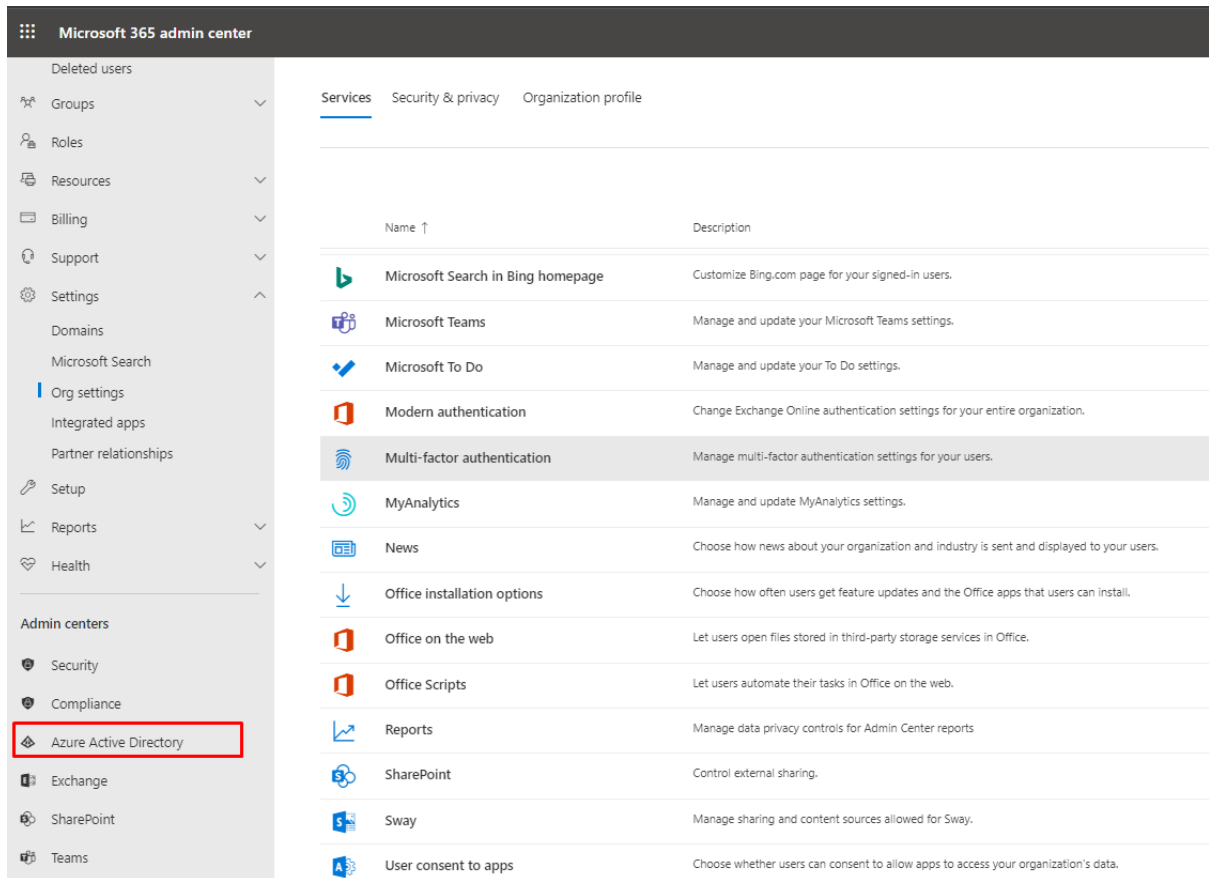


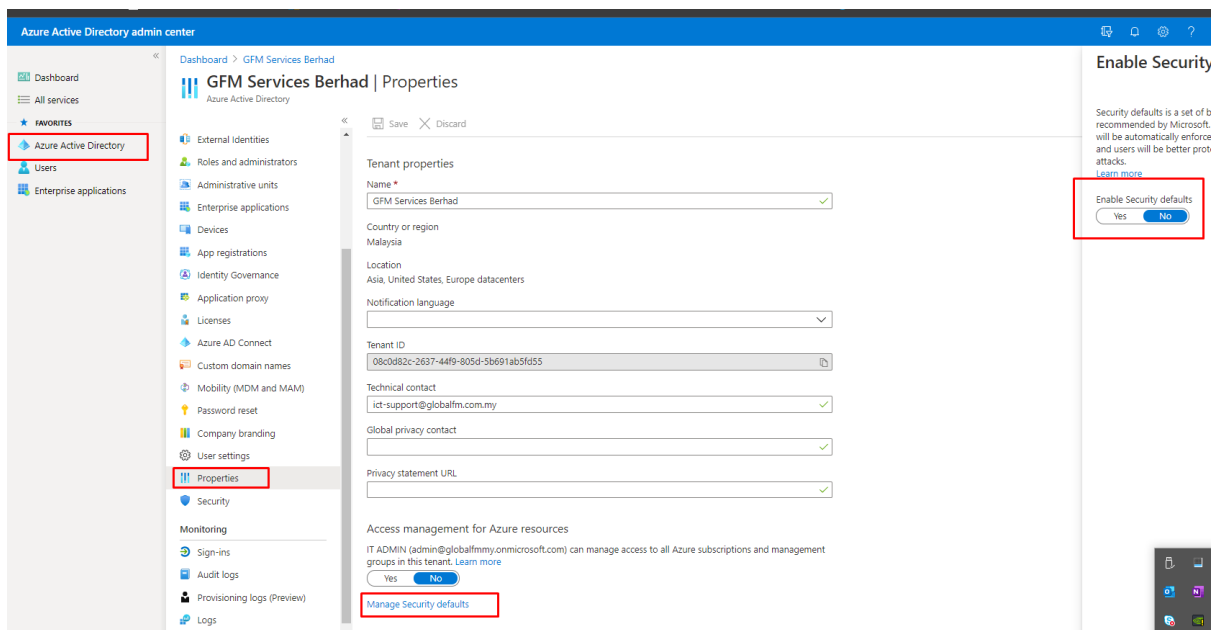
## Enable for whole organisation:

In admin portal: click Azure Active Directory



The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation menu with categories like 'Deleted users', 'Groups', 'Roles', 'Resources', 'Billing', 'Support', 'Settings', 'Domains', 'Microsoft Search', 'Org settings', 'Integrated apps', 'Partner relationships', 'Setup', 'Reports', and 'Health'. Under 'Admin centers', 'Azure Active Directory' is highlighted with a red box. The main content area shows a list of services under the 'Services' tab, with columns for 'Name' and 'Description'. The 'Multi-factor authentication' service is highlighted.

Name ↑	Description
Microsoft Search in Bing homepage	Customize Bing.com page for your signed-in users.
Microsoft Teams	Manage and update your Microsoft Teams settings.
Microsoft To Do	Manage and update your To Do settings.
Modern authentication	Change Exchange Online authentication settings for your entire organization.
<b>Multi-factor authentication</b>	Manage multi-factor authentication settings for your users.
MyAnalytics	Manage and update MyAnalytics settings.
News	Choose how news about your organization and industry is sent and displayed to your users.
Office installation options	Choose how often users get feature updates and the Office apps that users can install.
Office on the web	Let users open files stored in third-party storage services in Office.
Office Scripts	Let users automate their tasks in Office on the web.
Reports	Manage data privacy controls for Admin Center reports
SharePoint	Control external sharing.
Sway	Manage sharing and content sources allowed for Sway.
User consent to apps	Choose whether users can consent to allow apps to access your organization's data.



The screenshot shows the Azure Active Directory admin center for 'GFM Services Berhad'. The left navigation pane has 'Azure Active Directory' and 'Properties' highlighted with red boxes. The main content area displays tenant properties such as Name, Country or region, Location, Notification language, Tenant ID, Technical contact, Global privacy contact, and Privacy statement URL. At the bottom, there is a 'Manage Security defaults' section with a 'Yes' button highlighted in red. On the right side, there is a 'Enable Security' panel with a 'Yes' button highlighted in red.

**Enable Security**

Security defaults is a set of b recommended by Microsoft. will be automatically enforce and users will be better prot attacks. [Learn more](#)

Enable Security defaults

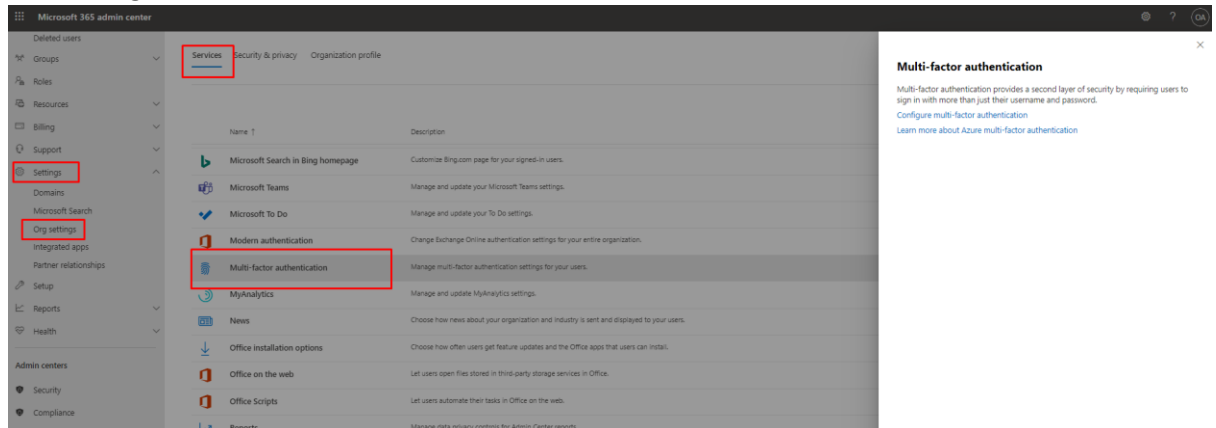
Yes No

Enable for whole organisation then select Yes.

This is Default -- Select No if you want to setup for each individual user differently.

## Enable MFA for individual user:

1. Login to admin.microsoft.com
2. Setting -> Org setting -> services
3. Look for Multi-factor Authentication
4. Click configure multi-factor authentication



- 5.
6. Select the user then click enable

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Sign-in allowed users Multi-Factor Auth status: Any

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	ABD A	abd@	Disabled
<input checked="" type="checkbox"/>	ABD	abd@	Disabled
<input type="checkbox"/>	ABDUL	abd@	Disabled
<input type="checkbox"/>	ABDUL	abd@	Disabled
<input type="checkbox"/>	Abdul	hidz@	Disabled

quick steps  
Enable  
Manage user settings

- 7.
8. After enable, will need to wait **a few hours** for it to take effect.

## End User login

9. <https://outlook.office.com>
10. Login with email address and password
11. Then it will prompt:



adamtest@globalfm.com.my

## More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Next](#)

- 12.
13. Click next

<https://account.activedirectory.windowsazure.com/proofup.aspx?culture=en-US>

Additional security verification

Secure your account by adding phone verification to your password. [View video](#) to know how to secure your account

**Step 1: How should we contact you?**

Authentication phone

Select your country or region

Method

Send me a code by text message

[Next](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft Legal | Privacy

- 14.
15. Select How Should we contact you?
  - a. Authentication phone - SMS
  - b. Mobile app – Microsoft Authenticator app
    - i. Can download from App store

Microsoft

## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

**Step 1: How should we contact you?**

Mobile app ▾

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the [Microsoft Authenticator app](#).

**Set up** Please configure the mobile app.

Next


©2020 Microsoft | [Legal](#) | [Privacy](#)

- 16.
17. Select receive notification for Verification
18. Then click set up button

## Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



If you are unable to scan the image, enter the following information in your app.

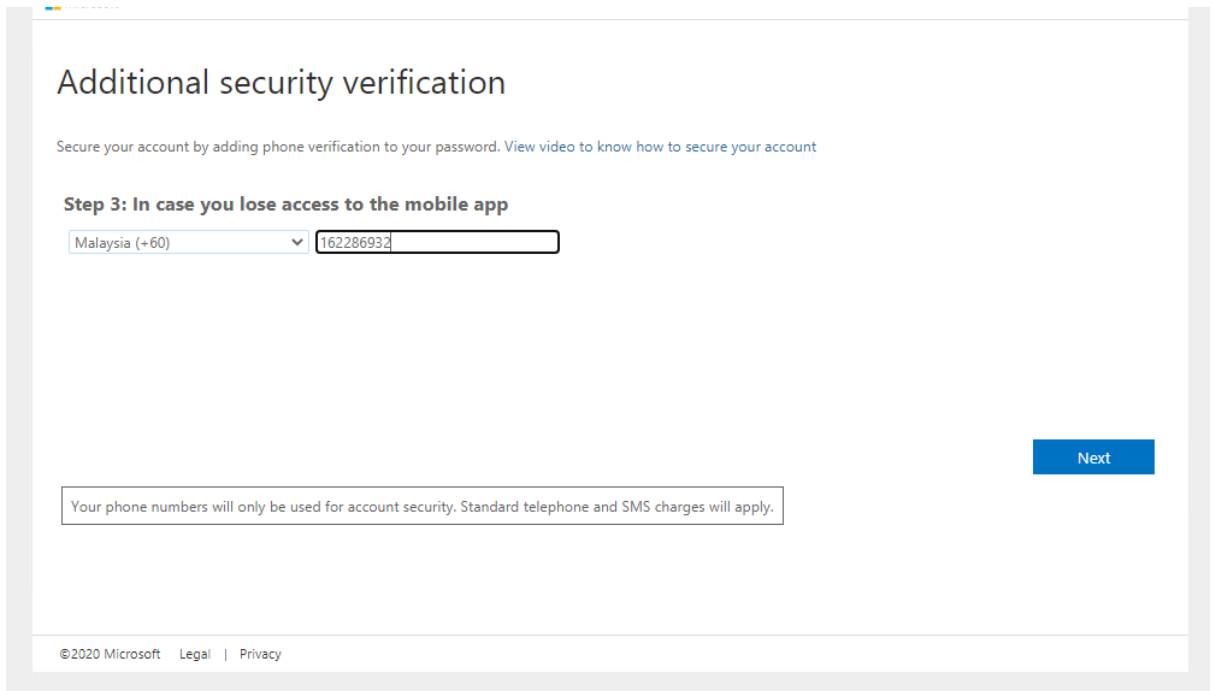
Code: 457 429 184

Url: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/549218822>

If the app displays a six-digit code, choose "Next".

**Next** cancel

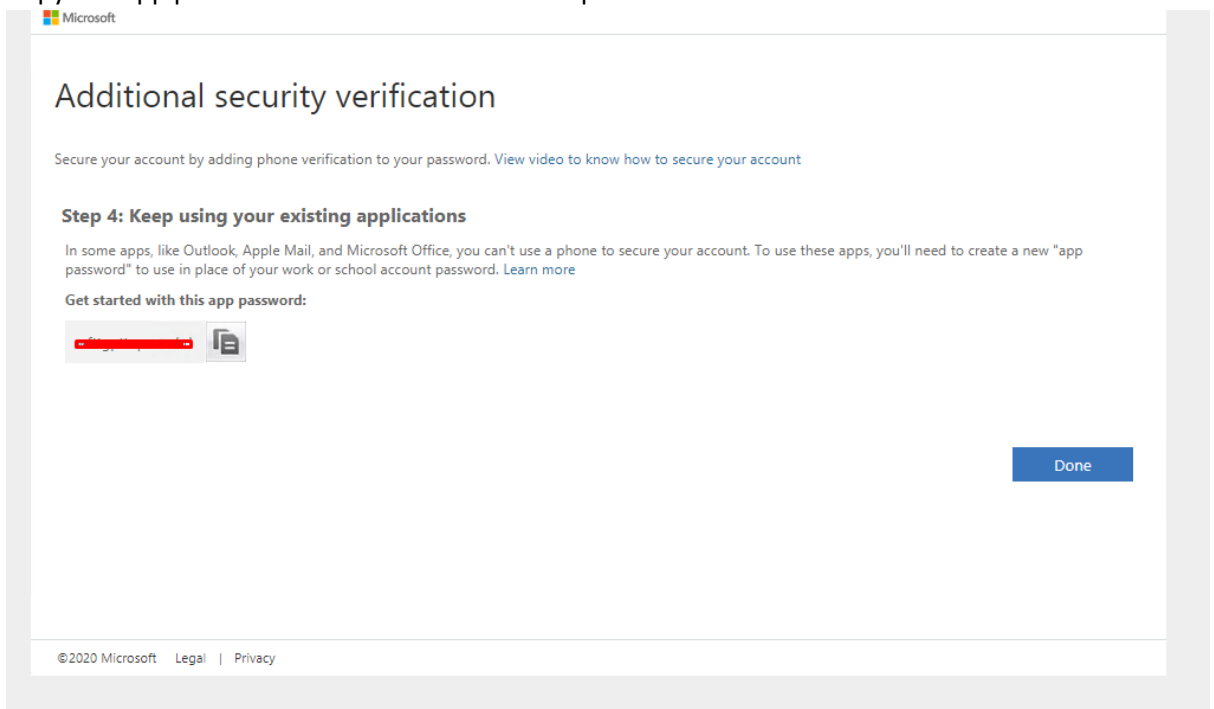
- 19.
20. Then click next
21. Will prompt to approve on phone



22.

23. Next

24. Copy the App password – this is needed for setup outlook



25.

26. Done

To Change:

27. Can Change the Authentication by login to <https://aka.ms/prooofup>

Setup user outlook for Standard user it will prompt for approval in phone authenticator app, for kiosk with pop3, then need to enter the password with App password (not your normal password)