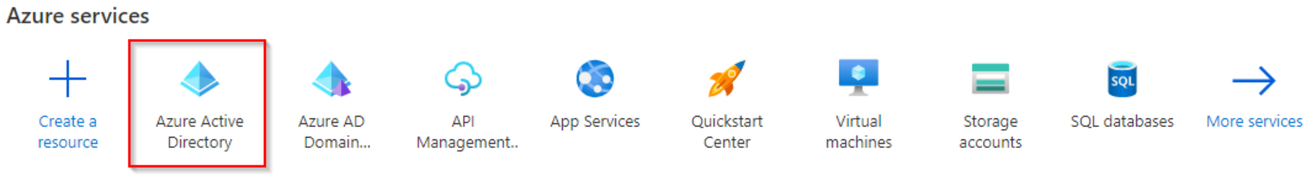
1 Quick Guide Azure Authentication for IMS

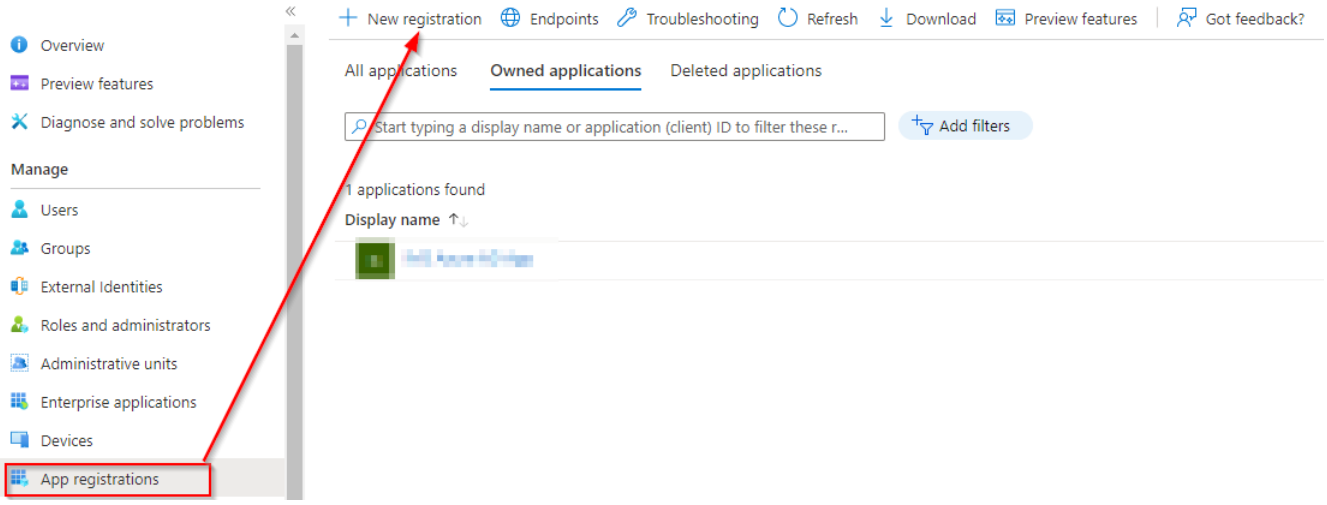
1.1 Disclaimer:

Not every step is described with text. This quick manual requires a bit of Azure AD knowledge to follow the steps on the pictures correctly.

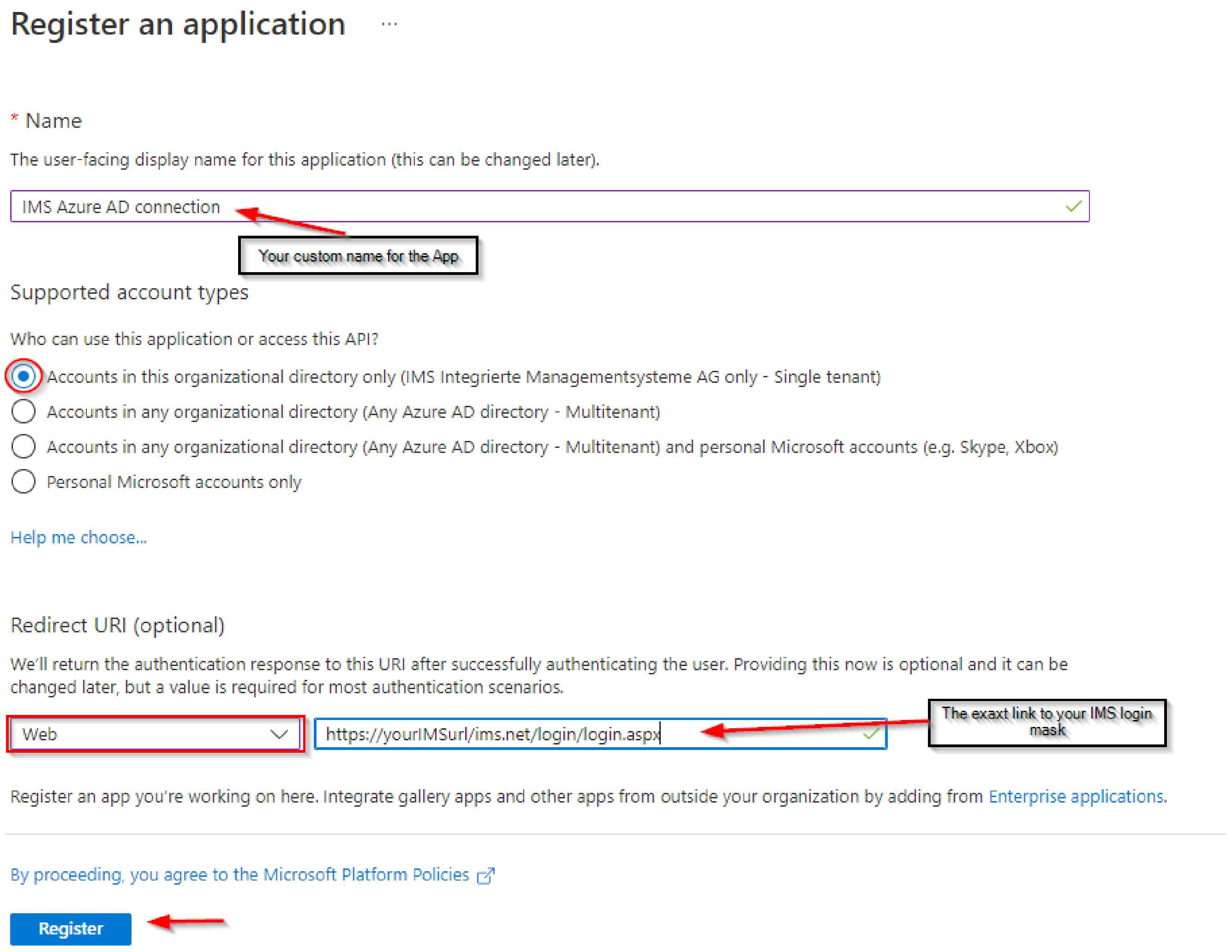
1.2 Change to the Azure AD blade:



1.3 Register an Azure AD app:



Klick on + New registration



Register an application ···

* Name

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

IMS Azure AD connection ✓

Your custom name for the App

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (IMS Integrierte Managementsysteme AG only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - 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://yourIMSurl/ims.net/login/login.aspx ✓

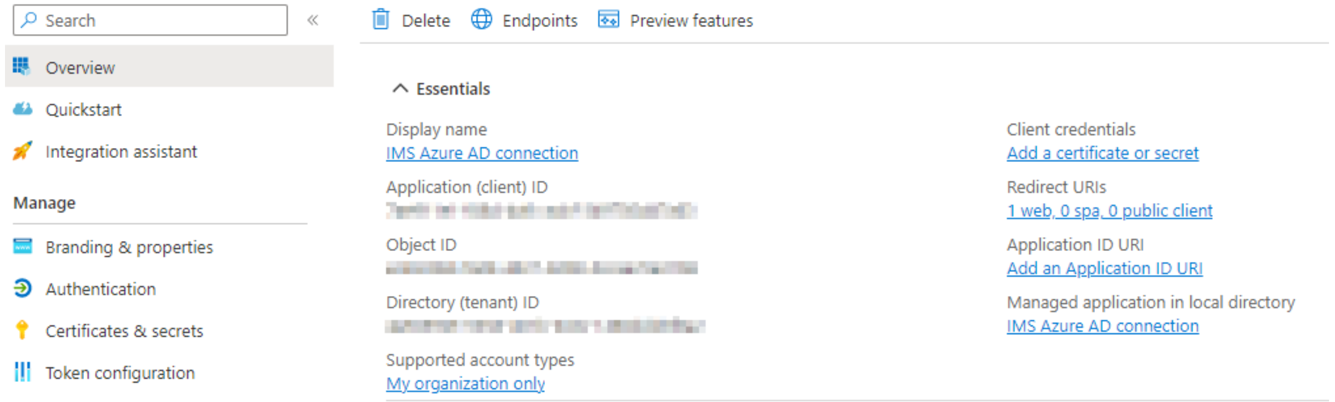
The exaxt link to your IMS login mask

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

Please make sure that the redirect URL points to your IMS login site, ending on …./login/login.aspx.

After clicking register, you will see a summary:



Essentials

Display name
IMS Azure AD connection

Application (client) ID
[redacted]

Object ID
[redacted]

Directory (tenant) ID
[redacted]

Supported account types
My organization only

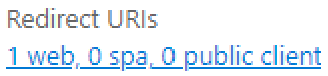
Client credentials
Add a certificate or secret

Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
IMS Azure AD connection

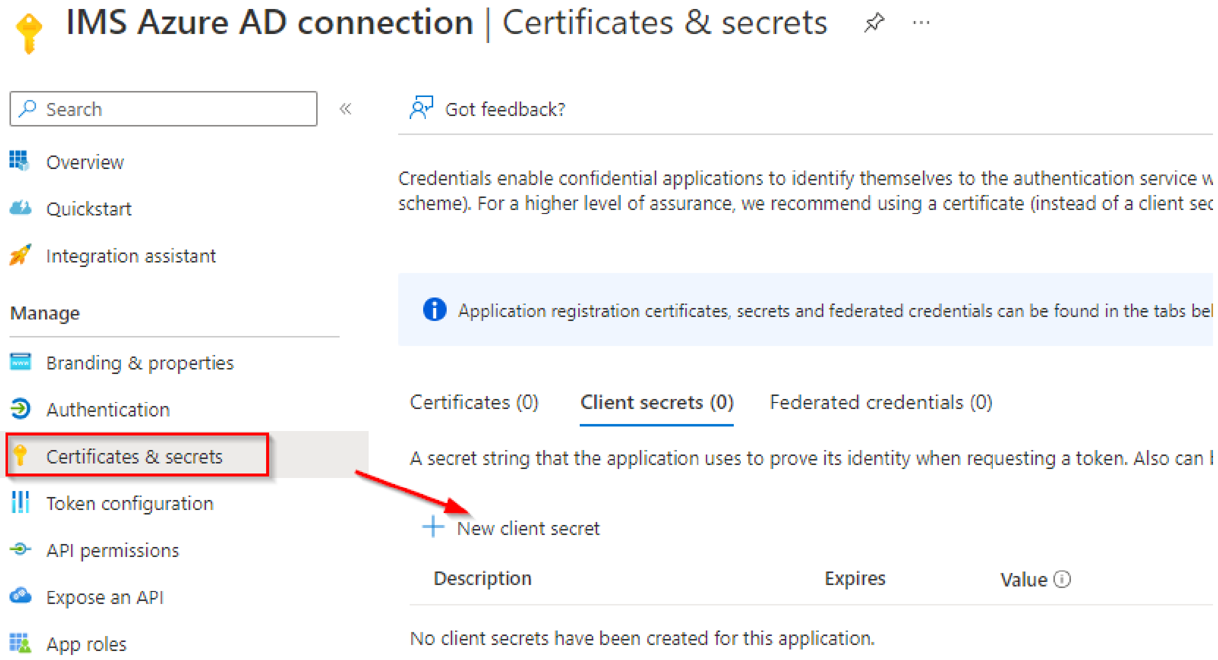
A redirect URL can be added/changed here



Redirect URIs
1 web, 0 spa, 0 public client

1.4 Add a secret to the app

**We (IMS) need that secret to properly connect the software with Azure AD.
Change to the blade “Certificates & secrets”, there, click on “New client secret”.**



IMS Azure AD connection | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service w
scheme). For a higher level of assurance, we recommend using a certificate (instead of a client sec

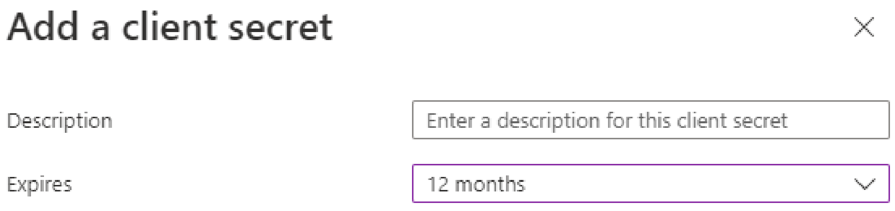
Application registration certificates, secrets and federated credentials can be found in the tabs bel

A secret string that the application uses to prove its identity when requesting a token. Also can b

Description	Expires	Value ⓘ

No client secrets have been created for this application.

Enter a Description and an expire date however you prefer. We (IMS) need to know when it expires to keep the service running properly.

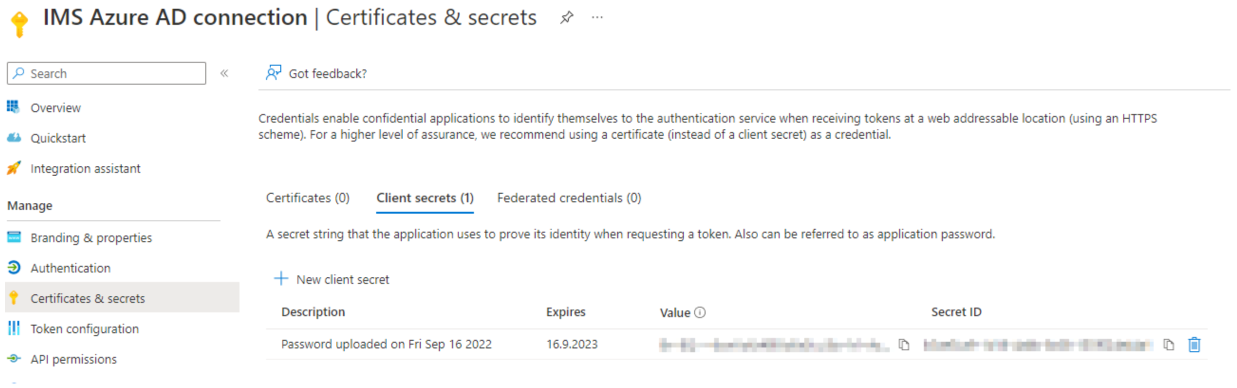


Add a client secret

Description: Enter a description for this client secret

Expires: 12 months

After you click create, you will see your created client secret:



IMS Azure AD connection | Certificates & secrets

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.

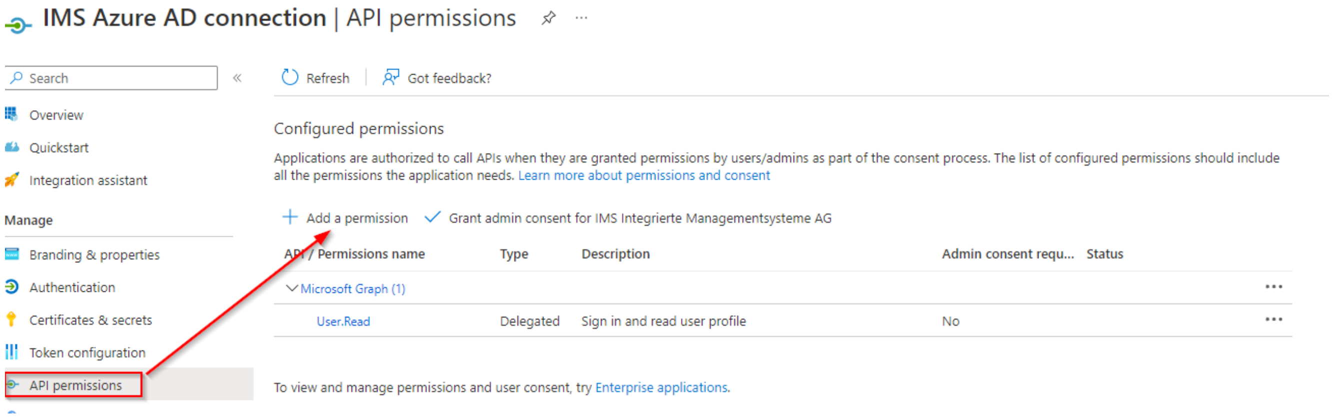
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
Password uploaded on Fri Sep 16 2022	16.9.2023	[redacted]	[redacted]

Keep in mind that you see the Value in cleartext only once! Copy it somewhere safe and trusted, or send it to us directly. After the page gets refreshed its starred out and can’t be accessed or copied again.

1.5 API permissions

Change to the blade “API permissions”:



IMS Azure AD connection | API permissions

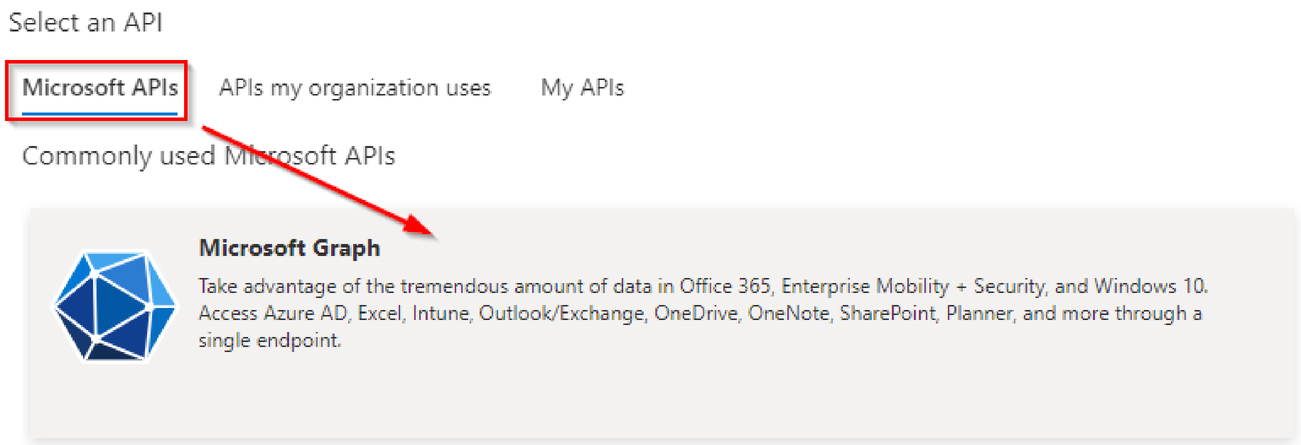
Configured permissions

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

+ Add a permission
✓ Grant admin consent for IMS Integrierte Managementsysteme AG

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.



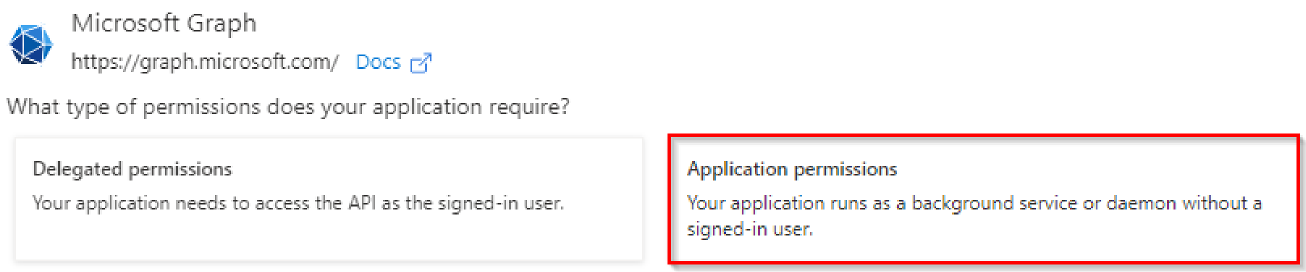
Select an API

Commonly used Microsoft APIs

Microsoft Graph

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

For this API please select application permissions.



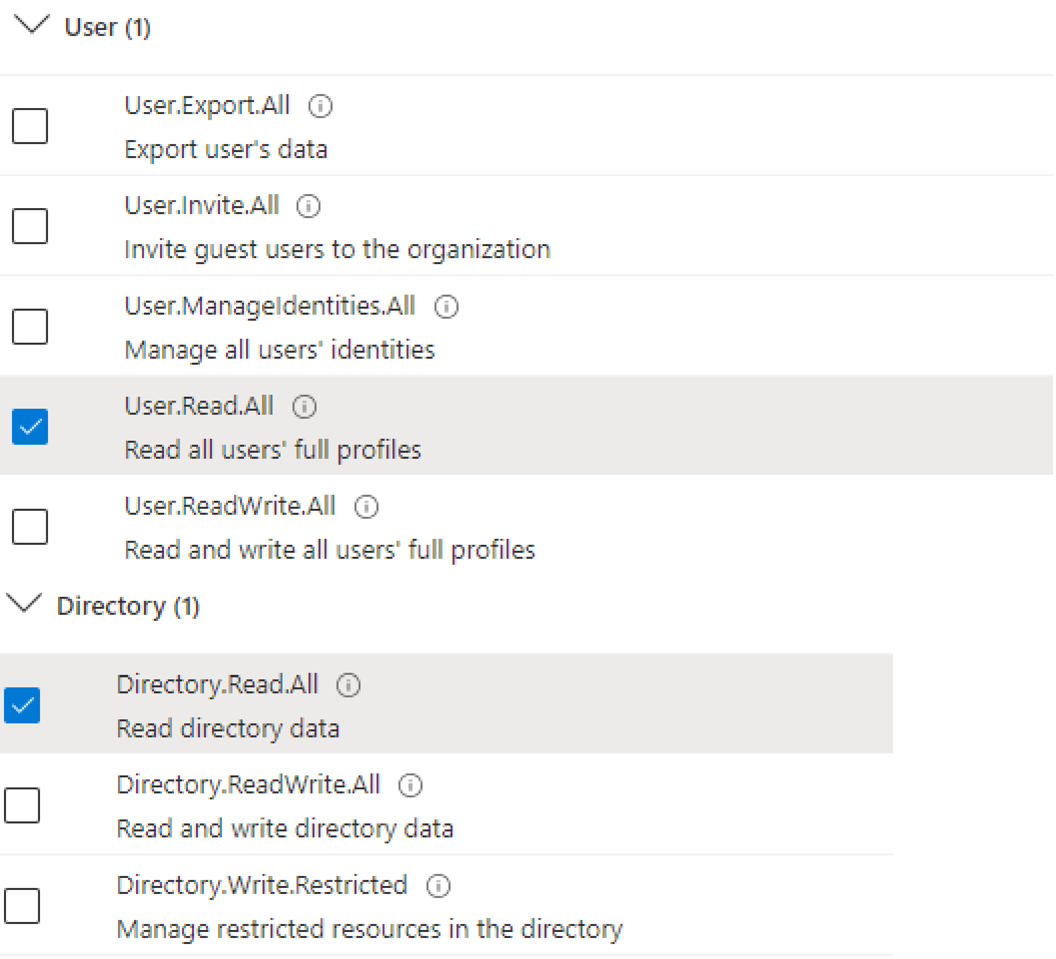
Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

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

Application permissions
Your application runs as a background service or daemon without a signed-in user.

The rights this app needs:



User (1)

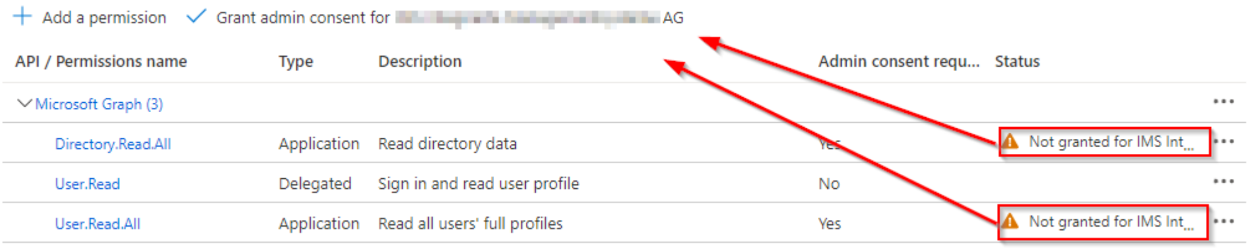
- ☐ User.Export.All ⓘ
  Export user's data
- ☐ User.Invite.All ⓘ
  Invite guest users to the organization
- ☐ User.ManageIdentities.All ⓘ
  Manage all users' identities
- ☑ User.Read.All ⓘ
  Read all users' full profiles
- ☐ User.ReadWrite.All ⓘ
  Read and write all users' full profiles

Directory (1)

- ☑ Directory.Read.All ⓘ
  Read directory data
- ☐ Directory.ReadWrite.All ⓘ
  Read and write directory data
- ☐ Directory.Write.Restricted ⓘ
  Manage restricted resources in the directory

To finish: Add permissions

Afterwards, grant admin consent (this should need to be done just once):

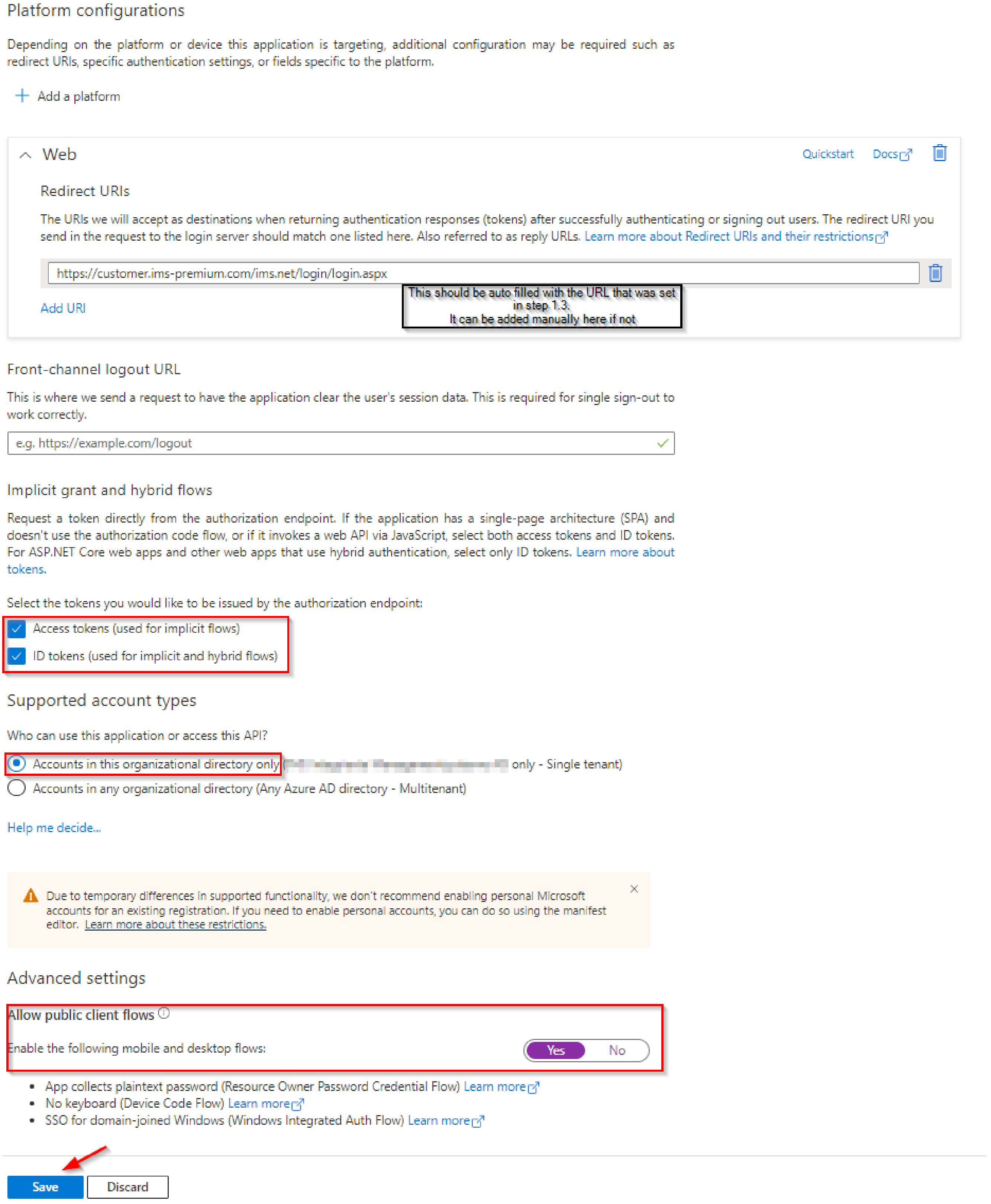


+ Add a permission ✓ Grant admin consent for [redacted] AG

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for IMS Int...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for IMS Int...

1.6 Authentication

Change to the blade 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://customer.ims-premium.com/ims.net/login/login.aspx

This should be auto filled with the URL that was set in step 1.3.
It can be added manually here if not

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 ([redacted] only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

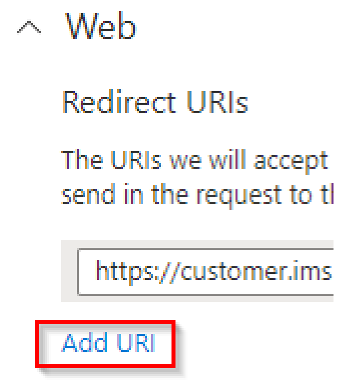
Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

You can add additional URLS (IMSEdu for example) here:



Web

Redirect URIs

The URIs we will accept
send in the request to tl

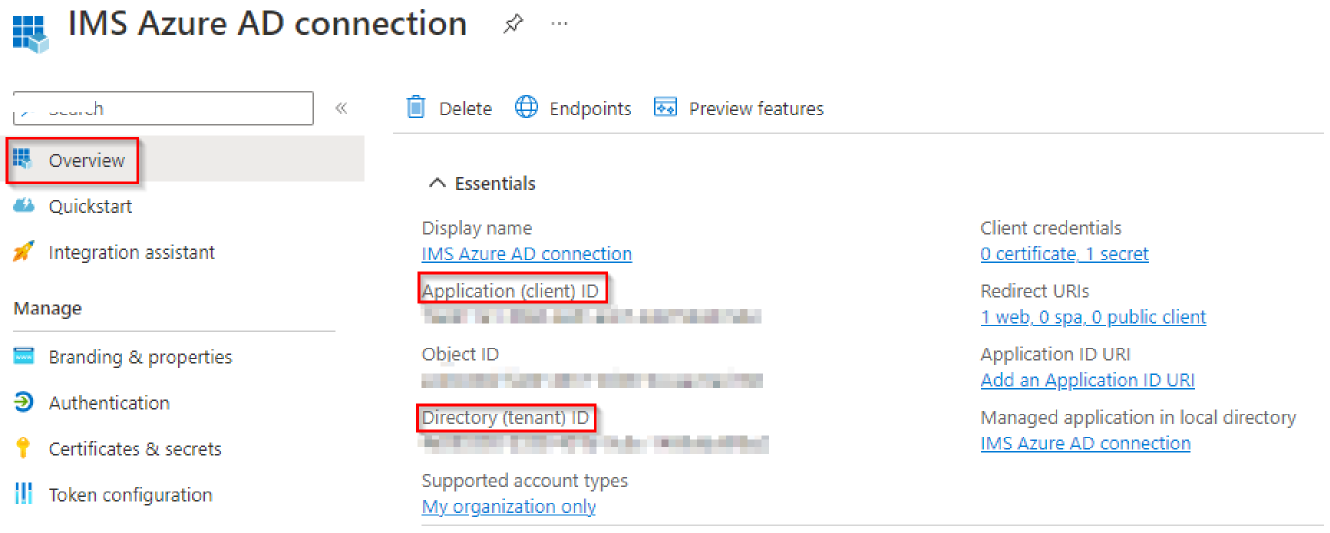
https://customer.ims

1.7 Needed Infos

For the software side of the configuration, we (IMS) need:

-Tenant ID
-App ID
-App client secret
-Redirect URL
-Username & Password of a granted user (if App auth. is set to delegate)

Check the “Overview” blade for the Tenant and AP id:



IMS Azure AD connection

Display name
IMS Azure AD connection

Application (client) ID
[redacted]

Object ID
[redacted]

Directory (tenant) ID
[redacted]

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
IMS Azure AD connection