REI3 - How to setup a Microsoft 365 mailbox for OAuth2

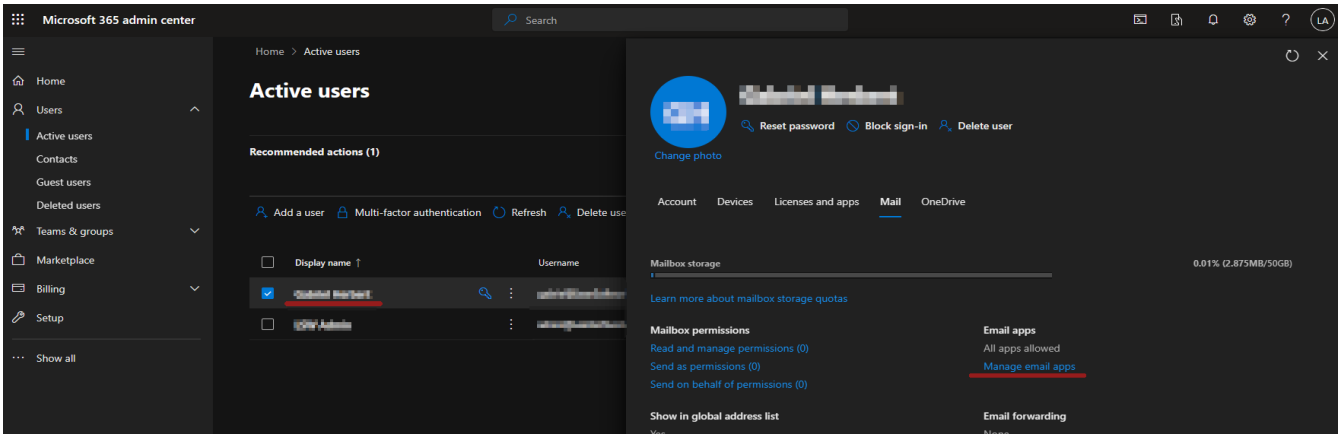
The following is a short introduction of how authentication between REI3 and an OAuth2 provider works. For just the setup instructions, read the next chapter.

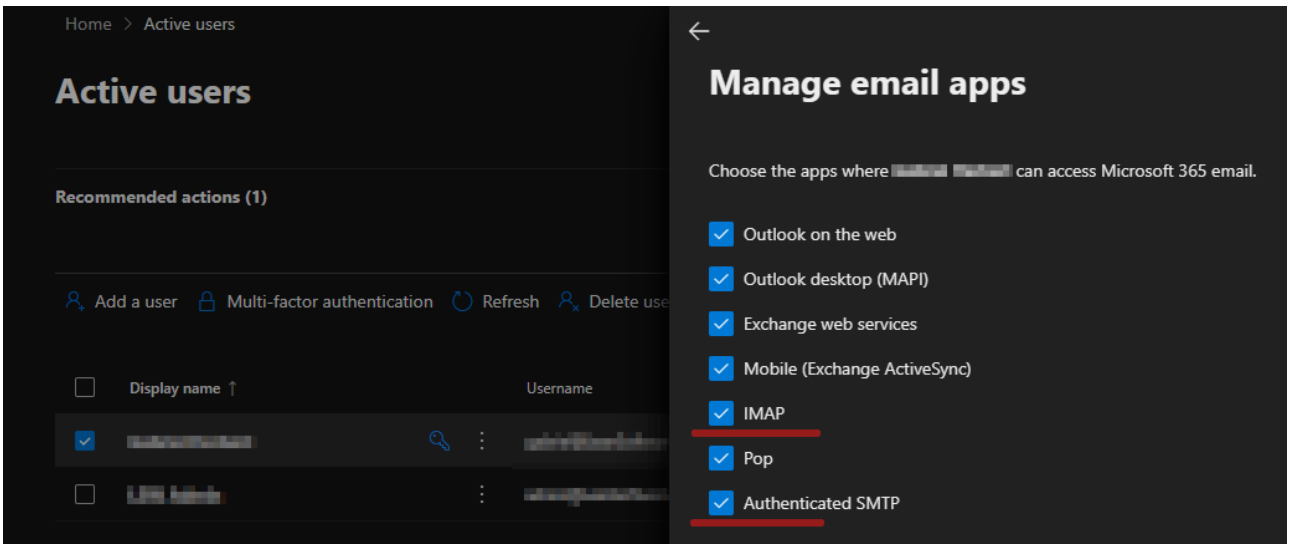
To send and receive emails, REI3 supports the OAuth2 standard for authentication. The OAuth2 standard includes different authentication schemes or 'flows' that serve various purposes. These flows can for example provide delegated access to resources owned by users or allow access in machine-2-machine communication scenarios.

The mailing feature in REI3 allows for sending and retrieving messages from one or multiple email accounts. It is best-practice that REI3 is the owner of the assigned mailboxes as it deletes messages after retrieving them - it should not be used to fetch messages from mailboxes accessed by people or other services. To access services over OAuth2, REI3 implements the 'client credentials flow'. This flow allows an owner (usually a server) to access owned resources (like a mailbox).

Setup instructions

1. Login into the MS365 admin panel (https://admin.microsoft.com/) with an admin account.
2. Make sure that SMTP & IMAP features are enabled for the REI3 mailbox.

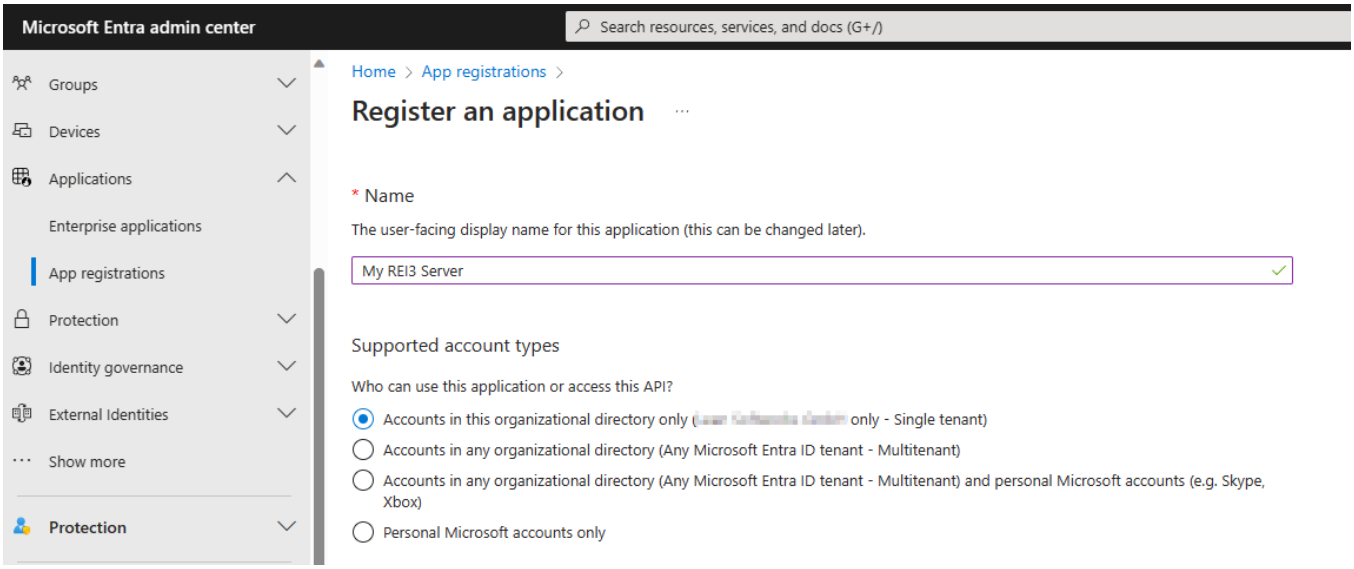




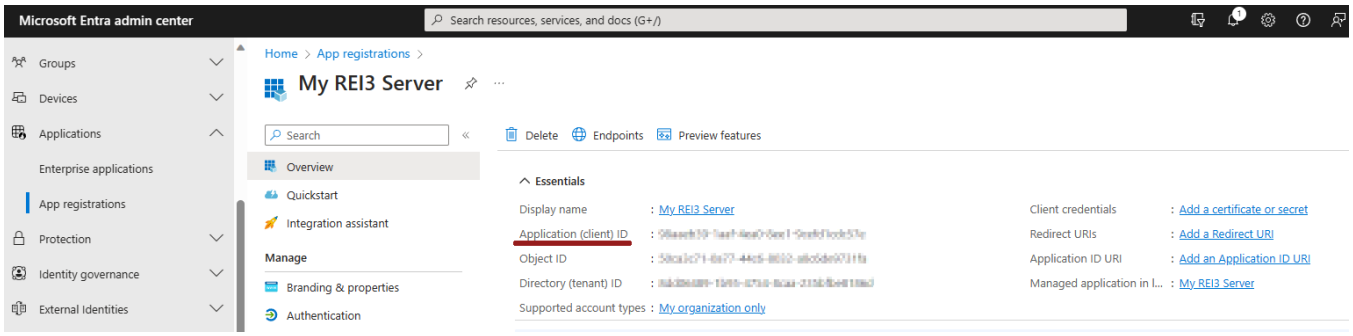
- Make sure that SMTP authentication is not disabled for the entire organization. This is a global setting. 'Legacy Authentication' is not required as we use 'Modern Authentication' via OAuth2.

3 Register REI3 as an application in Microsoft Entra (https://entra.microsoft.com/).

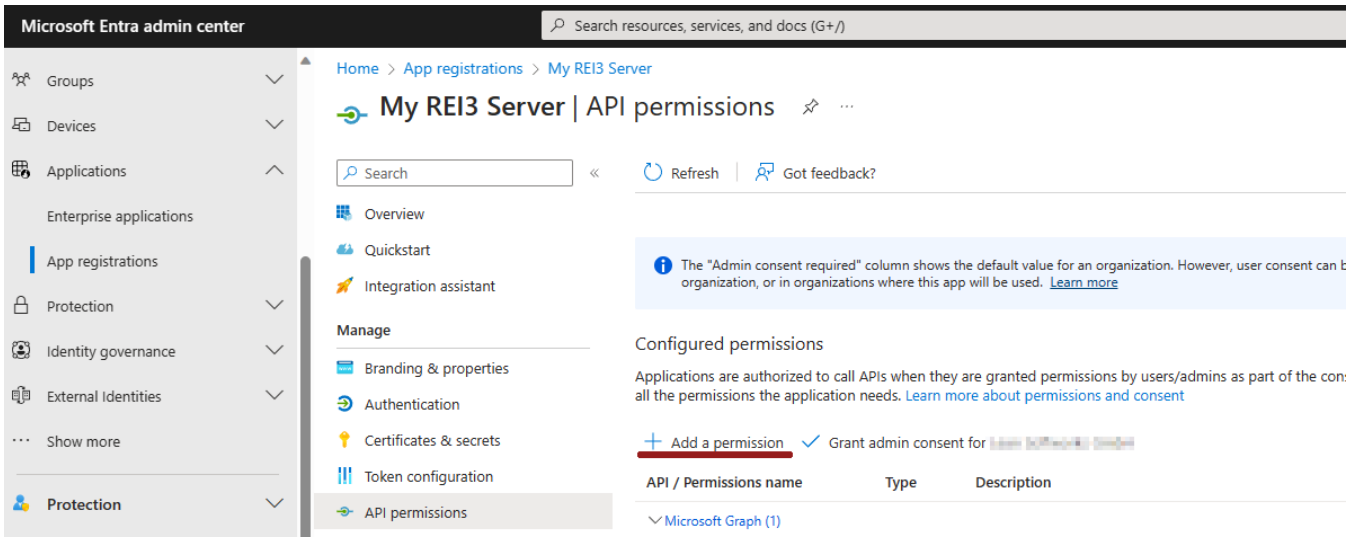
- For 'client credentials flow' (which we are doing here), only an application name is required for registration. This name can be anything (like 'My REI3 Server'). In most scenarios the single tenant mode is appropriate. A redirect URI is not required.



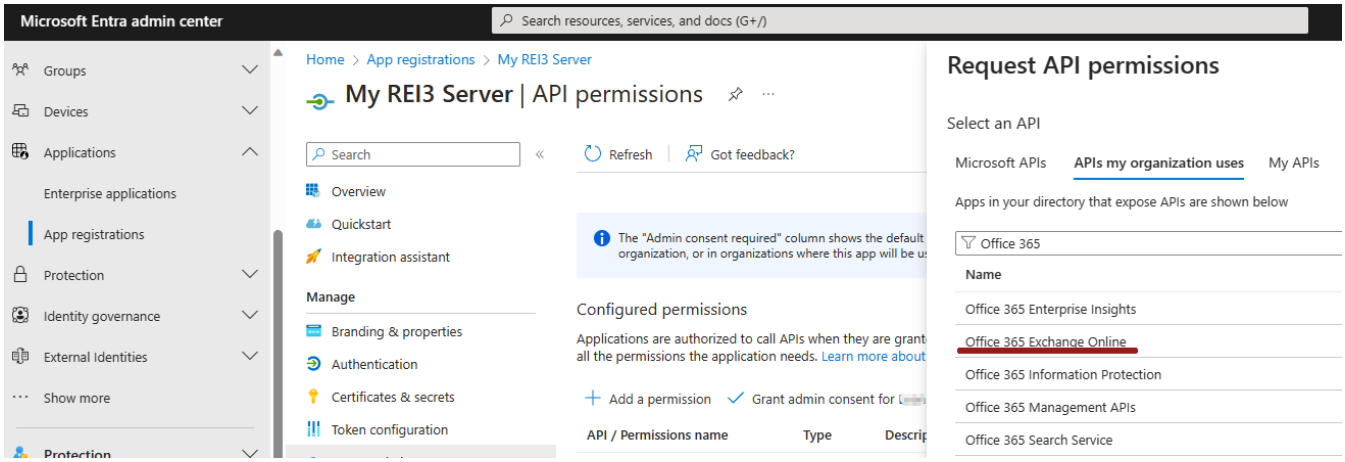
4 Select the newly created application and copy the 'Application (client) ID'.



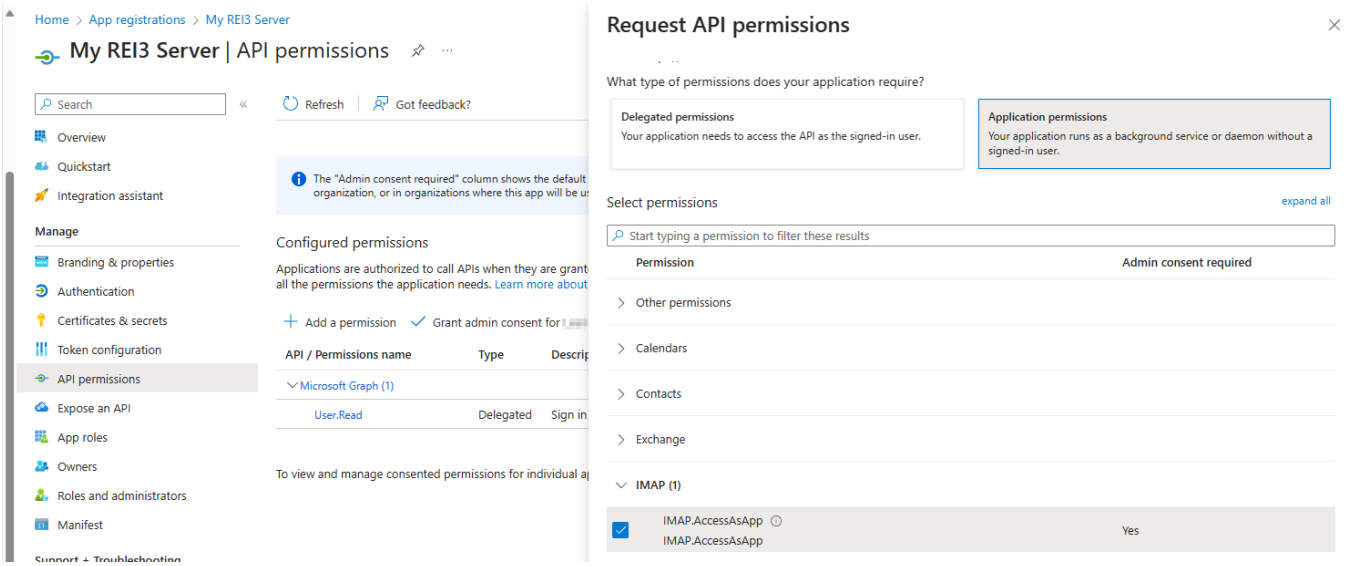
4.1 Go to 'API permissions' and click on 'Add a permission'.



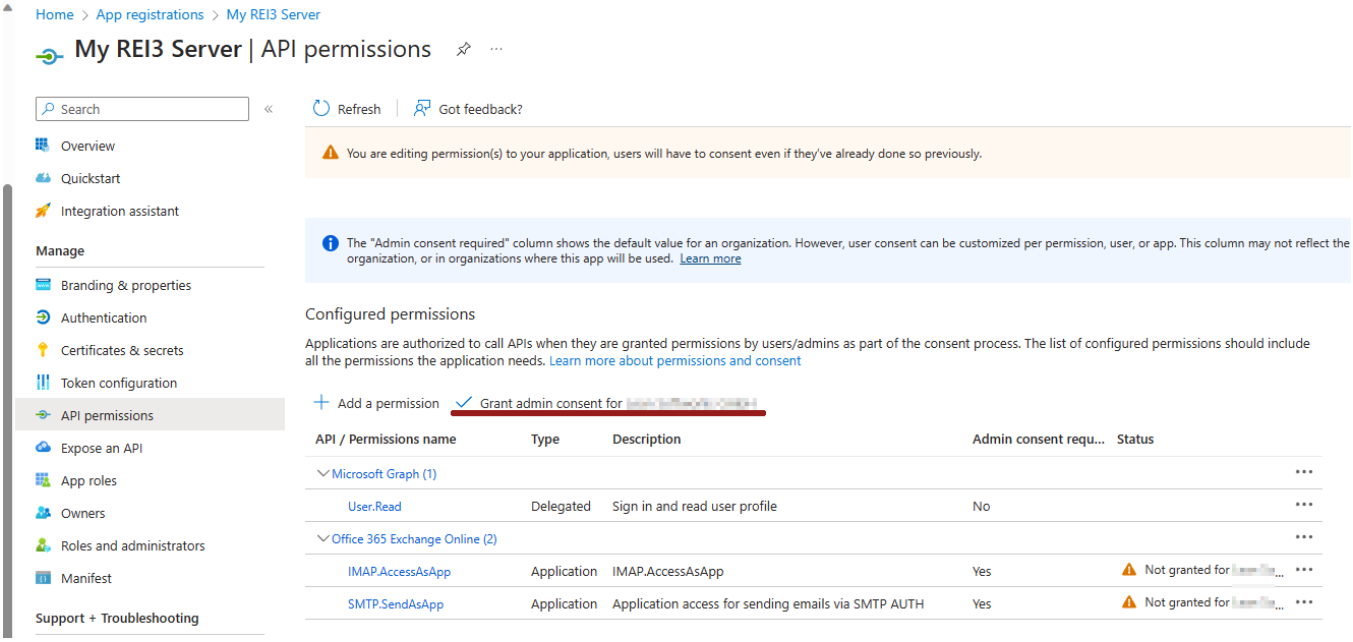
4.2 Select 'APIs my organization uses' and then select 'Office 365 Exchange Online'.



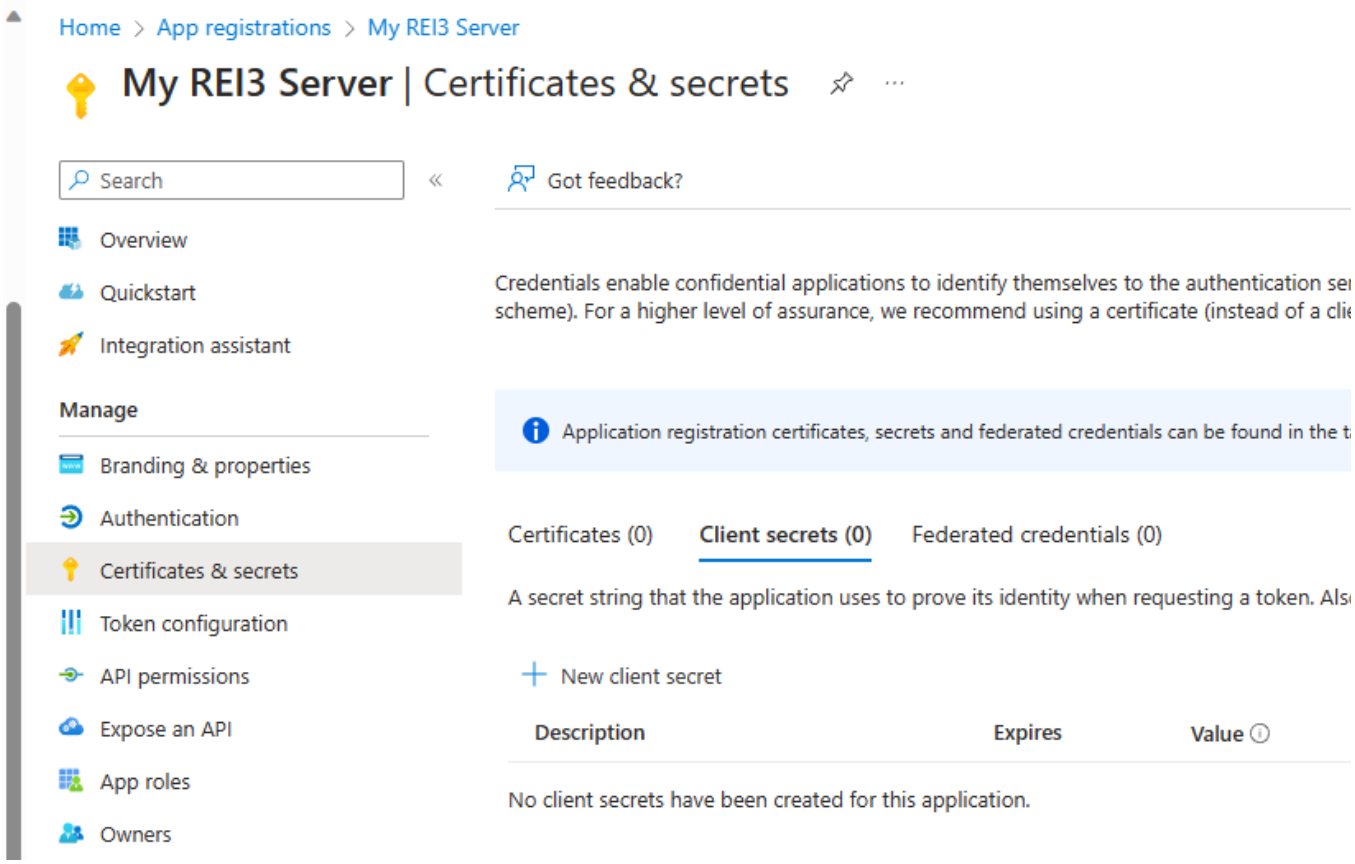
4.3 Under 'Application permissions', select 'IMAP.AccessAsApp' and 'SMTP.AccessAsApp'.

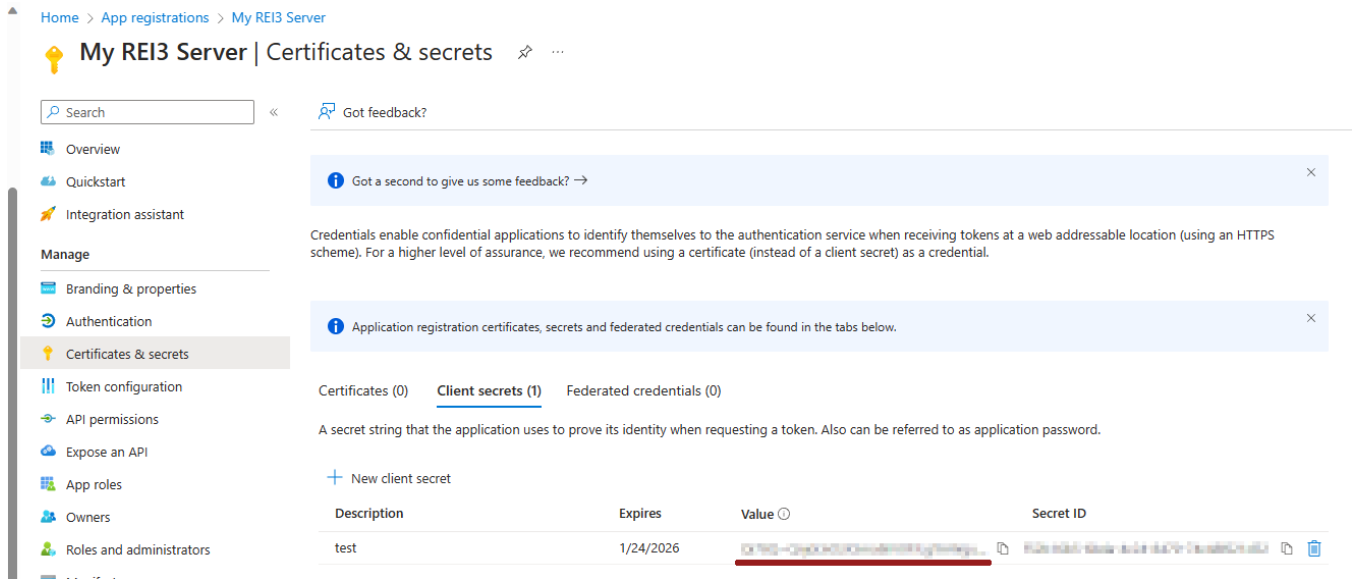


4.4 After saving, make sure to 'Grant admin consent for YOUR_TENANT_NAME'.

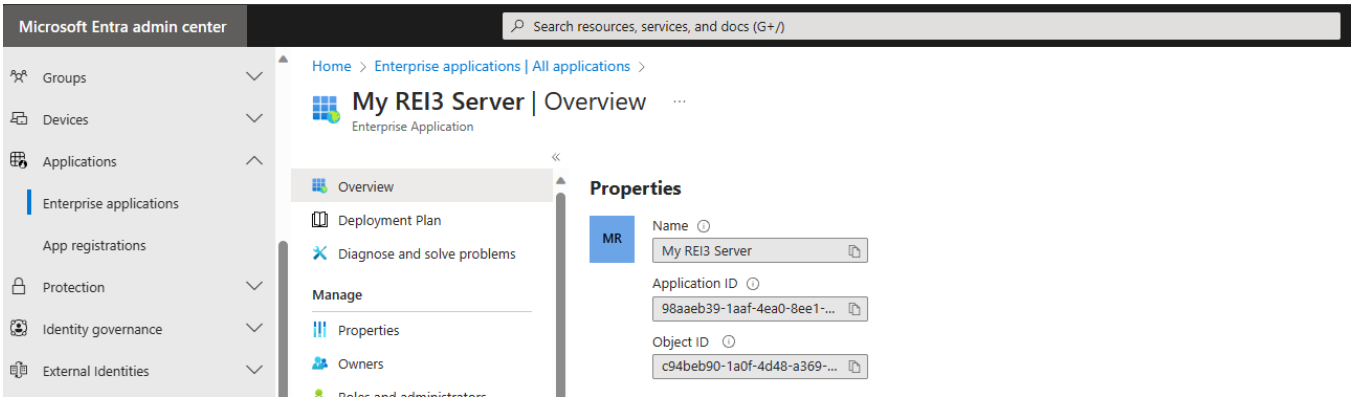


5 Create a client secret for the application. Copy the secret value immediately. It will not be available later.





6 Go to 'Enterprise applications', click on the new application and copy the 'Object ID'.



7 Connect to Microsoft Exchange Online via Powershell.

7.1 `Import-module ExchangeOnlineManagement`

- If this module is not available: `Install-Module -Name ExchangeOnlineManagement`

7.2 `New-ServicePrincipal -AppId APPLICATION_CLIENT_ID -ObjectId OBJECT_ID`

- This step registers your application as service principle in Exchange Online so that it can be authorized to access mailing ressources.
- The application client ID and object ID were created in the steps above.

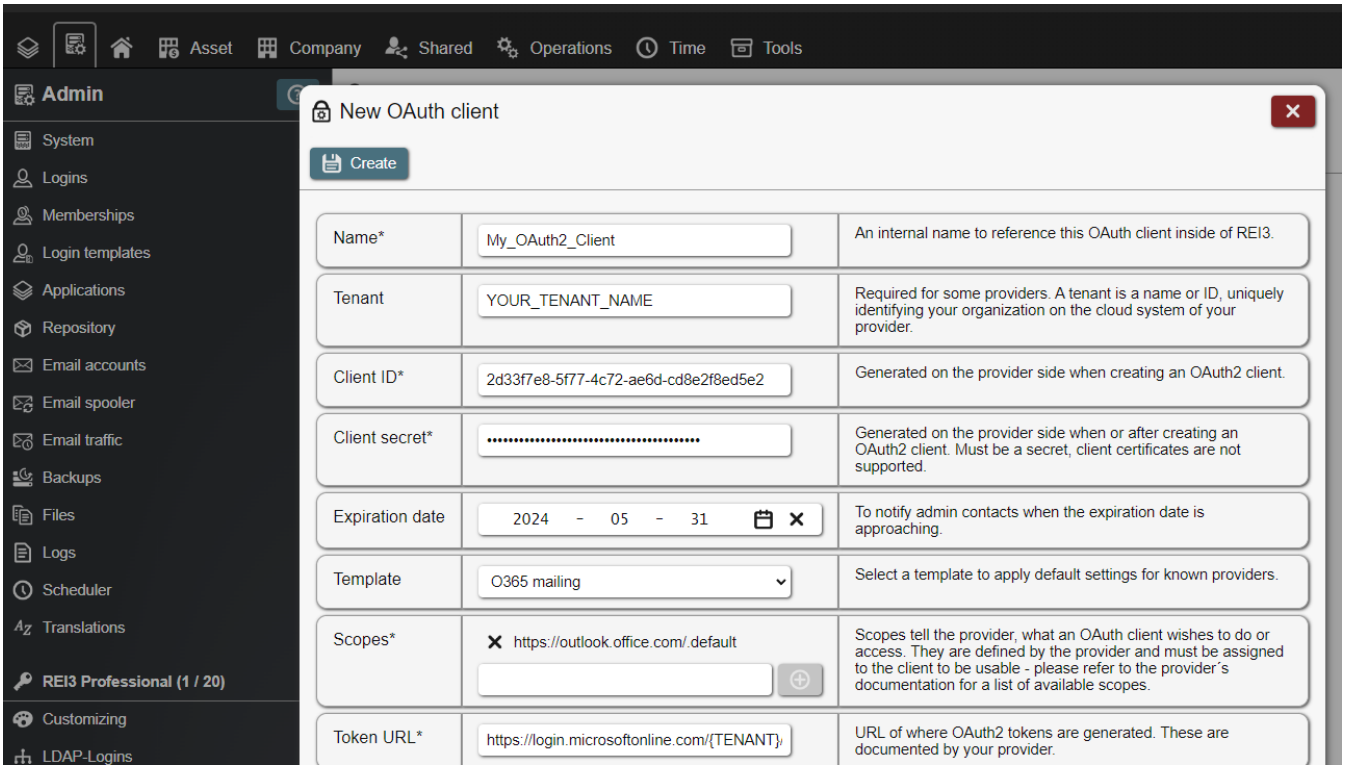
7.3 `Add-MailboxPermission -Identity "user@my-domain.com" -User OBJECT_ID -AccessRights FullAccess`

- This step gives full access permissions for the given mailbox to the newly created service principle.

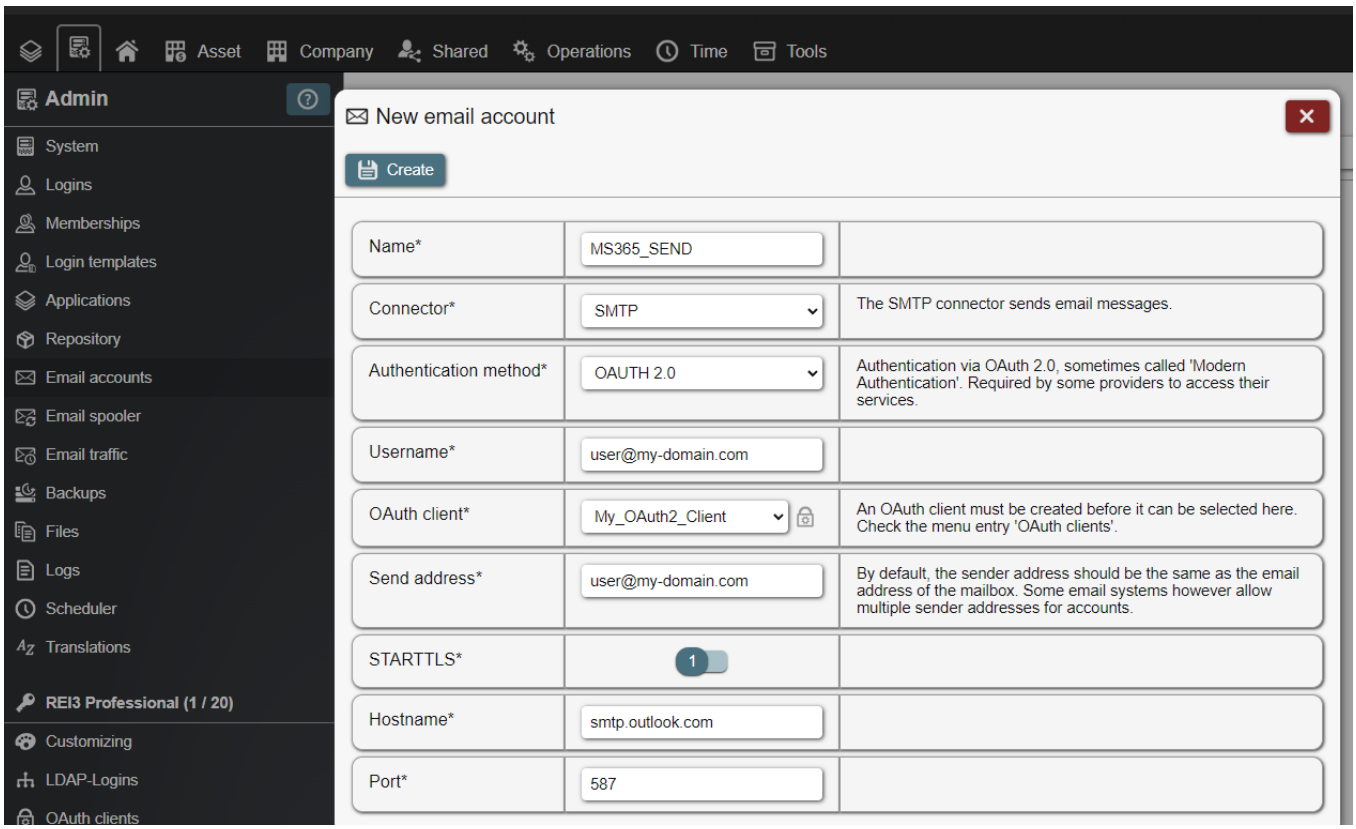
8 Log into REI3.

8.1 Create a new OAuth client.

- Make sure to enter the expiration date, chosen for the client secret so that REI3 can inform admin contacts when the expiration date is upcoming. When it expires, you need to create a new secret – all other settings (API permissions, exchange online settings, etc.) are unaffected and do not need to be redone.



8.2 Create one or two email accounts, for SMTP and/or IMAP, depending on your needs.



9 The setup should now be complete. To test successful authentication, you can try to send an email in the admin panel via the ‚Test email' feature under ‚Email accounts':