Microsoft Entra ID SSO for Proxmox

> **Prerequisites:** Ability to create an app registration with delegated standard rights. Proxmox should be installed and access to the Datacenters Realms section should be possible.

Proxmox allows various external authentication services via protocols such as Active Directory, LDAP or OpenID Connect. We will use the latter for the Microsoft Entra ID connection and SSO functionality.

Limitations

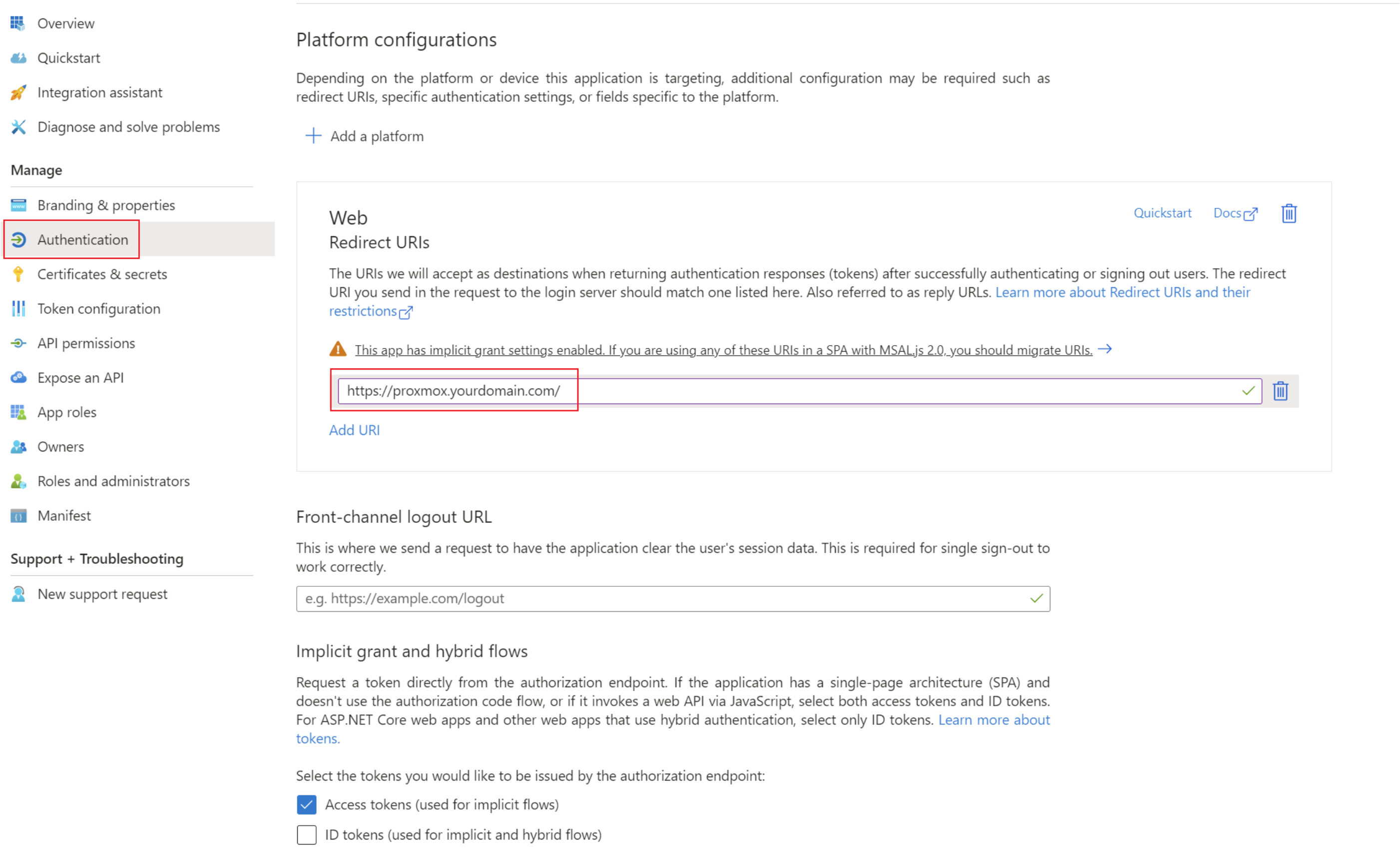
Proxmox allows the automatic creation of user objects, but is otherwise relatively limited compared to other applications, as it does not use the OAUTH 2.0 standard but only handles logins via Open ID Connect. These certain limitations must be taken into account when introducing this setup.

In addition, logins will only be possible for the Webgui. The login on the individual cluster nodes is still regulated via the Linux authentication of the individual hosts. This means that no console connections can be made to the host shells with the Microsoft Entra ID user objects.

Create App Registration

First, an app registration including client secret must be created in Microsoft Entra ID. All settings can be left at the default values. Important settings are the Redirect URIs under the Authentication tab. Set these URIs to your external or internal domain on which Proxmox is available. These URIs will be used for Microsoft Entra ID to know where to redirect the user in case of successful logins.

- **Authentication Type:** Web
- **Redirect URIs:** https://proxmox.yourdomain.com/



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.

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. →

https://proxmox.yourdomain.com/

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.

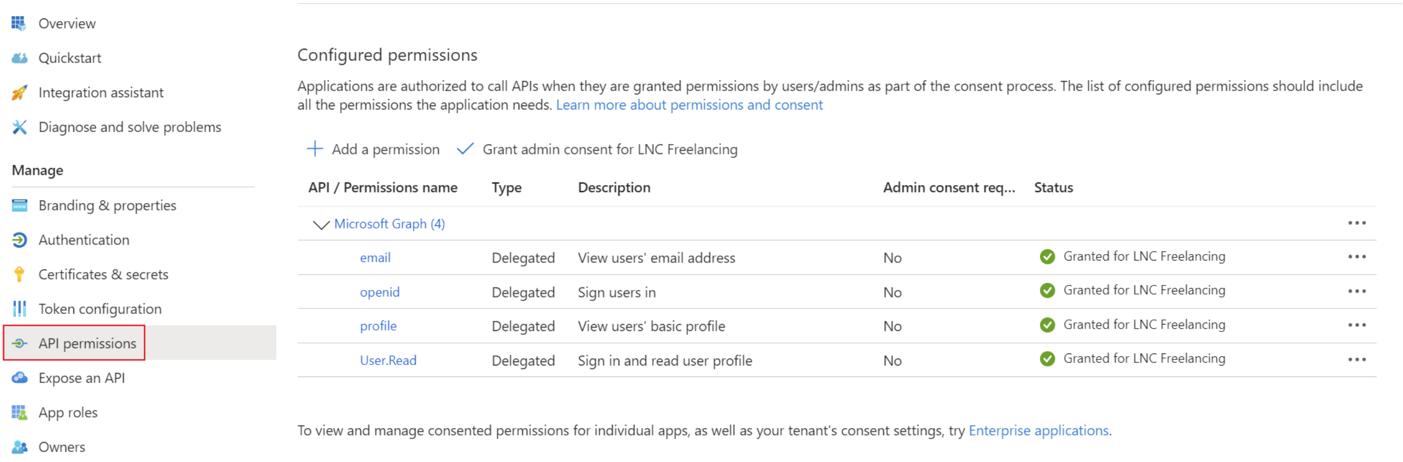
Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

Add the corresponding permissions for OpenID Connect as delegated permissions and grant admin consent for your tenant.

- **Permissions:** Delegated OpenId permissions (email, offline_access, openid, profile)



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 name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
email	Delegated	View users' email address	No	✓ Granted for LNC Freelancing
openid	Delegated	Sign users in	No	✓ Granted for LNC Freelancing
profile	Delegated	View users' basic profile	No	✓ Granted for LNC Freelancing
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for LNC Freelancing

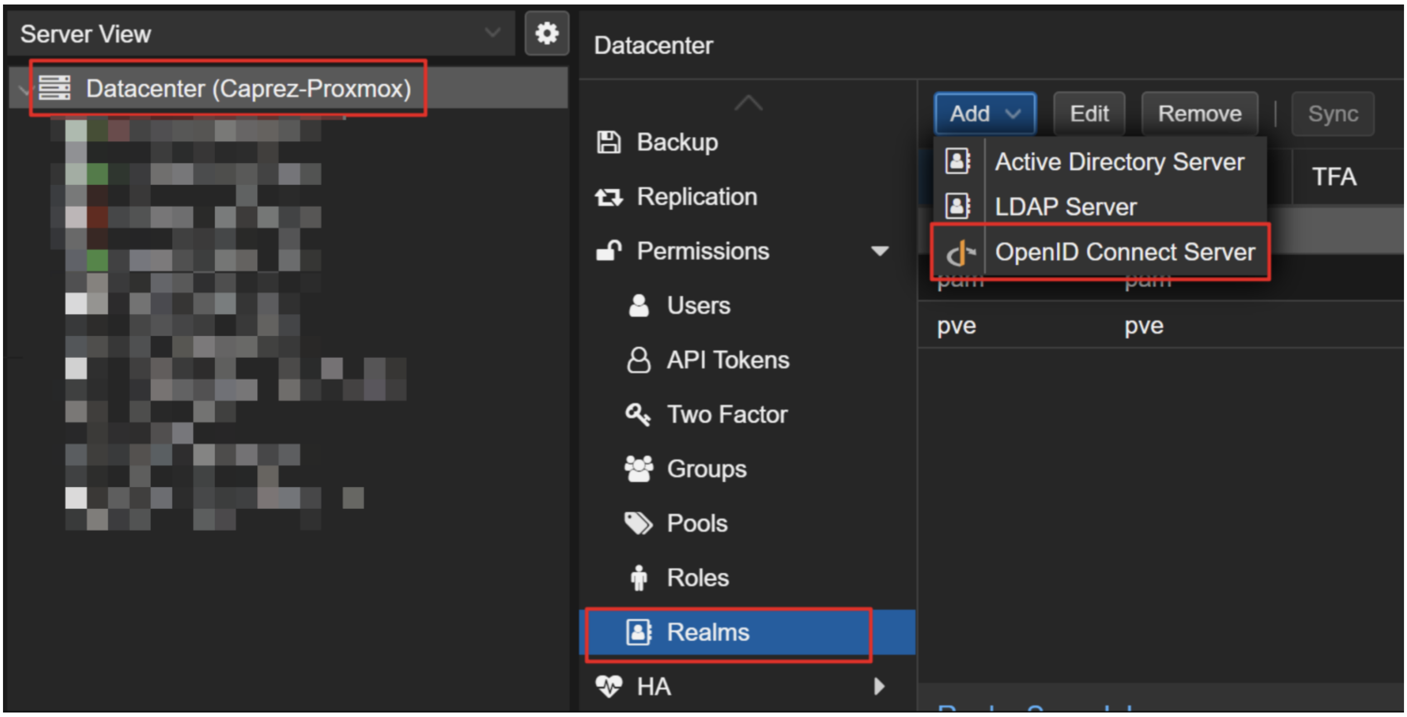
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Create a client secret for the application and save the tenant ID, application ID and client secret in your password manager. You can find instructions for this information here: Get app details and grant permissions to app registration

Setup Microsoft Entra ID in Proxmox Realm

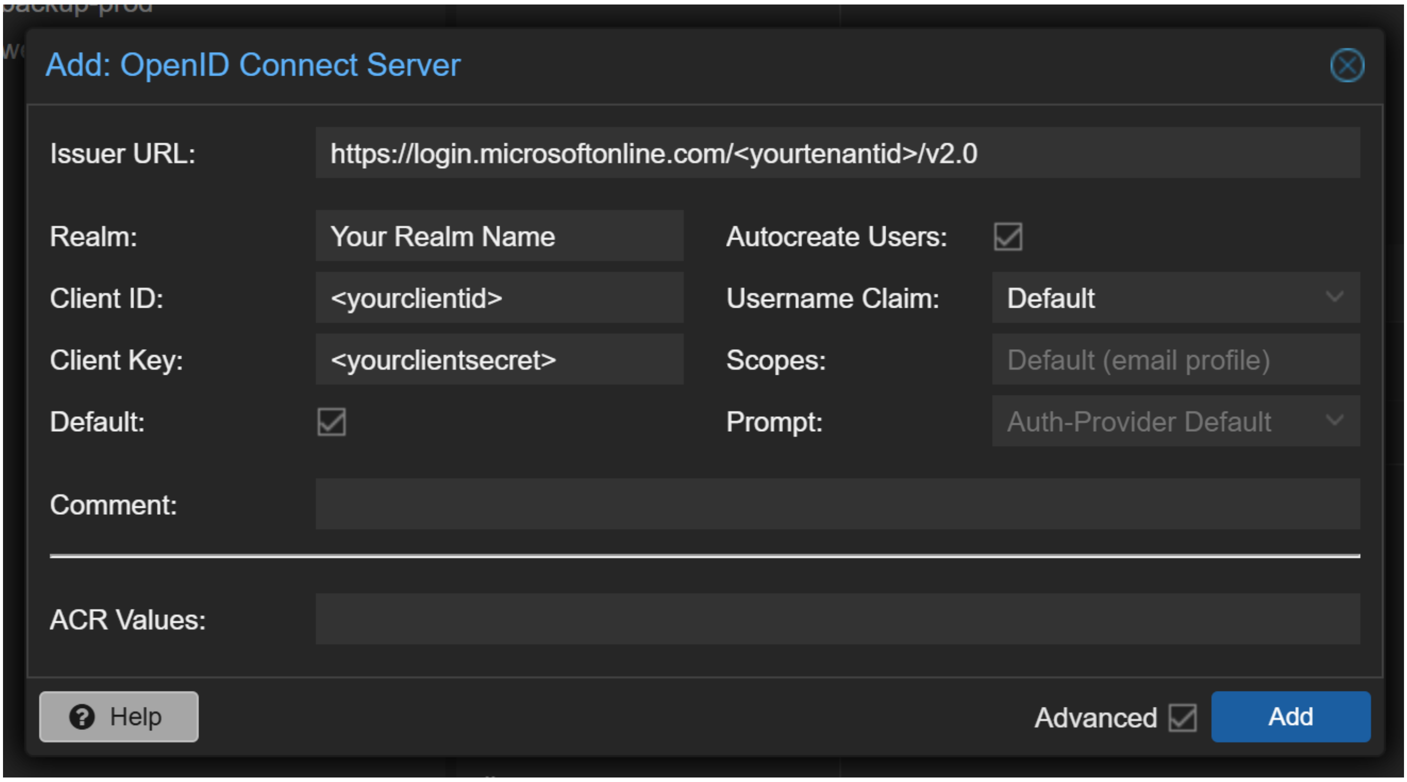
This step requires the authentication details TenantID, ClientID, Client Secret from the first step.

In the Proxmox web interface select "Datacenter" -> "Realms" -> "Add" -> "OpenID Connect Server". There you can enter the credentials from Microsoft Entra ID. Enter the information as described here:



- **Issuer URL:** https://login.microsoftonline.com/<yourtenantid>/v2.0
- **Realm:** This is the id of the installed authentication provider. The name must be lower case and without special characters.
- **Client ID:** Enter your ClientID from the App Registration of your Microsoft Entra ID.
- **Client Key:** Here you have to enter the Client Secret.
- **Default:** If this box is checked, the default auth provider on the sign in screen will be this method.
- **Autocreate Users:** If this is enabled all user who have permission to sign in to your App Registration, are automatically signed up as user objects in Proxmox. As you can still manage permissions within the App Registration this is usually recommended.
- **Scopes:** This allows you to receive multiple parameters from the Microsoft Entra ID user object. The Access Token is requested with these scopes at login. The default values are usually sufficient.
- **Prompt:** This setting defines which action Proxmox should perform when users log in. The default options are sufficient for the Microsoft Entra ID login.
- **Comment:** Enter a name that will be displayed to the end user on the login screen in the auth provider selection.

After these settings are properly configured your users should be able to sign into Proxmox web interface. After sign in the default grouping, role and permissions mechanisms from Proxmox take place.



Add: OpenID Connect Server

Issuer URL: https://login.microsoftonline.com/<yourtenantid>/v2.0

Realm:	Your Realm Name	Autocreate Users:	☑
Client ID:	<yourclientid>	Username Claim:	Default
Client Key:	<yourclientsecret>	Scopes:	Default (email profile)
Default:	☑	Prompt:	Auth-Provider Default

Comment:

ACR Values:

Advanced ☑

Revision #6
Created 19 July 2024 12:15:16
Updated 22 July 2024 12:27:36 by Luca Noah Caprez