

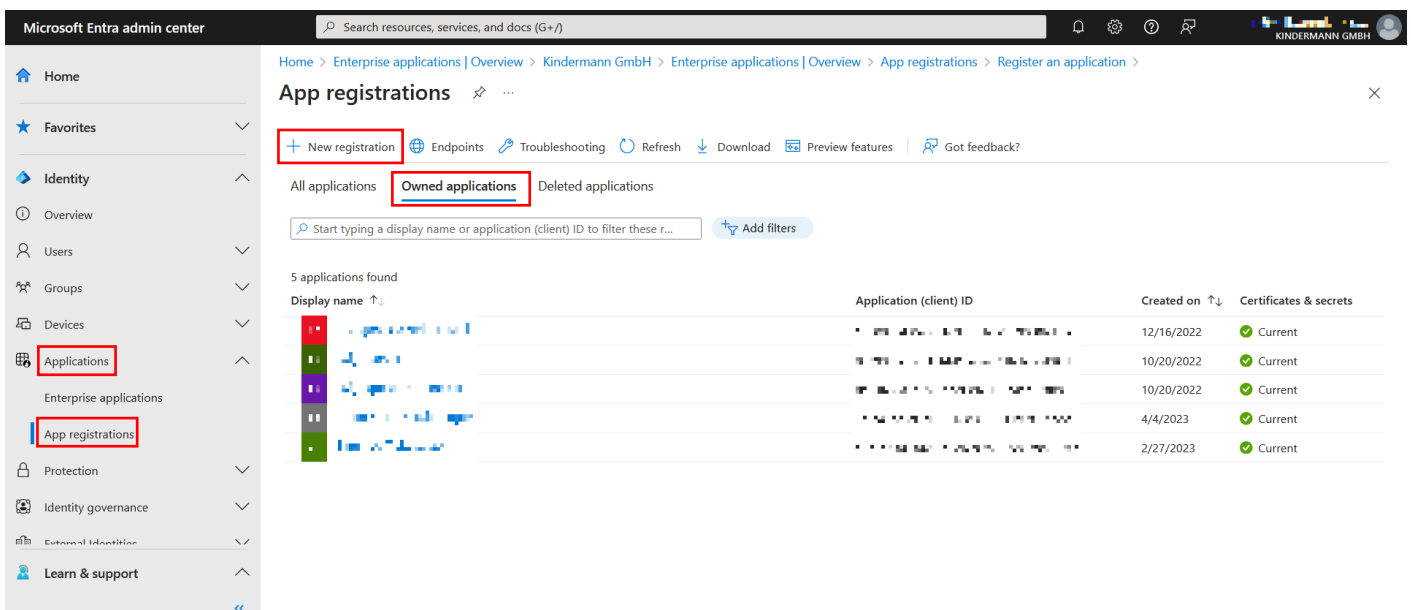
## Introduction

The following document describes the setup of an "Enterprise Application", which is necessary for the use of OpenSpaces in combination with Microsoft 365 and Exchange Online. After successful setup, you will receive the parameters for logging the OpenSpaces service to the Exchange Server using **Modern Auth** (OAuth2). These can then be entered in the Windows Setup Tool of OpenSpaces.

## Creating the Enterprise Application

The Enterprise Application is set up in Microsoft Entra ID (formerly Azure Active Directory). This can be reached after logging in with an administrator account under <https://entra.microsoft.com/>. Under "Applications", click on "App registrations" and then on "Owned applications".

Now click on "+ New registration" and follow the next steps.

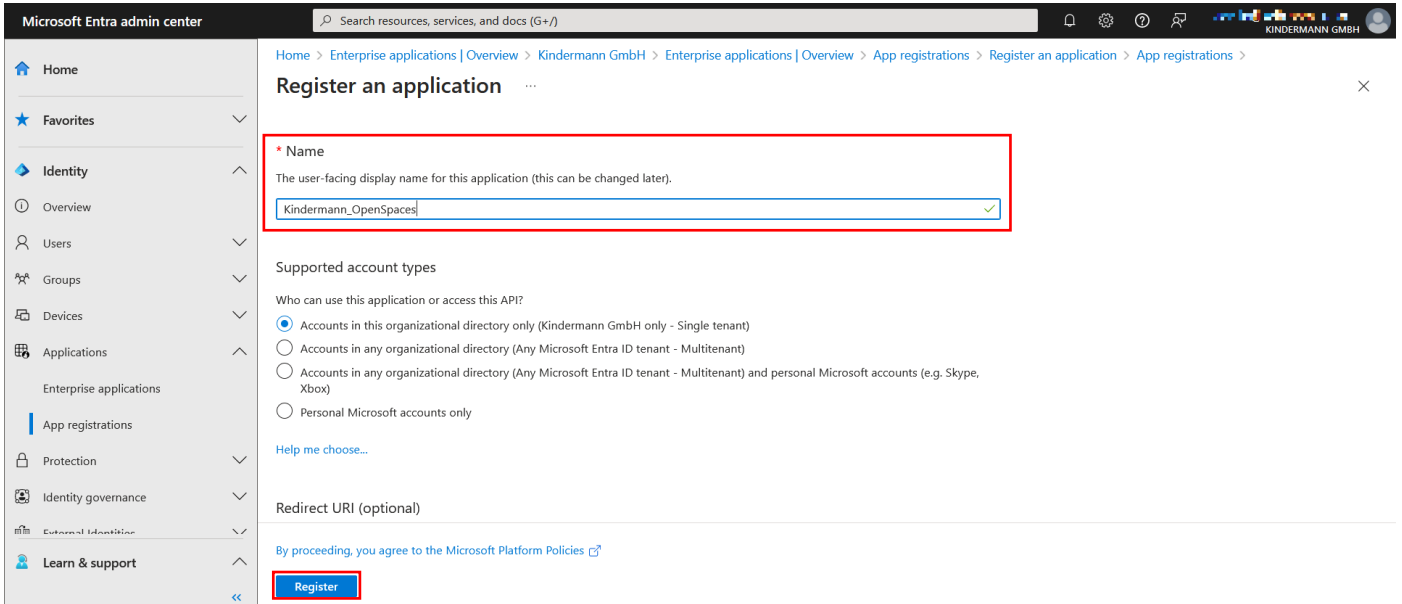


The screenshot shows the Microsoft Entra admin center interface. The left navigation pane has 'Applications' and 'App registrations' highlighted with red boxes. The main content area shows the 'App registrations' page with a '+ New registration' button also highlighted with a red box. Below the navigation, there are tabs for 'All applications', 'Owned applications' (highlighted with a red box), and 'Deleted applications'. A search bar is present with the text 'Start typing a display name or application (client) ID to filter these r...'. Below the search bar, it says '5 applications found'. A table lists the applications with columns for 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'. The table contains 5 rows of application data.

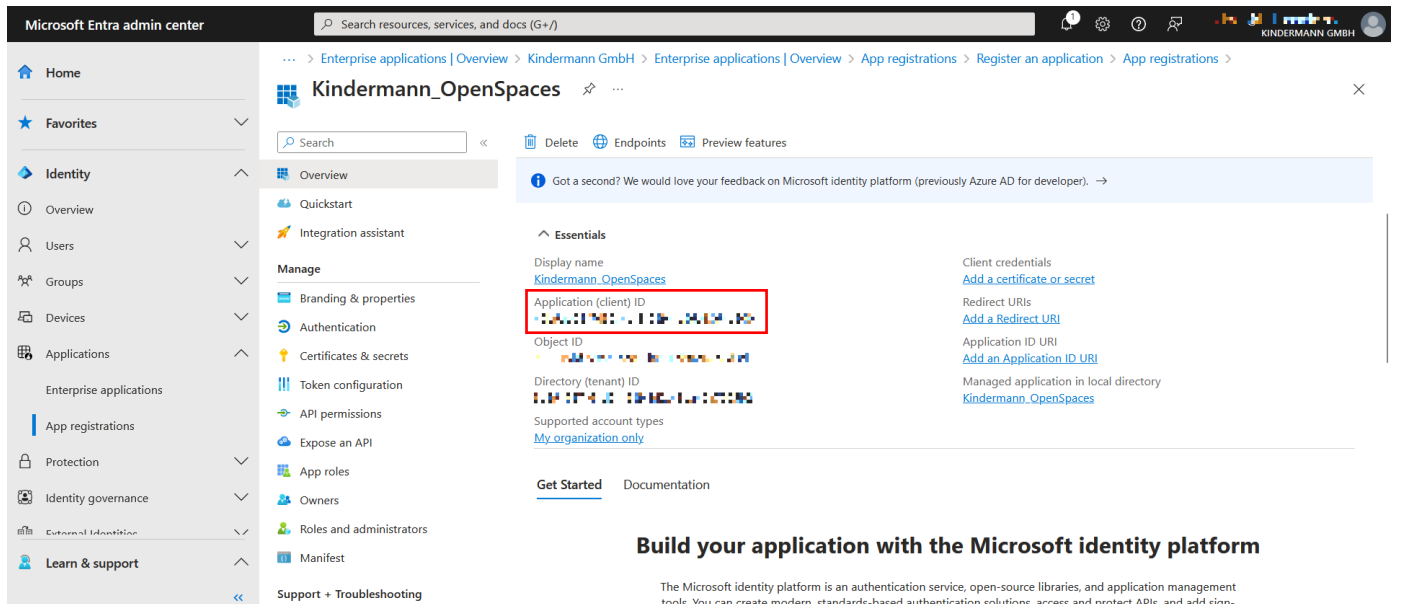
Display name	Application (client) ID	Created on	Certificates & secrets
[Red icon]	[Red icon]	12/16/2022	Current
[Blue icon]	[Blue icon]	10/20/2022	Current
[Purple icon]	[Purple icon]	10/20/2022	Current
[Green icon]	[Green icon]	4/4/2023	Current
[Green icon]	[Green icon]	2/27/2023	Current

In the next window, assign a unique, freely selectable name for the application. In our example, we assign "Kindermann\_OpenSpaces". For "Supported account types", select the first option "Accounts in this organizational directory only ([company identifier] only - Single tenant)".

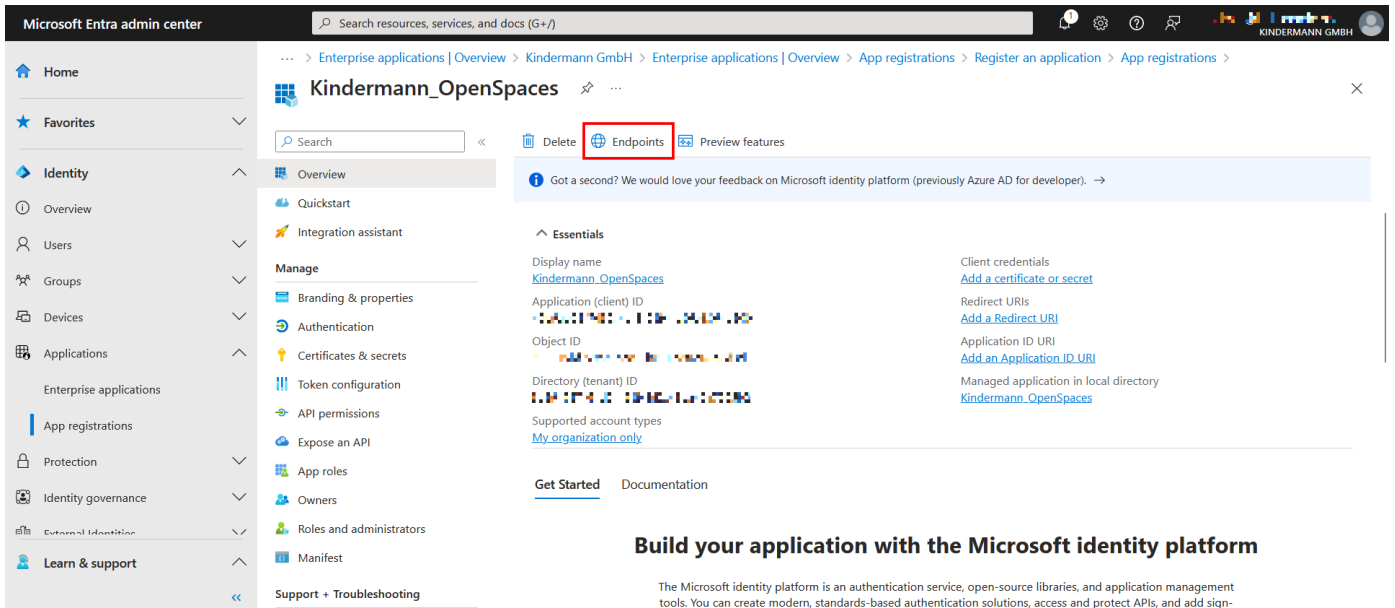
Confirm with "Register".



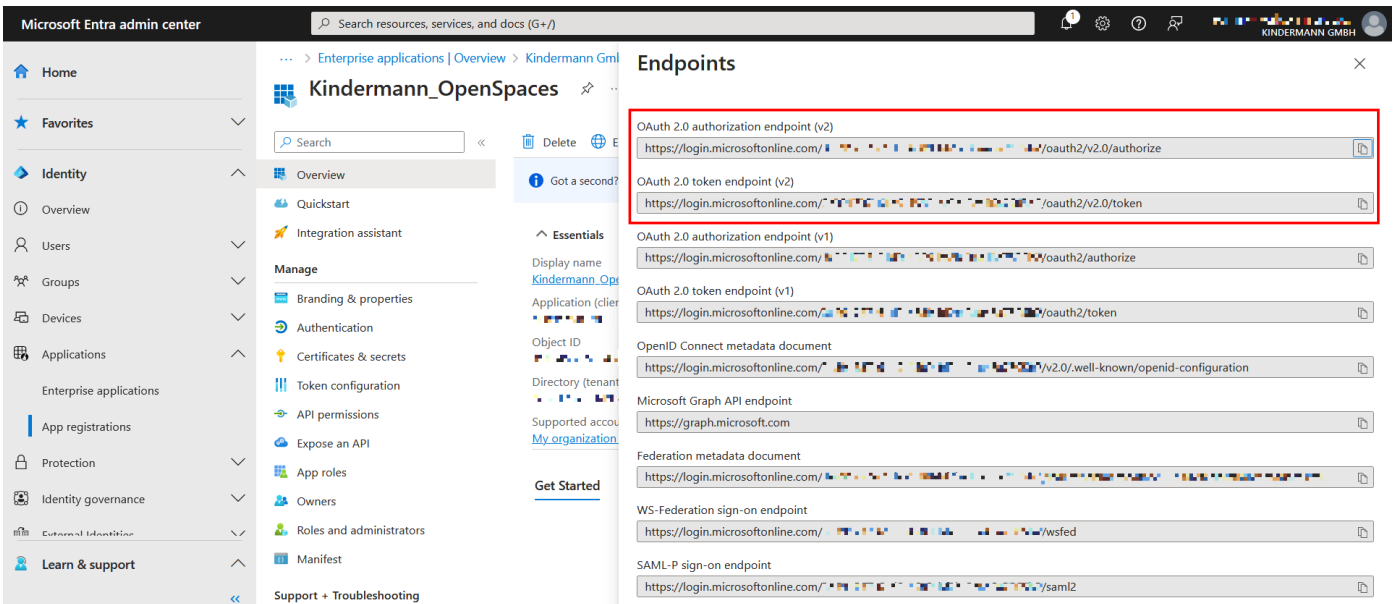
This completes the application. In the next display, you can already see the required "Application (client) ID". Copy/note them; a later readout is possible.



Above the "Application (client) ID" you will find the button "Endpoints". Click on it.

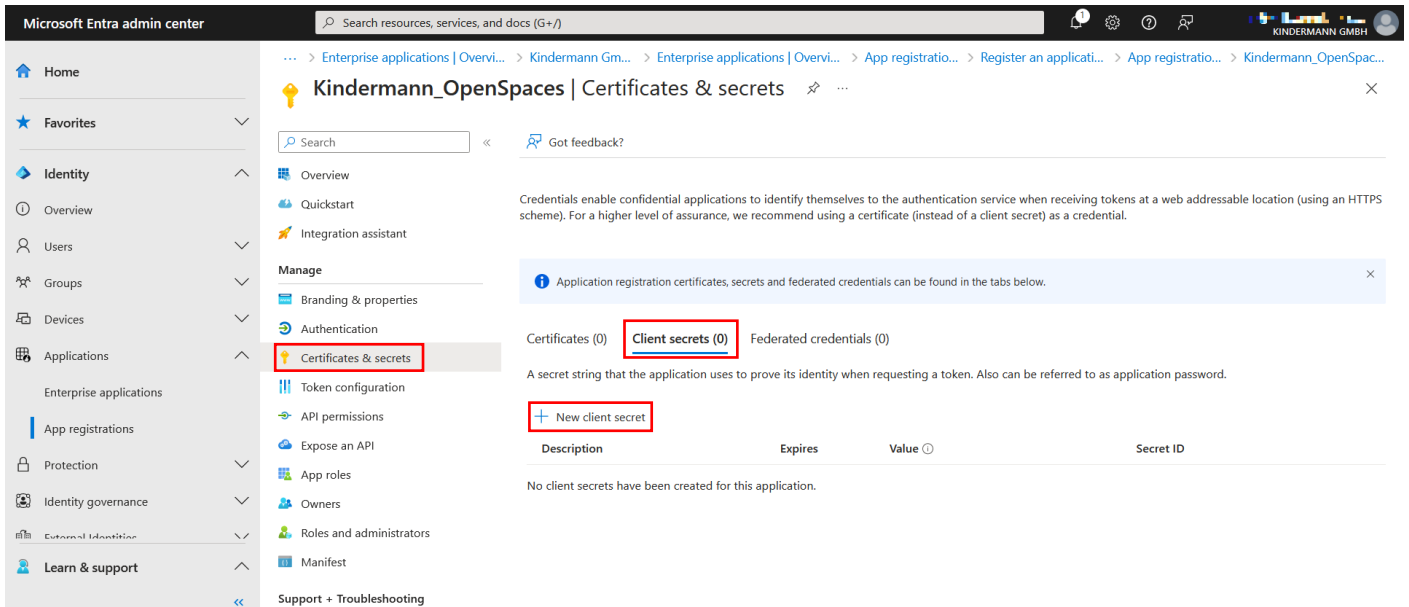


A window will appear on the side in which you can find the required "OAuth 2.0 authorization endpoint (v2)" and the "OAuth 2.0 token endpoint (v2)". Copy/note both URLs. These can also be retrieved later.



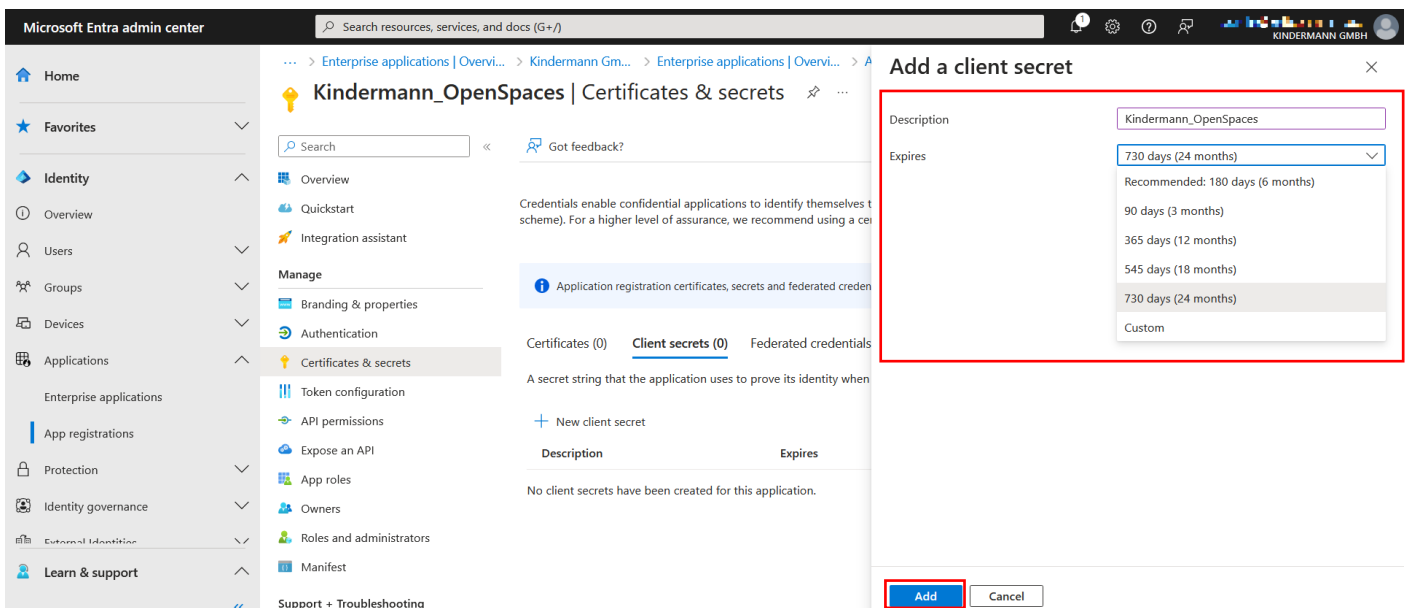
## Creating a Client Secret

The next step is to create the password that the application uses to authenticate itself. Switch to the "Certificates & secrets" tab, then to "Client secrets" and add "+ New client secret":

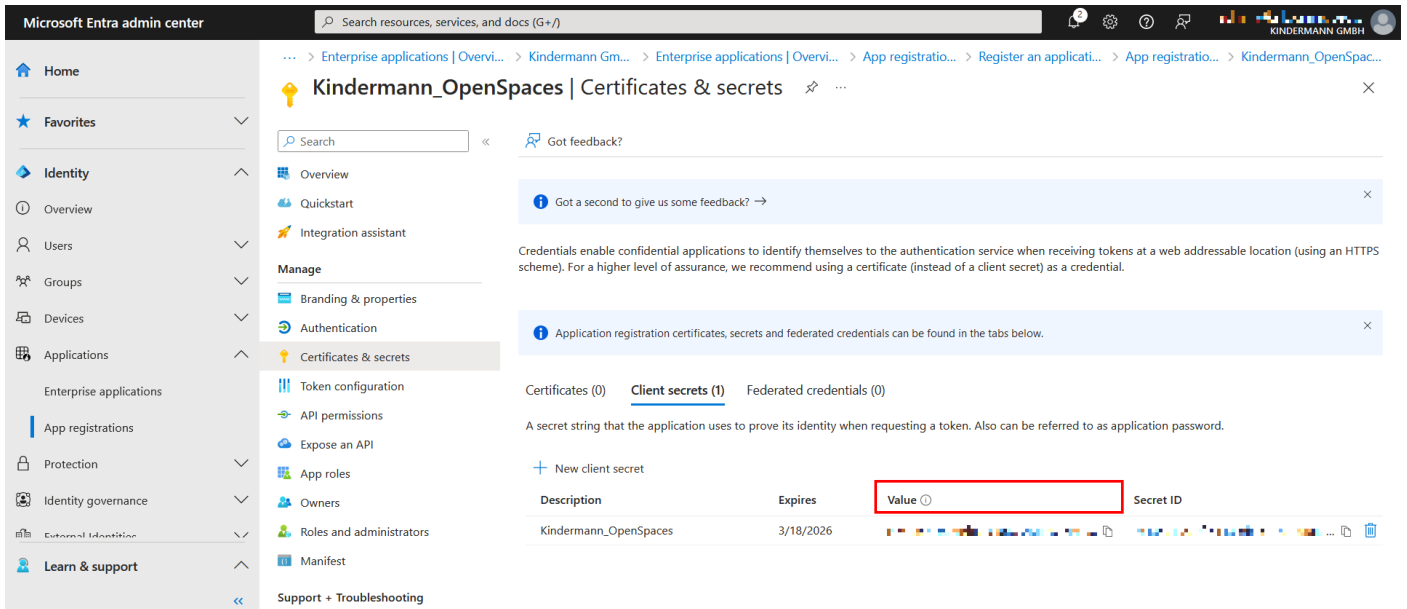


A window collapses from the right. Enter a name for the secret, we will use "Kindermann OpenSpaces" in this example. Set the "Expires" expiration date to the desired value. We use the maximum of 24 months here. Click "Add" to create the secret.

We put a reminder in our own calendar to create a new secret in 2 years. To do so, this section of the instructions can simply be repeated.

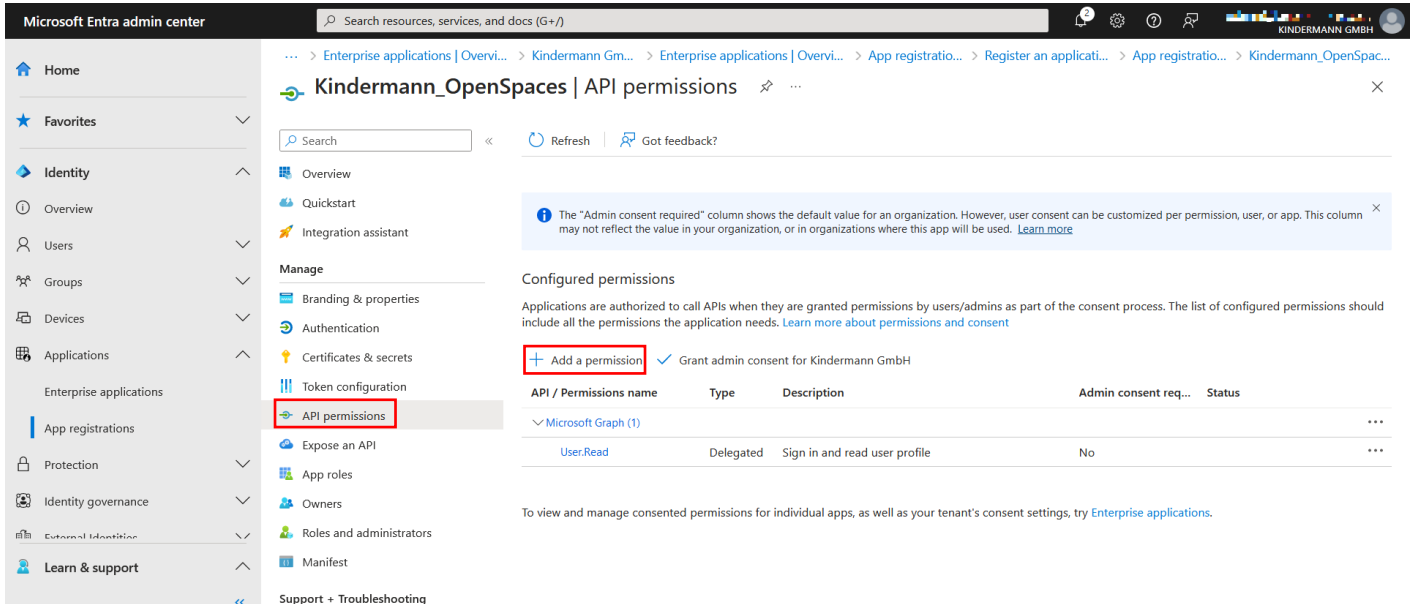


The window will then retract, and a new list entry will appear in the background. In it, you can see the name, the expiration date, "Value" and the "Secret ID". The "Value" is the client secret and **must be documented directly here**, as it can no longer be viewed afterwards.

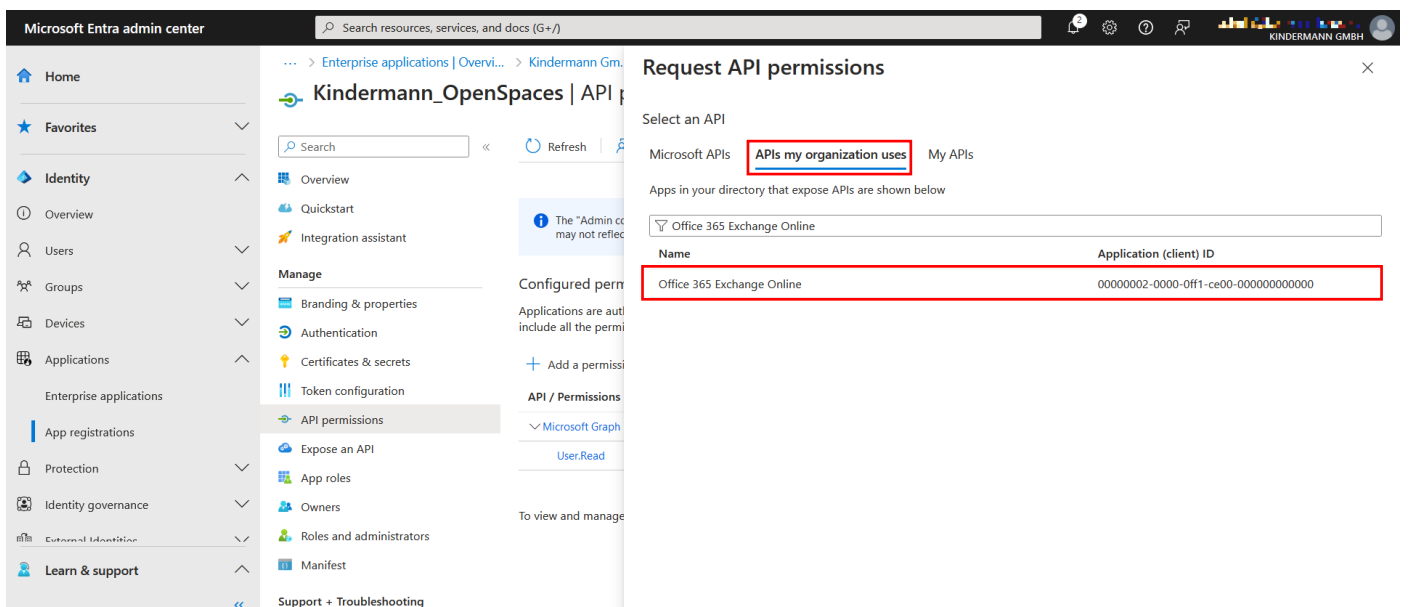


## Set permissions

For the permission, it is now necessary to determine what can be done via the OpenSpaces service. The settings can be found under "API permissions". Click on "+ Add a permission".



From the right, a window opens again. Select the "APIs my organization uses" tab and search for "Office 365 Exchange Online". Click on the entry.

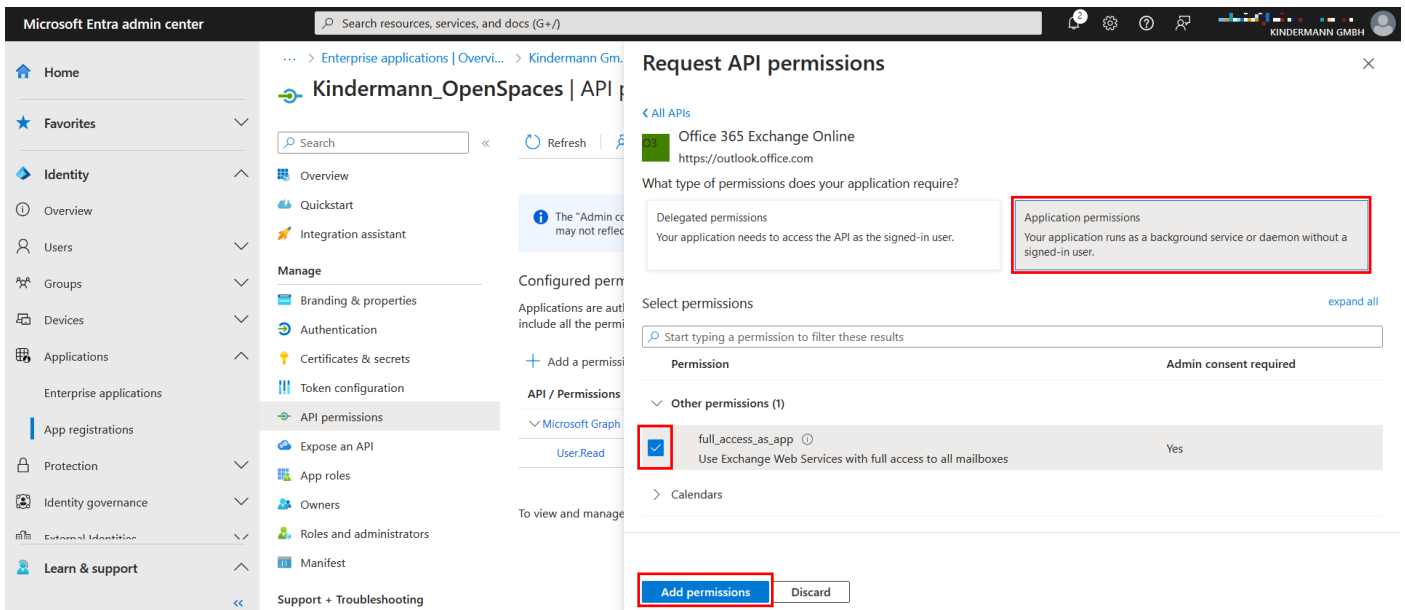


Next, select "Application permissions" and the configurable permissions will appear below it. Tick "full\_access\_as\_app" under "Other permissions" and save with "Add permissions" at the bottom.

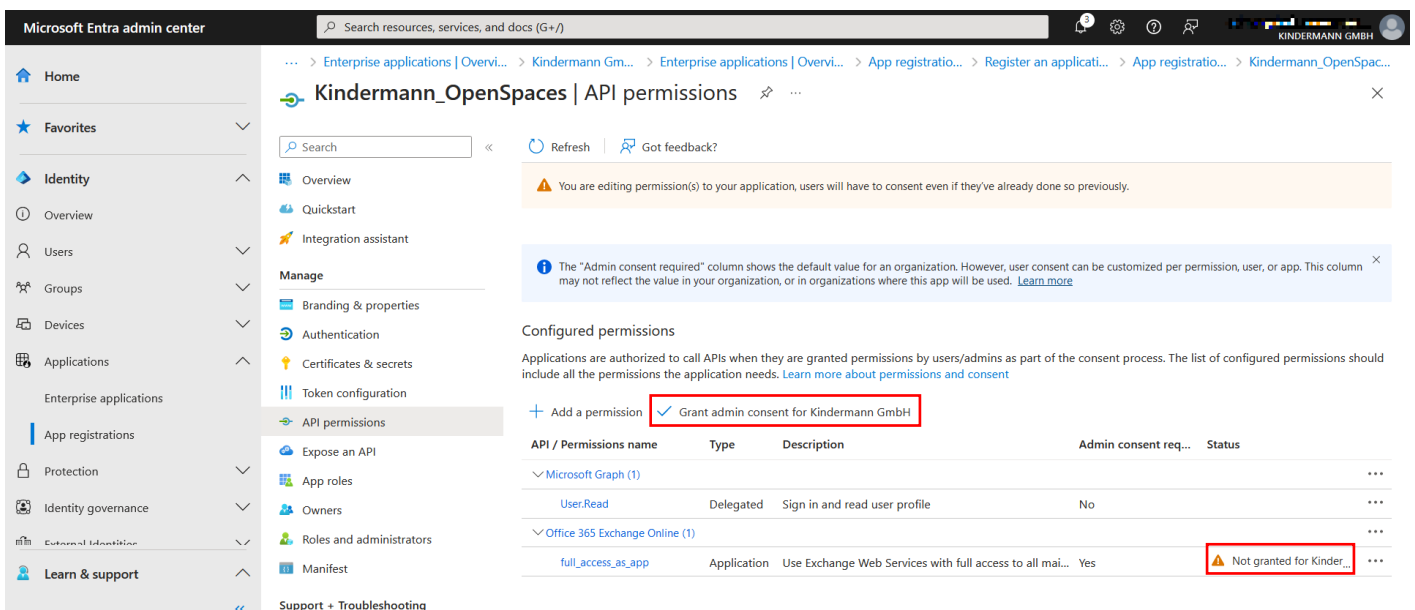
To set up OpenSpaces for the first time, this setting must be set.

If the service is not to be granted full permissions to all mailboxes, these can be restricted to those (room) mailboxes later.

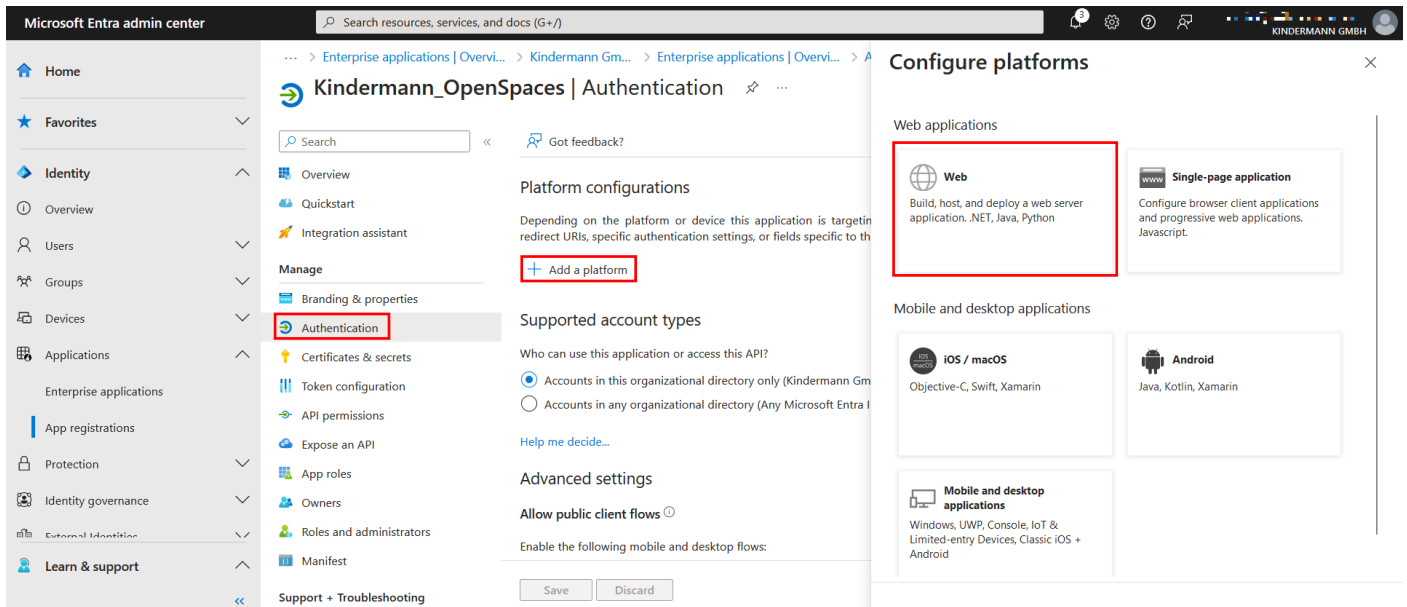
To do this, jump to page 9 after the successful setup.



For the authorization to be applied, it must then be released with administrative permissions. To do this, click on "Grant admin consent for [company name]" in the overview.



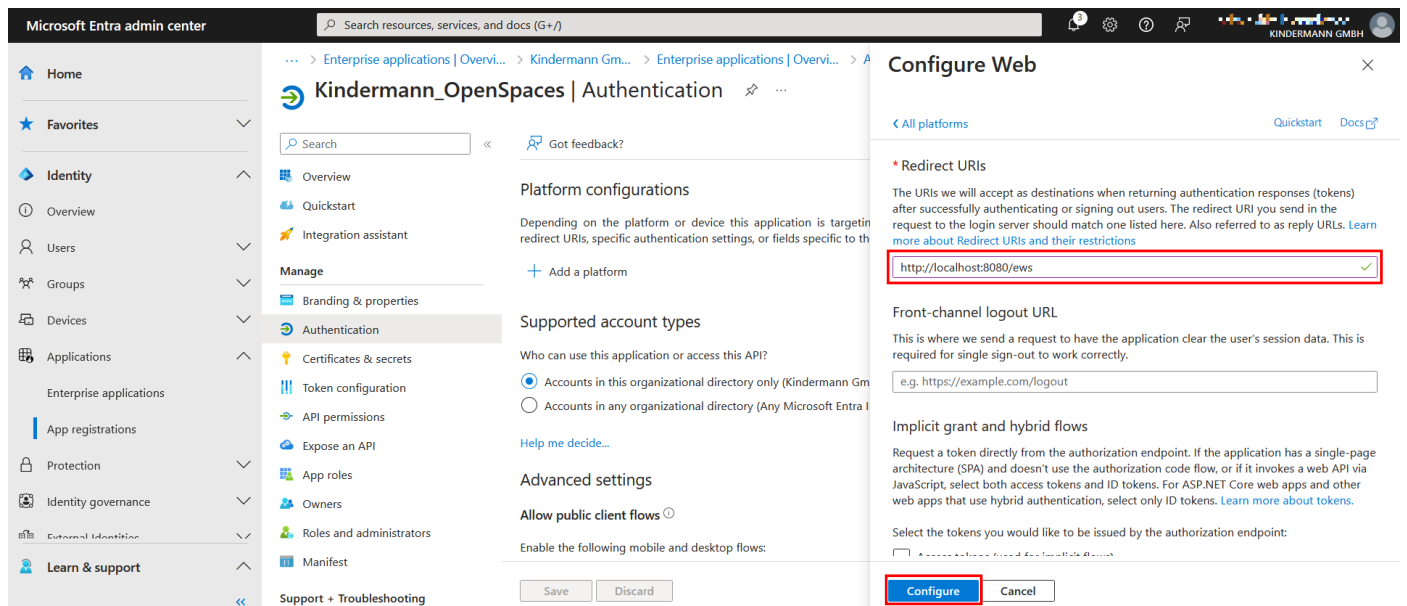
One last step is still necessary. Switch to the "Authentication" tab in the overview and select "Add a platform" to create a redirect URL. From the right, a window opens again, in which "Web" must be selected.



For the redirect URL, enter the following address:

<http://localhost:8080/ews>

Confirm with "Configure".



This completes the configuration of the Enterprise Application in Microsoft Entra ID, and you should have the following data:

App ID / Client Secret / Auth Endpoint / Token Endpoint / Redirect URL

**You can now proceed with the configuration in the main manual** and enter the data in the configurator. You can also check the connection to the server there.



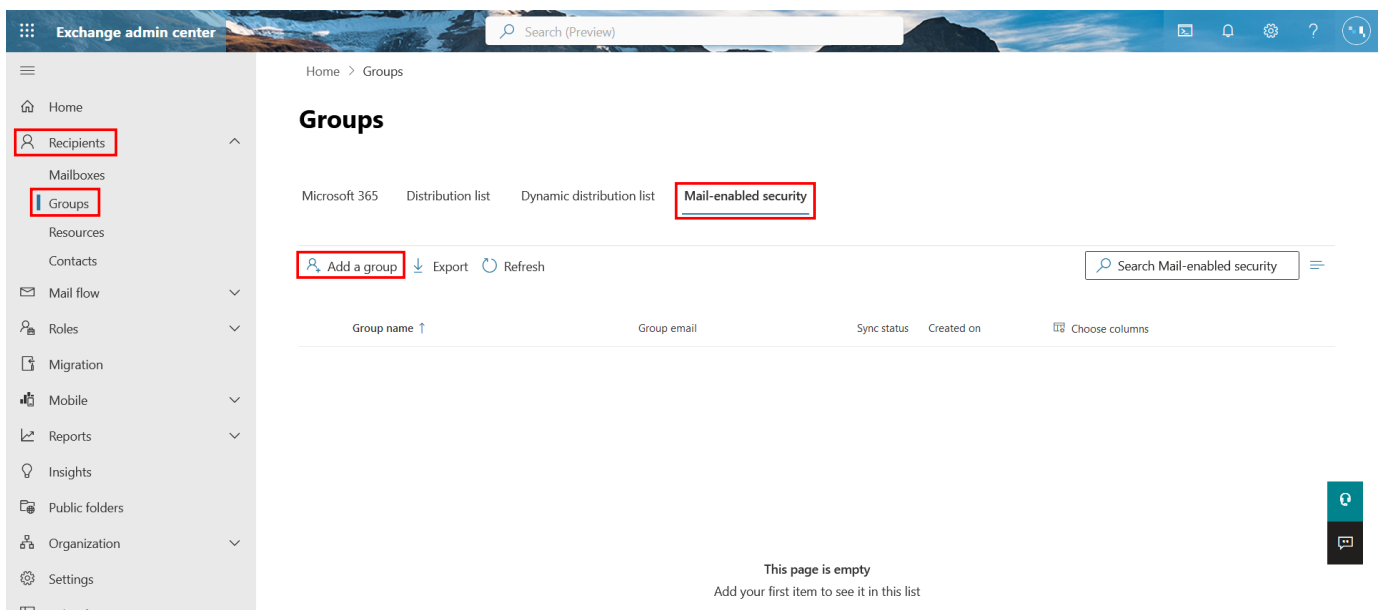
## Optional: Restrict permissions to specific mailboxes

If desired, the authorization of the service can be restricted so that it cannot be read to the calendars of all mailboxes.

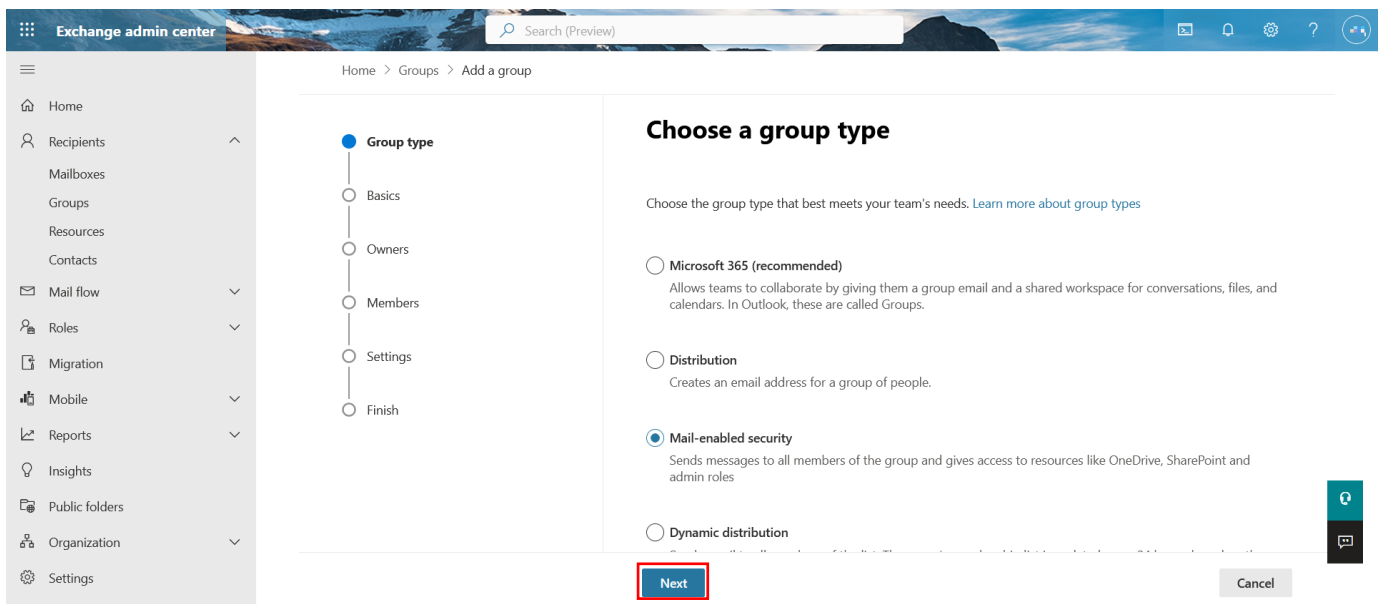
This becomes necessary if "full\_access\_as\_app" is not permitted without restriction.

Source: <https://docs.microsoft.com/de-de/graph/auth-limit-mailbox-access#configure-applicationaccesspolicy>

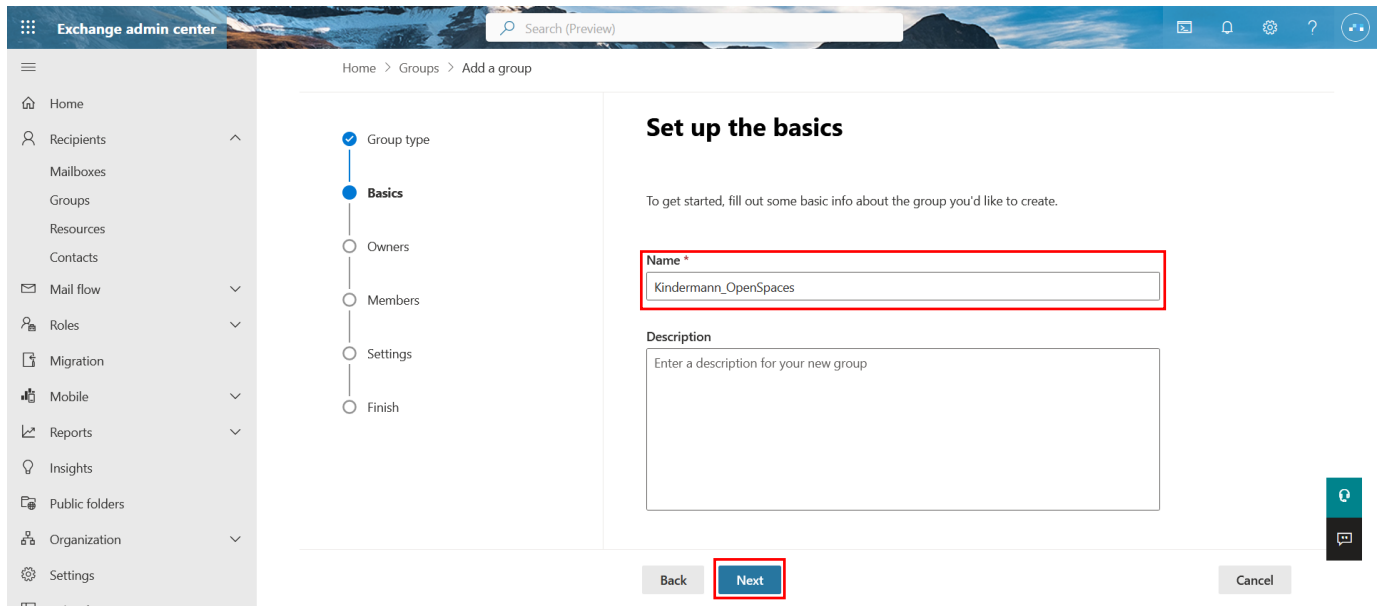
An email-enabled security group is required for setup. This can be created in the Exchange Online Admin Center in the "Recipients" tab under "Groups". Select "Mail-enabled security" and create such a group under "Add a group".



In the following screen, you can click directly on "Next" if "Mail-enabled security" is selected.

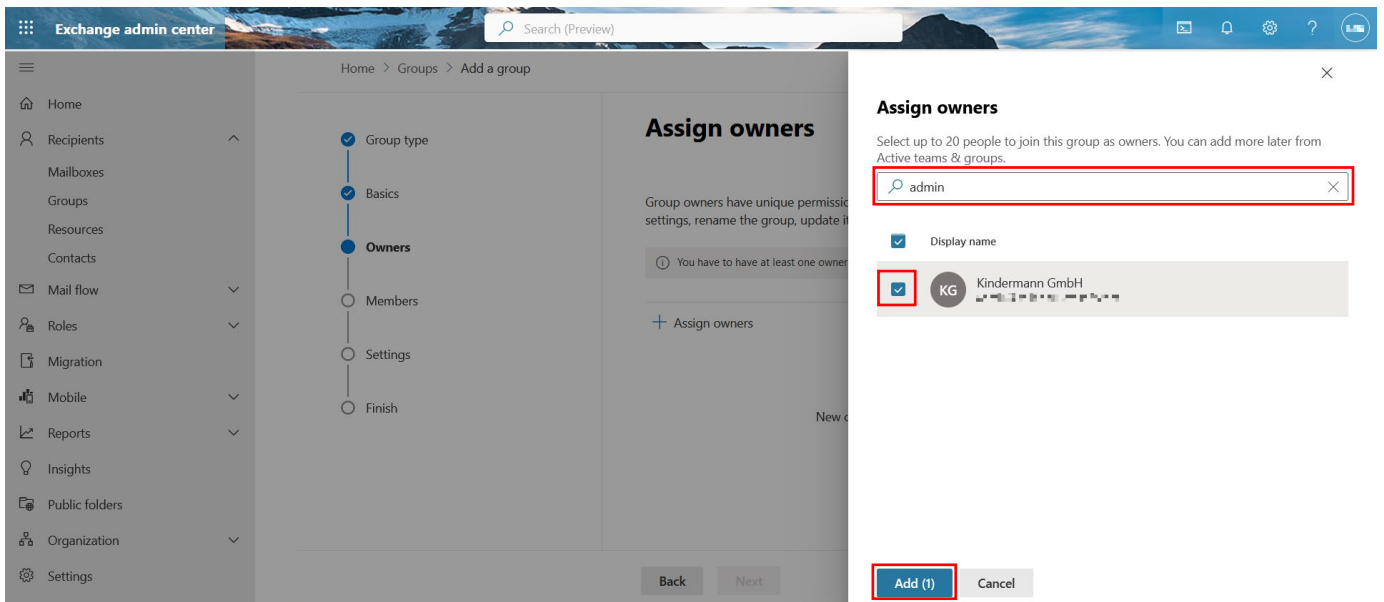


Choose a plausible display name (e.g.: Kindermann\_OpenSpaces). Since the notes are optional, you can go straight to "Next".



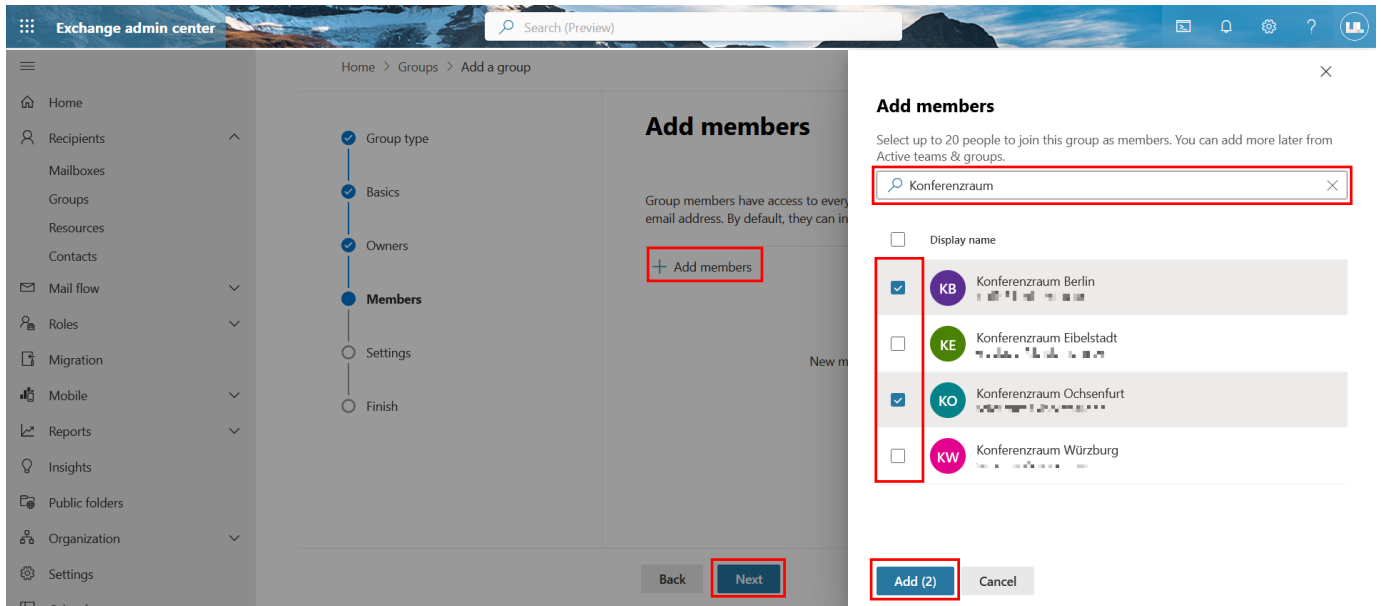
In the next window, use the search field to find the owner of the group and tick the box below. Close the dialog with "Add [number]" and then click on "Next" again.

We recommend the admin address as the owner.

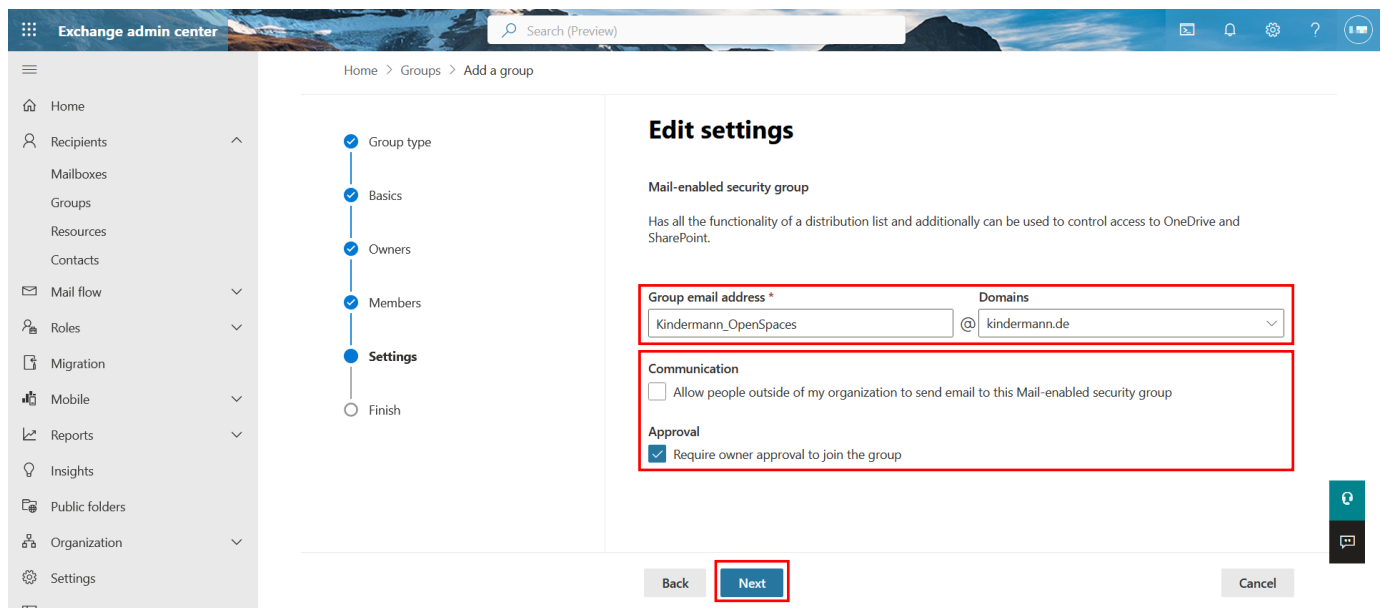


As a member, you can set up the mailboxes under "Add members" that you would like to share with OpenSpaces. You can search for them using the search field, tick them and add them with "Add [number]". The window closes automatically.

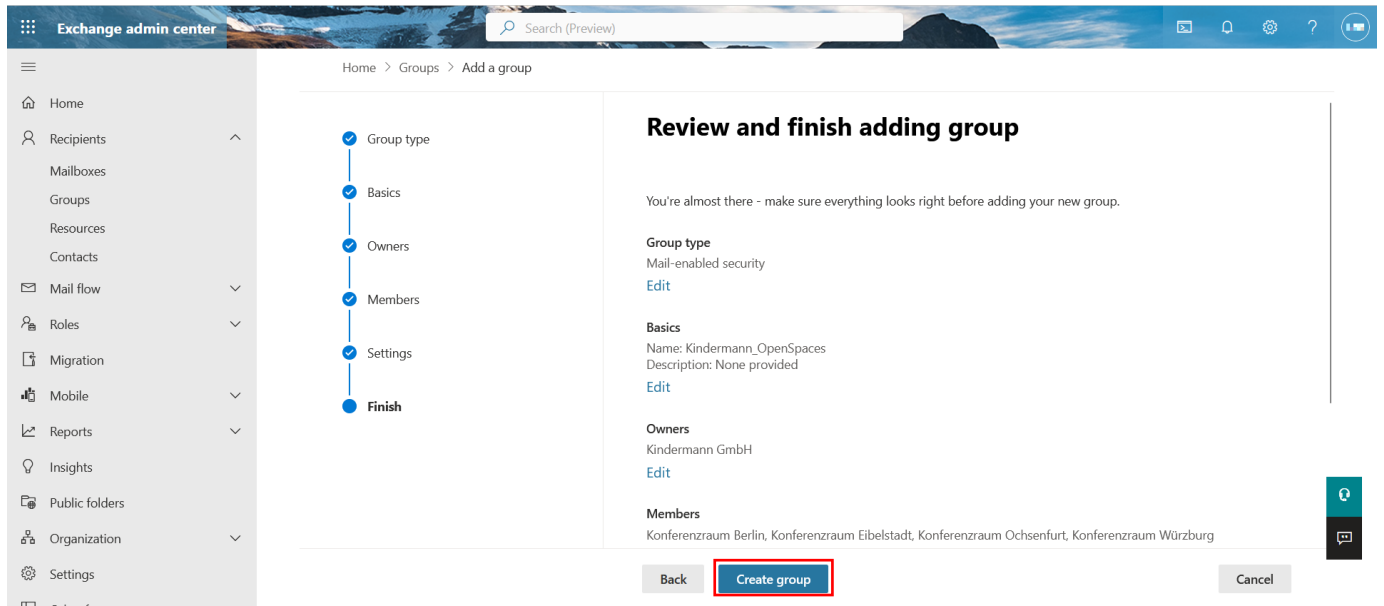
Once you have added all of them, click "Next" to confirm.



In the last step, assign an email address for the group and write it down / copy it. The address will then be required. Check the boxes as shown so that unauthorized interactions with the newly created group are excluded. Click "Next" to confirm.



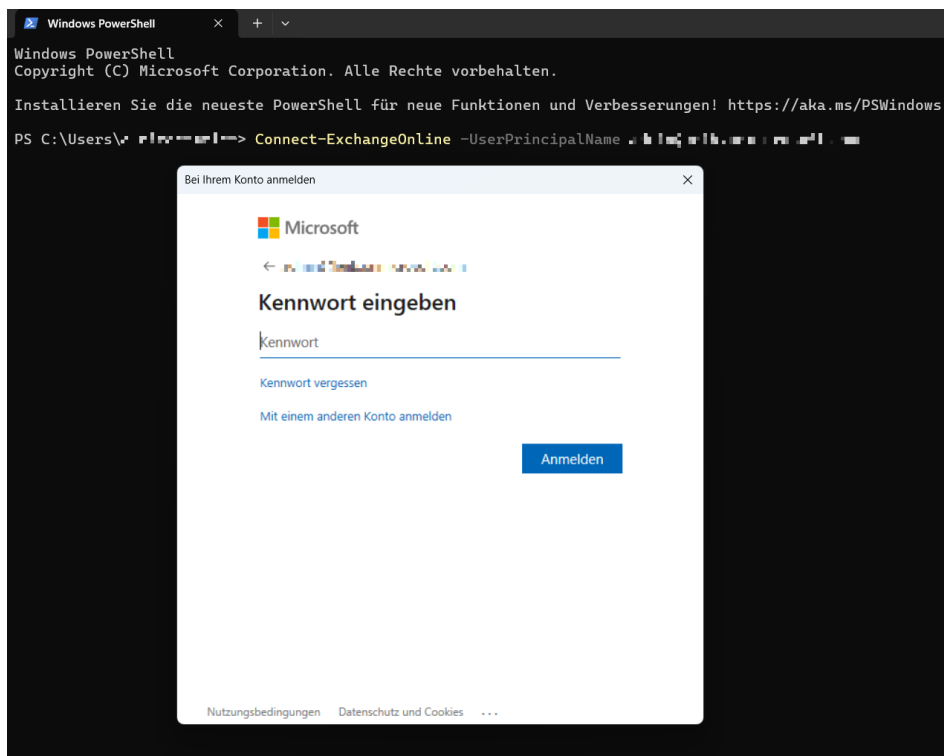
Check your entries and create the group with "Create group".



Once the group has been created, the app can be restricted to that group. This can be done via a PowerShell CMDlet.

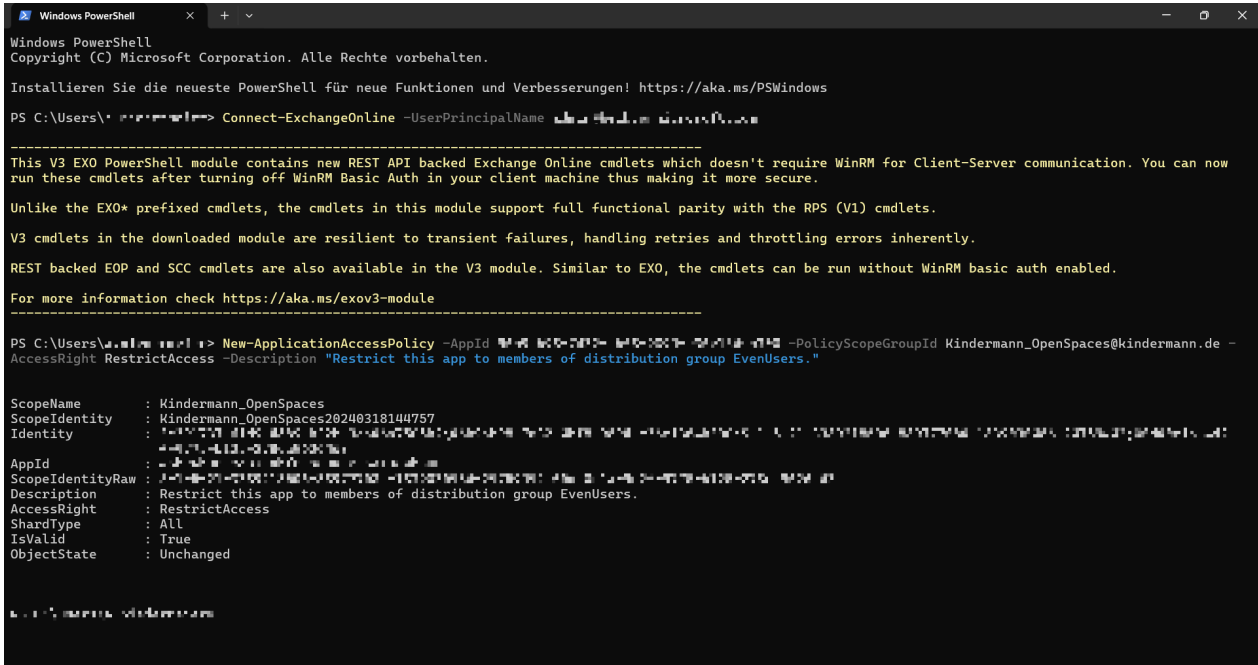
Open PowerShell and connect to your Exchange Online Server:

```
Connect-ExchangeOnline -UserPrincipalName [email address of your admin account]
```



Then run the following command to restrict the application to the group:

```
New-ApplicationAccessPolicy -AppId [Your Application (client) ID] -PolicyScopeGroupId [Your Group Email Address] -AccessRight RestrictAccess -Description "Restrict this app to members of distribution group EvenUsers."
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Installieren Sie die neueste PowerShell für neue Funktionen und Verbesserungen! https://aka.ms/PSWindows

PS C:\Users\...> Connect-ExchangeOnline -UserPrincipalName ...

-----
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module
-----

PS C:\Users\...> New-ApplicationAccessPolicy -AppId ... -PolicyScopeGroupId Kindermann_OpenSpaces@kindermann.de -
AccessRight RestrictAccess -Description "Restrict this app to members of distribution group EvenUsers."

ScopeName      : Kindermann_OpenSpaces
ScopeIdentity   : Kindermann_OpenSpaces20240318144757
Identity       : ...
AppId          : ...
ScopeIdentityRaw : ...
Description    : Restrict this app to members of distribution group EvenUsers.
AccessRight    : RestrictAccess
ShardType      : ALL
IsValid        : True
ObjectState    : Unchanged
```

This means that OpenSpaces is limited to the members of the group. The group and its members can also be customized in the Exchange Online admin center.