Guide to creating a tenant using modern authentication

Version 3.1

Welcome to our step-by-step guide to modern authentication!

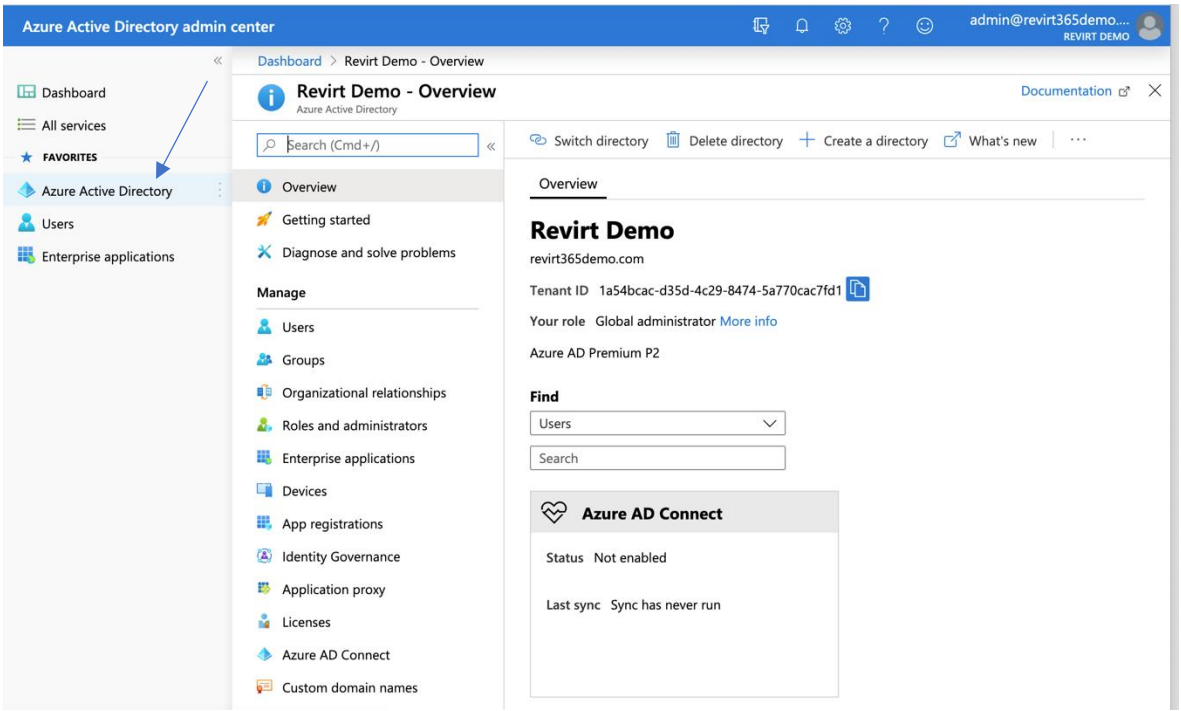
We look forward to showing you how you customise your service account for modern authentication, so you can move on with setting up your Microsoft 365 management portal.

Please keep the following important points in mind:

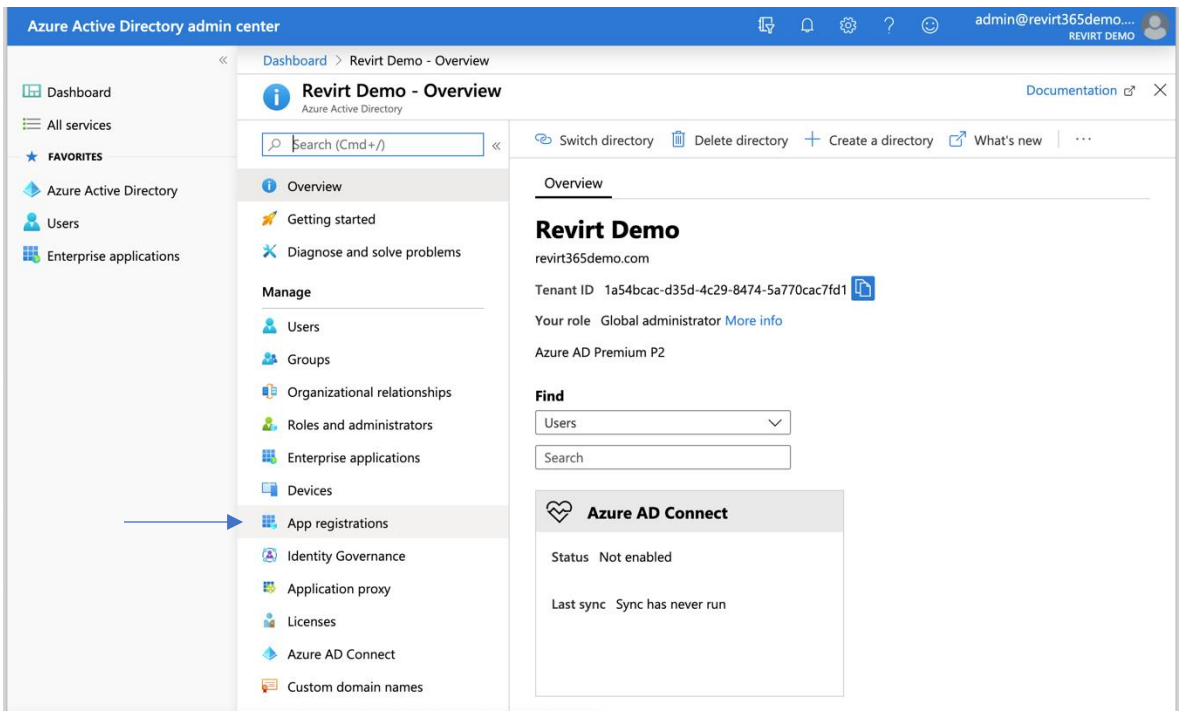
Modern authentication and 2FA go hand in hand, so 2FA is required. The same goes for admin rights which you need in order to perform the steps in this guide.

Part 1: How you add an app registration in Azure

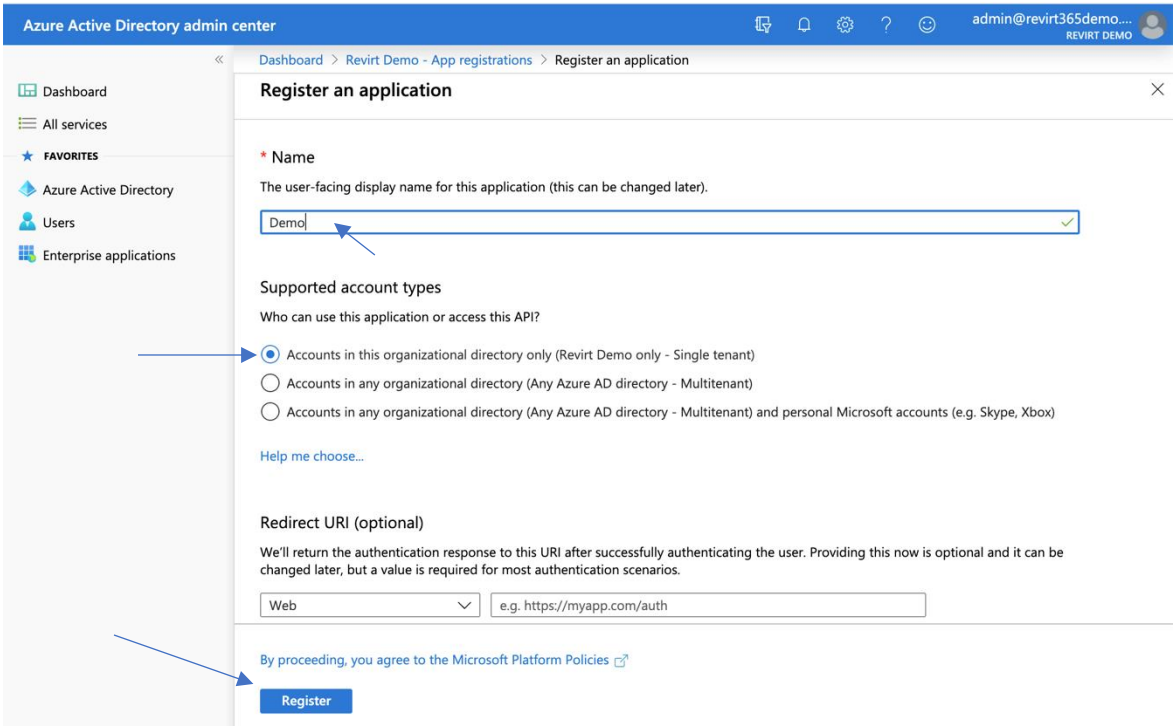
- Log into the Azure portal with your admin account.
- Click on “Azure Active Directory” (look under “More services” to the right, if you don’t see it).



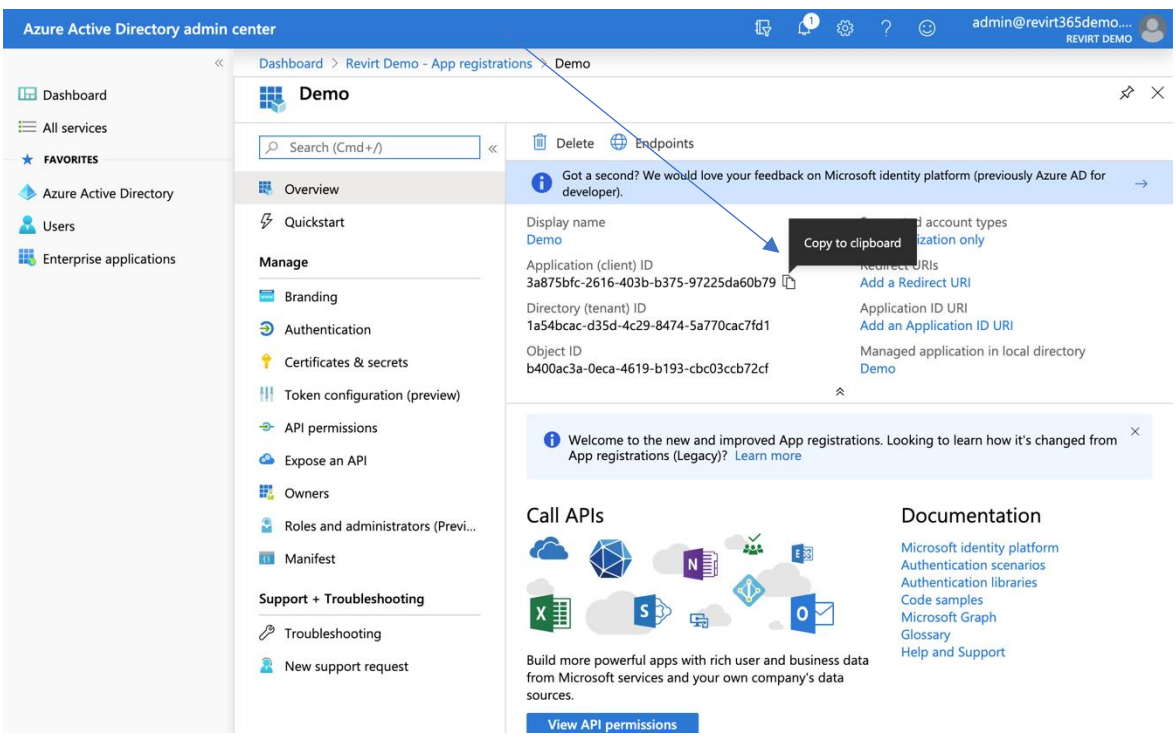
- Click on “App registrations”



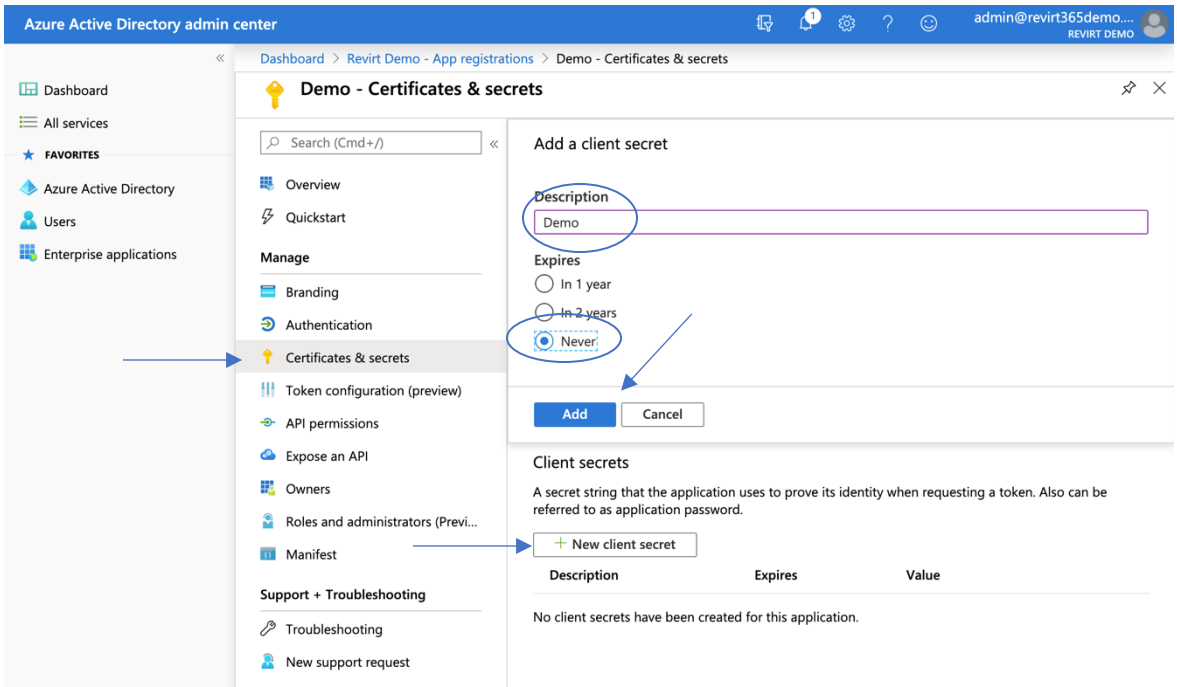
- Click on “New registration” and enter a name. We recommend using a name that makes it easy to identify in the future. For instance, "Microsoft 365 Backup"
- Make sure you check the single tenant option under “Supported account types”.
- Click on “Register”.



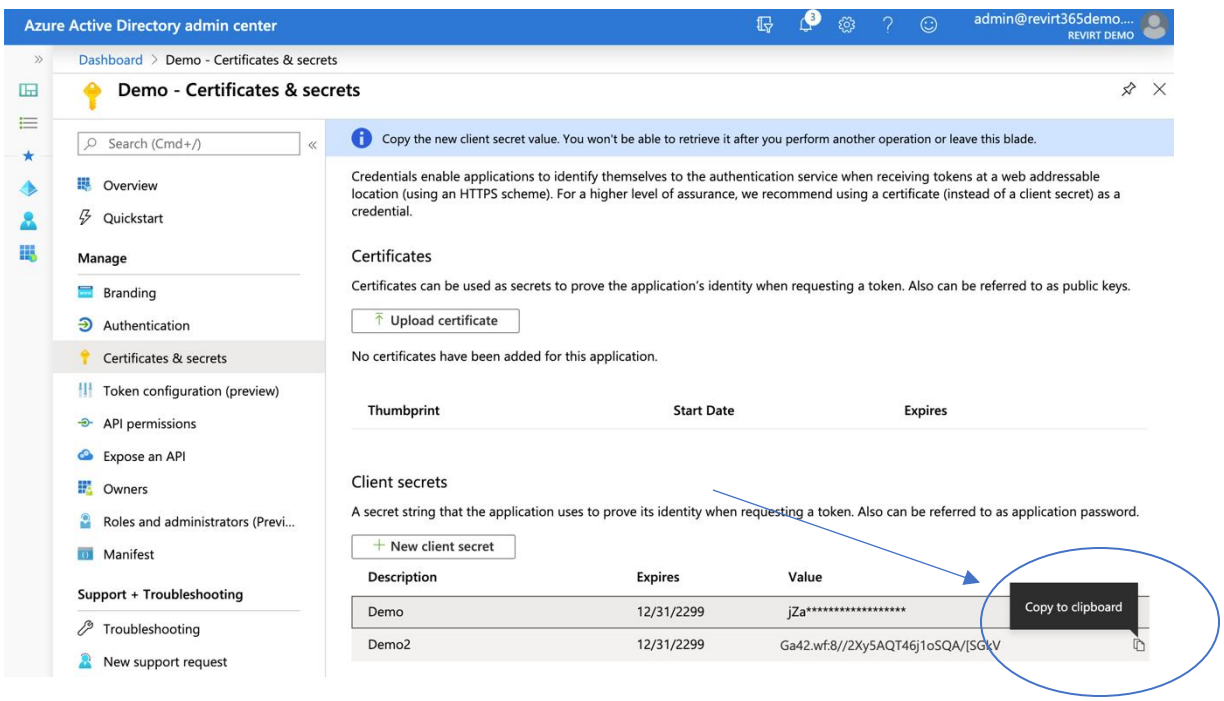
- Copy the application ID and save it, as you **will** need it later.



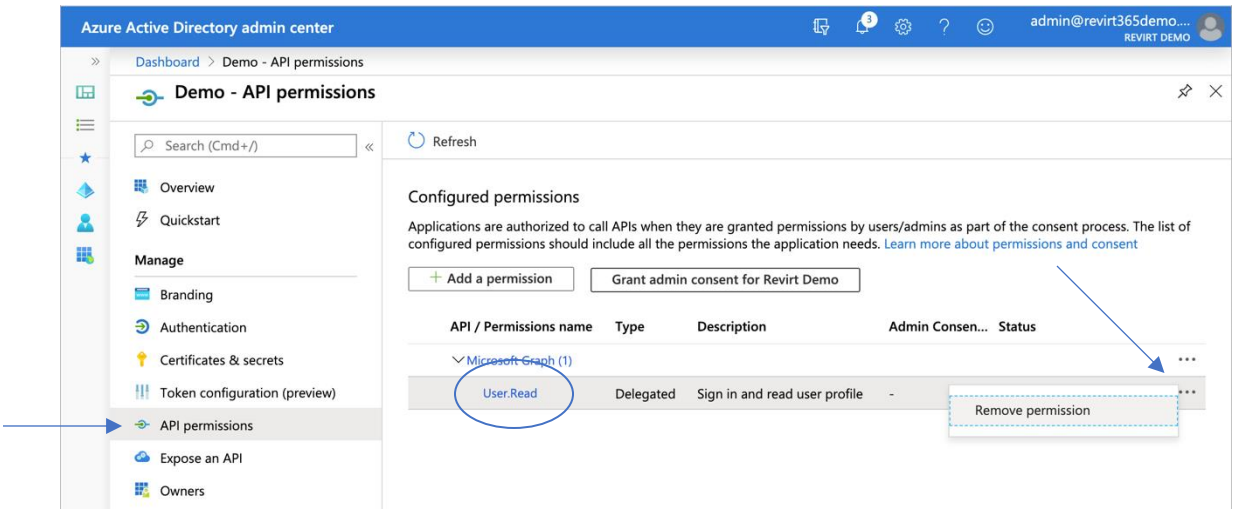
- Select “Certificates and secrets”.
- Click on “New client secret” and name it in the ”Description”. We recommend you choose the “Never” option under “Expires”
- Click “Add”.



- Copy your secret key by clicking the copy icon to the right. It is important to copy the secret key upon creating the key, since it is not possible to access at any other time later on.



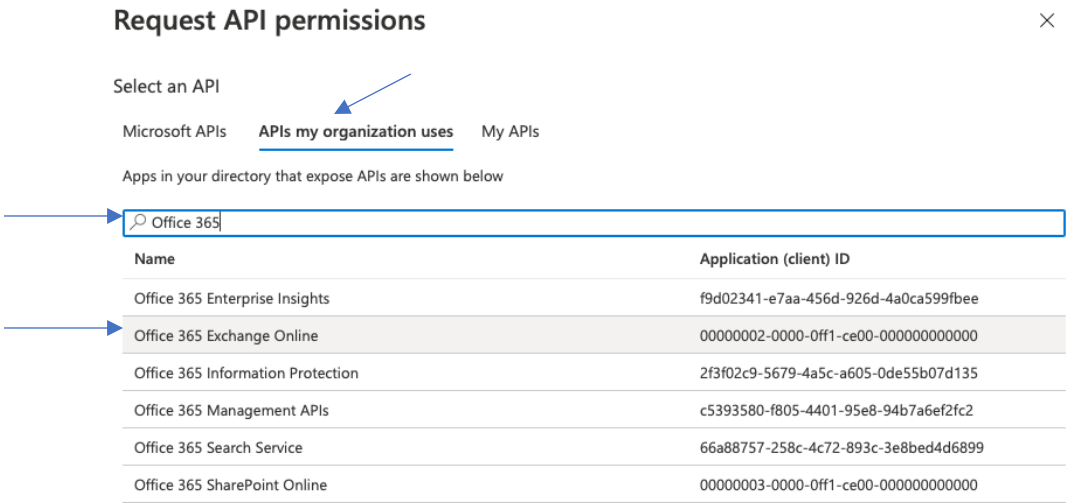
- Click on “API permissions” to the left and remove the “User.Read” setting.

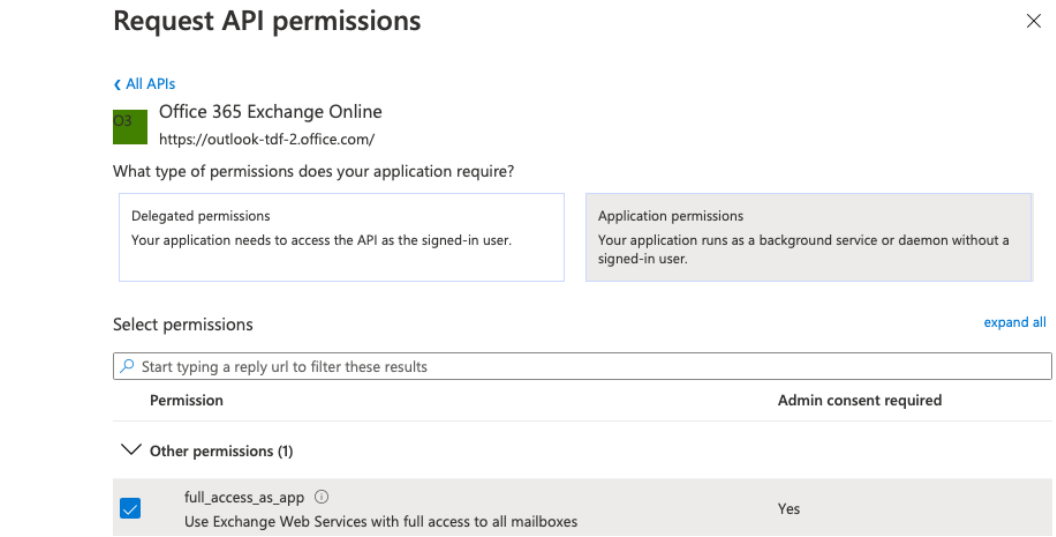


- Click “Add a permission” and select “Microsoft Graph”. Make sure that all these permissions is set and then click “Add permissions”.
    - **Under “delegated permissions”:**
        - OpenId permissions / offline_access
        - Directory / Directory.Read.All
        - Group / Group.ReadWrite.All
    - **Under “application permissions”:**
        - Directory / Directory.Read.All
        - Group / Group.Read.All
        - Group / Group.ReadWrite.All
        - Sites / Sites.ReadWrite.All
        - TeamSettings / TeamSettings.ReadWrite.All

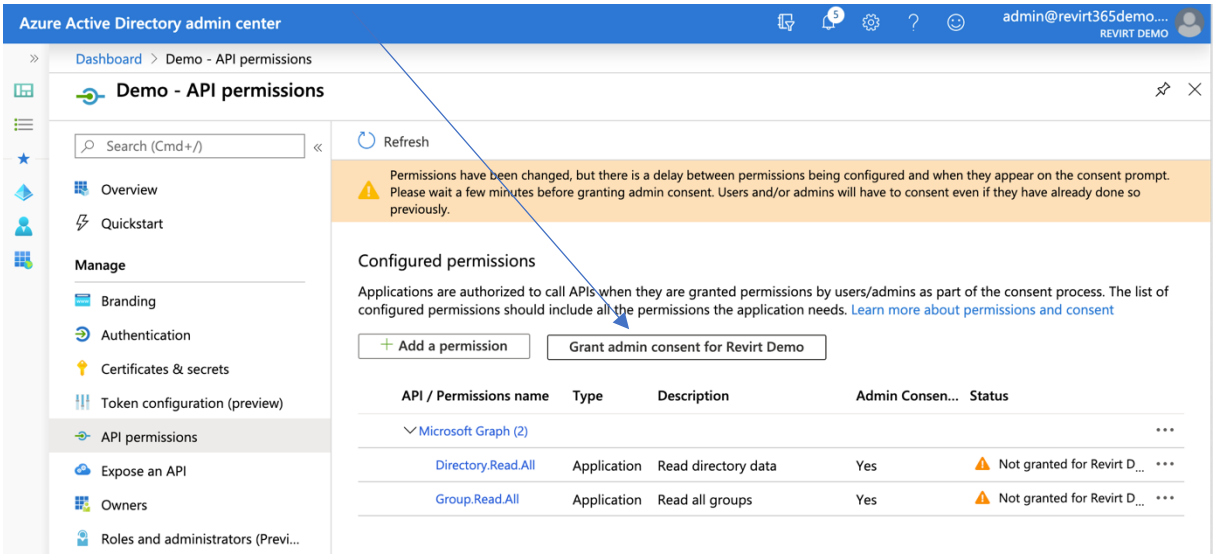
- Click “Add a permission” again and select “SharePoint”. Make sure that **all** these permissions is set and then click “Add permissions”.
    - **Under “delegated permissions”:**
        - AllSites / AllSites.FullControl
        - User / User.ReadWrite.All
    - **Under “application permissions”:**
        - Sites / Sites.FullControl.All
        - User / User.Read.All

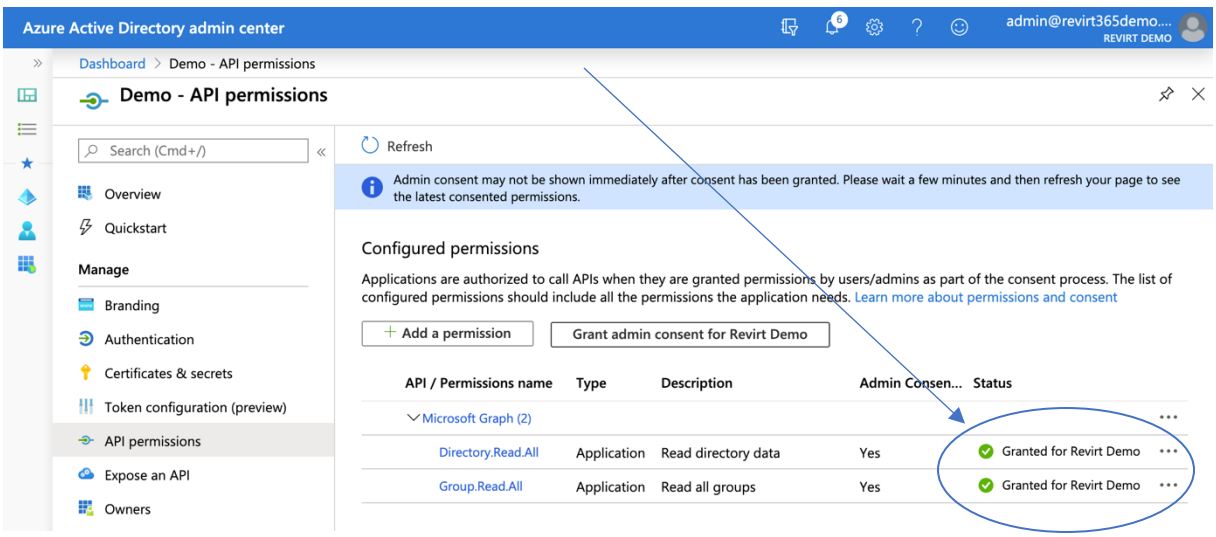
- Click “Add a permission” again. Select the “APIs my organization uses” pane in top of the window. Select (or search for) “Office 365 Exchange Online”. Make sure that **all** these permissions is set and then click “Add permissions”.
  - **Under “delegated permissions”:**
    - EWS / EWS.AccessAsUser.All
  - **Under “application permissions”:**
    - Other permissions / full_access_as_app





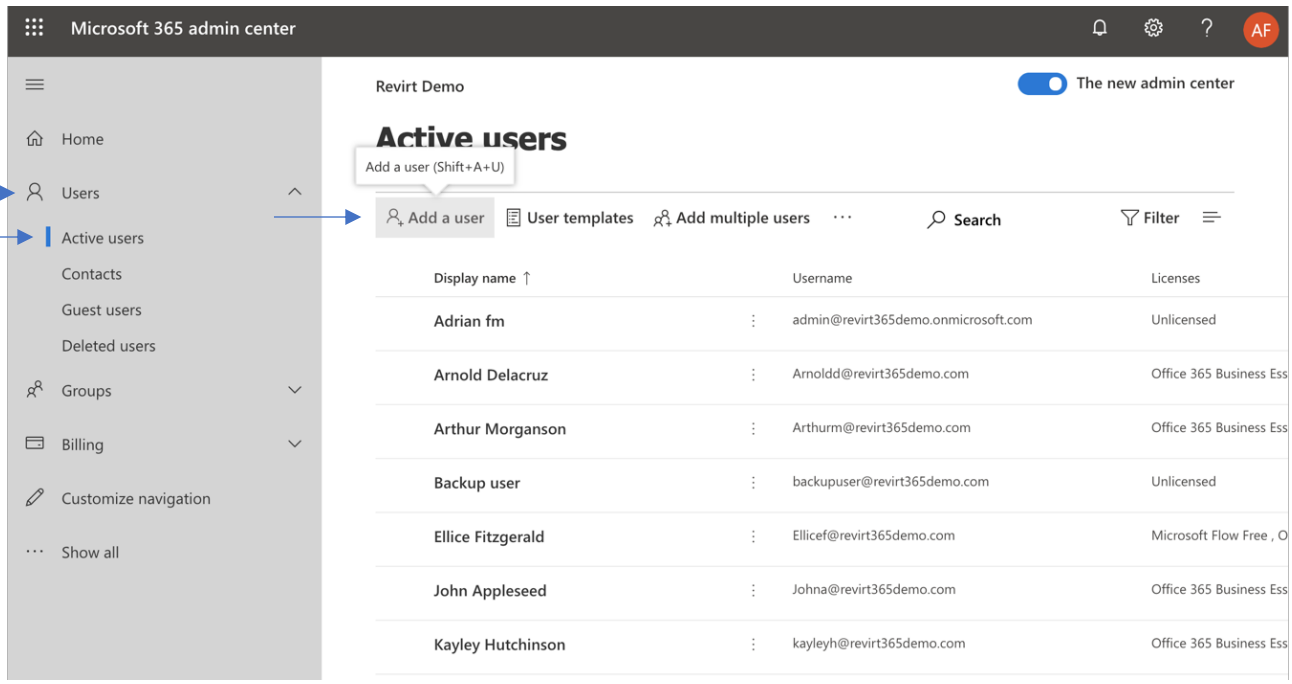
- Click on “Grant admin consent for <your name>” next to “Add permission” button. Each line of permissions should change to “granted” status with a green check mark.
- You might be asked to log in and accept. This may take a short while



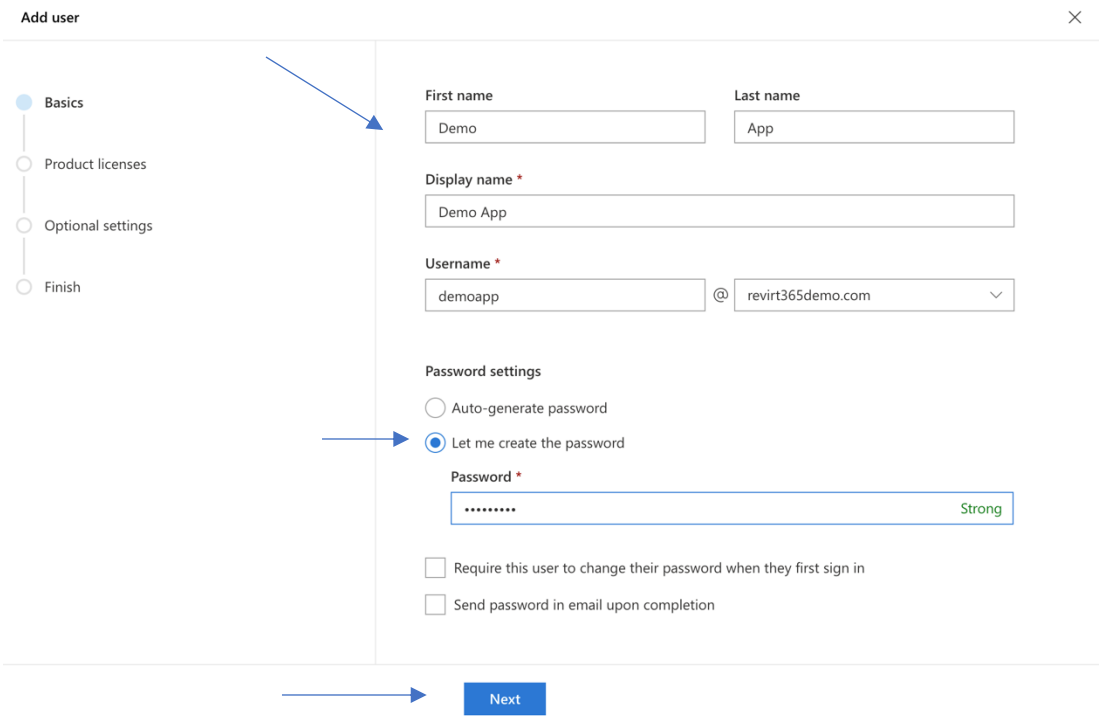


Part 2: How you set up the specific user to connect our software with Microsoft 365

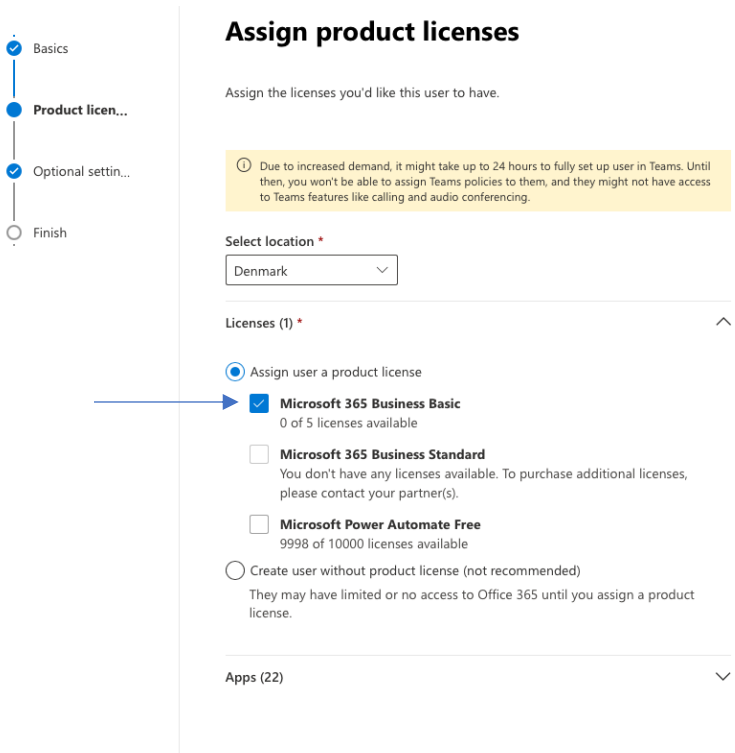
- Visit https://admin.microsoft.com and log in with an admin account.
- Click on “Users” and then “Active users” and then “Add a user” to add a new user.



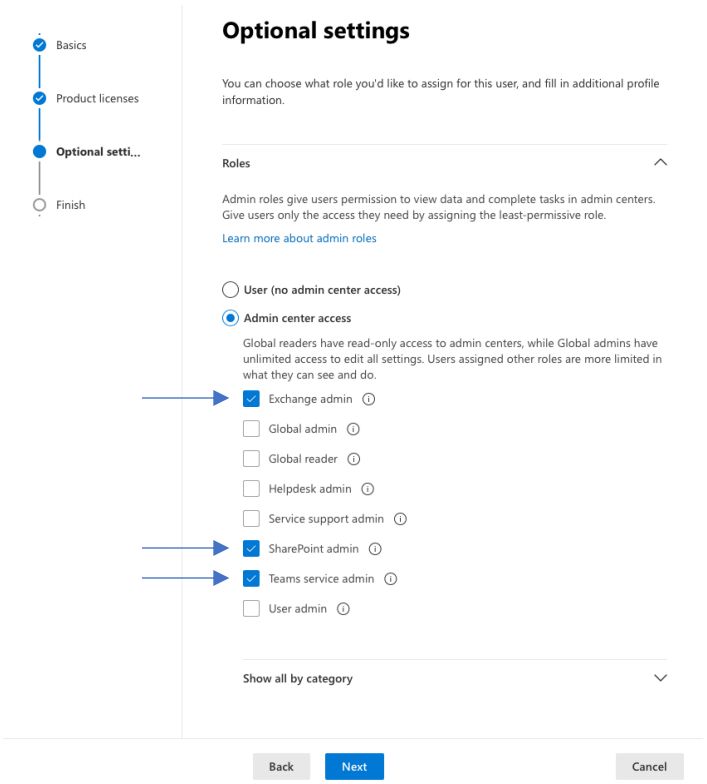
- Name your user. We recommend that you use a name that makes it easy to find later.
- We recommend you check “Let me create the password” for security reasons. Make sure that none of the other checkboxes are checked.
- Click “Next”.



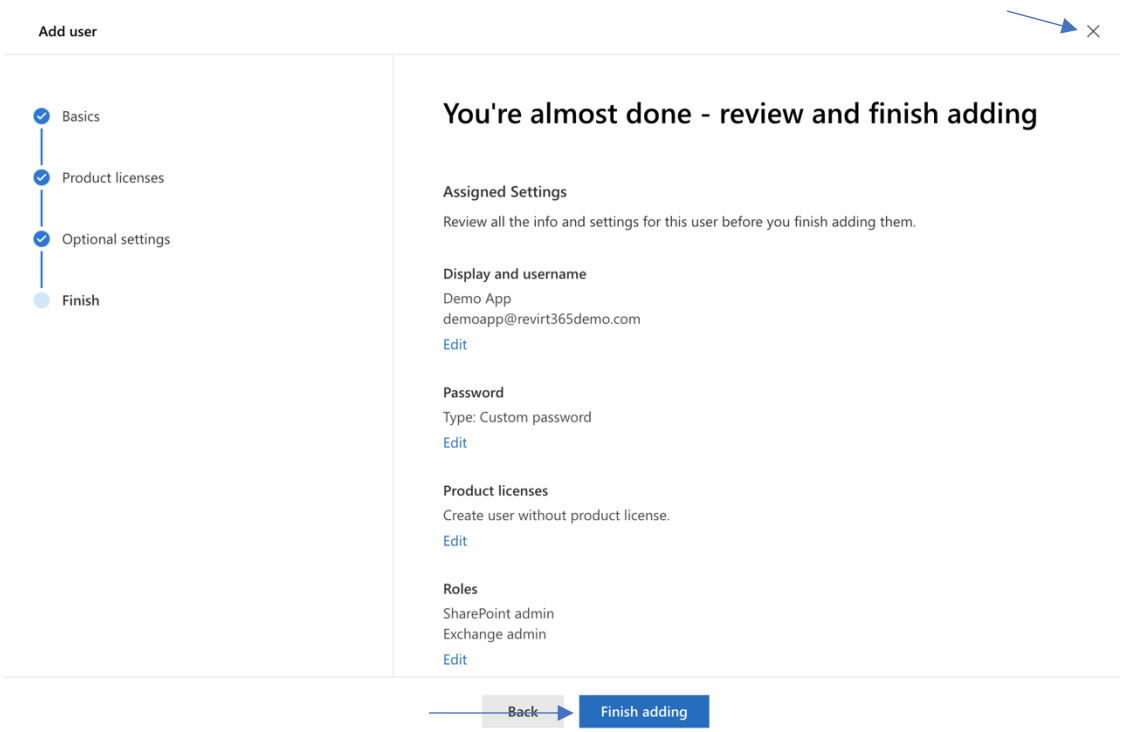
- Select a license where Teams is included. Click “Next”.



- Click on “Roles”, select “Admin center access”
- Check “Exchange admin”, “SharePoint admin” and “Teams admin”
- Click “Next”.

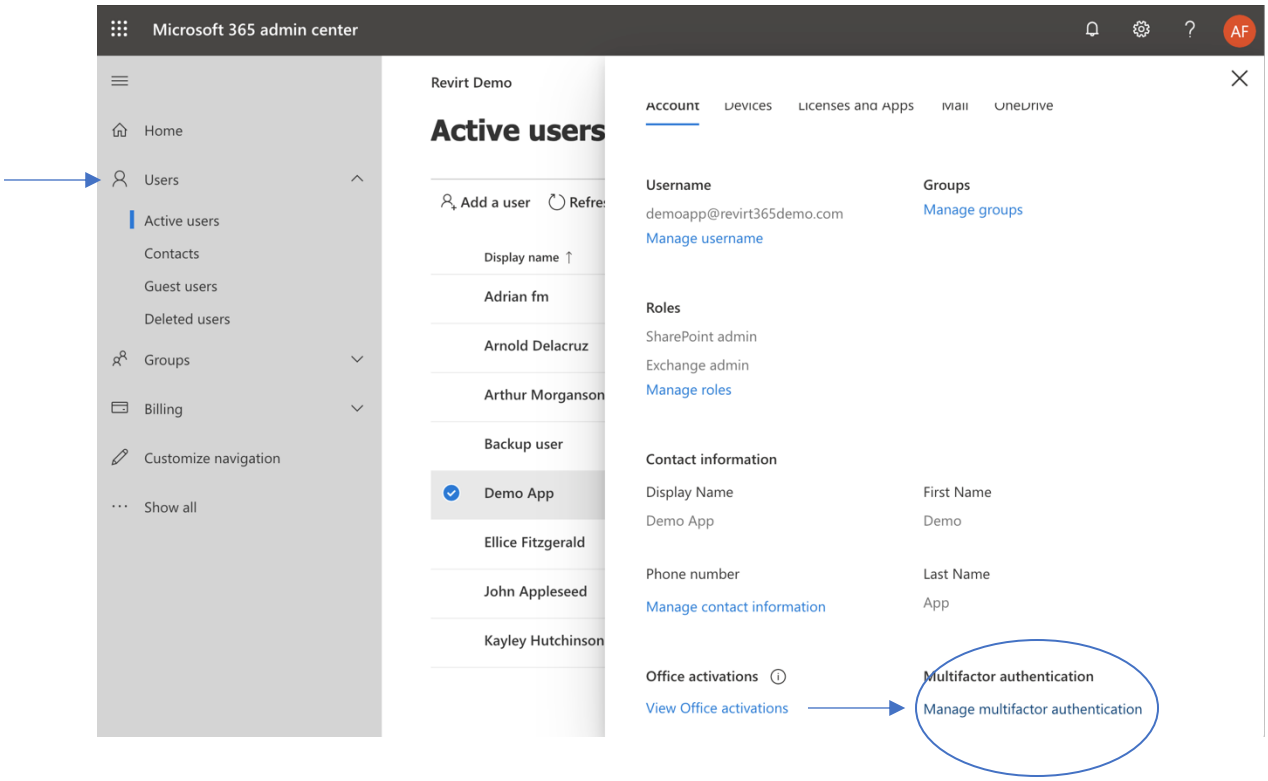


Click on “Finish adding” and then “Close”.

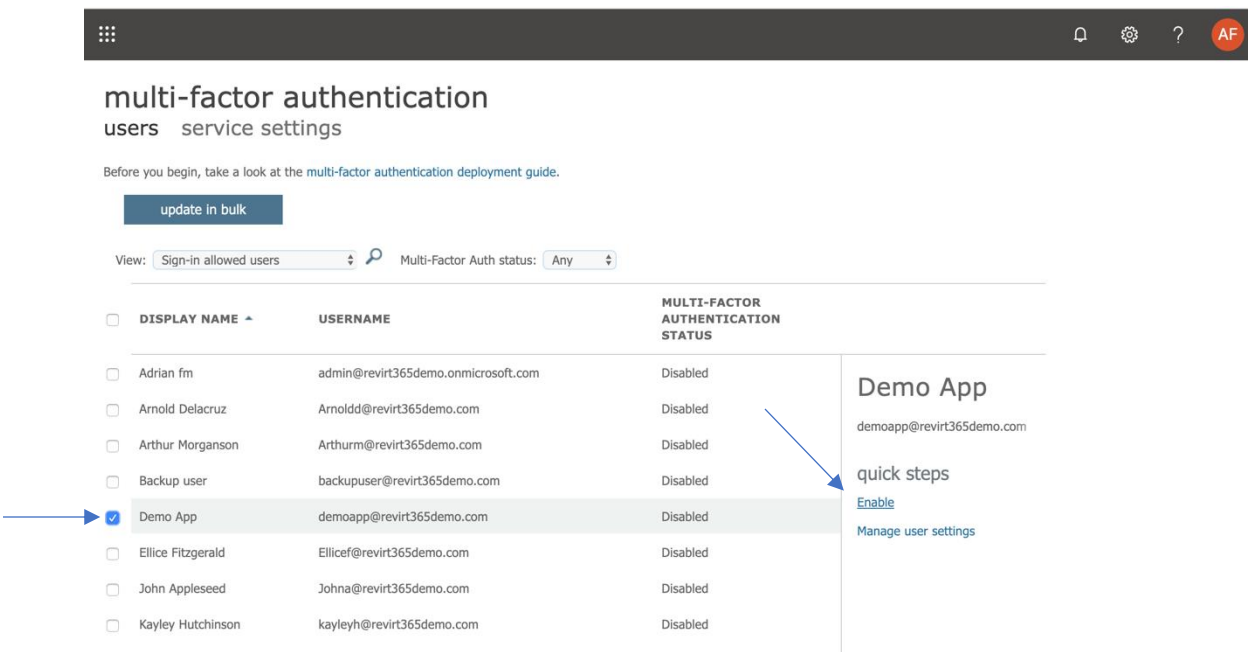


Make sure that the 2FA is set as “Enforced” for your new user.

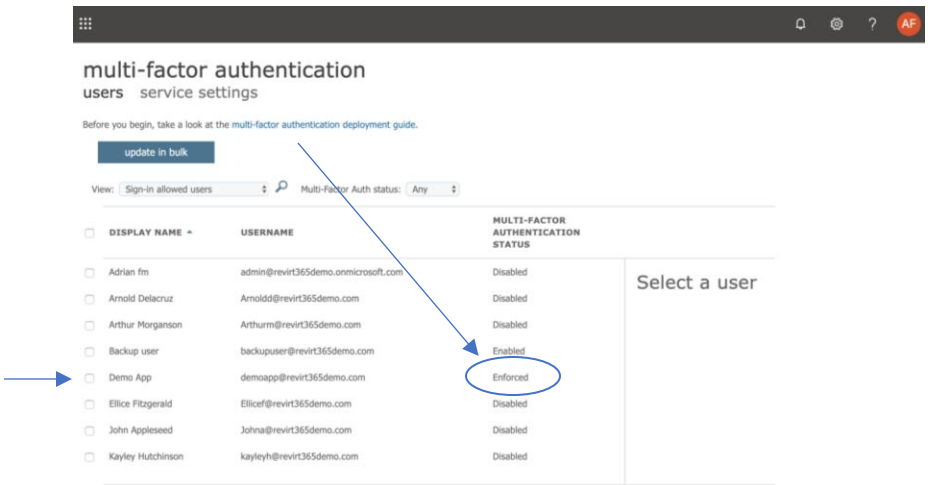
- Click on your user and select “Manage multifactor authentication”



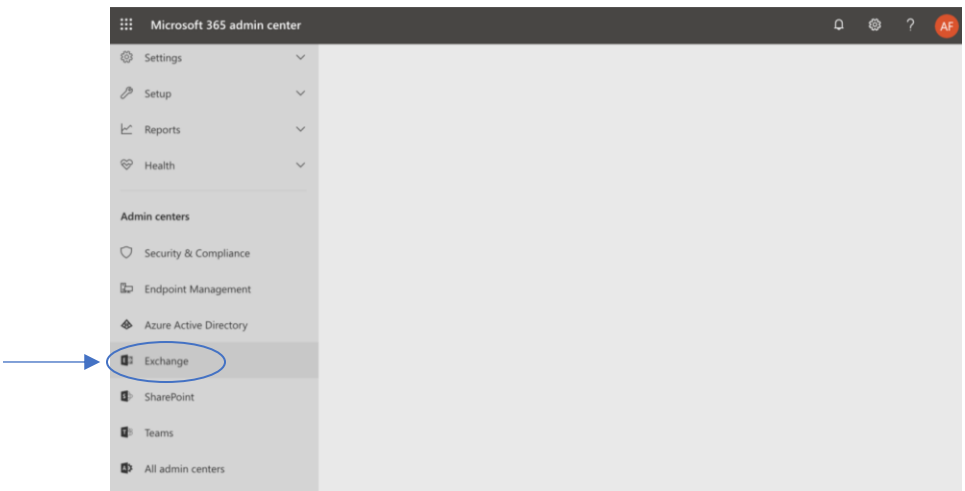
Select your user and click on “Enable” under "Quick steps"
Click on “Activate multi-factor auth” and “Close”.



1. Select your user again
2. Click on “Enforce multi-factor auth” and “Close”
3. Check that your user status is now “Enforced”



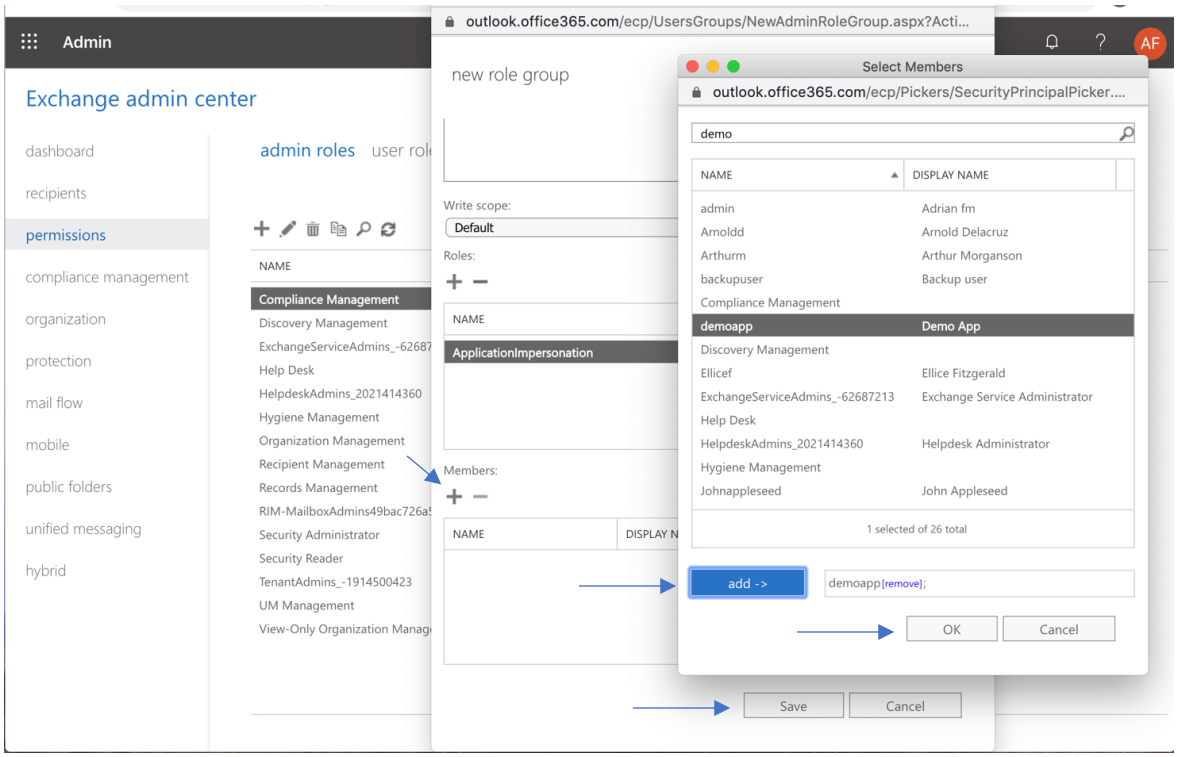
From the main menu Select "Exchange" under “Admin centers”



1. Click on “Permissions” and on the “+” sign
2. Name your role as preferred.
3. Click on the “+” sign under “Roles” and select “ApplicationImpersonation” from the menu

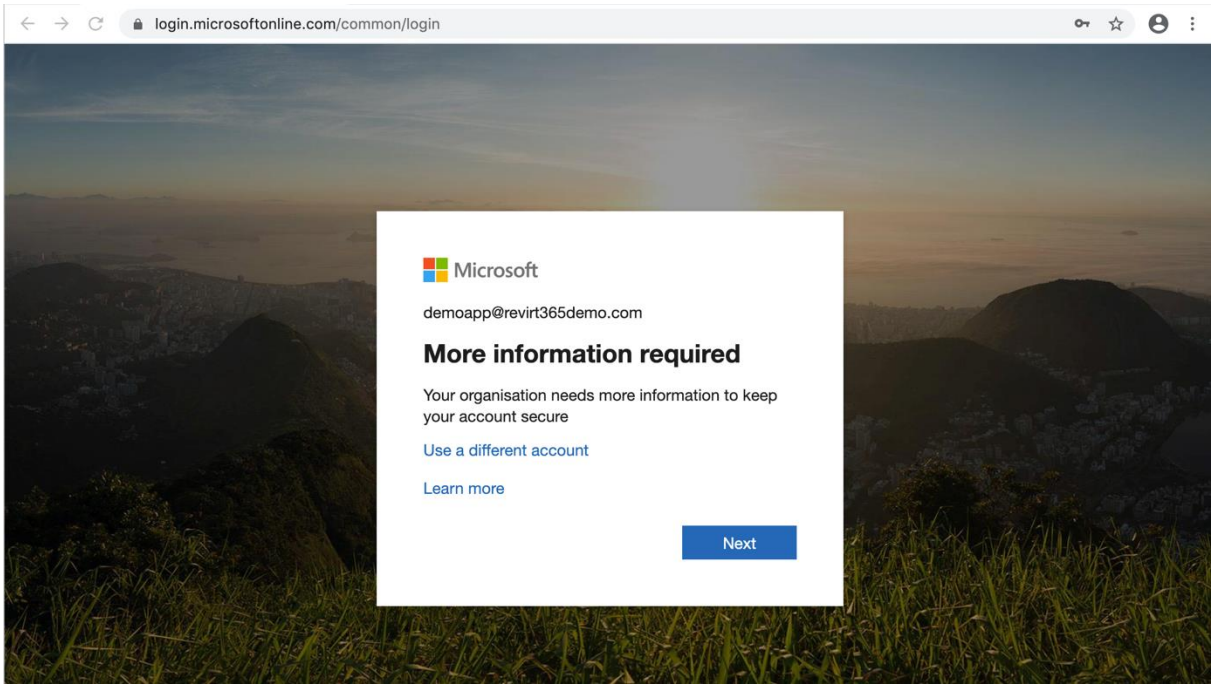
Role	Description
Role Management	Required to grant the *ApplicationImpersonation* role.
ApplicationImpersonation	Required to back up Exchange data.
Organization Configuration	Required to manage role assignments.
View-Only Configuration	Required to obtain necessary configuration parameters.
View-Only Recipients	Required to view mailbox recipients.
Mailbox Search or **Mail Recipients**	Required to back up groups.

Under “Members”, please click on the “+ “sign, select your new user, click “Add” and “OK” and “Save”. Afterwards, close this window.

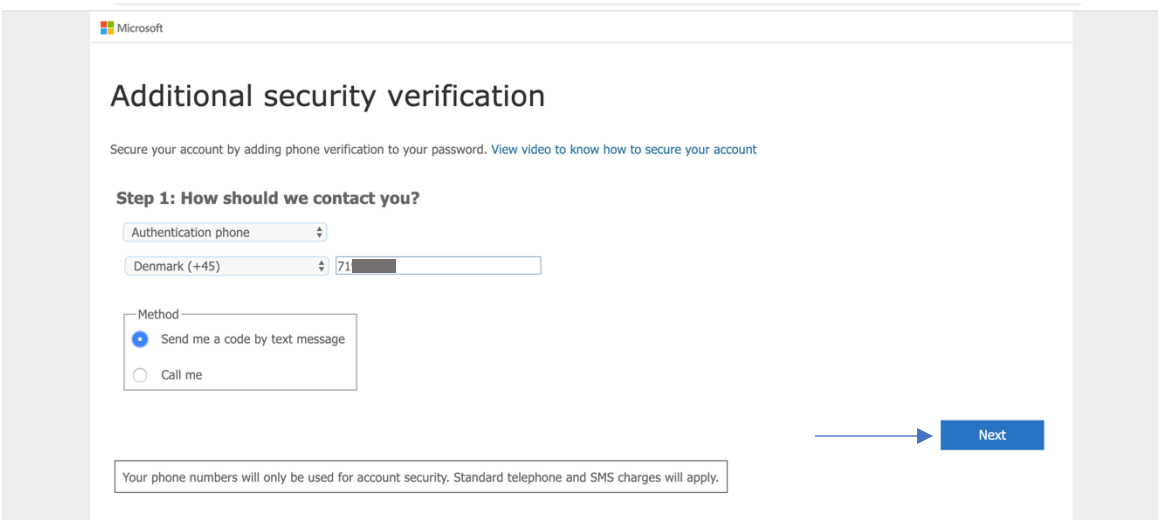


Part 3: Creating an app password to connect to your backup software with Office365

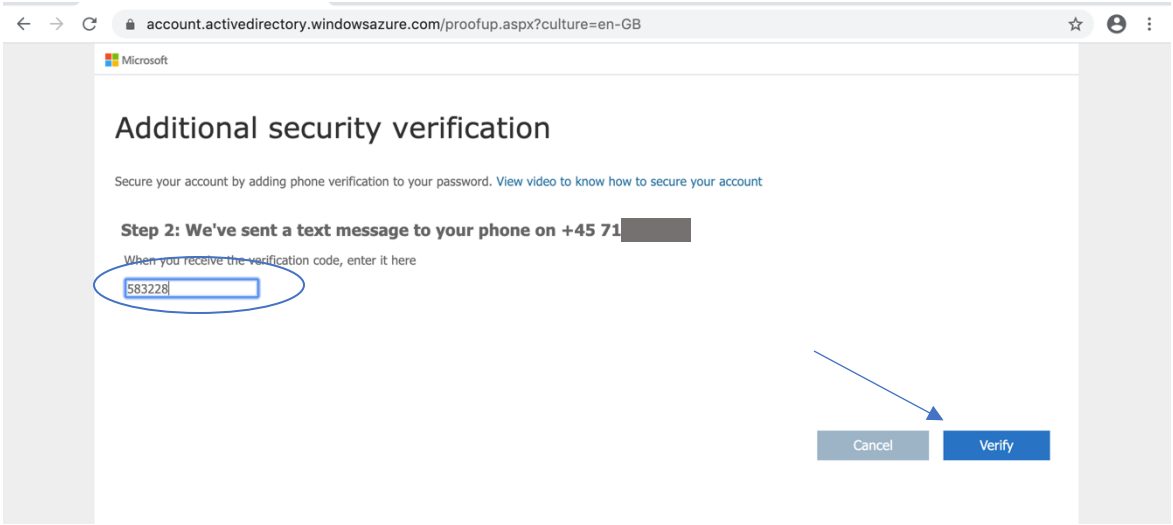
Go to portal.microsoft.com and log in with your new user. Please note that as this is the first logon, so further information might be requiered, including 2FA information.



Step 2:
Select country, add your mobile number and click “Next”.

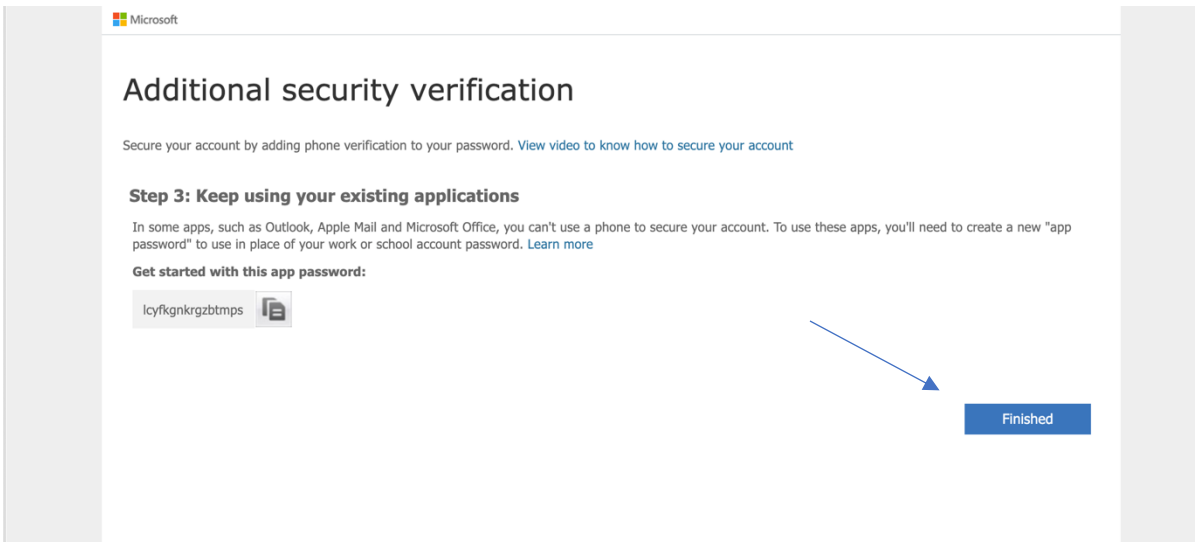


Step 3:
Enter the code that you have received via text from Microsoft and click on “Verify”



The following page will take you to an app password. Please store it somewhere safe, because you will need it for later.

Step 4:
Click on “Finished.



And that’s it! You can now add your tenant to your backup software using modern authentication!