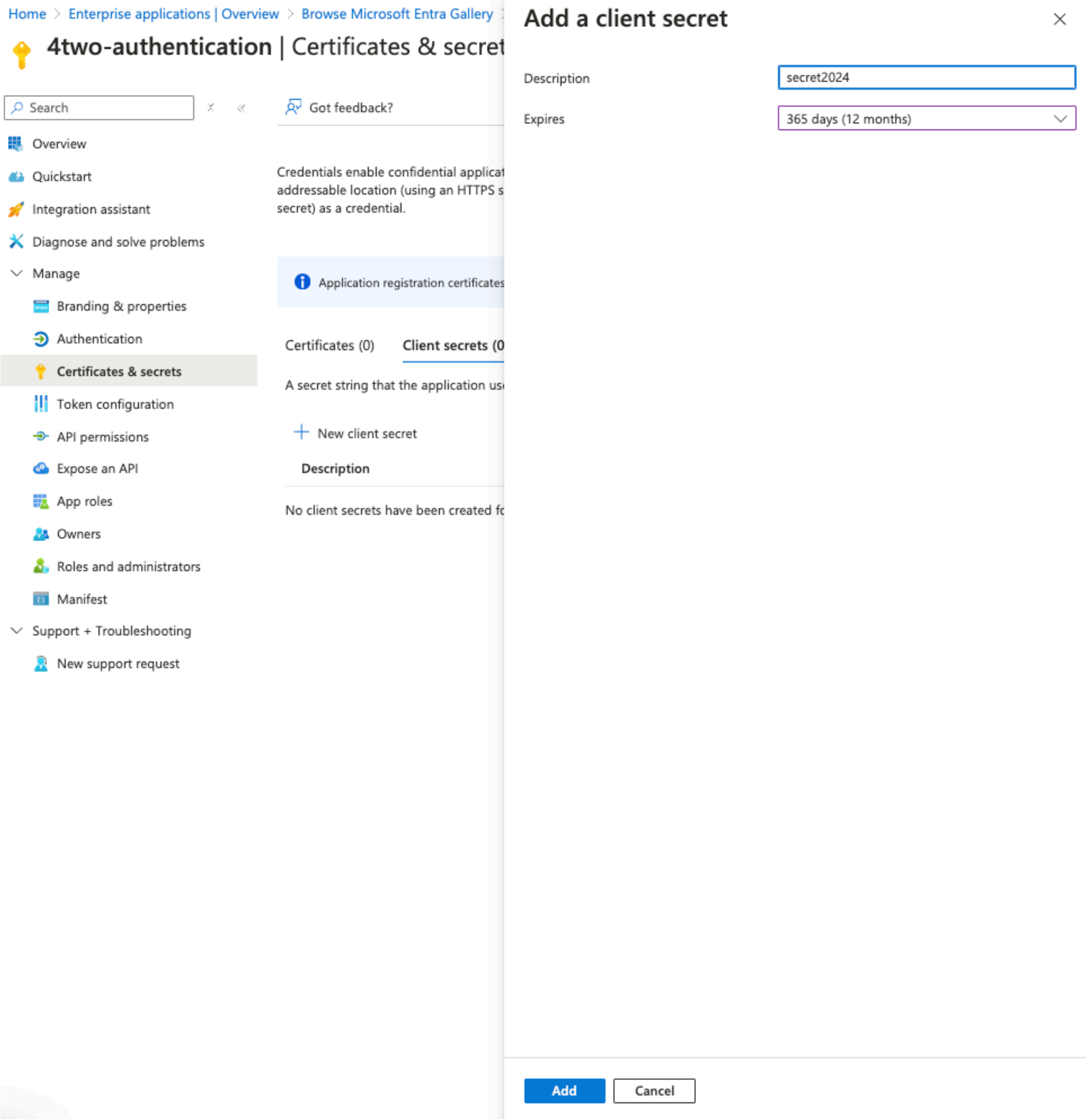
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

5.2.4 Fill in the *description* and select the *expiration*

Note: Refresh the client secret of the Application registration before it expires. Users will no longer be able to login to the 4Two site after it expires.



Credentials enable confidential applicat addressable location (using an HTTPS s secret) as a credential.

Application registration certificates

A secret string that the application us

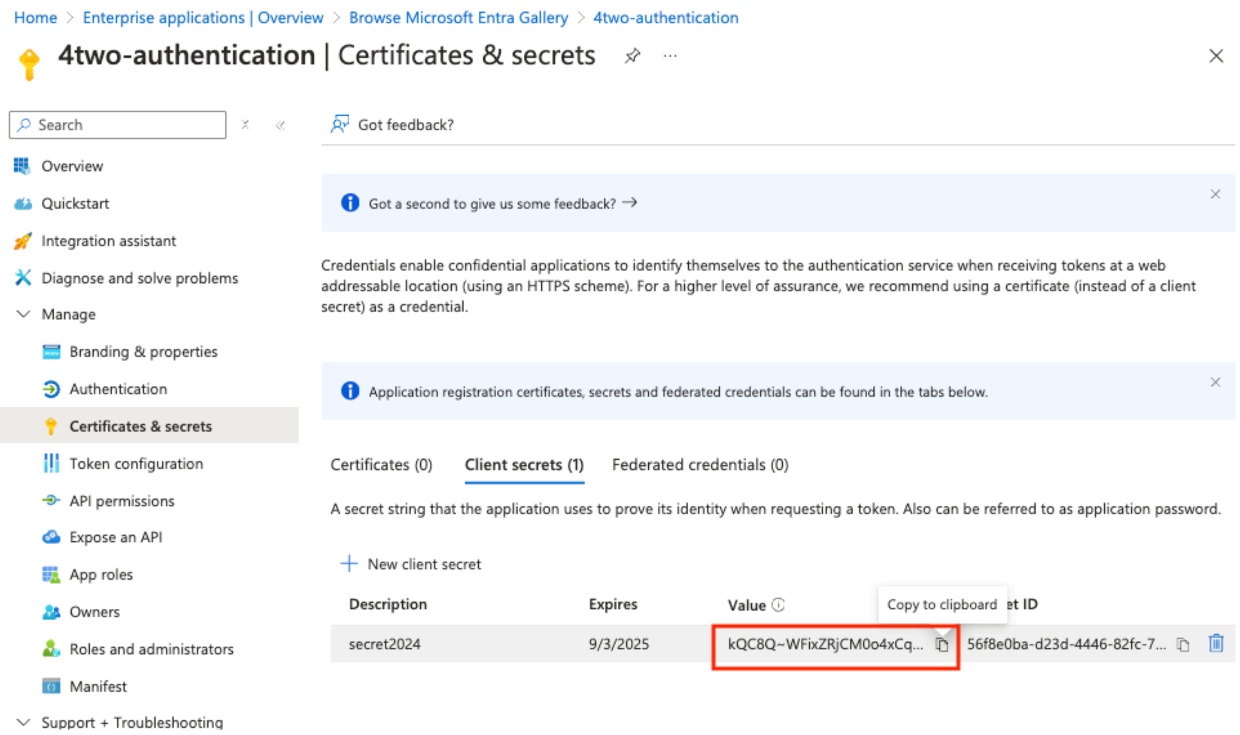
No client secrets have been created fo

Description: secret2024

Expires: 365 days (12 months)

5.2.5 Copy the secret value

This value is needed for step 6.2



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.

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

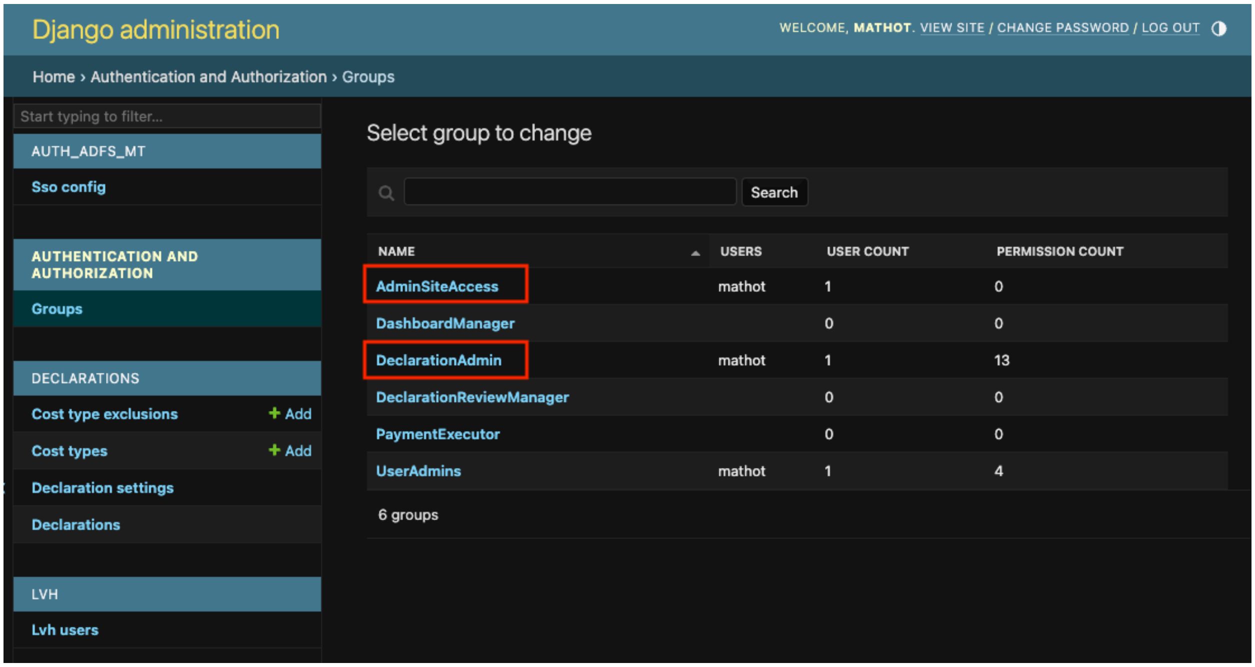
Description	Expires	Value	et ID
secret2024	9/3/2025	kQC8Q~WFixZRjCM0o4xCq...	56f8e0ba-d23d-4446-82fc-7...

6 Configuring SSO in 4two

6.1 Go to the admin page of your 4two site and login

URL: *https://<your-company-name>.4two.nl/admin/*

Note: You need an account with access to the admin page. Your user account needs to be assigned to the *AdminSiteAccess* and *DeclarationAdmin* groups.



Django administration
WELCOME, MATHOT. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Authentication and Authorization › Groups
Start typing to filter...
AUTH_ADFS_MT
Sso config
AUTHENTICATION AND AUTHORIZATION
Groups
DECLARATIONS
Cost type exclusions
+ Add
Cost types
+ Add
Declaration settings
Declarations
LVH
Lvh users
Search

Select group to change

NAME	USERS	USER COUNT	PERMISSION COUNT
AdminSiteAccess	mathot	1	0
DashboardManager		0	0
DeclarationAdmin	mathot	1	13
DeclarationReviewManager		0	0
PaymentExecutor		0	0
UserAdmins	mathot	1	4

6 groups

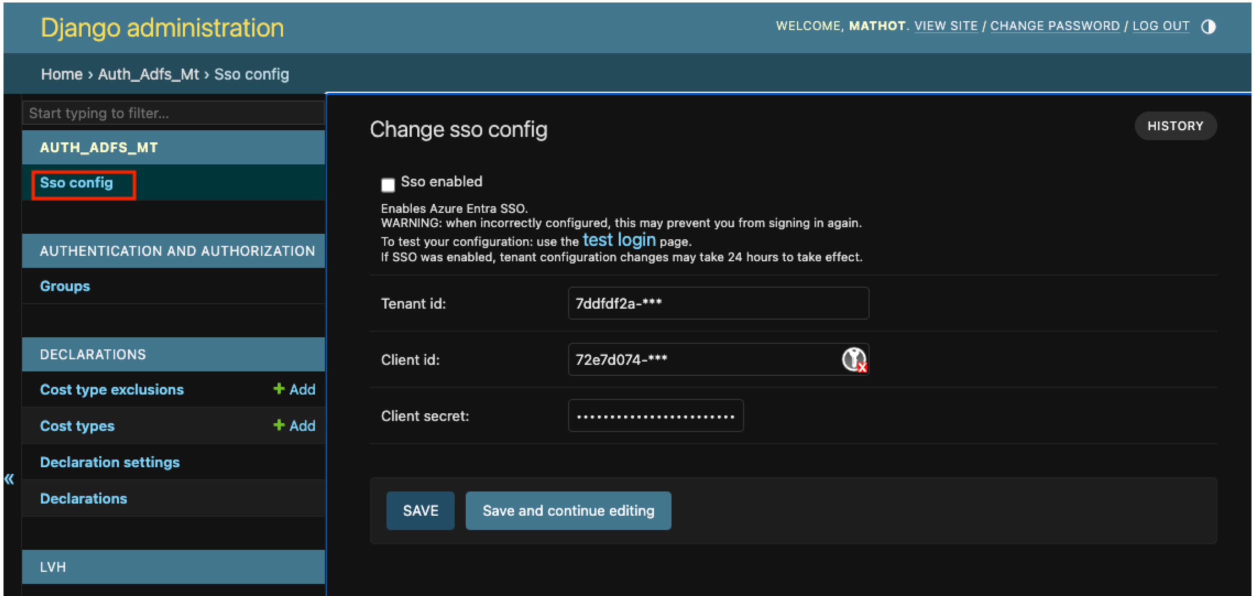
6.2 SET THE AUTH ADFS SSO SETTINGS

6.2.1 Go to the *Sso config* section of the admin page.

6.2.2 Fill in the Tenant ID, Client ID and Client Secret

You obtained these in steps 5.1.2 and 5.2.5

6.2.3 Select Save and continue editing


Django administration
WELCOME, MATHOT. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Auth_Adfs_Mt › Sso config
Start typing to filter...
AUTH_ADFS_MT
Sso config
AUTHENTICATION AND AUTHORIZATION
Groups
DECLARATIONS
Cost type exclusions + Add
Cost types + Add
Declaration settings
Declarations
LVH
HISTORY
SAVE
Save and continue editing

Change sso config

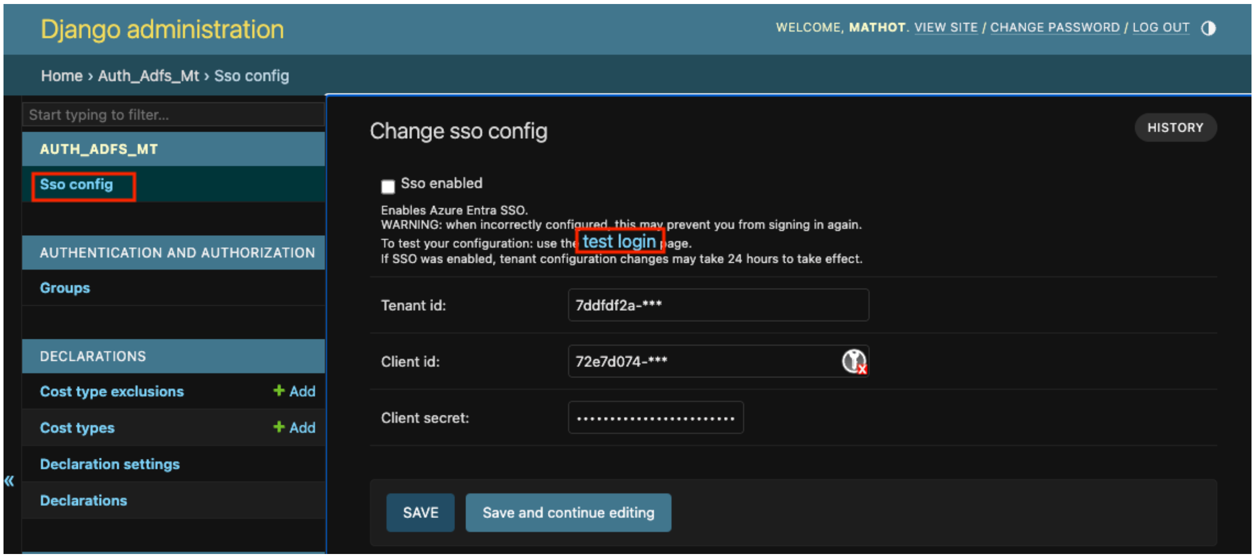
□ Sso enabled

Enables Azure Entra SSO.
WARNING: when incorrectly configured, this may prevent you from signing in again.
To test your configuration: use the test login page.
If SSO was enabled, tenant configuration changes may take 24 hours to take effect.

Tenant id:	7ddfdf2a-***
Client id:	72e7d074-***
Client secret:	••••••••••••••••••••••••

6.3 *FINALLY TEST THE SSO CONNECTION BY CLICKING TEST LOGIN*

This should direct you to Microsoft to login with your Microsoft account. If you are already logged in, you may be logged in instantly and directed to the home page of 4Two.


Django administration
WELCOME, MATHOT. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Auth_Adfs_Mt › Sso config
Start typing to filter...
AUTH_ADFS_MT
Sso config
AUTHENTICATION AND AUTHORIZATION
Groups
DECLARATIONS
Cost type exclusions + Add
Cost types + Add
Declaration settings
Declarations
HISTORY
SAVE
Save and continue editing

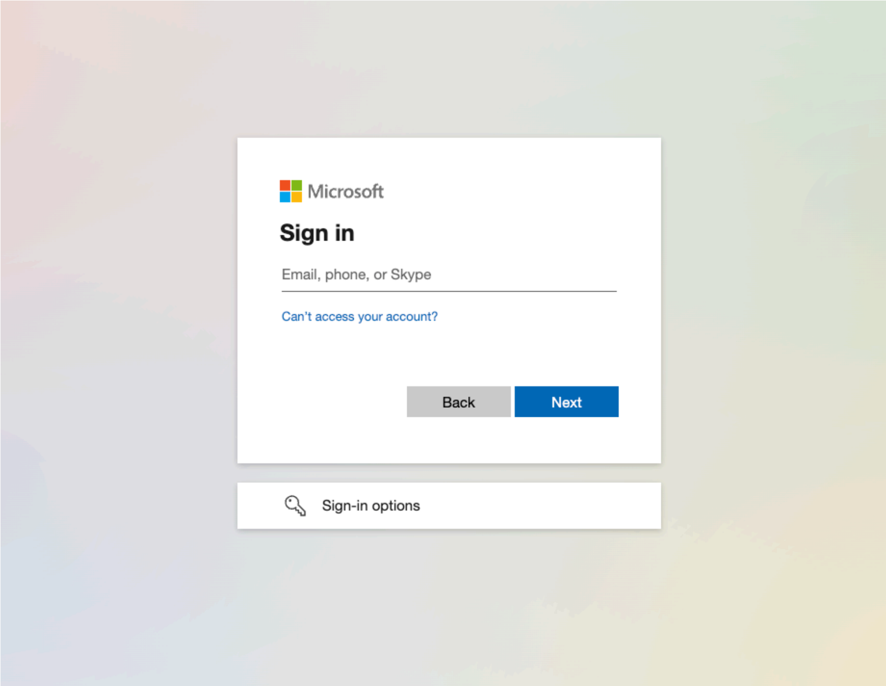
Change sso config

□ Sso enabled

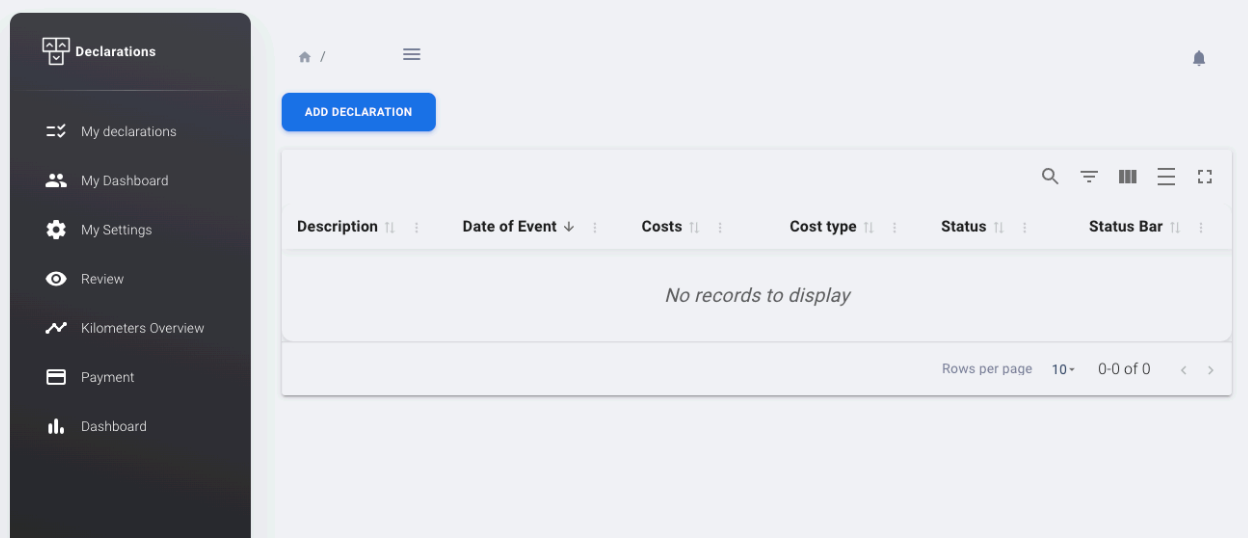
Enables Azure Entra SSO.
WARNING: when incorrectly configured, this may prevent you from signing in again.
To test your configuration: use the test login page.
If SSO was enabled, tenant configuration changes may take 24 hours to take effect.

Tenant id:	7ddfdf2a-***
Client id:	72e7d074-***
Client secret:	••••••••••••••••••••••••

Microsoft login page



Access to the application

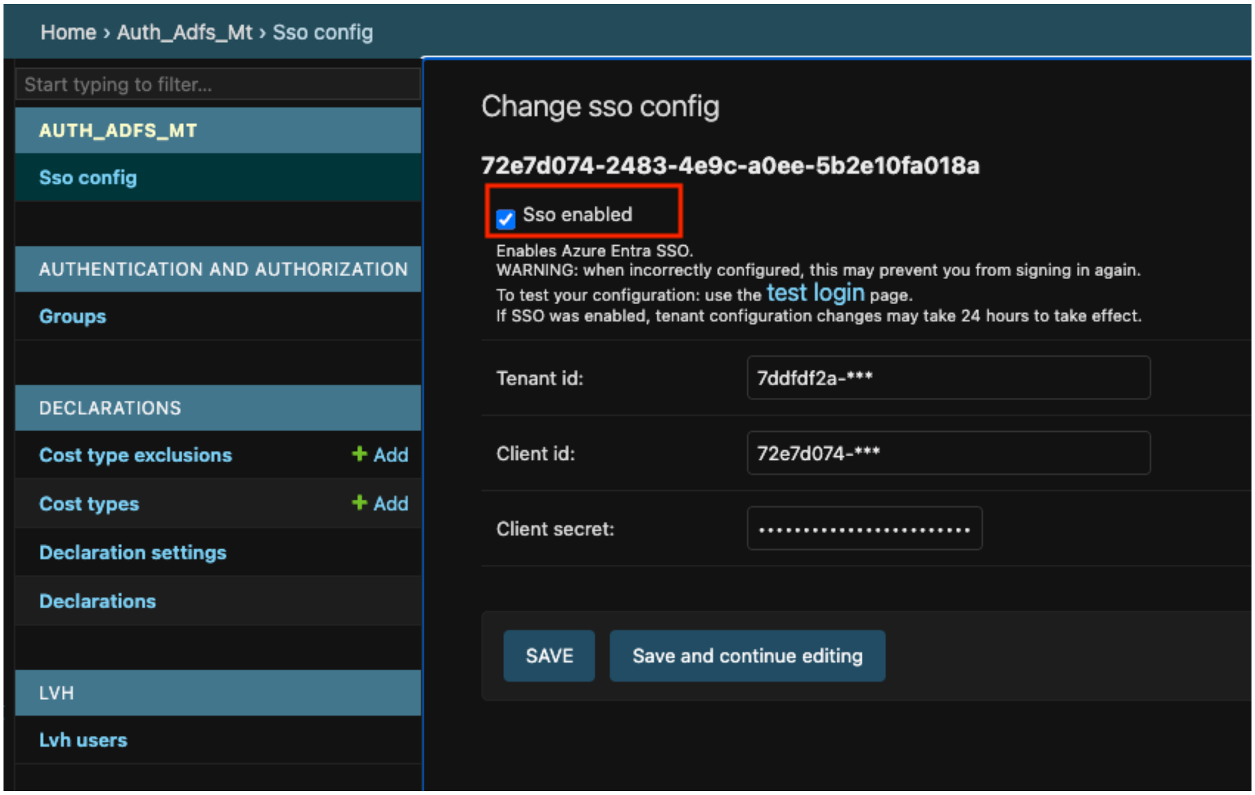


Description	Date of Event ↓	Costs	Cost type	Status	Status Bar

No records to display

6.4 ENABLE SSO

If you have successfully tested the connection, you can enable SSO for the entire organization. Note that this will disable the username-password authentication. You will from now on only be able to login with Microsoft or until SSO is disabled again.


Home › Auth_Adfs_Mt › Sso config
Start typing to filter...
AUTH_ADFS_MT
Sso config
AUTHENTICATION AND AUTHORIZATION
Groups
DECLARATIONS
Cost type exclusions + Add
Cost types + Add
Declaration settings
Declarations
LVH
Lvh users
Change sso config
SAVE
Save and continue editing

72e7d074-2483-4e9c-a0ee-5b2e10fa018a

☑ Sso enabled

Enables Azure Entra SSO.
WARNING: when incorrectly configured, this may prevent you from signing in again.
To test your configuration: use the test login page.
If SSO was enabled, tenant configuration changes may take 24 hours to take effect.

Tenant id: 7ddfdf2a-***

Client id: 72e7d074-***

Client secret: ························