



Australian Government  
Defence

# CadetNet M365

## *Multifactor Authentication Pre-Registration Help Guide*

*September 2025*

## Contents

|                                                               |   |
|---------------------------------------------------------------|---|
| Overview of CadetNet M365 .....                               | 2 |
| What is MFA? .....                                            | 2 |
| Why do we have to use MFA?.....                               | 2 |
| Microsoft Authenticator Installation.....                     | 3 |
| How to install Microsoft Authenticator .....                  | 3 |
| What if I don't own or have access to a smartphone? .....     | 3 |
| How to install Microsoft Authenticator on iOS device .....    | 4 |
| How to install Microsoft Authenticator on Android device..... | 6 |
| Microsoft Authenticator Setup .....                           | 7 |
| How to setup Microsoft Authenticator for CadetNet M365 .....  | 7 |



## Overview of CadetNet M365

CadetNet M365 is made up of two key parts:

1. CadetNet Enterprise Application (CEA) used by over 30,000 ADF Cadets and Adult Volunteers providing online management of Personnel, Activities, Logistics, Facilities, WHS, Learning and Administration modules.
2. Microsoft 365 (M365) providing a single enterprise solution that is secure and flexible to enable:
  - Collaboration across cadets and staff
  - File sharing and storage
  - Access to communication tools like Microsoft Teams

The CadetNet M365 environment can be accessed via CadetNet laptops, personal laptops, PCs, tablets and mobile phones (also referred to as BYOD devices).

With this new online collaboration platform, end users will be required to use multifactor authentication (MFA). This Multifactor Authentication Help Guide has been developed to support users to manage and set up MFA for the first time for a seamless login to CadetNet M365.

### What is MFA?

MFA is a security method that requires users to provide two or more different types of identification to access a device, application, or online service, adding extra layers of protection to prevent unauthorised access. MFA keeps your personal information and accounts secure. It also helps protect Defence's applications and systems against threats.

### Why do we have to use MFA?

Username and passwords are information that can be easily discovered and used to take over not just your CadetNet account but also other personal or work accounts if you have repeated the same password.

Having an extra step can be inconvenient at first, but remember that taking shortcuts leaves your system more vulnerable. It helps to avoid spending hours later on trying to regain access to your accounts and dealing with the consequences of your data being stolen.



## Microsoft Authenticator Installation

### How to install Microsoft Authenticator

It is recommended to use the Microsoft Authenticator App because it provides the most secure sign-in experience and seamless integration with Microsoft 365.

**Please note:** you do not need to download the Microsoft Authenticator application if you already have it. You will be able to set up another profile in Microsoft Authenticator for CadetNet. Follow the steps in the section of ***how to add a CadetNet account*** to an already installed Microsoft Authenticator on your mobile device.

**Note:** If you are having issues with the Microsoft Authenticator app, please check if your mobile device meets the minimum operating systems (OS) requirements:

- Android 8.0 for Android
- iOS 15.0 for Apple

If your mobile device does not meet this requirement, the Microsoft Authenticator app will not be supported. It is recommended that you either update your device to the latest OS prior to installing.

### What if I don't own or have access to a smartphone?

Defence is working on a solution to support you. In the meantime, you can download an authentication application to a tablet (Microsoft Authenticator app [iOS](#) and [Android](#)), laptop or PC ([2Fast – Two Factor Authenticator](#) or another preferred Authenticator app) that you own or can readily access when you need to use CadetNet. This application will provide you with the code you need to authenticate, however you will need to make sure your device is kept secure.

If this doesn't work for you, talk to your unit command to obtain printed versions of activity schedules, communication notifications, forms, and training material. Support will be considered on a case by case basis.

**Note:** If you work in an area that does not allow you to access your smart device (e.g. Defence Zone 3), please use the call option detailed in **step 4** of *“How to setup Microsoft Authenticator for CadetNet M365”* within this Help Guide.

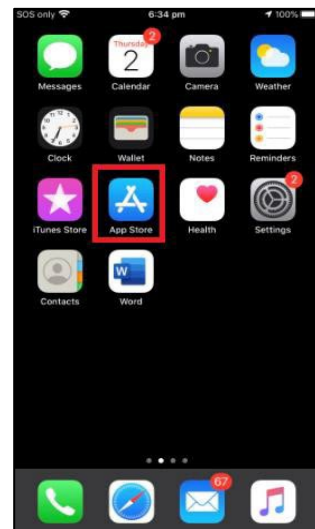


## How to install Microsoft Authenticator on iOS device

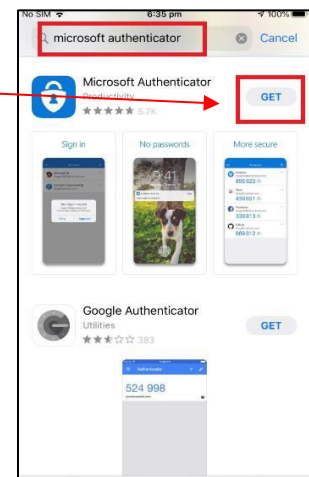
Follow the steps in this section to install Microsoft Authenticator on your mobile device.

**Note:** If you have already installed an Authenticator application on your smart device? Please proceed to page 7 of this Help Guide.

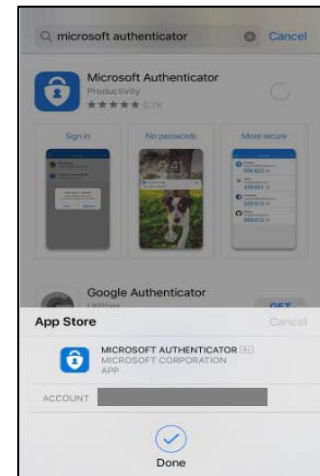
1. On your iOS device, open App Store



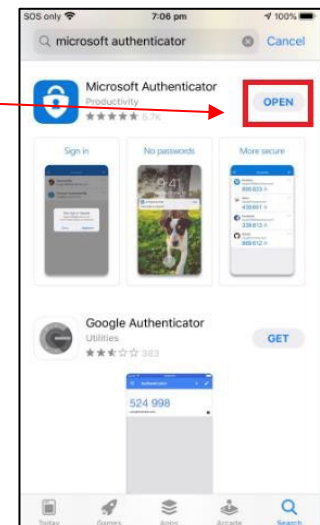
2. In App Store, go to Search bar and enter 'Microsoft Authenticator', and select, then select **Get** to install the app



3. You might be asked to enter Apple ID password or Touch/Face ID if you have Apple account security setup. If you do not have the setup, the app will be installed without this



4. The Microsoft Authenticator app is installed when the status changed into **Open** (Image)



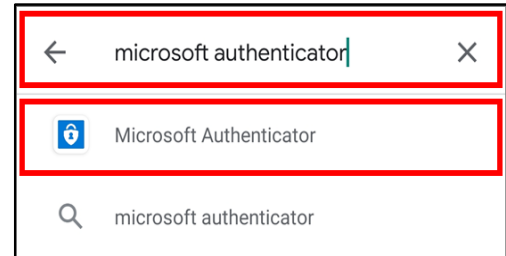
5. You will now be able to find the Microsoft Authenticator app on the main screen of your smart device.



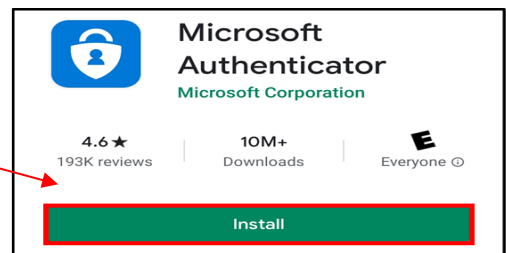
## How to install Microsoft Authenticator on Android device

Follow the steps in this section to install Microsoft Authenticator on your mobile device.

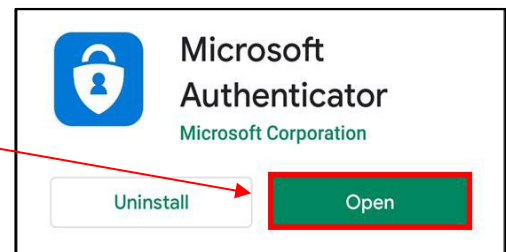
1. With your Android device, **search** 'Microsoft Authenticator' in the application store (e.g. Play Store). **Select** the Microsoft Authenticator application from the search results



2. Select Install



3. Once installed, select Open to launch the Microsoft Authenticator app



4. You will now be able to find the Microsoft Authenticator app on the main screen of your smart device



## Microsoft Authenticator Setup

### How to setup Microsoft Authenticator for CadetNet M365

This includes your first time setting up MFA or if you require an MFA reset. Follow the steps in this section to setup Microsoft Authenticator app for CadetNet.

1. Open a browser on your CadetNet laptop, personal laptop, PC or tablet and navigate to <https://myprofile.microsoft.com>

2. Enter your CadetNet sign in email details which will be different across each Cadet Organisation as follows;

- [jane.doe@cadetnet.gov.au](mailto:jane.doe@cadetnet.gov.au)
- [jane.doe@armycadets.gov.au](mailto:jane.doe@armycadets.gov.au)
- [jane.doe@navycadets.gov.au](mailto:jane.doe@navycadets.gov.au)
- [jane.doe@airforcecadets.gov.au](mailto:jane.doe@airforcecadets.gov.au)

Microsoft  
Sign in  
Jane.Doe@cadets.gov.au  
Can't access your account?  
Next

3. Enter your current CadetNet password

Microsoft  
←  
Enter password  
.....  
Forgot my password  
Use a certificate or smart card  
Sign in

Microsoft  
@cadetnet.gov.au  
Let's keep your account secure  
We'll help you set up another way to verify it's you.  
Use a different account  
Learn more about verifying your identity  
Next

4. Here is where you select which option you would like to use to register your MFA?

If you would like to receive a call or text to sign in with a code? Please select this link and progress to **Step 13** of this Help Guide.

If you have installed Microsoft Authenticator on your smart device, please select **Next** and continue to **Step 5** of this Help Guide.

If you are using **2Fast – Two Factor Authenticator** or another preferred third party desktop Authenticator app, please select this link and follow the instructions for your chosen app.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

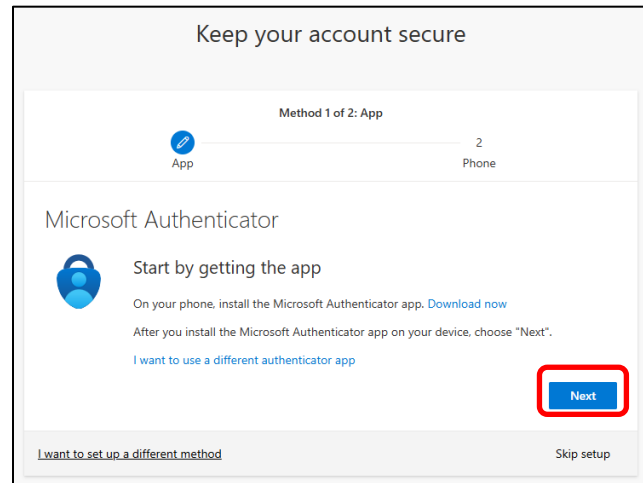
[I want to use a different authenticator app](#)

[Next](#)

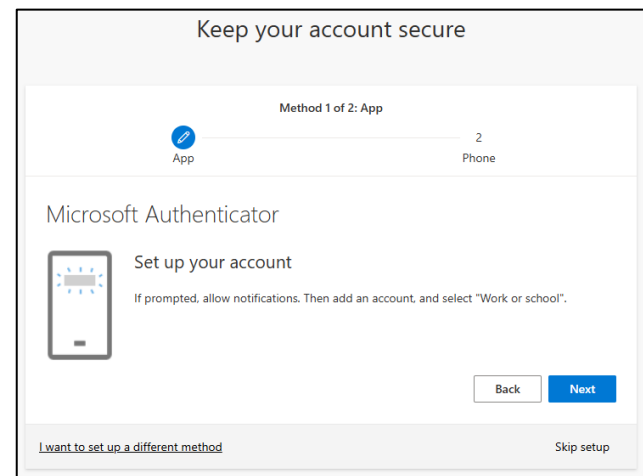
[I want to set up a different method](#)



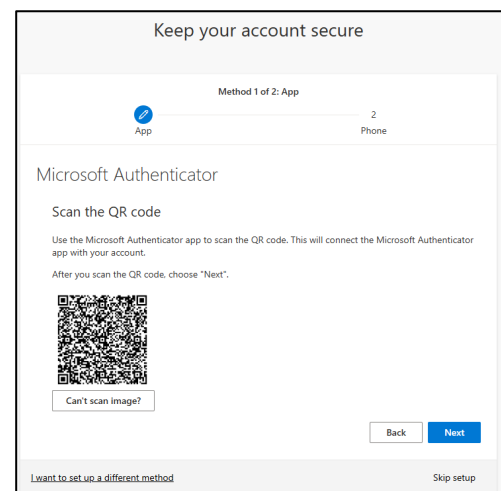
5. Before continuing with this option, you will be required to have completed Steps 1 to 4 of ***How to Install Multifactor Authenticator*** of this Help Guide. Once you have downloaded the Microsoft Authenticator app on your smart device; Select ***Next***



6. Now, follow the prompt to set up your Microsoft Authenticator app, and then Select ***Next***



7. This will issue a one-time QR code - Use the Microsoft Authenticator app on your smart device to scan the QR code. This will connect the Microsoft Authenticator app to your account.



8. The following steps will guide you through the syncing with your mobile Microsoft Authenticator app;

**Step 1** - Open your Authenticator app on your mobile device

**Step 2** - Select Add Account

**Step 3** - Select Work or School Account

**Step 4** – Now select Scan QR Code

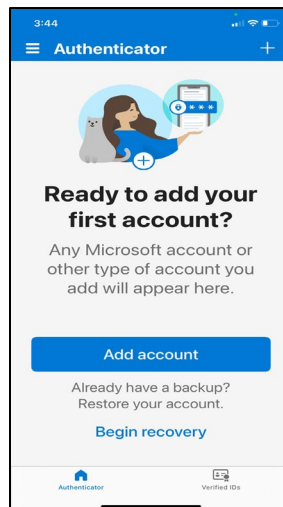
**Step 5** - Hold your smart device camera towards the QR code presented on your screen

**Step 6** – Now you will see that you CadetNet sign in email has successfully loaded.

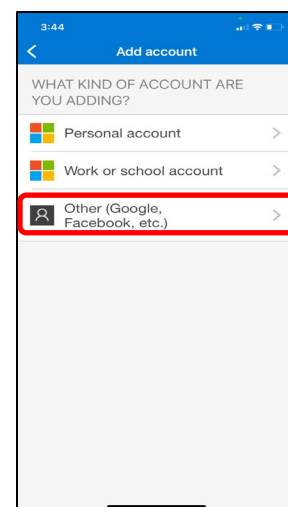
**Step 1**



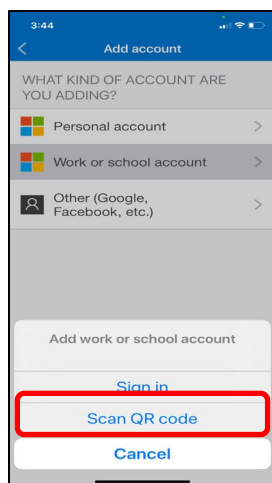
**Step 2**



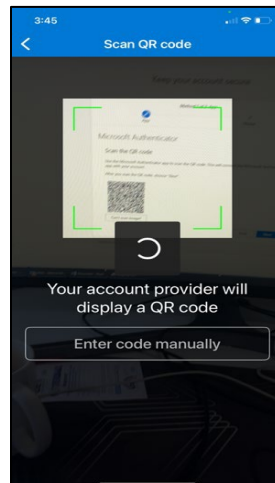
**Step 3**



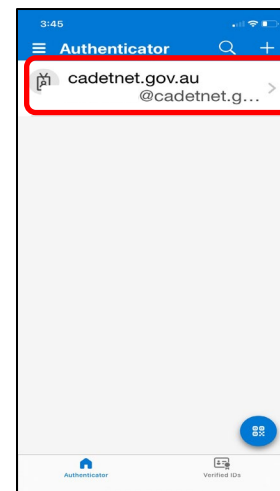
**Step 4**



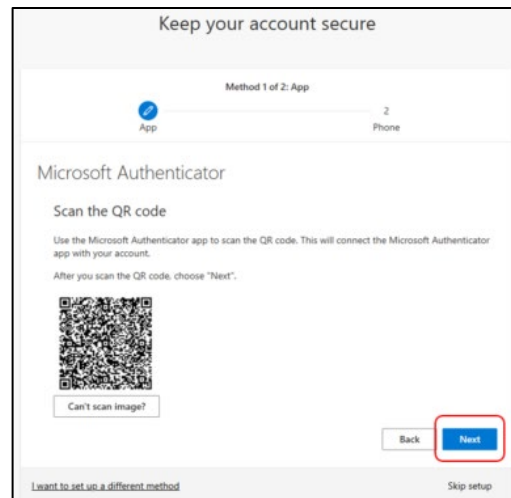
**Step 5**



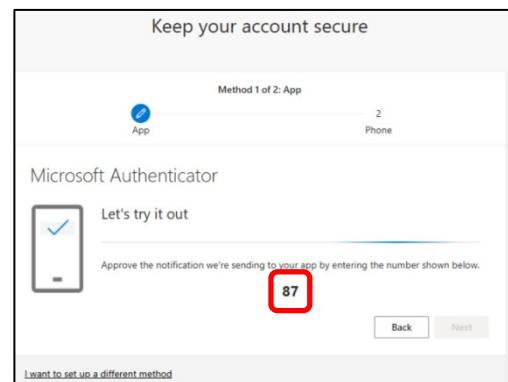
**Step 6**



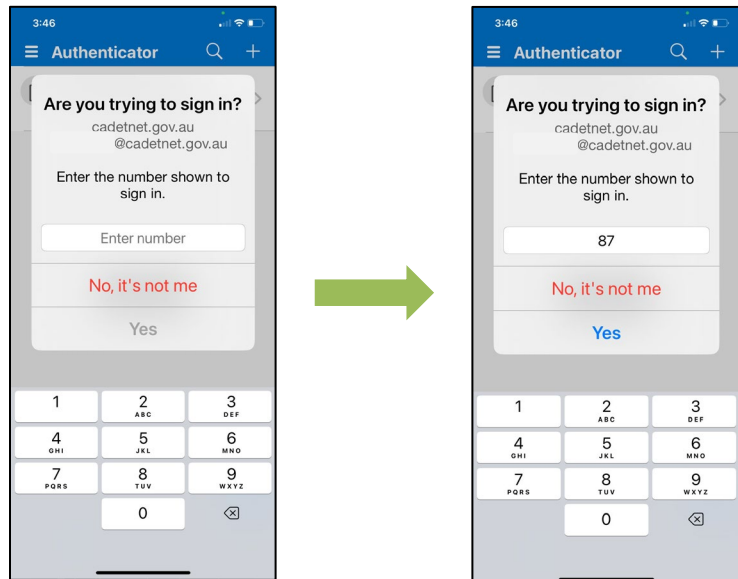
9. Now that you have scanned the QR code, Select **Next**.



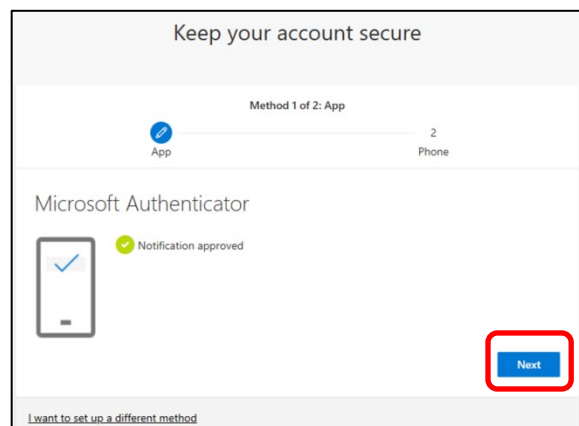
10. This will generate a one-time code to be entered in to your Microsoft Authenticator app on your smart device.



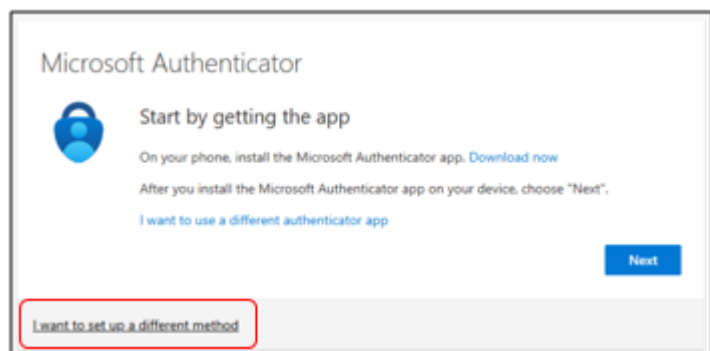
11. Enter your one-time code into your smart device authenticator app.



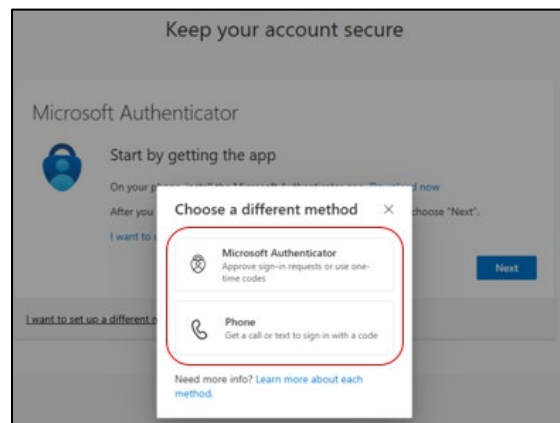
12. When the *Notification approved* message appears on the webpage, select **Next**. And progress to **Step 19** of this *Help Guide*.



13. Here you have opted to get a call or text message sent to your mobile device in **Step 4** of the *Help Guide*;



14. Choose your preferred method



15. Now, complete the required fields; selecting Country Code (Australia (61+)) and entering your mobile number then select **Next**.

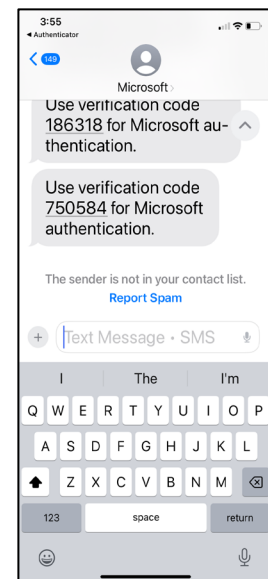
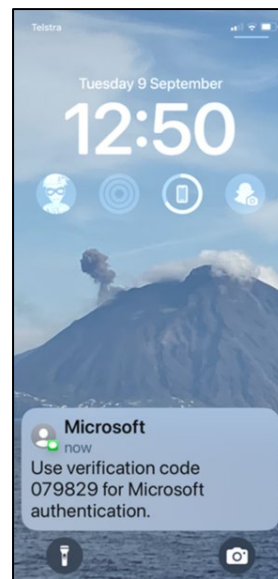
**Note:** This will initiate a validation code to be sent as a text message or you will receive a call to your mobile phone. **If you opted for a call** please proceed to **Step 19** of the *Help Guide*.

16. Depending on your device; you may need to complete this validation prompt before progressing through to the next screen. A new code will generate after each attempt until you get it right!

If this screen does NOT display, please proceed to **Step 17** of this *Help Guide*.

17. One-time Validation Code text message will be sent to your smart device.

**Note:** The code displayed in this guide is only an example. You will need to refer to your mobile to retrieve your onetime validation code.



18. Enter your one-time 6 digit validation code sent to your mobile. Select Next

Keep your account secure

Method 2 of 2: Phone

Email Phone

Phone

We just sent a 6 digit code to +61 Enter the code below.

Enter code [Resend code](#)

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

[I want to set up a different method](#) [Skip setup](#)

19. Once Verification is complete, Select **Next**

Keep your account secure

Method 2 of 2: Phone

Email Phone

Phone

Verification complete. Your phone has been registered.

[Next](#)

[Skip setup](#)

20. **Congratulations!** You have successfully Pre-Registered your MFA set up, Please select **Done**,

Method 2 of 2: Done

App Phone

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Phone +61

Microsoft Authenticator

[Done](#)

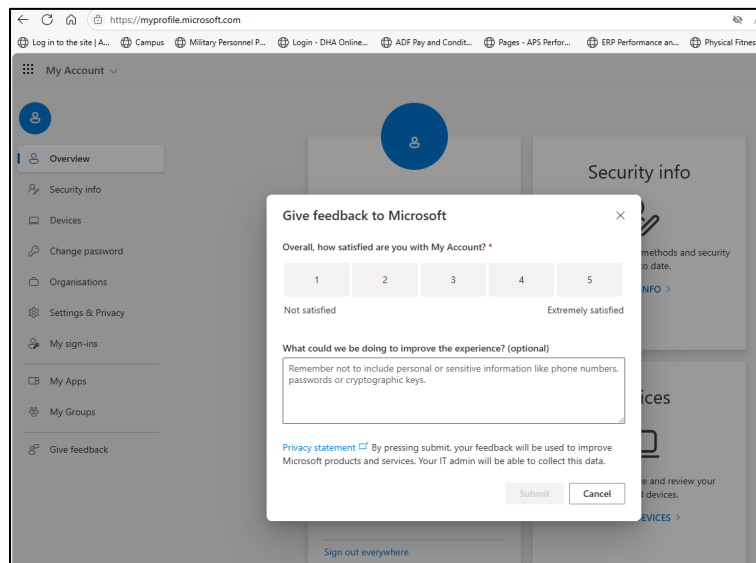


21. If you are using a shared device (CadetNet Laptop) select **NO**.

If you are using a BYOD then you can select **YES**.



22. Microsoft will automatically prompt you for feedback, Please select **Cancel**



23. This will default to the Microsoft home page. As this is only an MFA Pre-Registration opportunity, you will be blocked from accessing any of the application until after System Go-Live.

