

REI3 - How to setup a Microsoft 365 mailbox for OAuth2

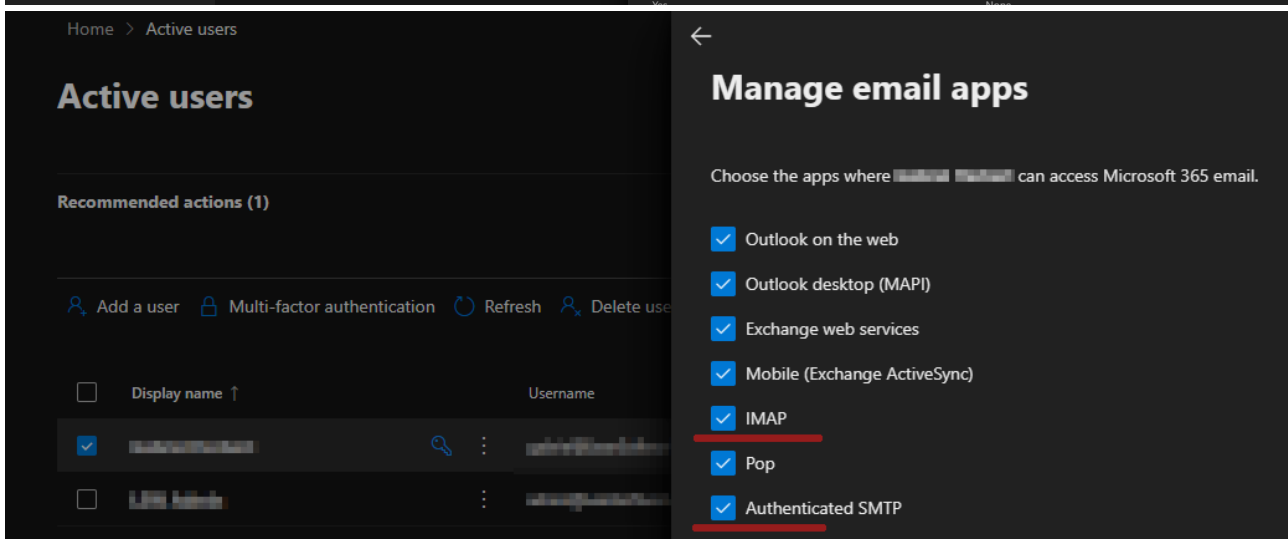
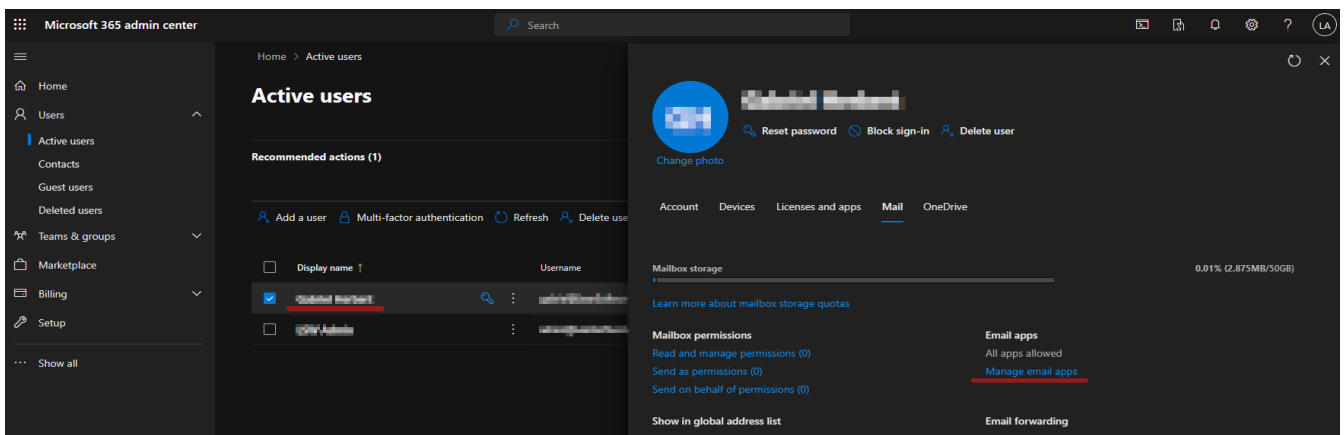
The following is a short introduction of how authentication between REI3 and an OAuth2 provider works. For just the setup instructions, read the next chapter.

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.

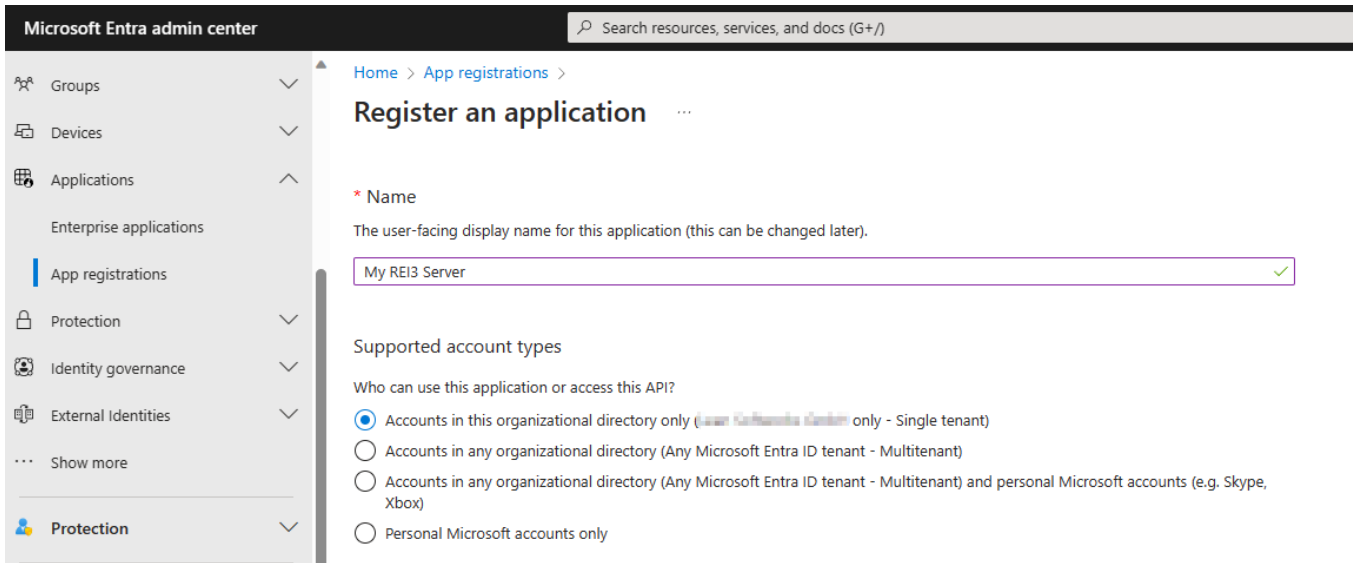
The mailing feature in REI3 allows for sending and retrieving messages from one or multiple email accounts. It is best-practice that REI3 is the owner of the assigned mailboxes as it deletes messages after retrieving them - it should not be used to fetch messages from mailboxes accessed by people or 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

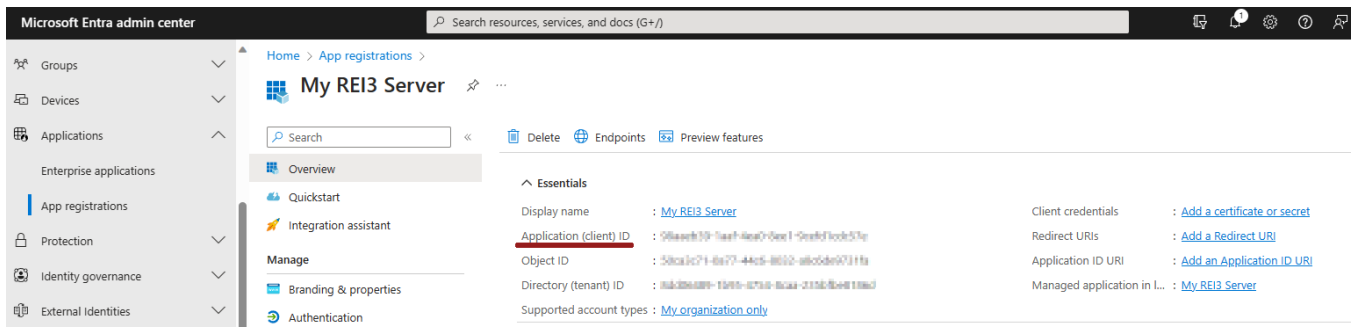
- 1 Login into the MS365 admin panel (<https://admin.microsoft.com/>) with an admin account.
- 2 Make sure that SMTP & IMAP features are enabled for the REI3 mailbox.



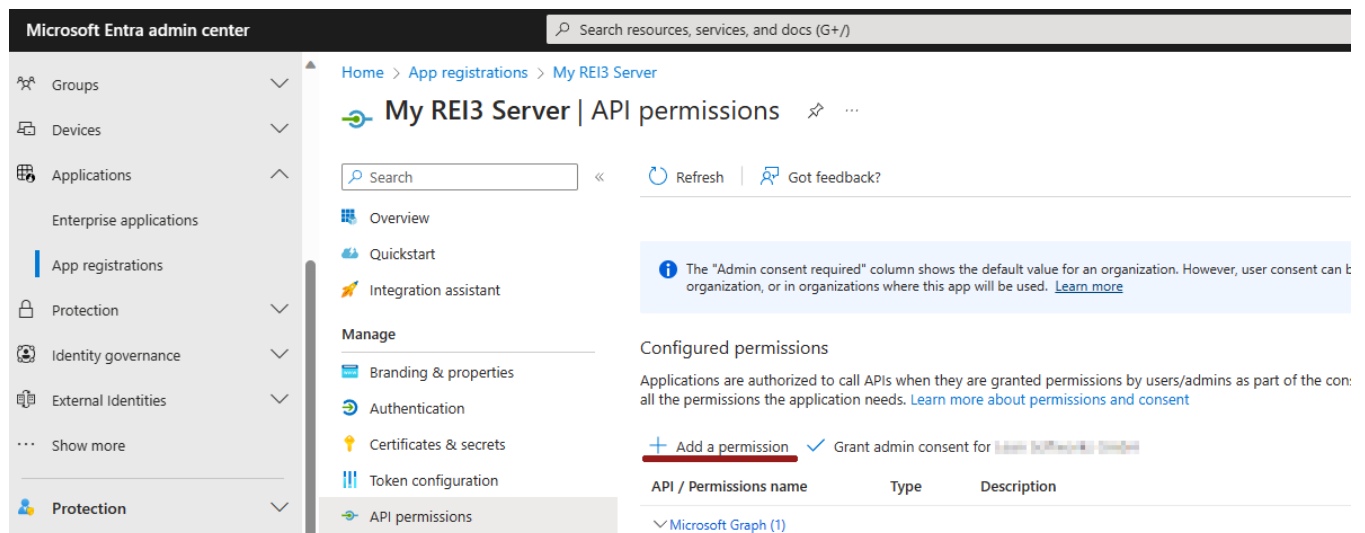
- Make sure that SMTP authentication is not disabled for the entire organization. This is a global setting. 'Legacy Authentication' is not required as we use 'Modern Authentication' via OAuth2.
- 3 Register REI3 as an application in Microsoft Entra (<https://entra.microsoft.com/>).
- For 'client credentials 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'.

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation pane with categories like Groups, Devices, Applications, and Protection. The main area is titled 'My REI3 Server | API permissions'. A 'Request API permissions' dialog is open, showing a search for 'Office 365' and a list of APIs. 'Office 365 Exchange Online' is selected and highlighted in red.

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

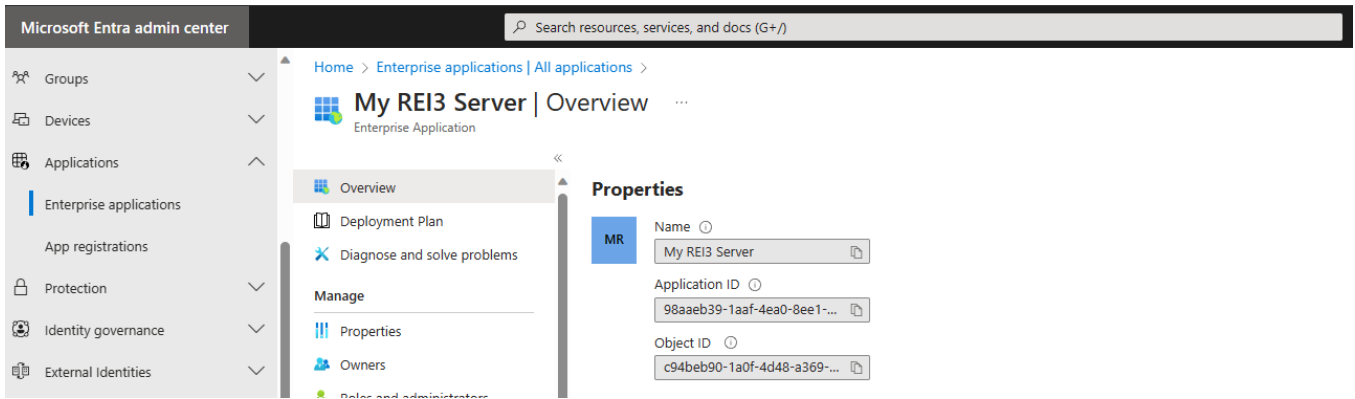
This screenshot shows the 'Request API permissions' dialog with the 'Application permissions' tab selected. A message asks 'What type of permissions does your application require?'. Below, the 'Select permissions' section shows a list of permissions. 'IMAP.AccessAsApp' is checked, and its 'Admin consent required' status is 'Yes'.

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

The screenshot shows the 'Configured permissions' table in the Microsoft Entra admin center. A warning message at the top states: 'You are editing permission(s) to your application, users will have to consent even if they've already done so previously.' The table lists permissions for 'Microsoft Graph' and 'Office 365 Exchange Online'. The 'IMAP.AccessAsApp' and 'SMTP.SendAsApp' permissions are marked as 'Admin consent required' and have a warning icon indicating they are not granted for the current user.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	
Office 365 Exchange Online (2)				
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	⚠ Not granted for [user]...
SMTP.SendAsApp	Application	Application access for sending emails via SMTP AUTH	Yes	⚠ Not granted for [user]...

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 resources.
- 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.

The screenshot shows the 'New OAuth client' form in the REI3 Admin interface. The form is titled 'New OAuth client' and has a 'Create' button. The form fields are as follows:

Name*	My_OAuth2_Client	An internal name to reference this OAuth client inside of REI3.
Tenant	YOUR_TENANT_NAME	Required for some providers. A tenant is a name or ID, uniquely identifying your organization on the cloud system of your provider.
Client ID*	2d33f7e8-5f77-4c72-ae6d-cd8e2f8ed5e2	Generated on the provider side when creating an OAuth2 client.
Client secret*	Generated on the provider side when or after creating an OAuth2 client. Must be a secret, client certificates are not supported.
Expiration date	2024 - 05 - 31	To notify admin contacts when the expiration date is approaching.
Template	O365 mailing	Select a template to apply default settings for known providers.
Scopes*	<input checked="" type="checkbox"/> https://outlook.office.com/.default	Scopes tell the provider, what an OAuth client wishes to do or access. They are defined by the provider and must be assigned to the client to be usable - please refer to the provider's documentation for a list of available scopes.
Token URL*	https://login.microsoftonline.com/{TENANT}	URL of where OAuth2 tokens are generated. These are documented by your provider.

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

The screenshot shows the 'New email account' form in the REI3 Admin interface. The form is titled 'New email account' and has a 'Create' button. The form fields are as follows:

Name*	MS365_SEND	
Connector*	SMTP	The SMTP connector sends email messages.
Authentication method*	OAUTH 2.0	Authentication via OAuth 2.0, sometimes called 'Modern Authentication'. Required by some providers to access their services.
Username*	user@my-domain.com	
OAuth client*	My_OAuth2_Client	An OAuth client must be created before it can be selected here. Check the menu entry 'OAuth clients'.
Send address*	user@my-domain.com	By default, the sender address should be the same as the email address of the mailbox. Some email systems however allow multiple sender addresses for accounts.
STARTTLS*	<input checked="" type="checkbox"/>	
Hostname*	smtp.outlook.com	
Port*	587	

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':

