

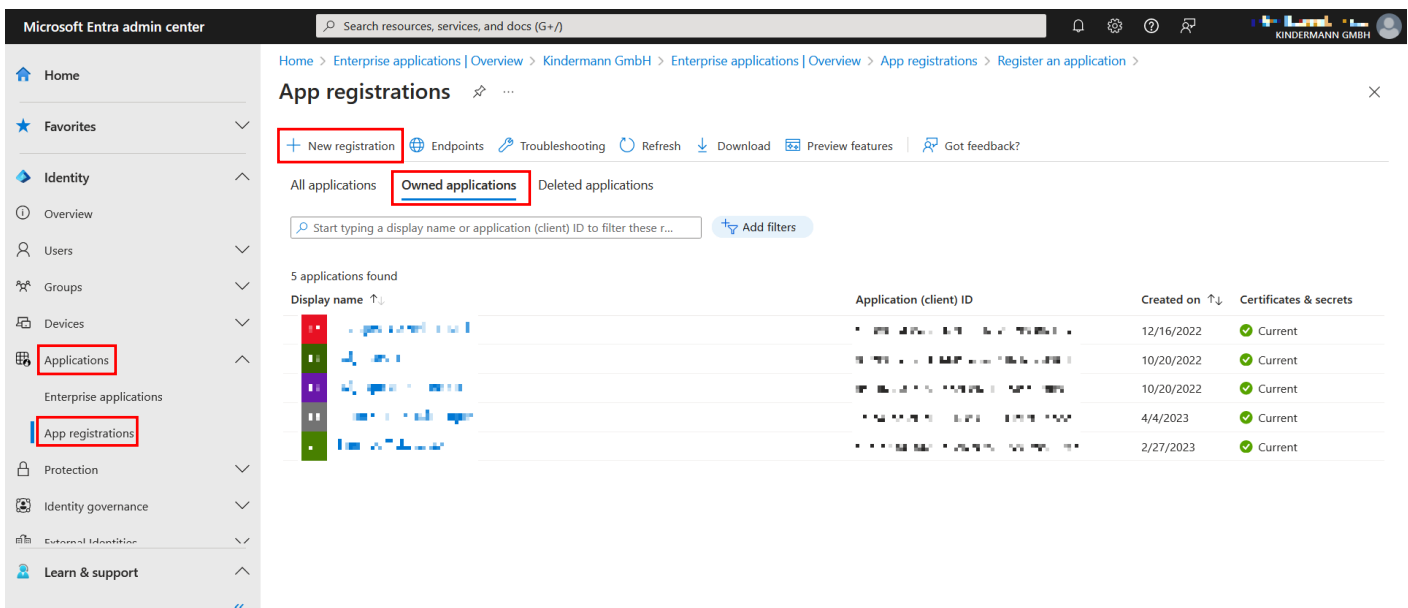
## Einleitung

Das nachfolgende Dokument beschreibt die Einrichtung einer „Enterprise Application“, welche für die Verwendung von OpenSpaces in Kombination mit Microsoft 365 und Exchange Online notwendig ist. Nach der erfolgreichen Einrichtung erhalten Sie die Parameter für das Anmelden des Dienstes OpenSpaces mittels **Modern Auth** (OAuth2) am Exchange Server. Diese können im Anschluss im Windows-Setup Tool von OpenSpaces eingetragen werden.

## Anlegen der Enterprise Application

Die Enterprise Application wird in Microsoft Entra ID (ehemals Azure Active Directory) eingerichtet. Diese ist nach einer Anmeldung mit einem Administratoraccount unter <https://entra.microsoft.com/> erreichbar. Klicken Sie unter „Applications“ auf „App registrations“ und anschließend auf „Owned applications“.

Klicken Sie nun auf „+ New registration“ und folgen Sie den nächsten Schritten.

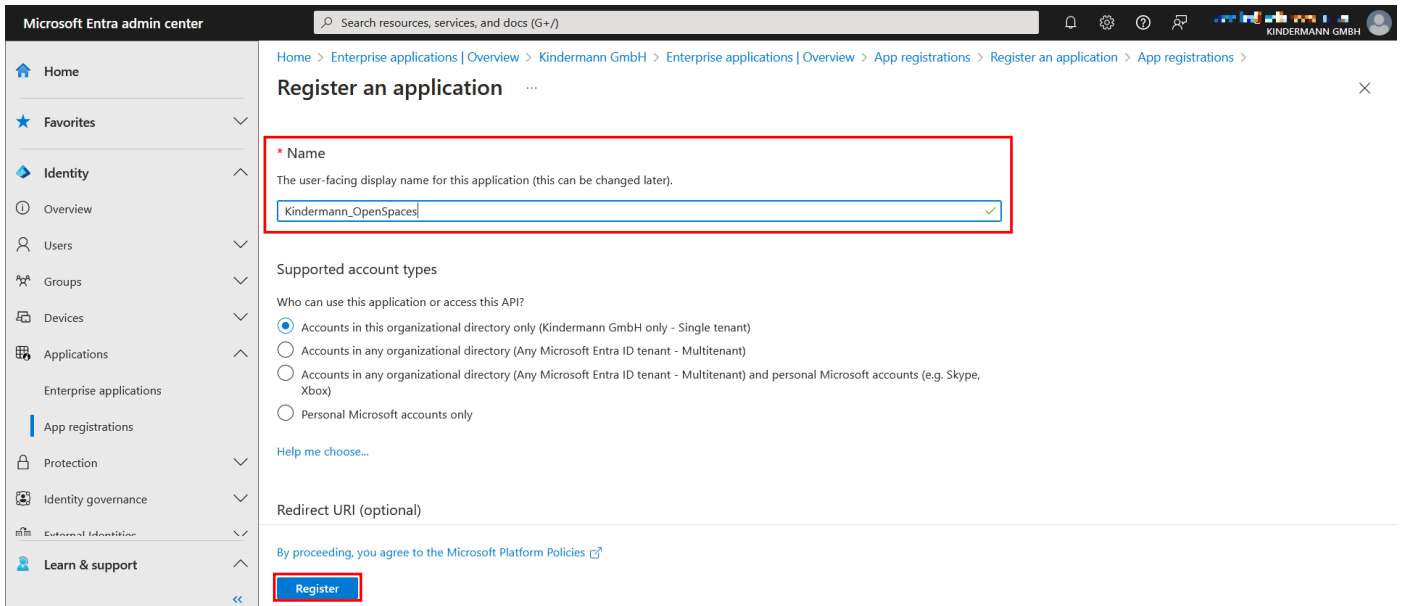


The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane has 'Applications' and 'App registrations' highlighted with red boxes. The main content area shows the 'App registrations' page with the 'Owned applications' tab selected. A table lists 5 applications with columns for Display name, Application (client) ID, Created on, and Certificates & secrets.

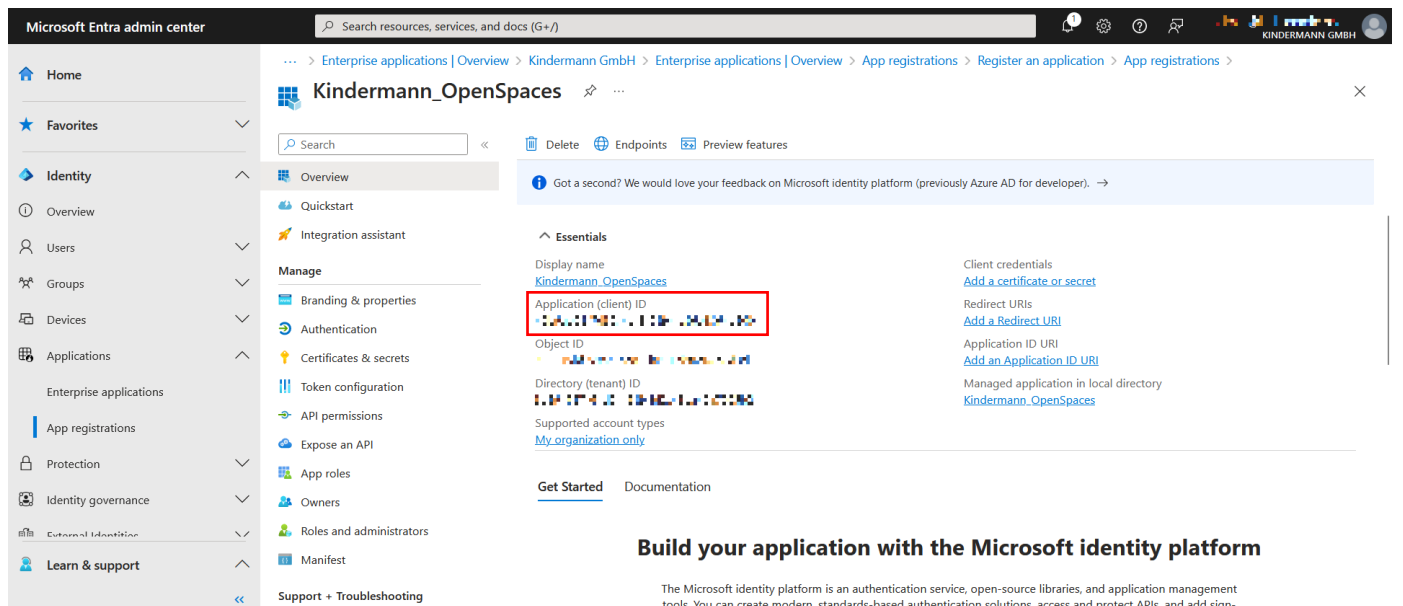
Display name	Application (client) ID	Created on	Certificates & secrets
[Redacted]	[Redacted]	12/16/2022	Current
[Redacted]	[Redacted]	10/20/2022	Current
[Redacted]	[Redacted]	10/20/2022	Current
[Redacted]	[Redacted]	4/4/2023	Current
[Redacted]	[Redacted]	2/27/2023	Current

Vergeben Sie im nächsten Fenster einen eindeutigen, frei wählbaren Namen für die Applikation. In unserem Beispiel vergeben wir „Kindermann\_OpenSpaces“. Wählen Sie als „Supported account types“ die erste Option „Accounts in this organizational directory only ([Unternehmenskennung] only - Single tenant)“.

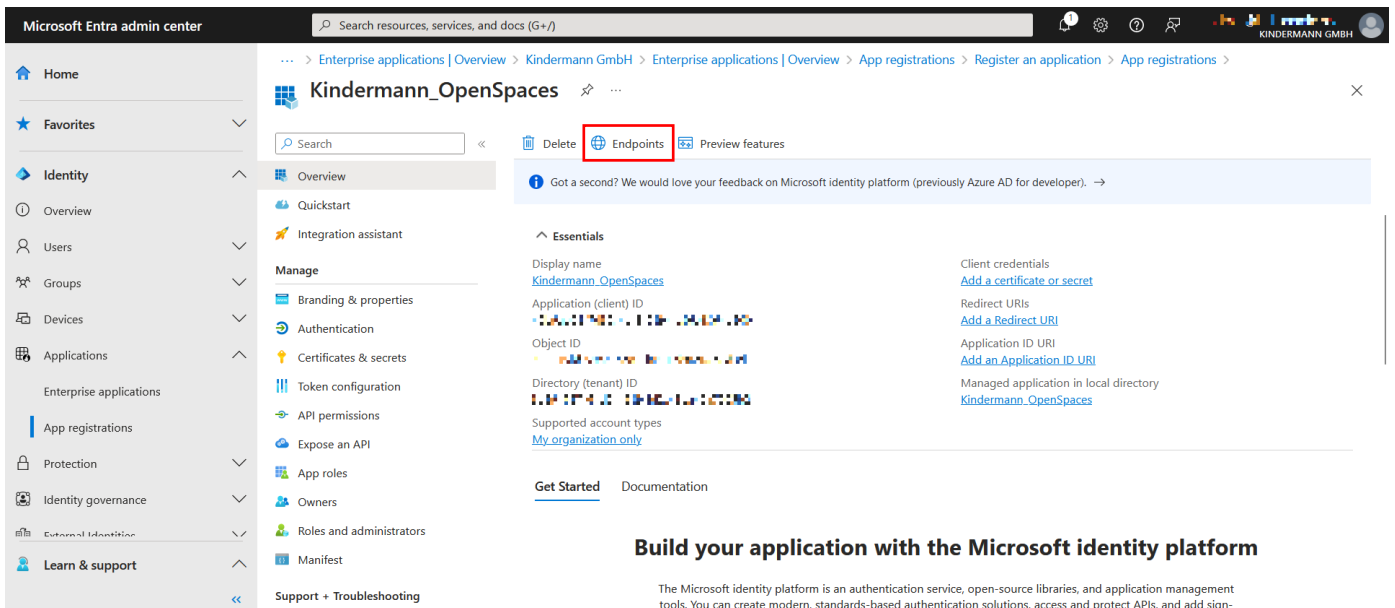
Bestätigen Sie mit “Register”.



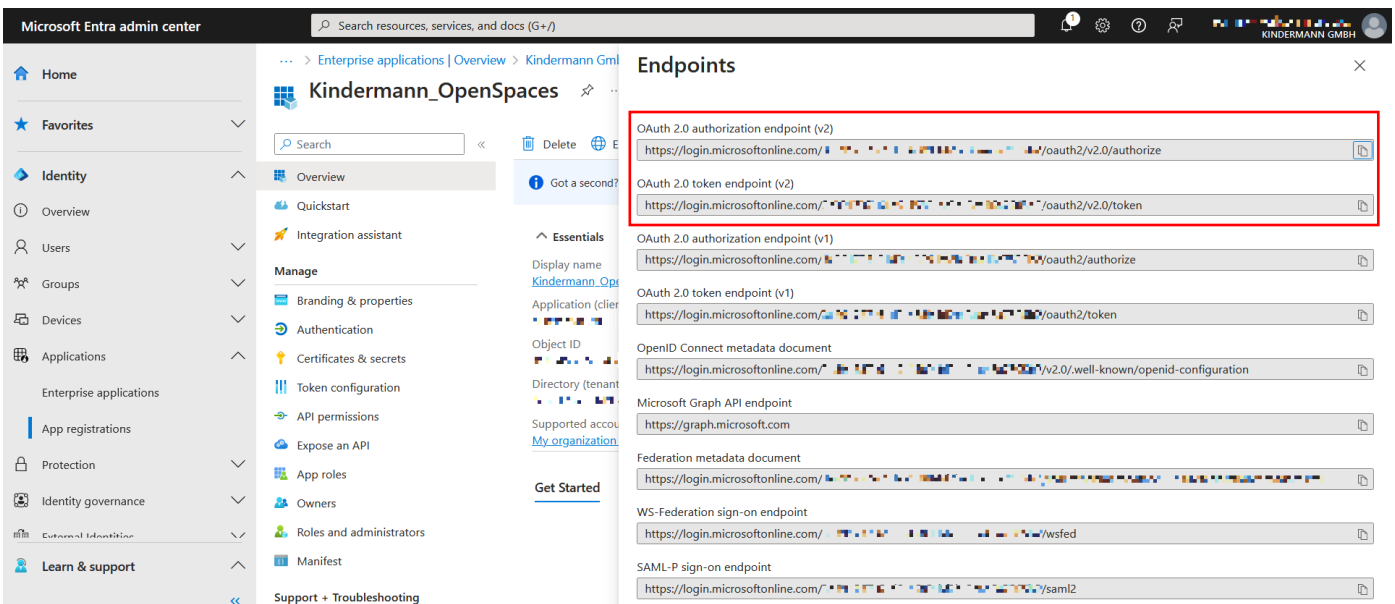
Damit ist die Applikation angelegt. In der nächsten Anzeige sehen Sie bereits die benötigte „Application (client) ID“. Kopieren / Vermerken Sie diese; ein späteres Auslesen ist möglich.



Über der „Application (client) ID“ finden Sie den Button „Endpoints“. Klicken Sie diesen an.

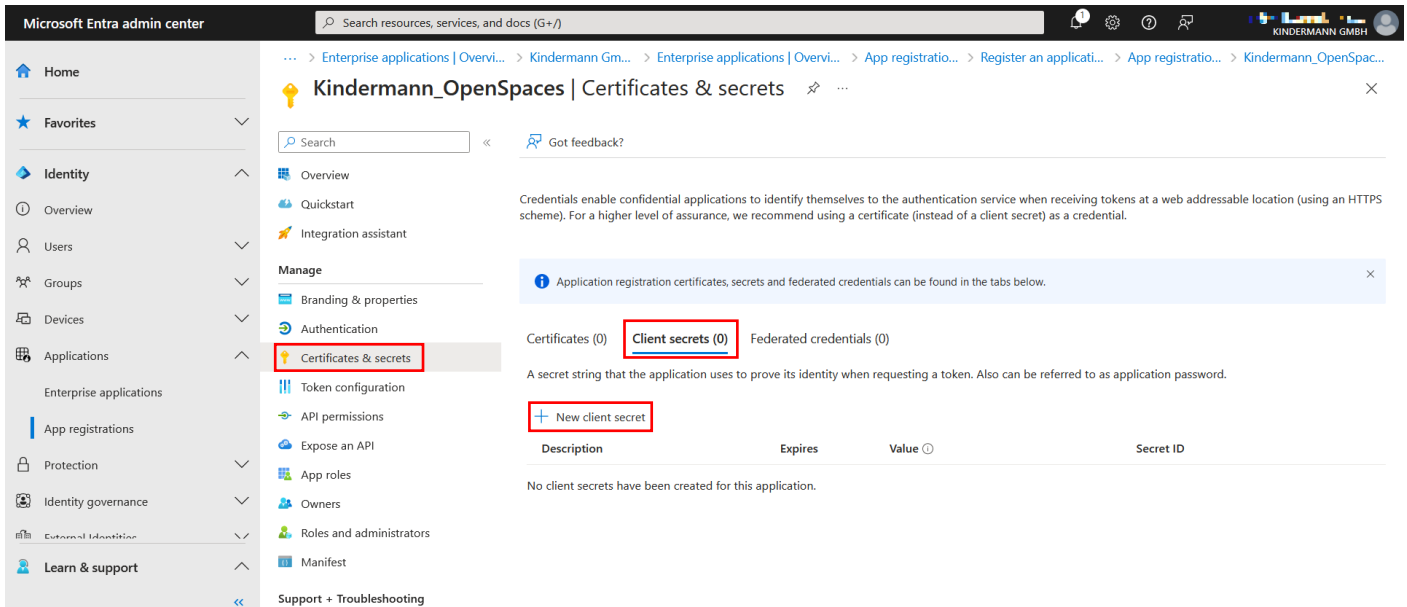


An der Seite erscheint ein Fenster, in der die benötigte „OAuth 2.0 authorization endpoint (v2)“ und die „OAuth 2.0 token endpoint (v2)“ zu finden ist. Kopieren / Vermerken Sie beide URLs. Auch diese können später noch abgerufen werden.



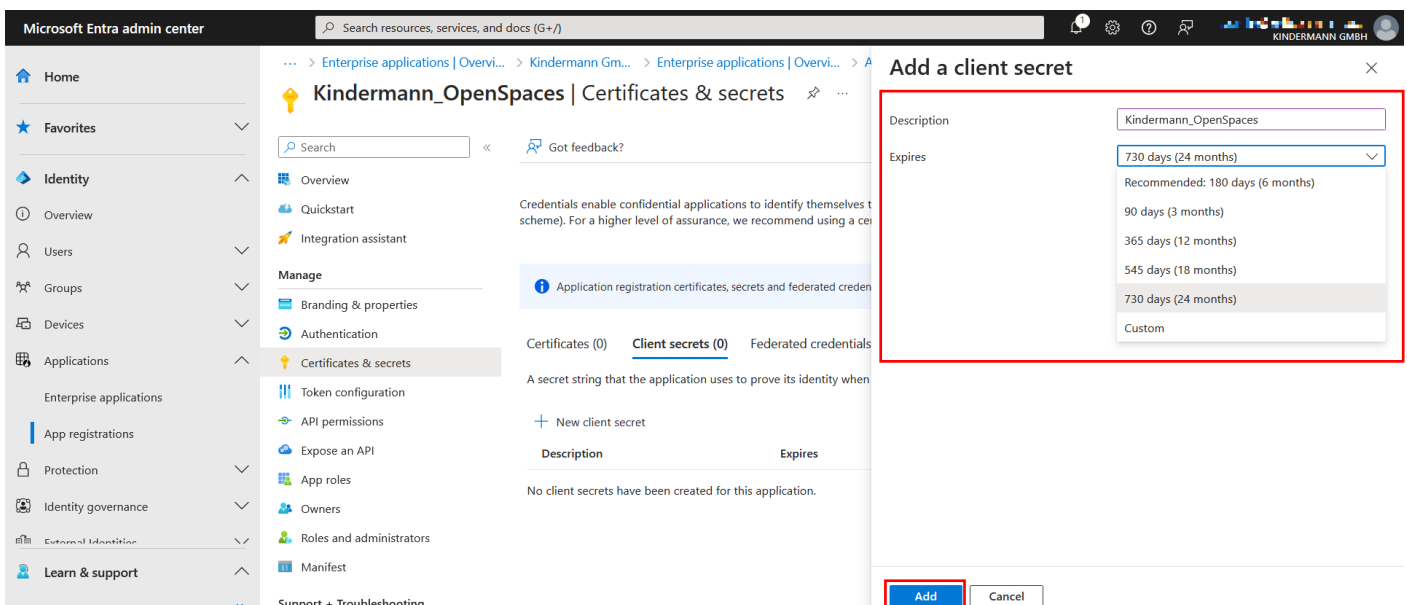
## Ein „Client Secret“ erstellen

Als nächstes muss das Kennwort erstellt werden, mit dem sich die Applikation authentifiziert. Wechseln Sie in den Reiter „Certificates & secrets“, dann auf „Client secrets“ und ergänzen mit „+ New client secret“ eben dieses:



Von rechts klappt ein Fenster ein. Geben Sie einen Namen für das Secret ein, wir verwenden in diesem Beispiel „Kindermann OpenSpaces“. Stellen Sie das Ablaufdatum „Expires“ auf den gewünschten Wert ein. Wir verwenden hier das Maximum von 24 Monaten. Klicken Sie auf „Add“, um das Secret zu erstellen.

Wir setzen uns direkt eine Erinnerung in den eigenen Kalender, um in 2 Jahren ein neues Secret anzulegen. Dafür kann dieser Abschnitt der Anleitung einfach wiederholt werden.



Daraufhin fährt das Fenster wieder ein und im Hintergrund erscheint ein neuer Listeneintrag. In diesem ist der Name, das Ablaufdatum, „Value“ und die „Secret-ID“ zu sehen. Die „Value“ ist das Client Secret und **muss hier direkt dokumentiert** werden, da es nicht mehr nachträglich eingesehen werden kann.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options like Home, Favorites, Identity, and Applications. The main content area is titled 'Kindermann\_OpenSpaces | Certificates & secrets'. It features a search bar, a 'Got feedback?' button, and a list of client secrets. The table below has columns for Description, Expires, Value, and Secret ID. The 'Value' column for the 'Kindermann\_OpenSpaces' entry is highlighted with a red box.

Description	Expires	Value	Secret ID
Kindermann_OpenSpaces	3/18/2026	[Redacted]	[Redacted]

## Berechtigungen festlegen

Für die Berechtigung muss nun noch festgelegt werden, was über den Dienst OpenSpaces durchgeführt werden darf. Die Einstellungen finden Sie unter „API permissions“. Klicken Sie auf „+ Add a permission“.

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is open, and the 'API permissions' option under 'App registrations' is highlighted with a red box. The main content area displays the 'Kindermann\_OpenSpaces | API permissions' page. A red box highlights the '+ Add a permission' button. Below this, a table lists the configured permissions:

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

Von rechts öffnet sich erneut ein Fenster. Wählen Sie den Reiter „APIs my organization uses“ und suchen Sie nach „Office 365 Exchange Online“. Klicken Sie den Eintrag an.

The screenshot shows the 'Request API permissions' dialog box in the Microsoft Entra admin center. The 'APIs my organization uses' tab is selected and highlighted with a red box. A search box contains the text 'Office 365 Exchange Online'. Below the search box, a table lists the results:

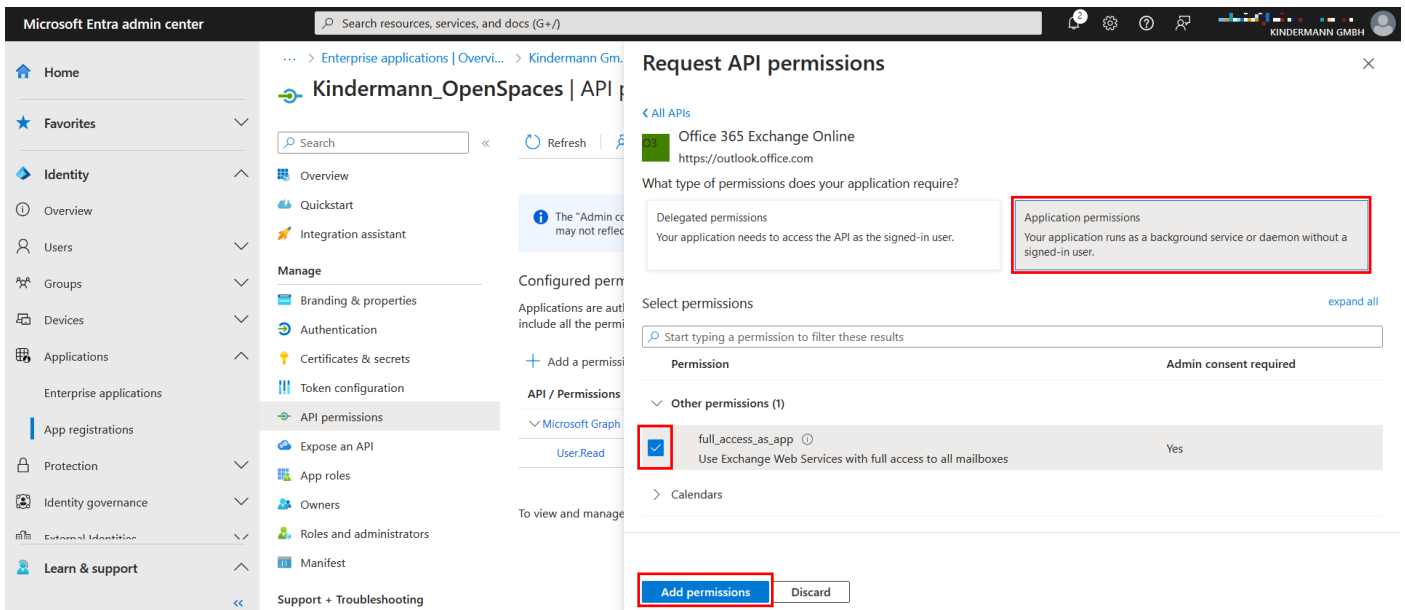
Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

Als nächstes wählen Sie „Application permissions“ aus, worauf die einstellbaren Berechtigungen darunter auftauchen. Aktivieren Sie unter dem Punkt „Other permissions“ den Haken „full\_access\_as\_app“ und speichern unten mit „Add permissions“.

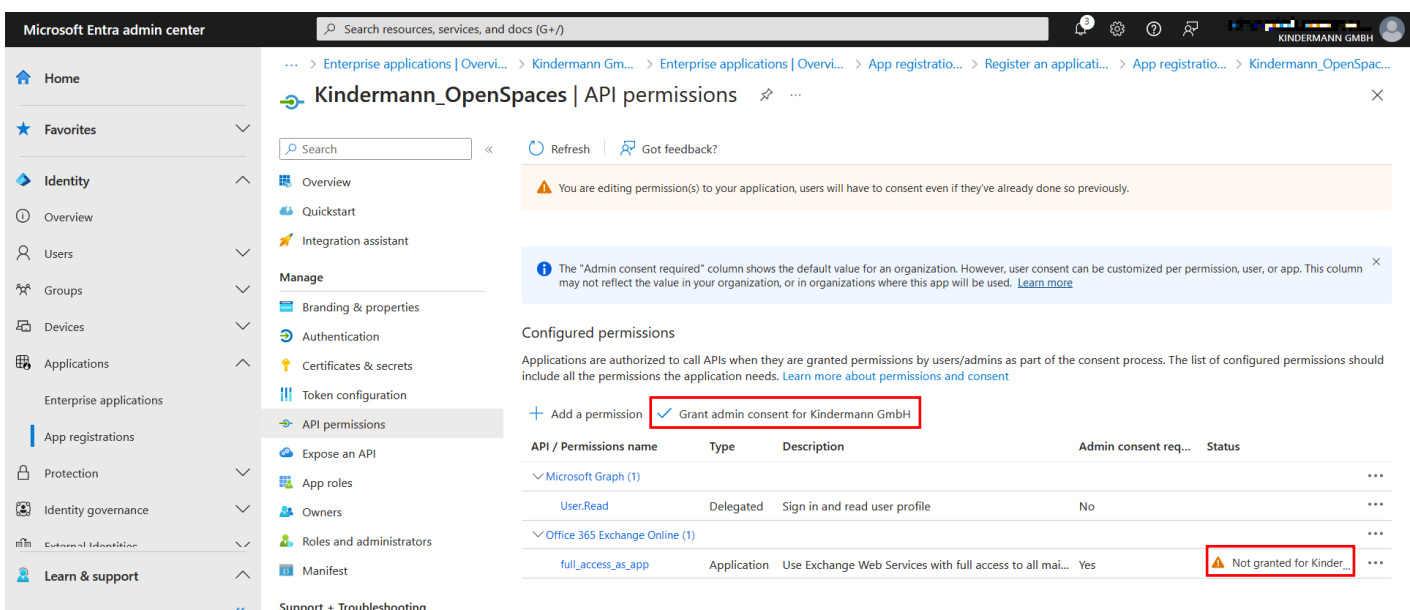
Zum ersten Einrichten von OpenSpaces muss diese Einstellung gesetzt werden.

Insofern der Dienst nicht auf alle Postfächer volle Berechtigungen bekommen soll, können diese im späteren Verlauf auf diejenigen (Raum-)Postfächer beschränkt werden.

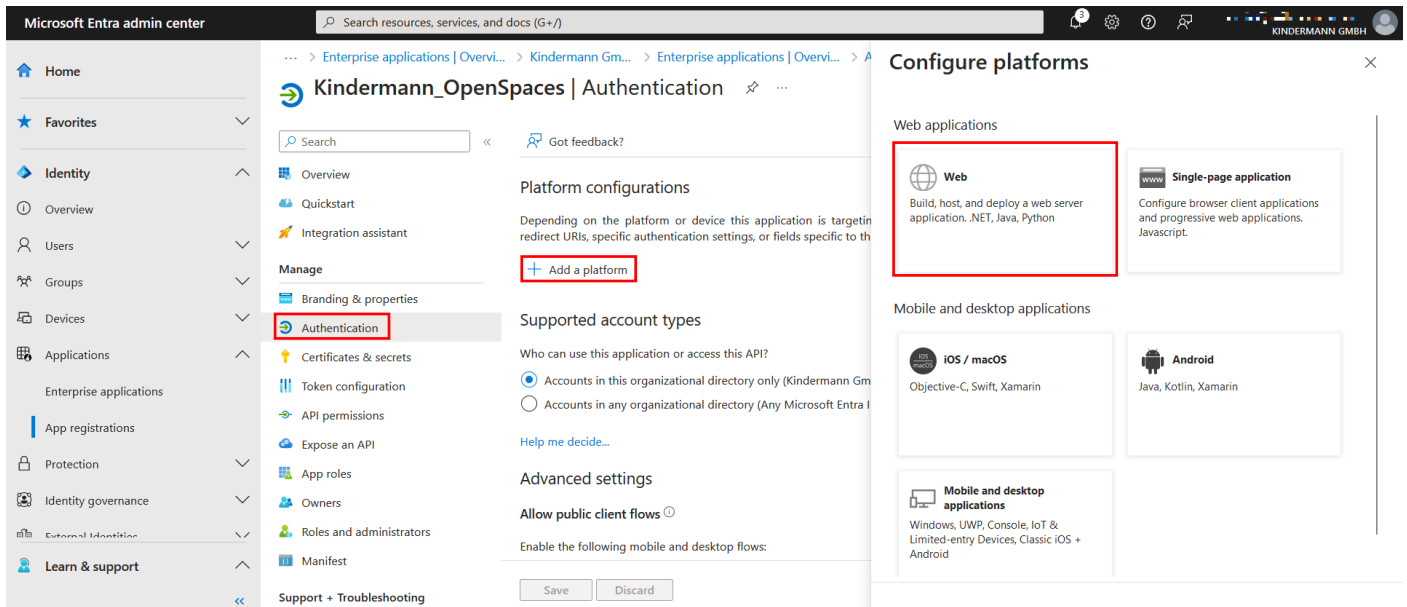
Springen Sie hierzu nach dem erfolgreichen Setup auf Seite 9.



Damit die Berechtigung angewendet wird, muss diese anschließend noch mit administrativen Berechtigungen freigegeben werden. Klicken Sie dafür in der Übersicht auf „Grant admin consent for [Unternehmensname]“.



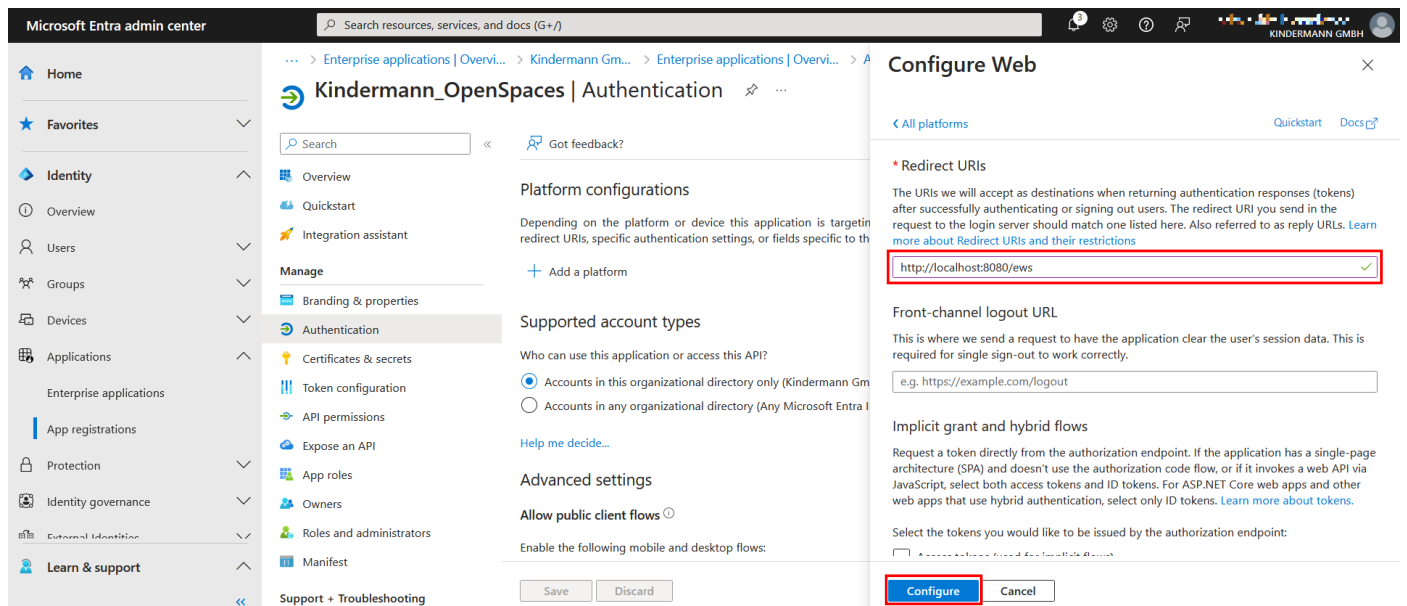
Ein letzter Schritt ist noch notwendig. Wechseln Sie in der Übersicht in den Reiter „Authentication“ und wählen „Add a platform“, um eine Redirect URL anzulegen. Von rechts klappt erneut ein Fenster auf, in dem „Web“ ausgewählt werden muss.



Geben Sie als Redirect URL die folgende Adresse an:

<http://localhost:8080/ews>

Bestätigen Sie mit „Configure“.



Damit ist die Konfiguration der Enterprise Application in Microsoft Entra ID abgeschlossen und Ihnen sollten folgende Daten vorliegen:

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

**Sie können nun mit der Konfiguration in der Hauptanleitung fortfahren** und die Daten in den Konfigurator eingeben. Ebenfalls können Sie dort die Verbindung zu Server prüfen.



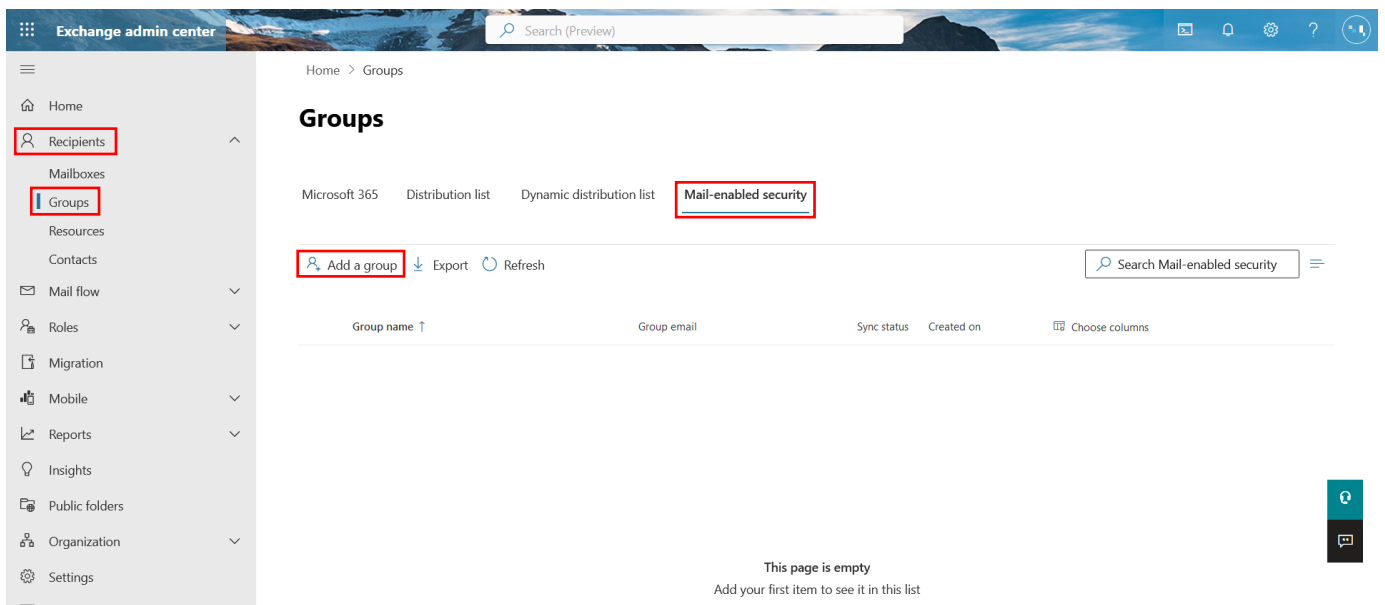
## Optional: Einschränken der Berechtigungen auf bestimmte Postfächer

Falls gewünscht kann die Berechtigung des Dienstes eingeschränkt werden, sodass dieser nicht auf die Kalender aller Postfächer ausgelesen werden können.

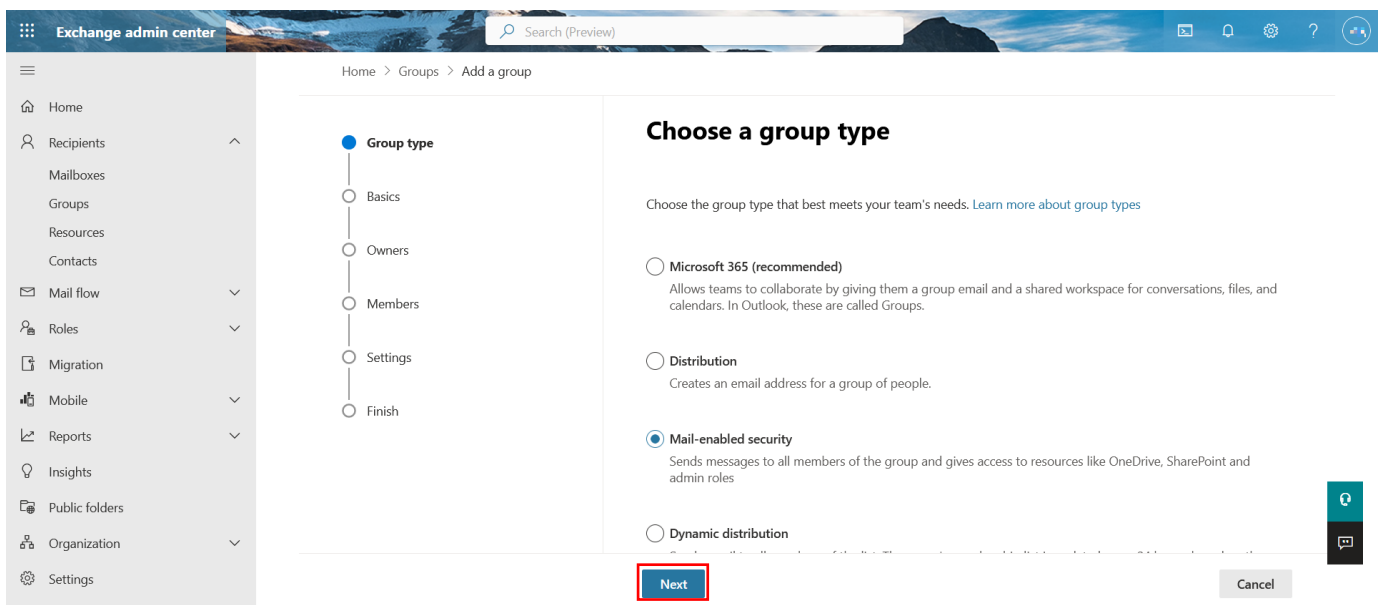
Dies wird notwendig, falls „full\_access\_as\_app“ nicht uneingeschränkt gestattet ist.

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

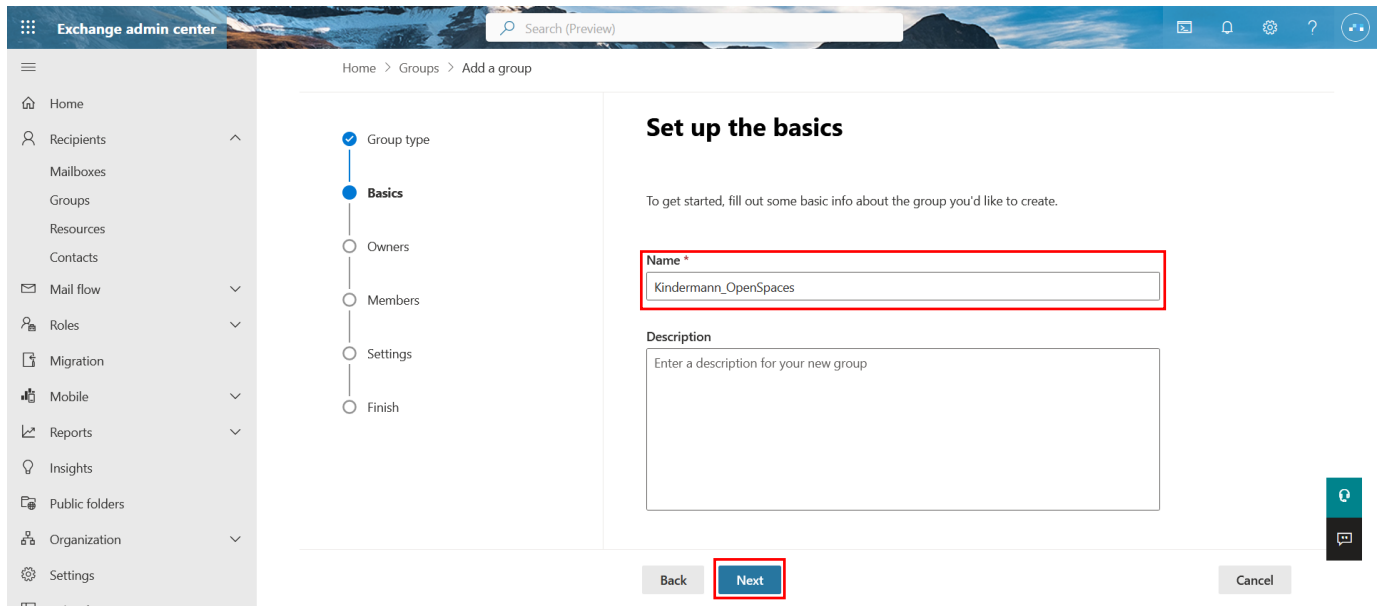
Für die Einrichtung wird eine E-Mail aktivierte Sicherheitsgruppe benötigt. Diese lässt sich im Exchange Online Admin Center im Reiter „Recipients“ unter „Groups“ anlegen. Wählen Sie „Mail-enabled security“ und legen Sie unter „Add a group“ ein solche Gruppe an.



Im folgenden Bildschirm können Sie bei angewählter „Mail-enabled security“ direkt auf „Next“ klicken.

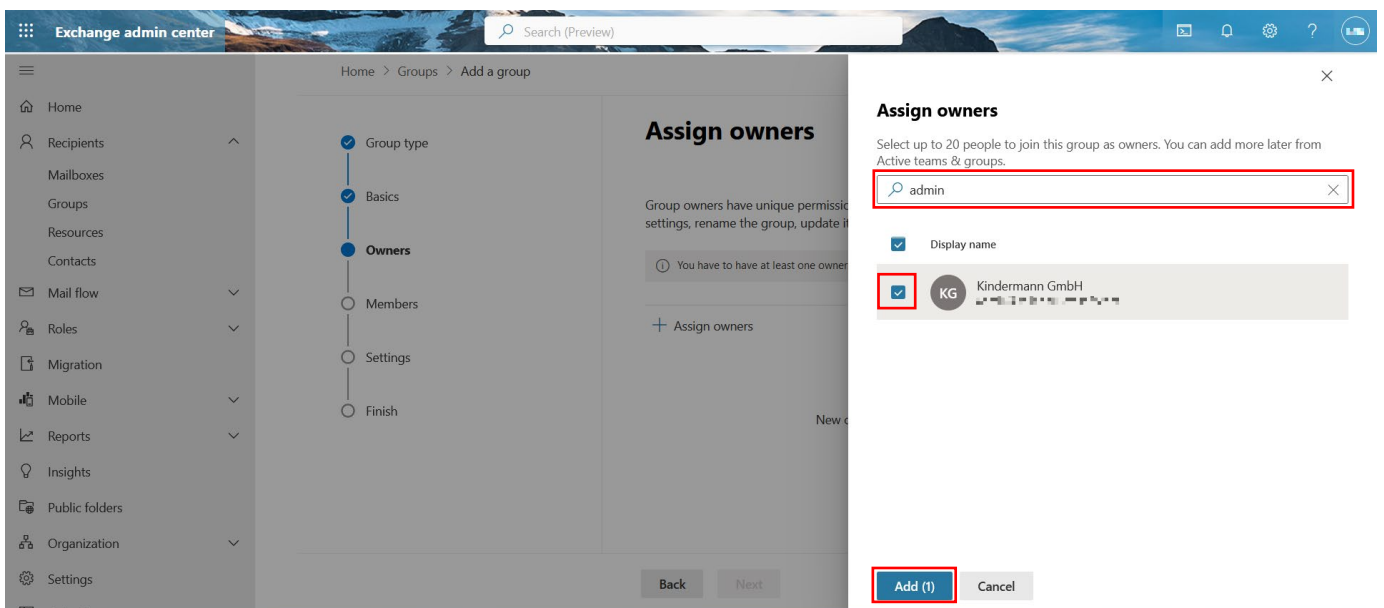


Wählen Sie einen plausiblen Anzeigenamen (z.B.: Kindermann\_OpenSpaces). Da die Notizen optional sind, können Sie direkt mit „Next“ fortfahren.



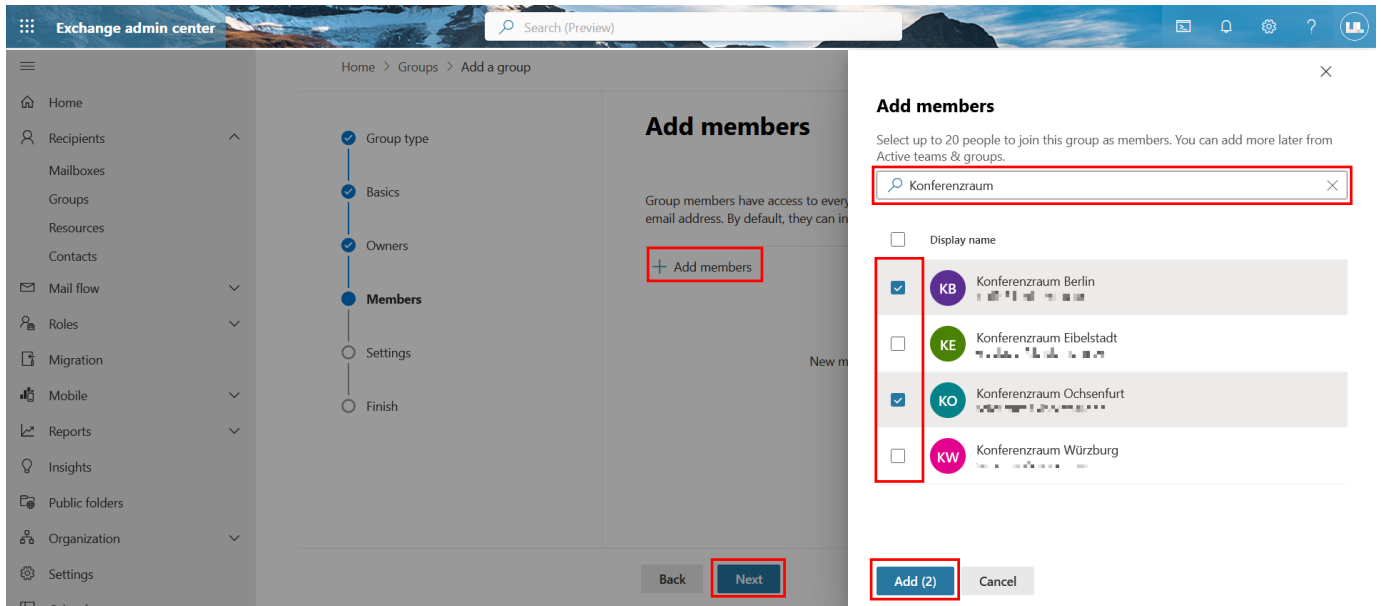
Suchen Sie im nächsten Fenster über das Suchfeld den Besitzer der Gruppe und haken Sie diesen unten an. Schließen Sie den Dialog anschließend mit „Add [Anzahl]“ und Klicken dann wieder auf „Next“.

Wir empfehlen die Admin-Adresse als Besitzer.

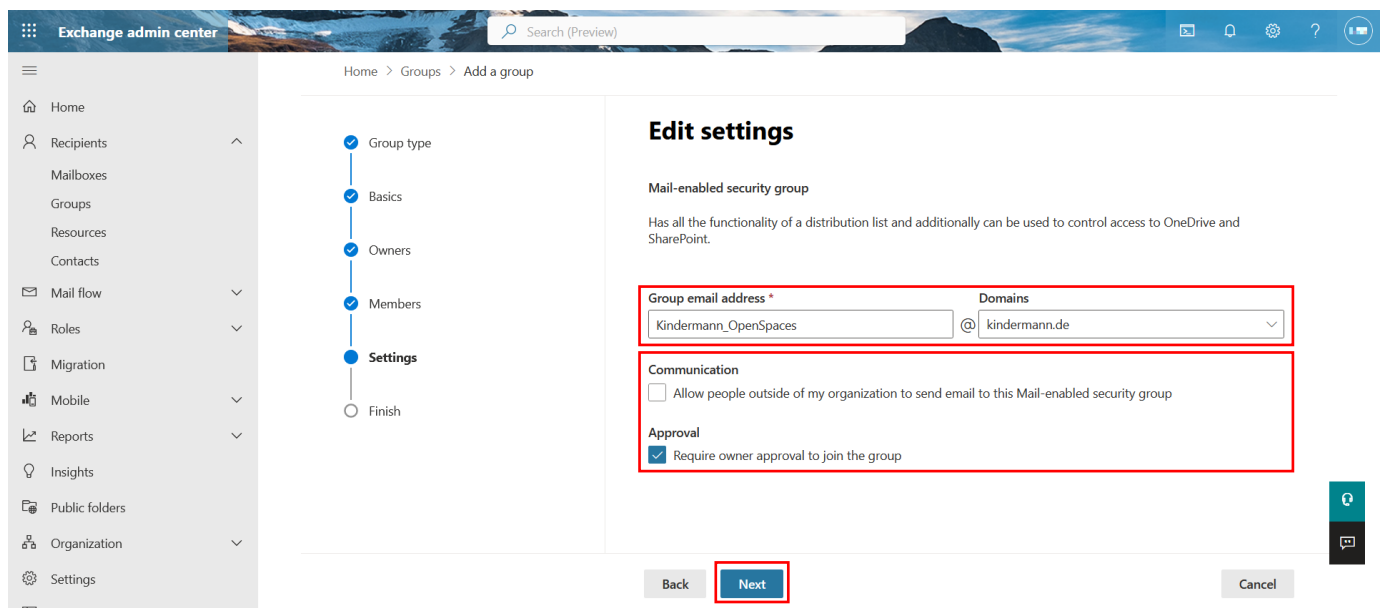


Als Mitglieder richten Sie unter „Add members“ die Postfächer ein, die Sie gern für den Abruf von OpenSpaces freigeben möchten. Diese können Sie über das Suchfeld suchen, anhaken und mit „Add [Anzahl]“ hinzufügen. Das Fenster schließt automatisch.

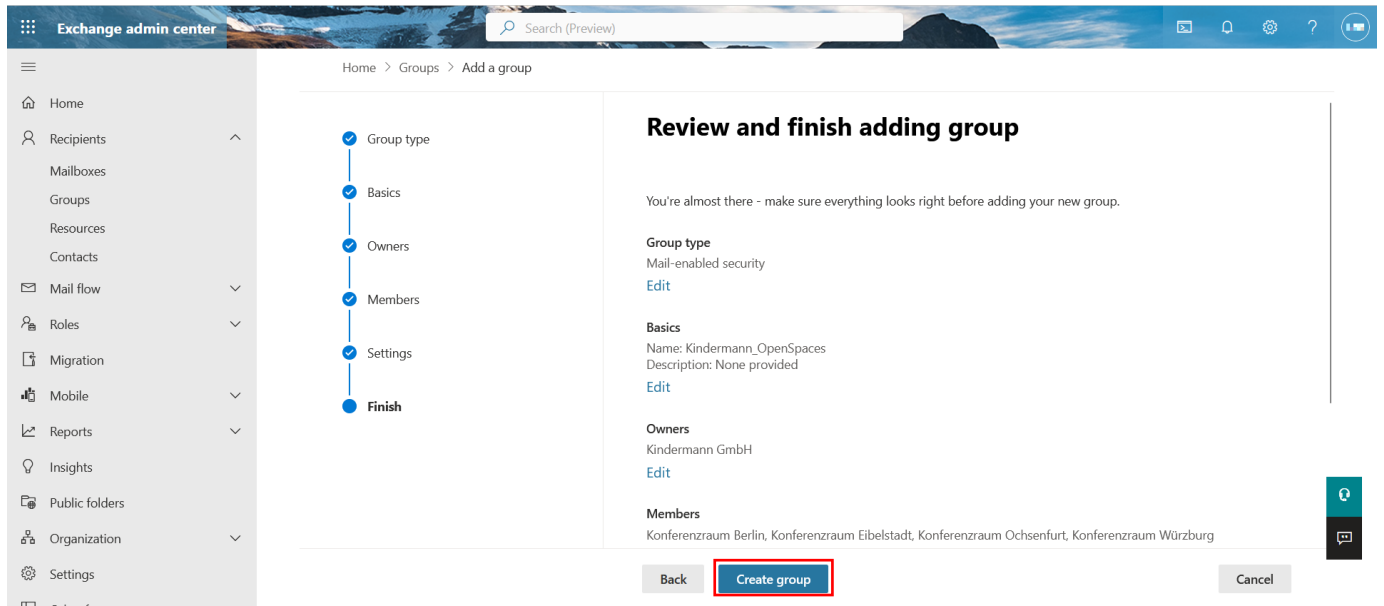
Wenn Sie alle hinzugefügt haben, bestätigen Sie mit „Next“.



Vergeben Sie im letzten Schritt eine Mail-Adresse für die Gruppe und notieren / kopieren Sie diese. Die Adresse wird anschließend benötigt. Setzen Sie die Haken wie abgebildet, sodass unbefugte Interaktionen mit der neu erstellten Gruppe ausgeschlossen sind. Bestätigen Sie mit „Next“.



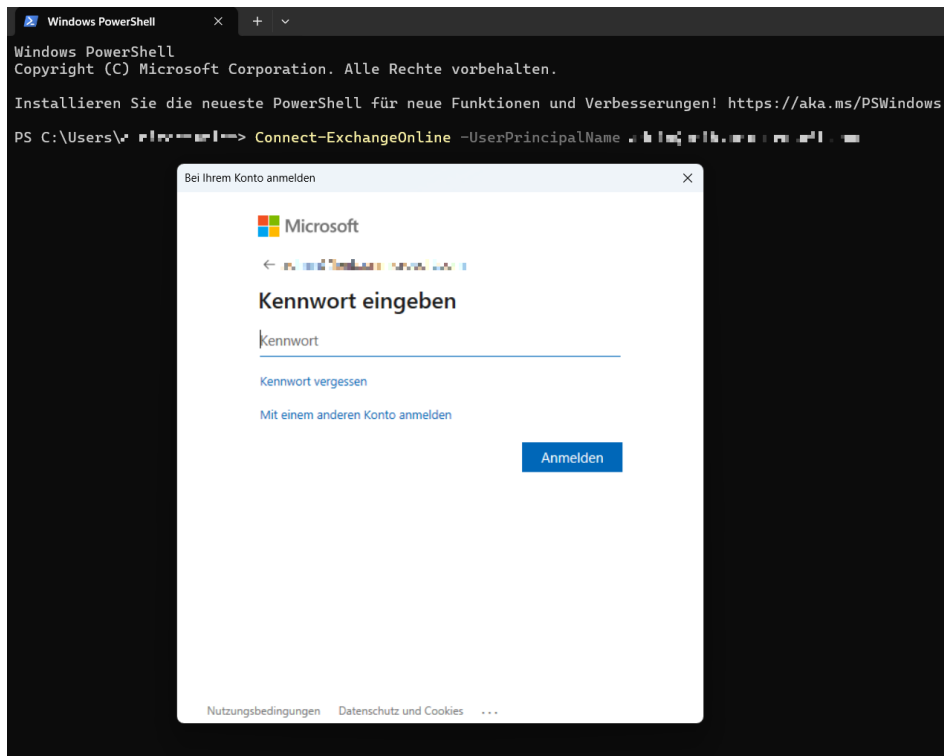
Prüfen Sie Ihre Eingaben und erstellen Sie die Gruppe mit „Create group“.



Nachdem die Gruppe angelegt wurde, kann die App auf diese Gruppe beschränkt werden. Dies geht über ein PowerShell CMDlet.

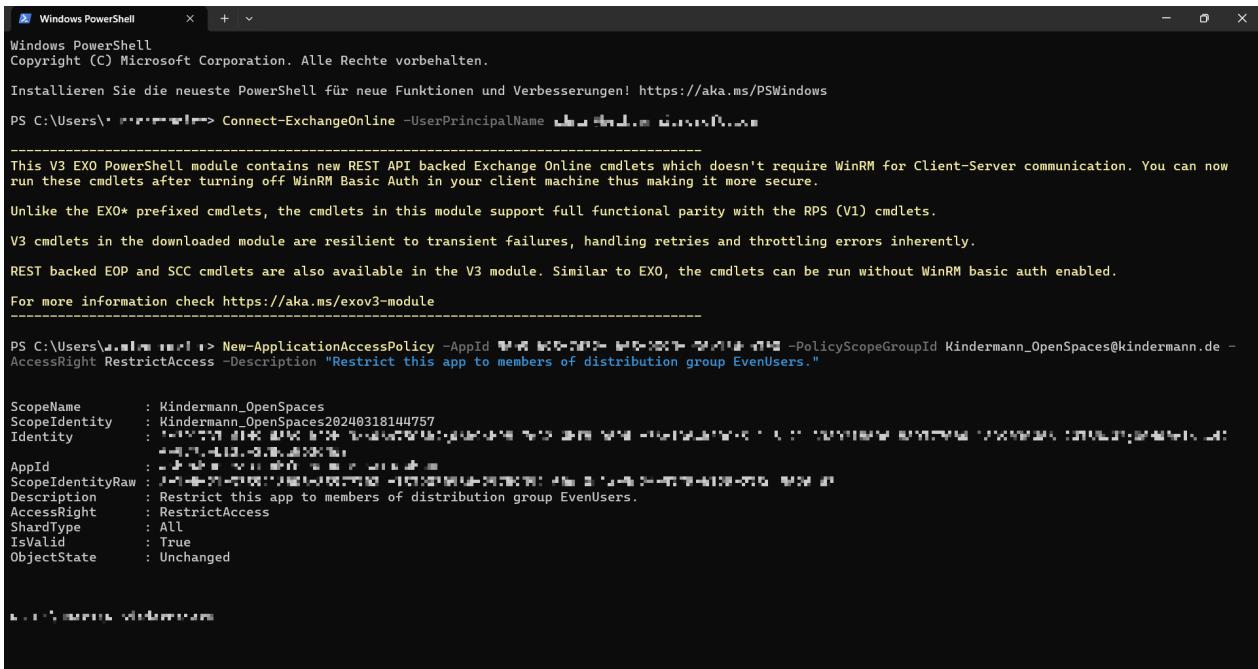
Öffnen Sie PowerShell und verbinden Sie sich mit Ihrem Exchange Online Server:

```
Connect-ExchangeOnline -UserPrincipalName [Mail Adresse Ihres Admin Accounts]
```



Anschließend führen Sie folgenden Befehl aus, um die Applikation auf die Gruppe zu beschränken:

```
New-ApplicationAccessPolicy -AppId [Ihre Application (client) ID] -PolicyScopeGroupId [Ihre Gruppen E-Mail Adresse] -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
```

Damit ist OpenSpaces auf die Mitglieder der Gruppe beschränkt. Die Gruppe und deren Mitglieder können auch nachträglich im Exchange Online Admin Center angepasst werden.