



Guide to creating a tenant using modern authentication

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

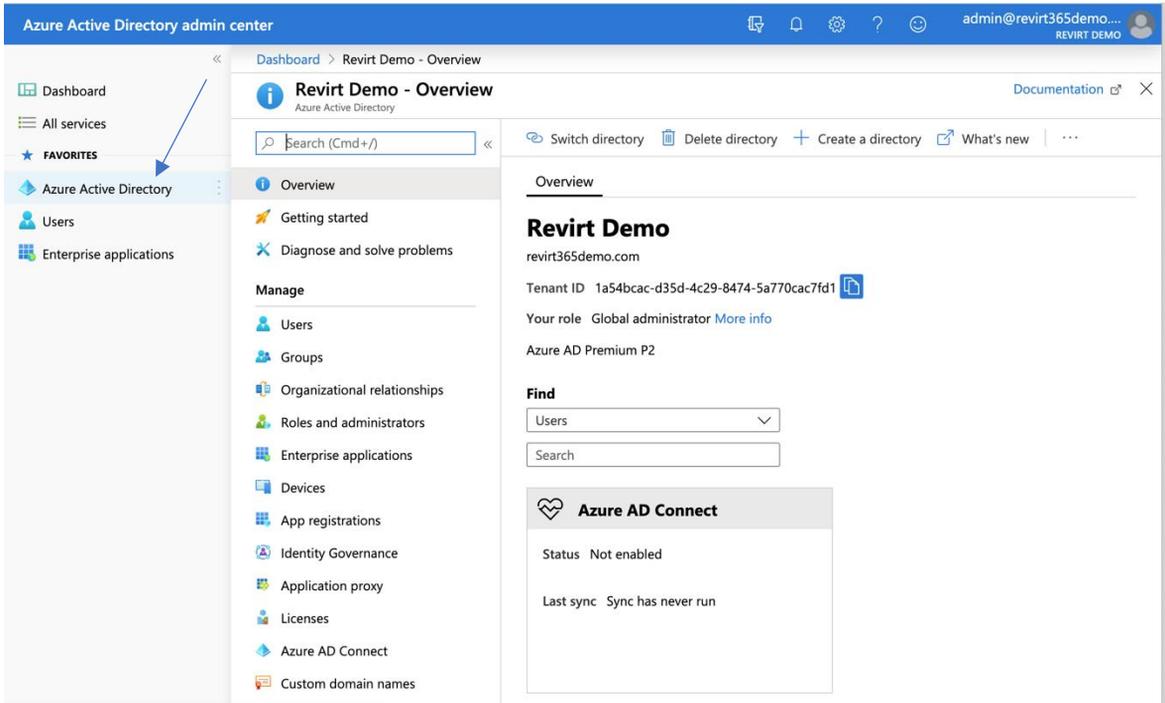
We look forward to showing you how you customise your service account for modern authentication, so you can move on with setting up your Microsoft 365 management portal.

Please keep the following important points in mind:

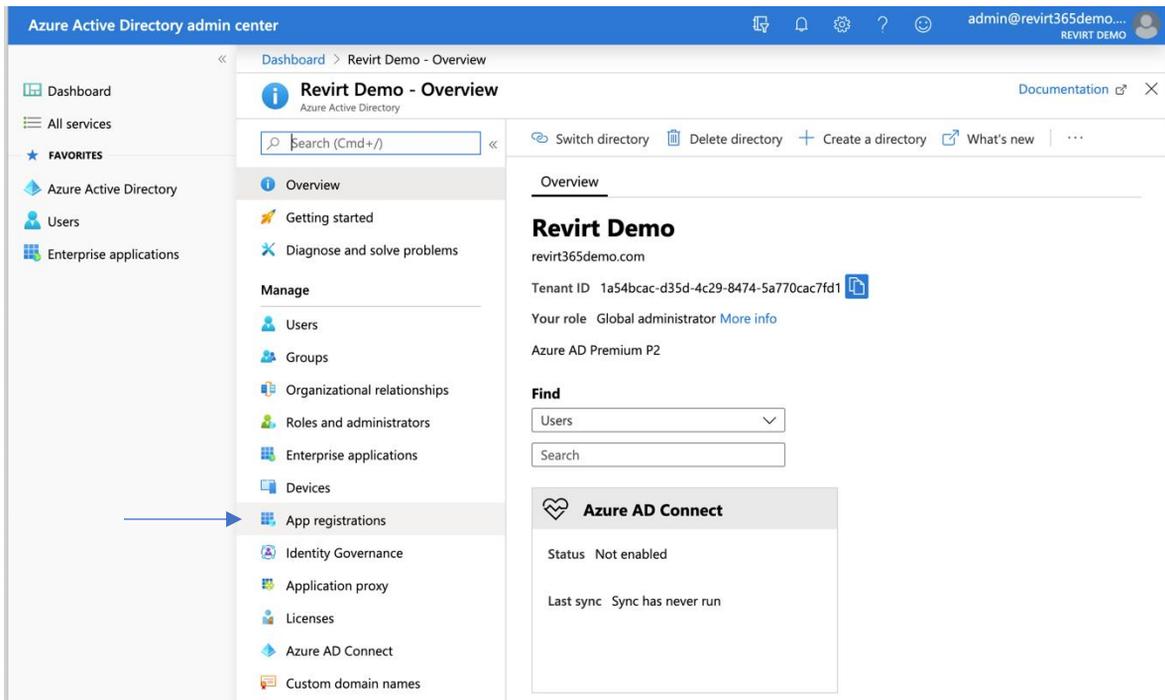
Modern authentication and 2FA go hand in hand, so 2FA is required. The same goes for admin rights which you need in order to perform the steps in this guide.

Part 1: How you add an app registration in Azure

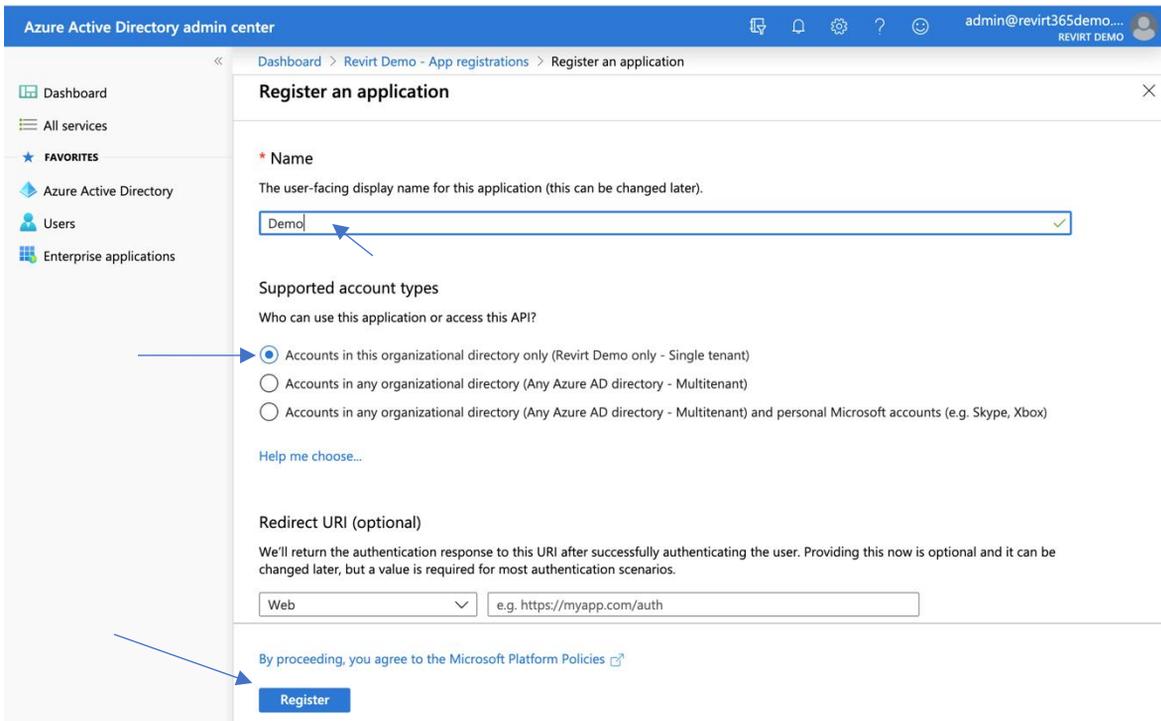
- Log into the Azure portal with your admin account.
- Click on “Azure Active Directory” (look under “More services” to the right, if you don’t see it).



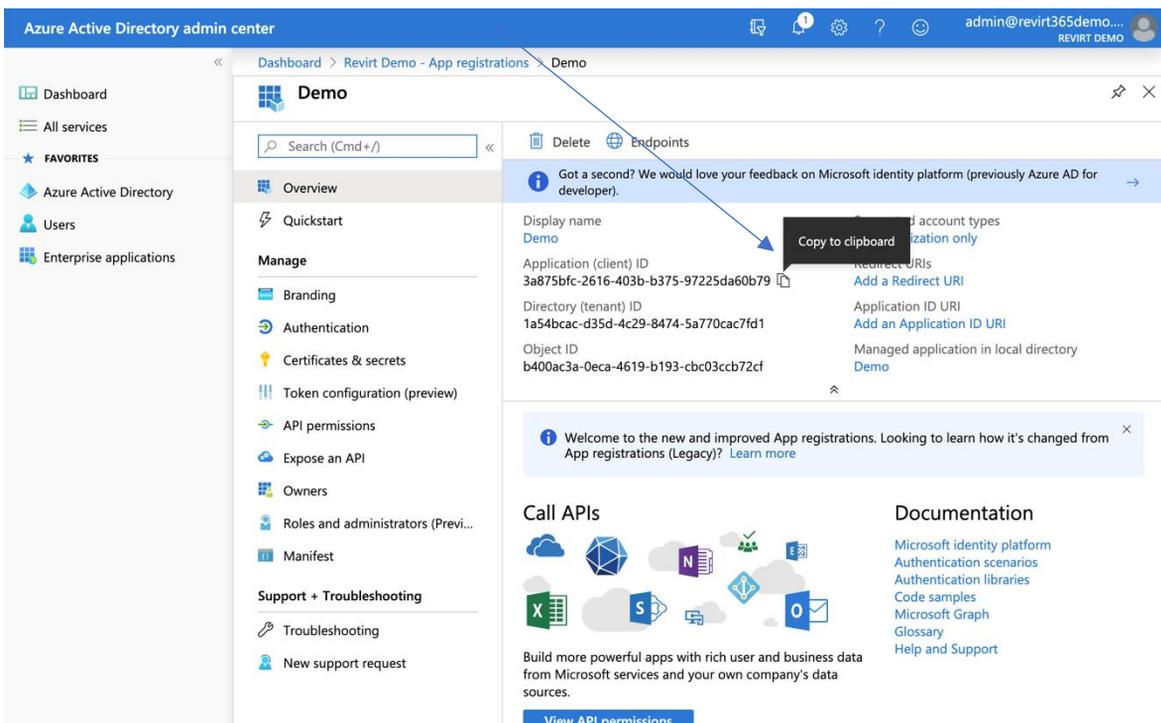
- Click on “App registrations”



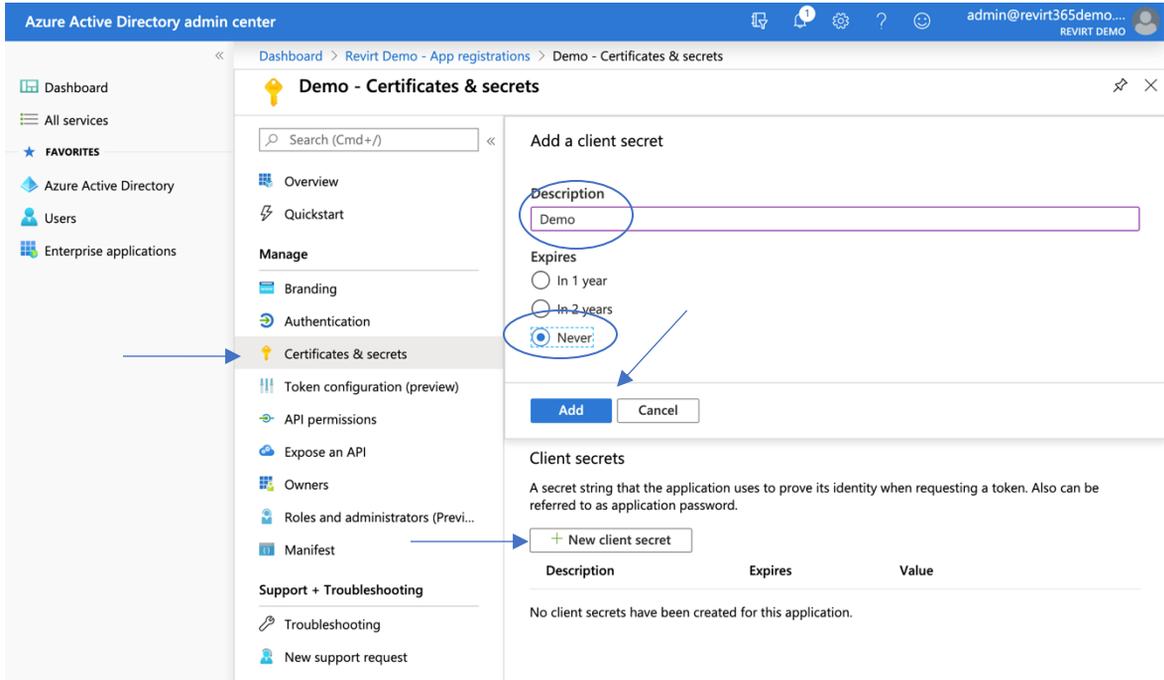
- Click on “New registration” and enter a name. We recommend using a name that makes it easy to identify in the future. For instance, "Microsoft 365 Backup"
- Make sure you check the single tenant option under “Supported account types”.
- Click on “Register”.



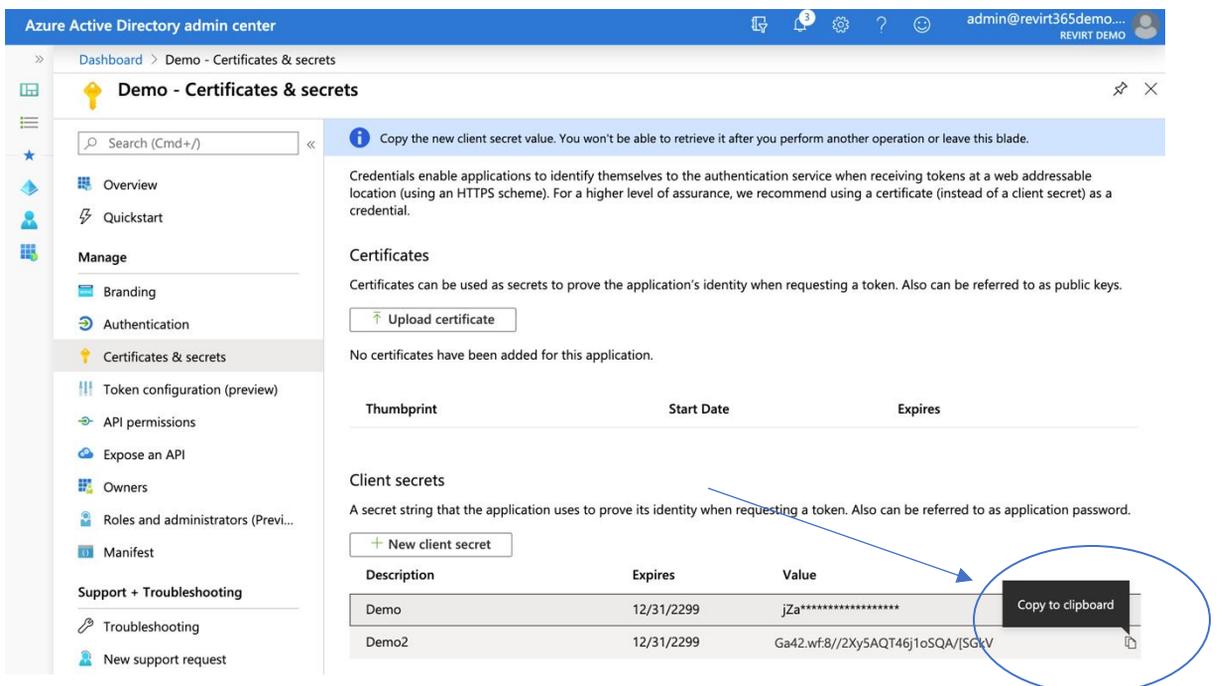
- Copy the application ID and save it, as you **will** need it later.



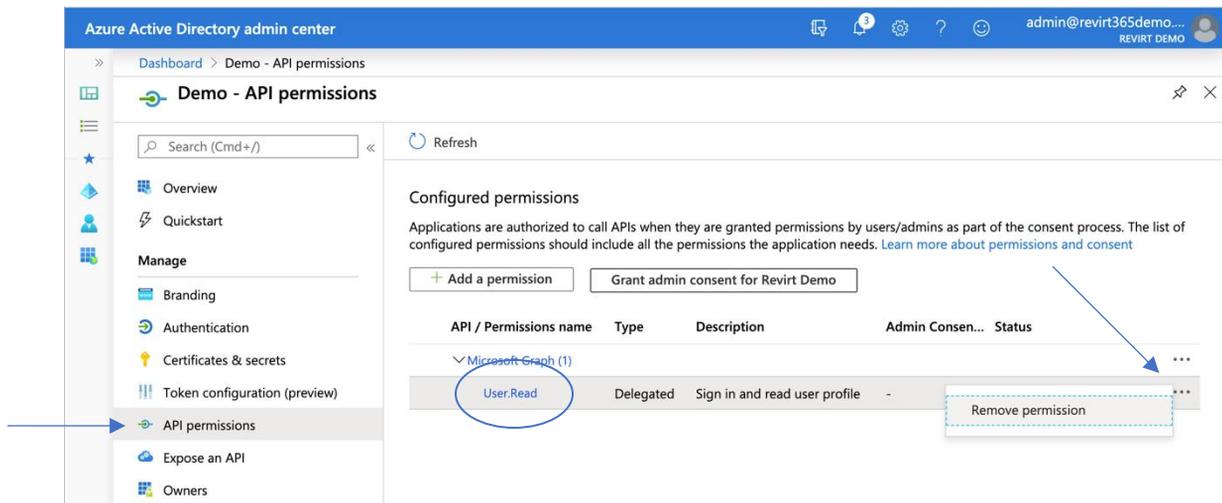
- Select “Certificates and secrets”.
- Click on “New client secret” and name it in the ”Description”. We recommend you choose the “Never” option under “Expires”
- Click “Add”.



- 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

Request API permissions



Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Office 365

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 Search Service	66a88757-258c-4c72-893c-3e8bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000

Request API permissions



< All APIs

Office 365 Exchange Online
https://outlook-tdf-2.office.com/

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

Start typing a reply url to filter these results

Permission

Admin consent required

Other permissions (1)

full_access_as_app ⓘ
Use Exchange Web Services with full access to all mailboxes

Yes

- 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

Azure Active Directory admin center

Dashboard > Demo - API permissions

Demo - API permissions

Search (Cmd+/) Refresh

Permissions have been changed, but there is a delay between permissions being configured and when they appear on the consent prompt. Please wait a few minutes before granting admin consent. Users and/or admins will have to consent even if they have already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Revirt Demo

API / Permissions name	Type	Description	Admin Consen...	Status
Microsoft Graph (2)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Revirt D... ⋮
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Revirt D... ⋮

Azure Active Directory admin center

Dashboard > Demo - API permissions

Demo - API permissions

Search (Cmd+/) Refresh

Admin consent may not be shown immediately after consent has been granted. Please wait a few minutes and then refresh your page to see the latest consented permissions.

Configured permissions

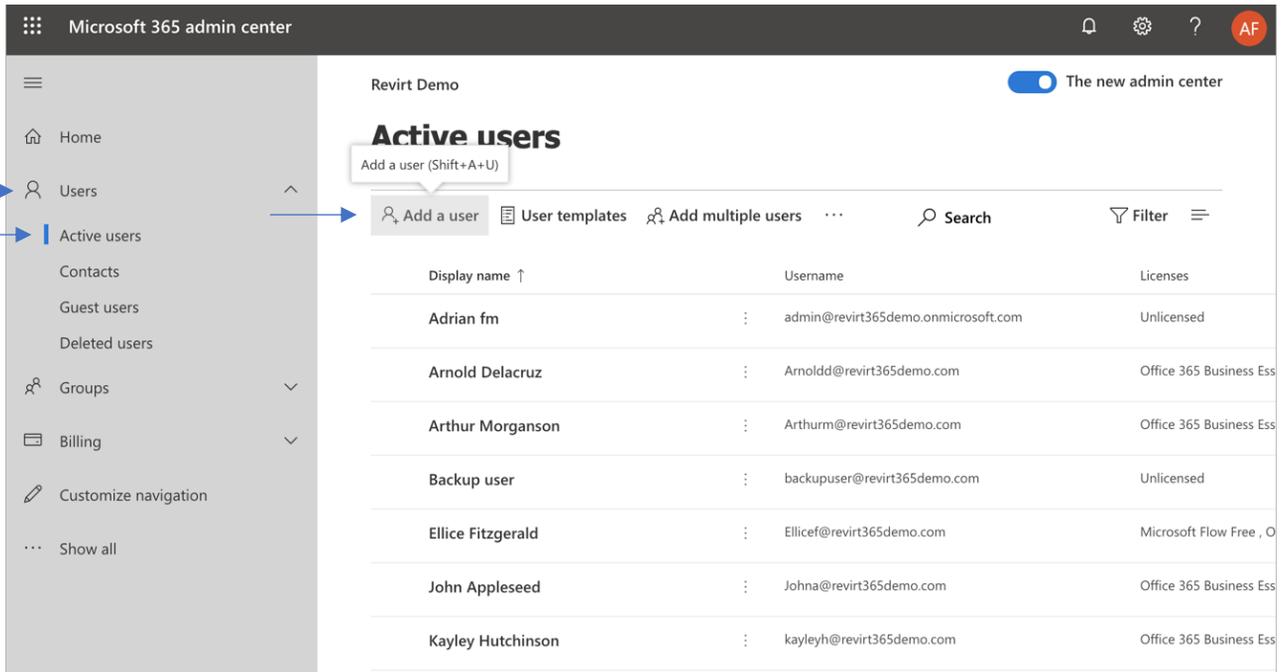
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Revirt Demo

API / Permissions name	Type	Description	Admin Consen...	Status
Microsoft Graph (2)				
Directory.Read.All	Application	Read directory data	Yes	✔ Granted for Revirt Demo ⋮
Group.Read.All	Application	Read all groups	Yes	✔ Granted for Revirt Demo ⋮

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.



Microsoft 365 admin center

Revirt Demo

The new admin center

Active users

Add a user (Shift+A+U)

Add a user User templates Add multiple users Search Filter

Display name ↑	Username	Licenses
Adrian fm	admin@revirt365demo.onmicrosoft.com	Unlicensed
Arnold Delacruz	Arnoldd@revirt365demo.com	Office 365 Business Ess
Arthur Morganson	Arthurn@revirt365demo.com	Office 365 Business Ess
Backup user	backupuser@revirt365demo.com	Unlicensed
Ellice Fitzgerald	Ellicef@revirt365demo.com	Microsoft Flow Free , O
John Appleseed	Johna@revirt365demo.com	Office 365 Business Ess
Kayley Hutchinson	kayleyh@revirt365demo.com	Office 365 Business Ess

- 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”.

Add user ×

Progress: Basics (selected), Product licenses, Optional settings, Finish

First name: Demo **Last name**: App

Display name *: Demo App

Username *: demoapp @ revirt365demo.com

Password settings

- Auto-generate password
- Let me create the password

Password *: Strong

- Require this user to change their password when they first sign in
- Send password in email upon completion

Next

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

Assign product licenses

Assign the licenses you'd like this user to have.

Warning: Due to increased demand, it might take up to 24 hours to fully set up user in Teams. Until then, you won't be able to assign Teams policies to them, and they might not have access to Teams features like calling and audio conferencing.

Select location *: Denmark

Licenses (1) *

- Assign user a product license
 - Microsoft 365 Business Basic**
0 of 5 licenses available
 - Microsoft 365 Business Standard**
You don't have any licenses available. To purchase additional licenses, please contact your partner(s).
 - Microsoft Power Automate Free**
9998 of 10000 licenses available
- Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

Apps (22)

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

Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.
[Learn more about admin roles](#)

User (no admin center access)

Admin center access

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

Exchange admin

Global admin

Global reader

Helpdesk admin

Service support admin

SharePoint admin

Teams service admin

User admin

Show all by category

[Back](#) [Next](#) [Cancel](#)

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

Add user

You're almost done - review and finish adding

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
Demo App
demoapp@revirt365demo.com
[Edit](#)

Password
Type: Custom password
[Edit](#)

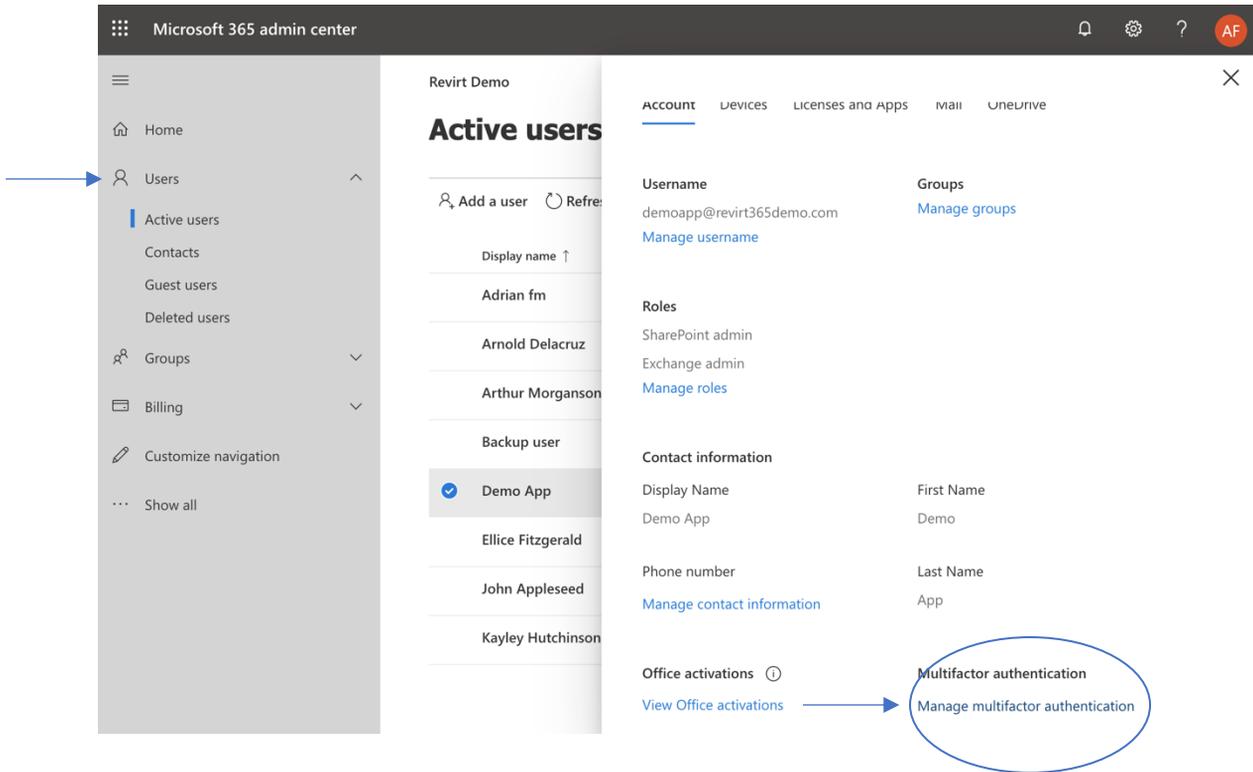
Product licenses
Create user without product license.
[Edit](#)

Roles
SharePoint admin
Exchange admin
[Edit](#)

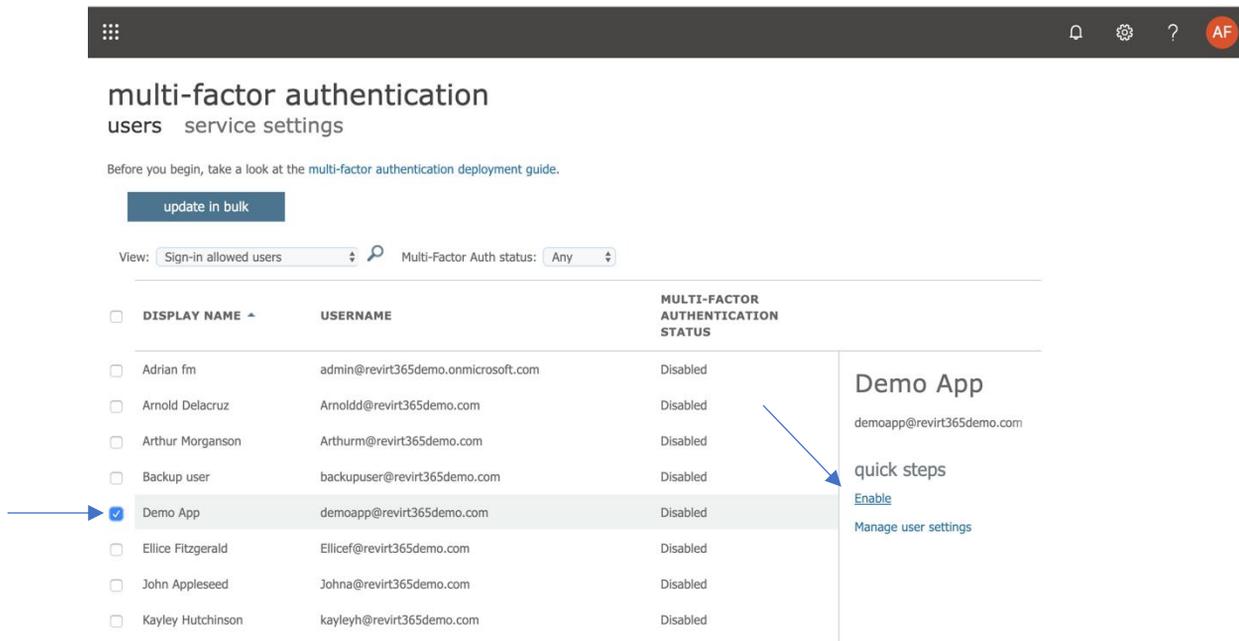
[Back](#) [Finish adding](#)

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

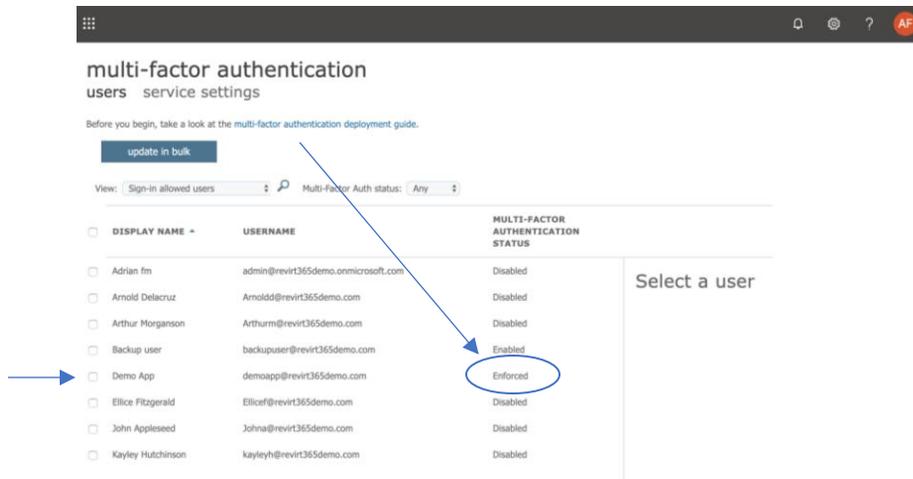
- Click on your user and select “Manage multifactor authentication”



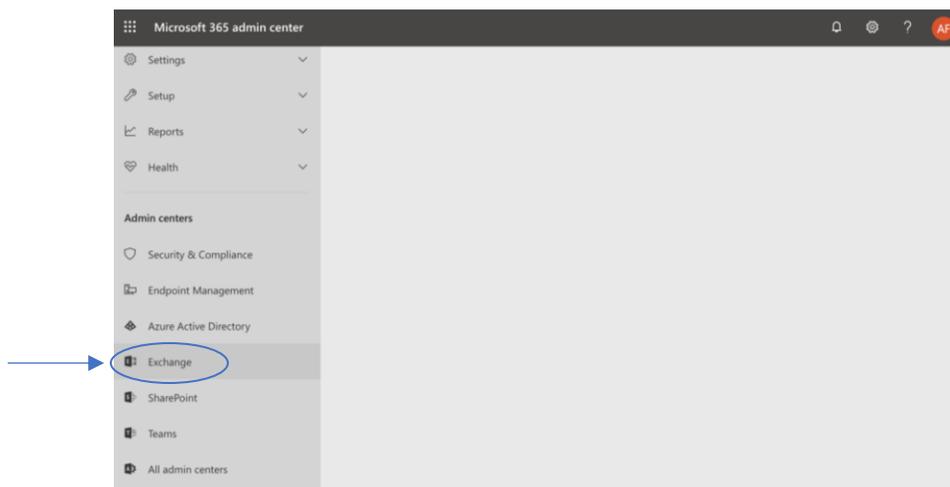
Select your user and click on “Enable” under "Quick steps"
Click on “Activate multi-factor auth” and “Close”.



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



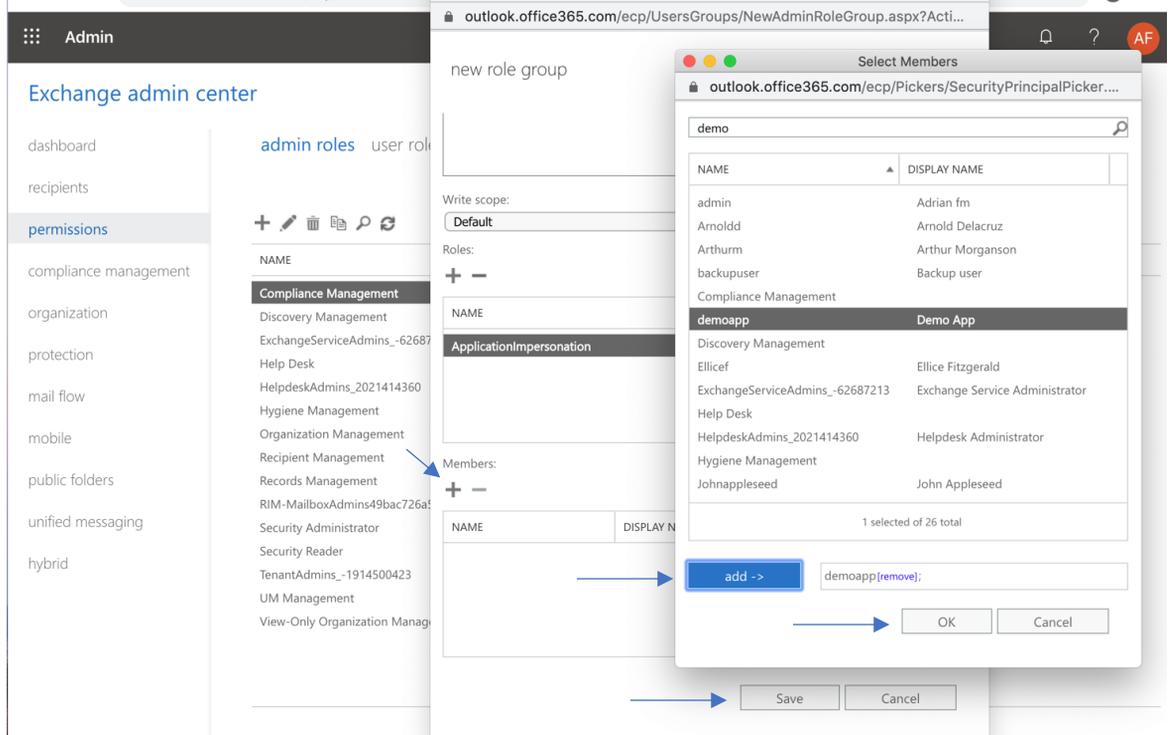
From the main menu Select "Exchange" under “Admin centers”



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

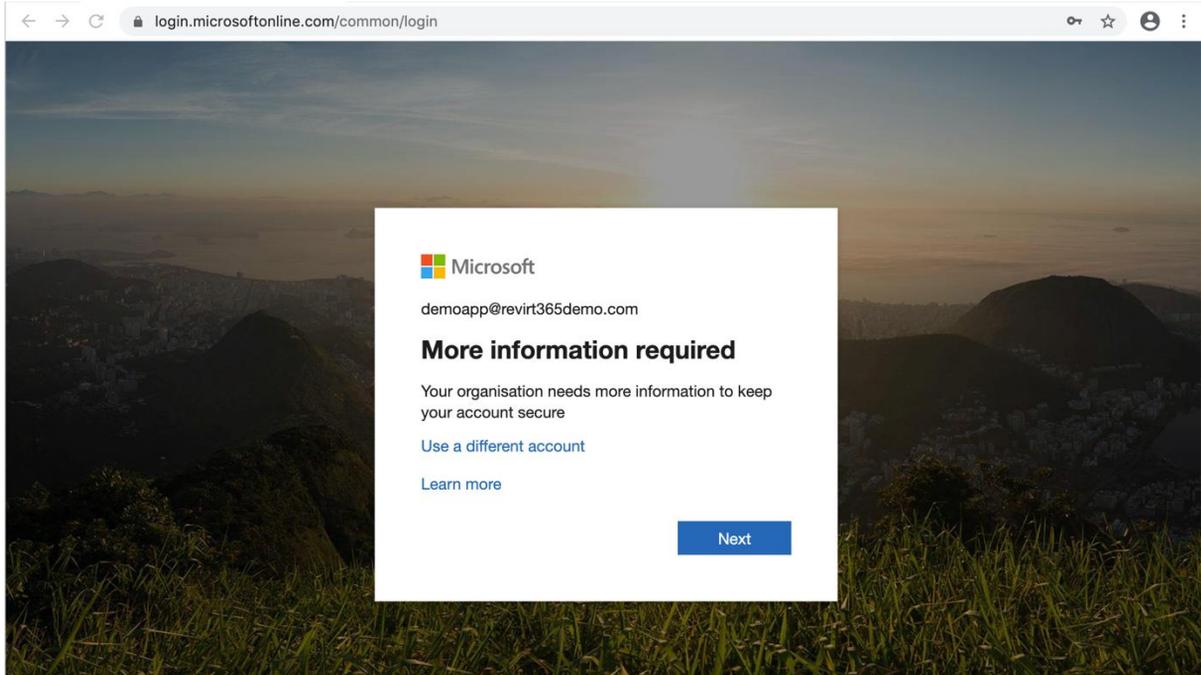
Role	Description
Role Management	Required to grant the <i>ApplicationImpersonation</i> role.
ApplicationImpersonation	Required to back up Exchange data.
Organization Configuration	Required to manage role assignments.
View-Only Configuration	Required to obtain necessary configuration parameters.
View-Only 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.



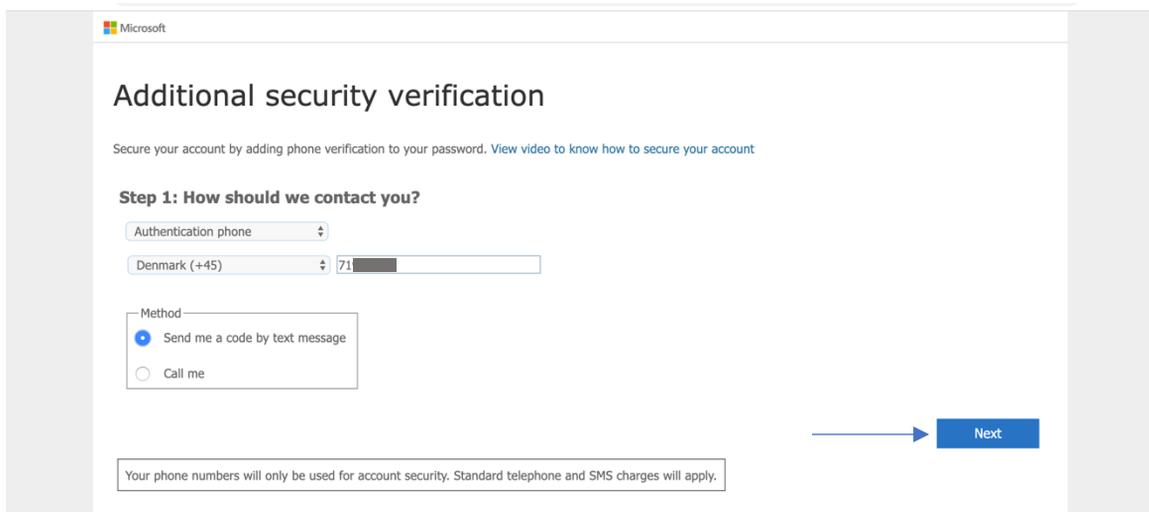
Part 3: Creating an app password to connect to your backup software with Office365

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 required, including 2FA information.



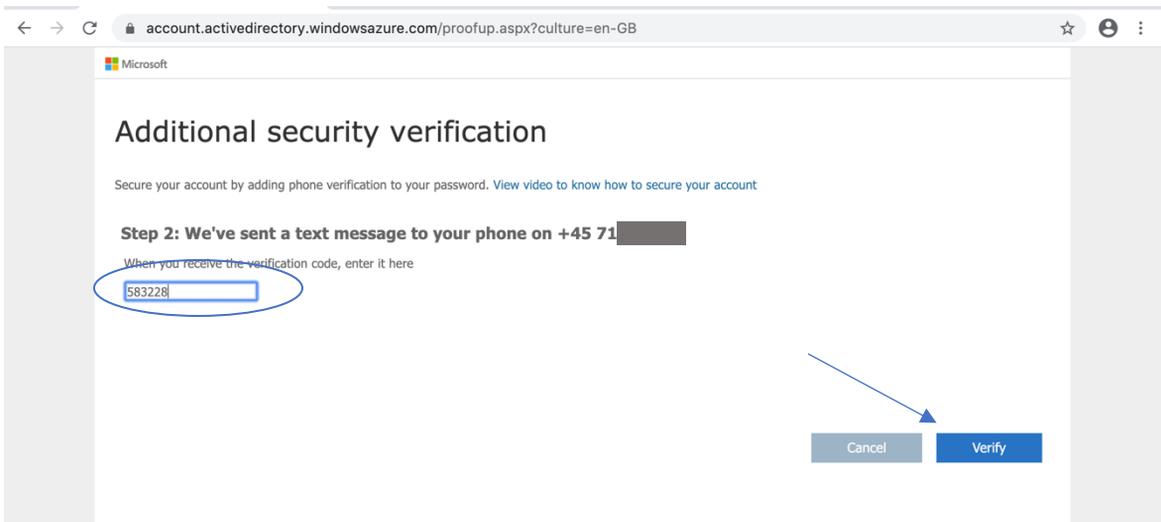
Step 2:

Select country, add your mobile number and click "Next".

A screenshot of the Microsoft 'Additional security verification' page. The page title is 'Additional security verification' and it includes the instruction 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. Under the heading 'Step 1: How should we contact you?', there is a form with the following elements: a dropdown menu for 'Authentication phone', a dropdown menu for 'Denmark (+45)' and a text input field containing '71'; a 'Method' section with two radio buttons: 'Send me a code by text message' (which is selected) and 'Call me'; and a blue 'Next' button with a blue arrow pointing to it. At the bottom, a small box contains the text: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

Step 3:

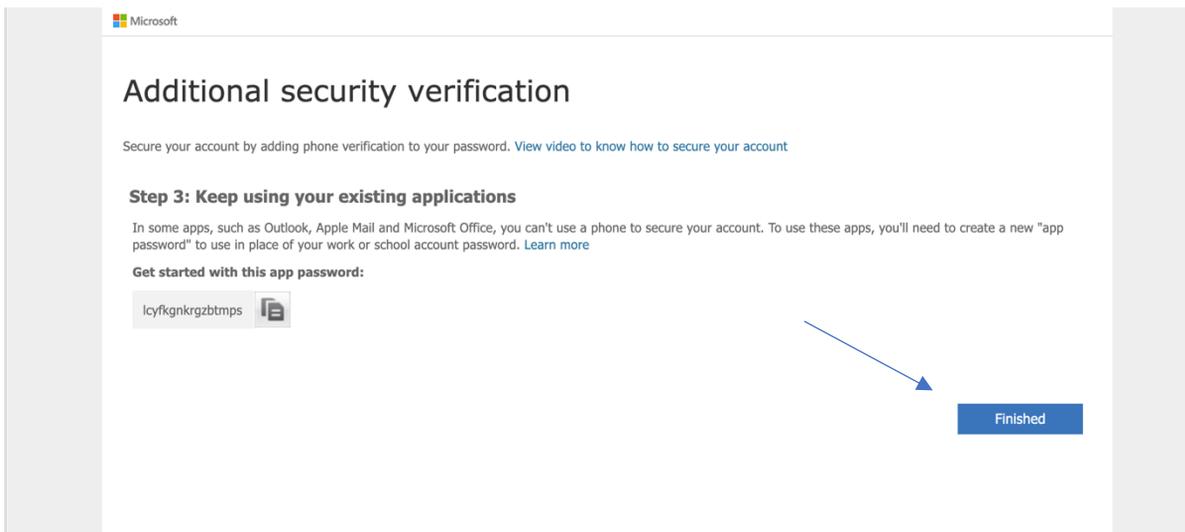
Enter the code that you have received via text from Microsoft and click on “Verify”



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!