



Australian Government
Defence



CadetNet M365

Microsoft Multifactor Authenticator (MFA) Help Guide

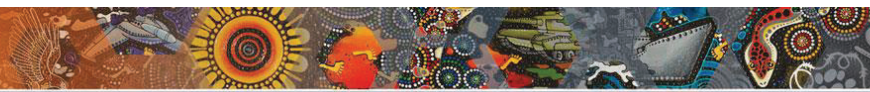
October 2025 – Version 1





Contents

Overview of CadetNet M365	1
What is MFA?	1
Why do we have to use MFA?	1
What if I don't own or have access to a smartphone?	1
Microsoft Authenticator Installation	2
How to install Microsoft Authenticator	2
Install Microsoft Authenticator App:	2
How to install Microsoft Authenticator on iOS device.....	2
How to install Microsoft Authenticator on Android device	4
Microsoft Authenticator Setup	5
How to setup Microsoft Authenticator for CadetNet M365.....	5
Set up SMS or Call as Authenticator?	11
Having Trouble Logging in?	14
Before Setting Up MFA	14
Update Your Browser:	14
Clear Browser Data	14
Check for Browser Extensions	15
I don't remember my username. What do I do now?	16
How do I reset my password?.....	16



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, provides 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 Personal Electronic Device (PED) 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?

Usernames 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 accounts and systems 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.

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](#)), and your laptop or PC 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 6** of “How to setup Microsoft Authenticator for CadetNet M365” within this Help Guide.

Microsoft Authenticator Installation

How to install Microsoft Authenticator

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

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, “**How to add a CadetNet account**” to an already installed Microsoft Authenticator on your mobile device.

Install Microsoft Authenticator App:

Download and install a recommended authenticator app, such as the [Microsoft Authenticator](#) or [Google 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.

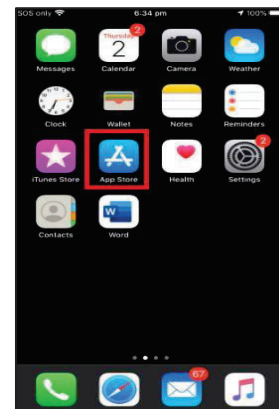


How to install Microsoft Authenticator on iOS device

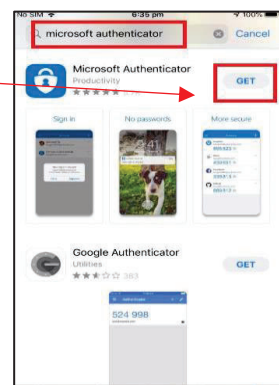
Follow the steps in this section to install Microsoft Authenticator on your mobile device.

Note: If you have already installed an Authenticator application on your smart device? Please proceed to **Page 5** of this Help Guide.

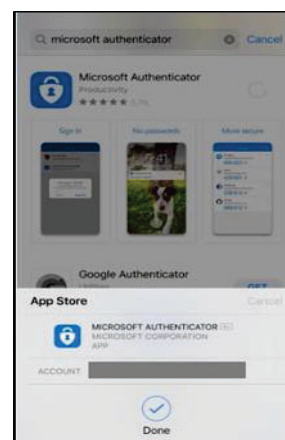
1. On your iOS device, open App Store



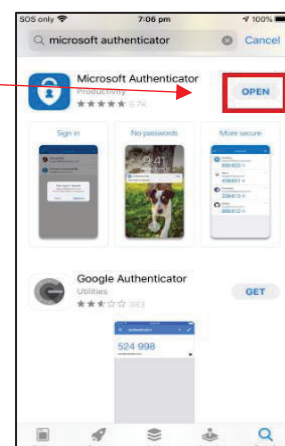
2. In App Store, go to Search bar and enter 'Microsoft Authenticator', and select, then select Get to install the app



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)



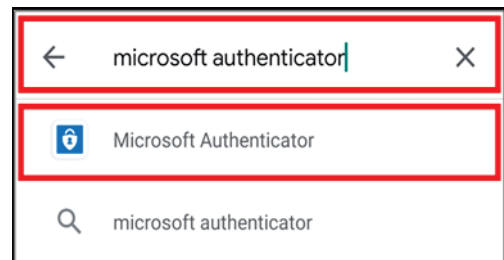
5. You will now be able to find the Microsoft Authenticator app on the main screen



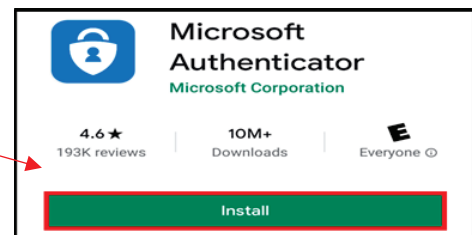
How to install Microsoft Authenticator on Android device

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

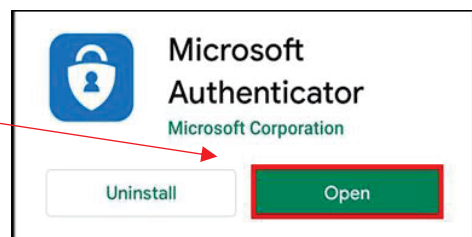
1. With your Android device, search 'Microsoft Authenticator' in the application store (e.g. Play Store). Select the Microsoft Authenticator application from the search results



2. Select Install



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



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



Microsoft Authenticator Setup

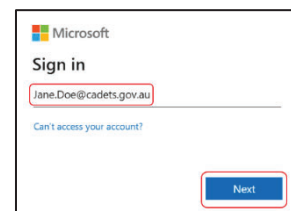
How to setup Microsoft Authenticator for CadetNet M365

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 for CadetNet.

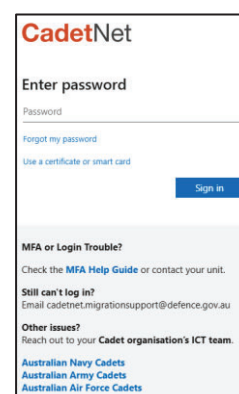
- Open a browser on your CadetNet laptop, personal laptop, PC or tablet and navigate to <https://m365.cloud.microsoft.mcas.ms/apps/>

- Enter your CadetNet sign in email details or User ID with your organisation domain which will be different across each Cadet Organisation as follows;

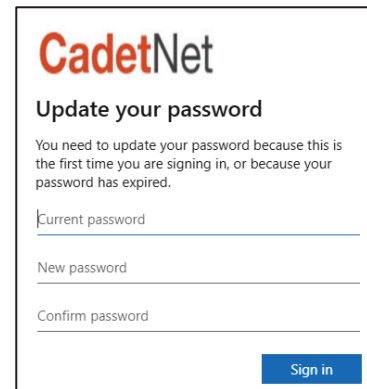
- jane.doe@armycadets.gov.au
- jane.doe@navycadets.gov.au
- jane.doe@airforcecadets.gov.au



- Enter your current CadetNet password



Note: This step will only apply if you have reset your password or if this is your first time logging in to CEA. Follow the prompts and select Sign in



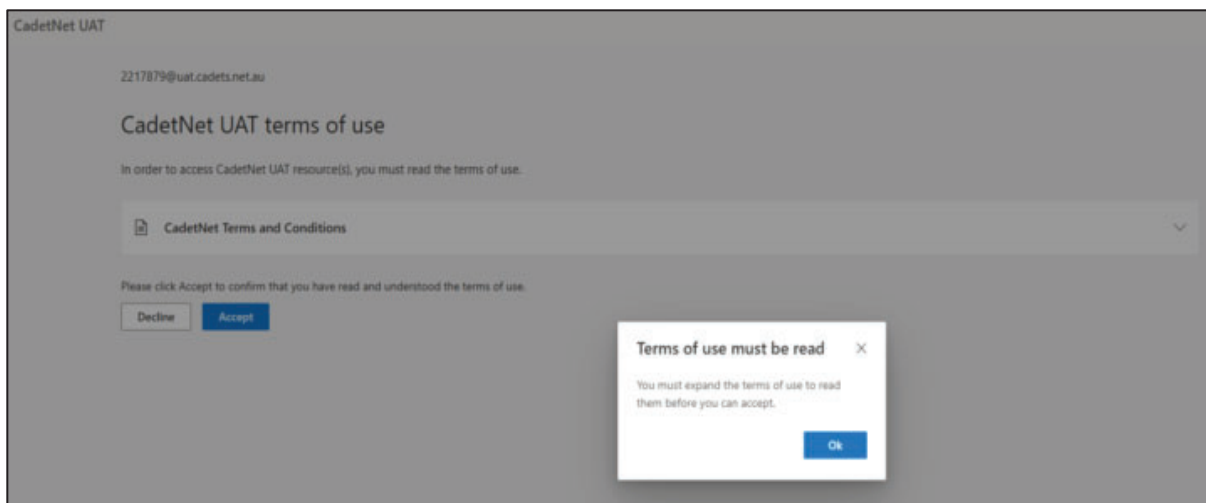
The screenshot shows the 'CadetNet' login page with the heading 'Update your password'. Below the heading, a message states: 'You need to update your password because this is the first time you are signing in, or because your password has expired.' There are three input fields labeled 'Current password', 'New password', and 'Confirm password'. A blue 'Sign in' button is located at the bottom right of the form.

4. Please read through Terms and Conditions and select **Accept**



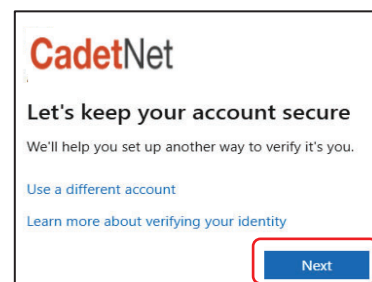
The screenshot shows the 'CadetNet UAT' terms of use screen. It displays the email address '2207124@uat.cadets.net.au' and the title 'CadetNet UAT terms of use'. A message states: 'In order to access CadetNet UAT resource(s), you must read the terms of use.' Below this, there is a link to 'CadetNet Terms and Conditions' with a red arrow pointing to it. At the bottom, there are two buttons: 'Decline' and 'Accept', with the 'Accept' button highlighted by a red box.

Note: You must open and read through the Terms and Conditions before progressing or you will be prompted to read.

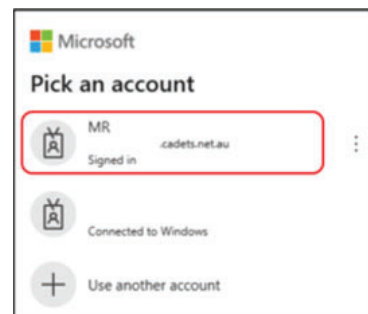


The screenshot shows the 'CadetNet UAT' terms of use screen, similar to the previous one, but with an error message. The error message is a white box with a red border and a red 'X' icon, containing the text: 'Terms of use must be read', 'You must expand the terms of use to read them before you can accept.', and an 'Ok' button. The 'Accept' button on the main screen is still highlighted by a red box.

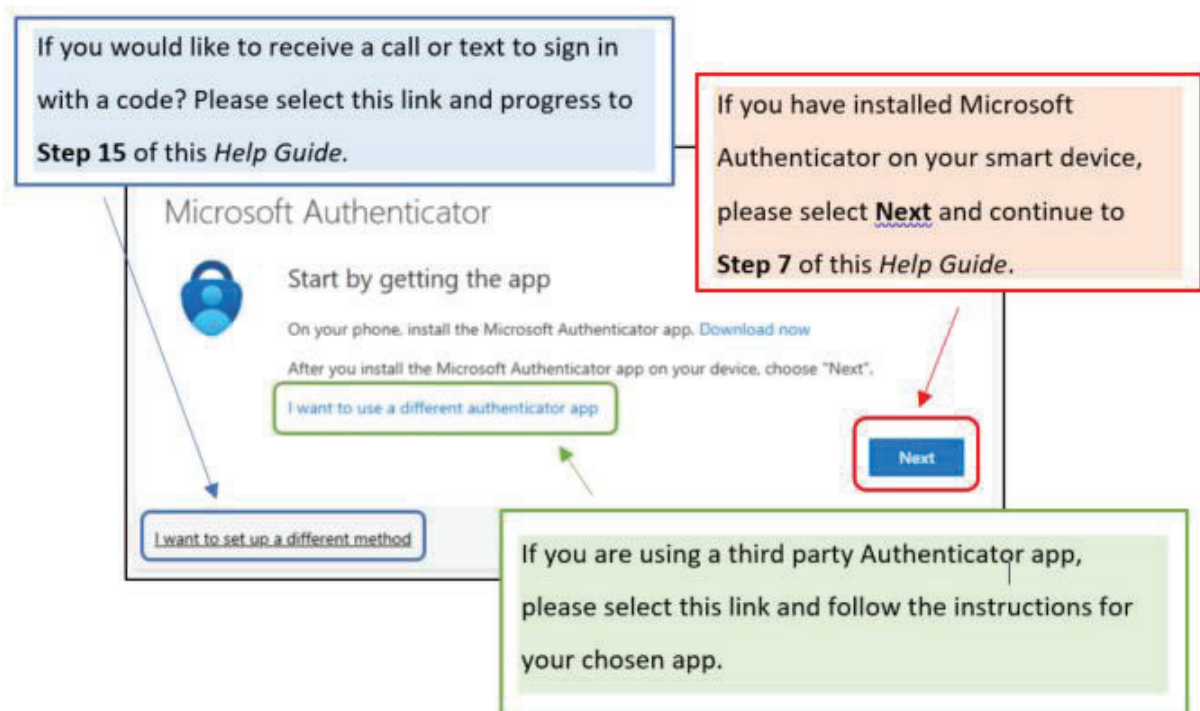
Once you have read and accepted the Terms and Conditions, you will now commence setting up your MFA. Select **Next**



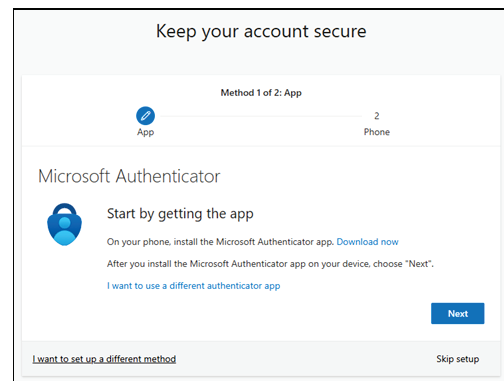
5. Select you CadetNet Account from the list



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



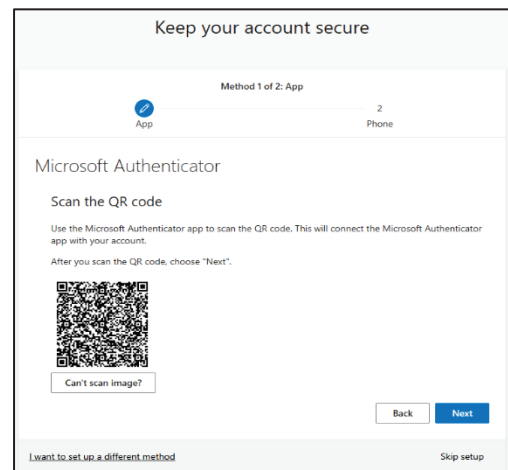
7. Before continuing with this option, you will be required to have completed Steps 1 to 4 of **“How to Install Multifactor Authenticator”** on **pages 2 to 5** of this Help Guide. Once you have downloaded the Microsoft Authenticator app on your smart device; Select Next



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

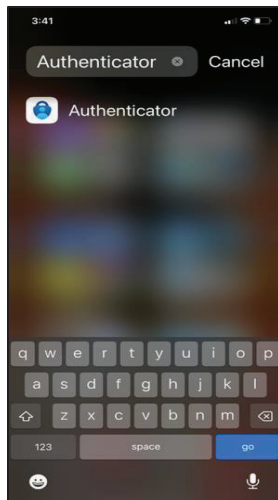


9. This will issue a one-time QR code - Use the Microsoft Authenticator app on your smart device to scan the QR code. This will connect the Microsoft Authenticator app to your account.

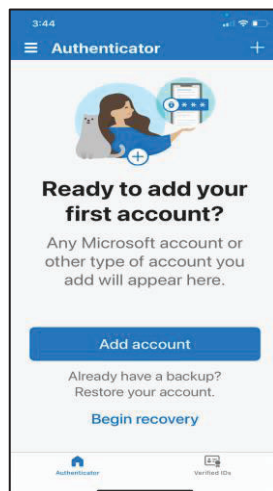


10. The following steps will guide you through the syncing with your mobile Microsoft Authenticator app;

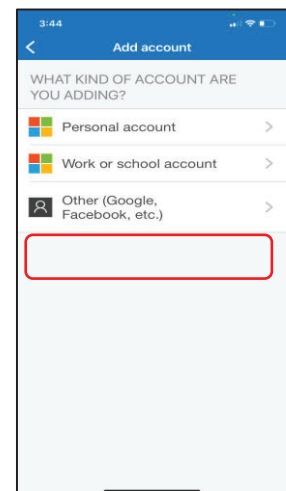
Step 1



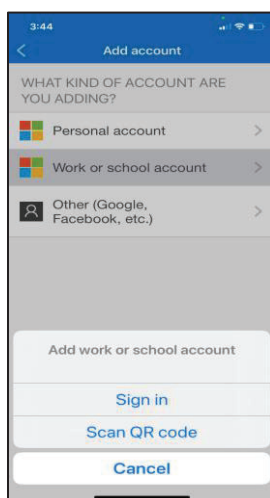
Step 2



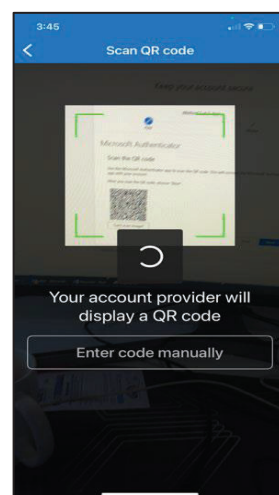
Step 3



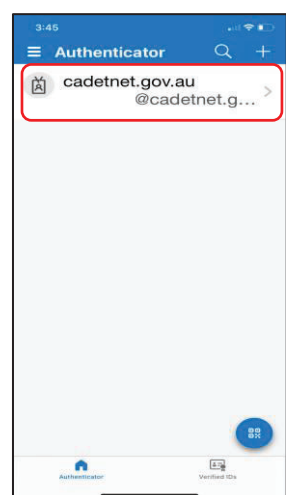
Step 4



Step 5



Step 6



Step 1 - Open your Authenticator app on your mobile device

Step 2 - Select Add Account

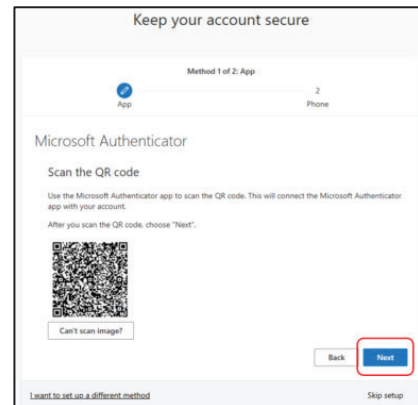
Step 3 - Select Work or School Account

Step 4 - Now select Scan QR Code

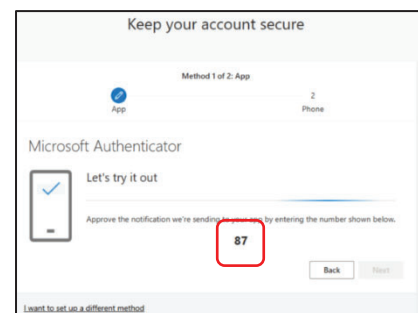
Step 5 - Hold your smart device camera towards the QR code presented on your screen

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

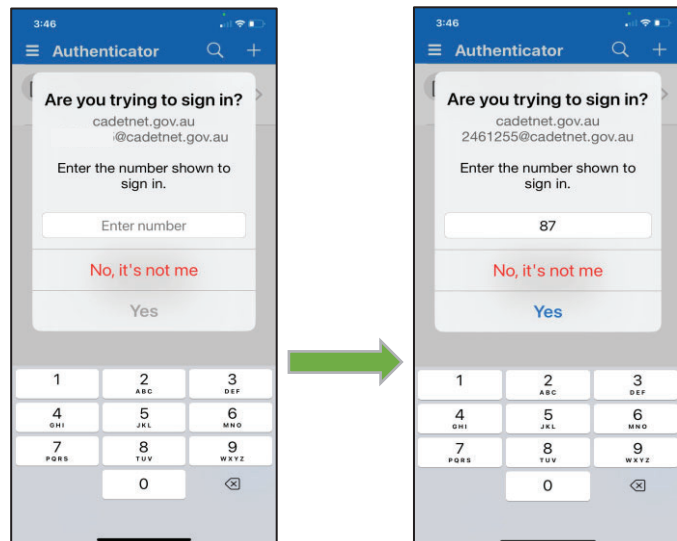
11. Now that you have scanned the QR code, Select **Next**



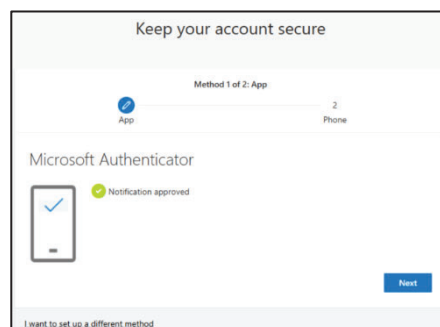
12. This will generate a one-time code to be entered in to your Microsoft Authenticator app on your smart device.



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

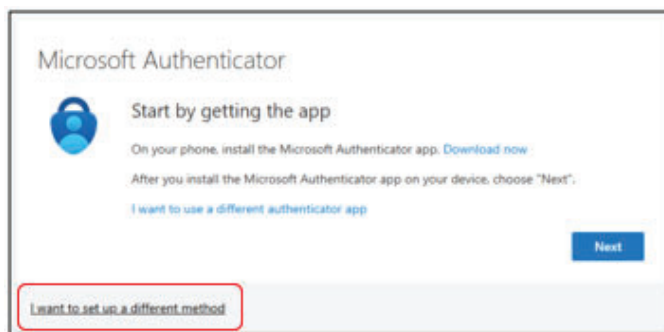


14. When the Notification approved message appears on the webpage, Select **Next**. And progress to **Step 23** of this Help Guide.

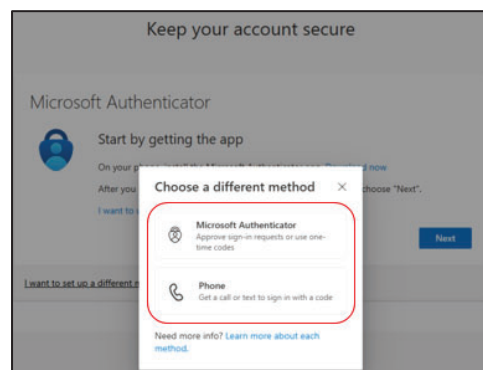


Set up SMS or Call as Authenticator?

15. Here you have opted to get a call or text message sent to your mobile device in **Step 6** of the Help Guide;

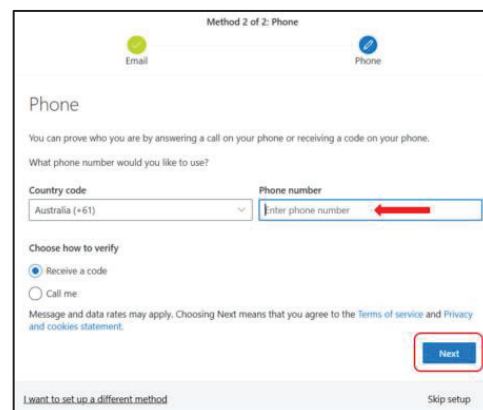


16. Choose your preferred method



17. 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 20** of the Help Guide.

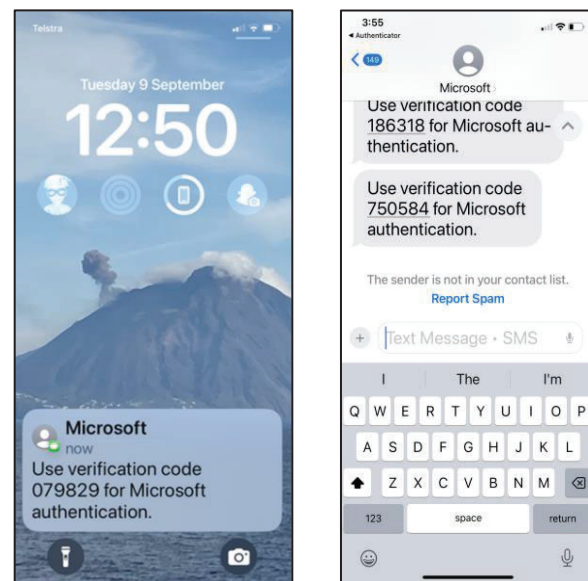


18. Depending on your device; you may need to complete this validation prompt before progressing through to the next screen. A new code will generate after each attempt until you get it right!

Note: If this screen does NOT display, please proceed to **Step 20** of this Help Guide.

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

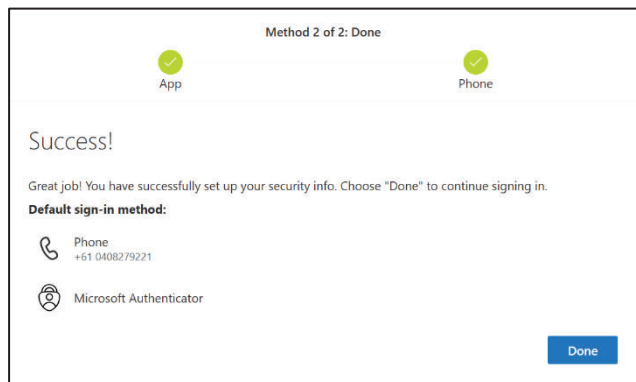
Note: The code displayed in this guide is only an example. You will need to refer to your mobile to retrieve your onetime validation code.



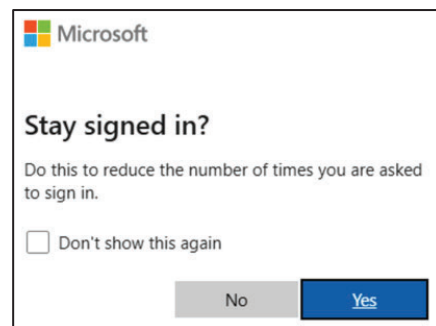
20. Enter your one-time 6 digit validation code sent to your mobile. Select **Next**

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

22. **Congratulations!** You have successfully completed your MFA set up, Please select **Done**

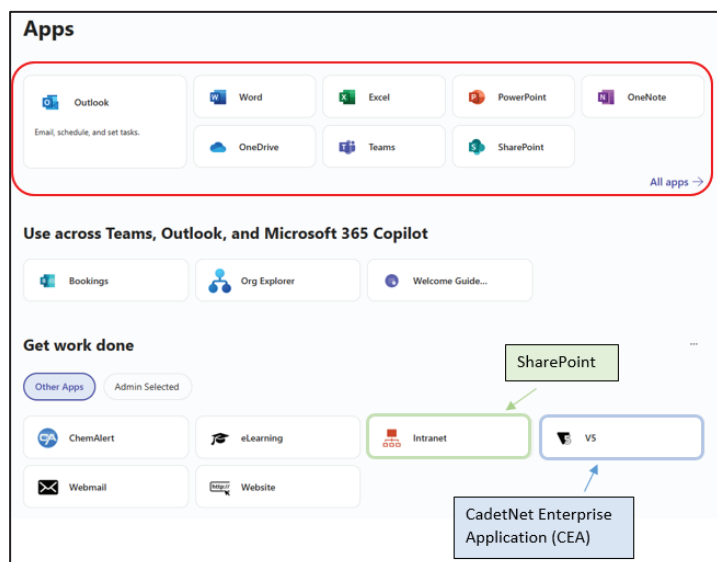


23. If you are using a shared device (CadetNet Laptop) select **NO**.
If you are using a PED then you can select **YES**



24. Welcome to Microsoft 365 Apps Homepage!

Here you can access all Microsoft applications as well as SharePoint and CadetNet CEA.



Having Trouble Logging in?

Here are some helpful tips and tricks that might help;

Before Setting Up MFA

Ensure your device is password protected, has updated antivirus software, your web browser is up-to-date, preferably a modern browser like Microsoft Edge or Google Chrome, and have an authenticator app installed on a mobile device. Also, check for any browser extensions that might interfere and clear your browser's cache and cookies.

Update Your Browser:

Use a Modern Browser: Ensure your browser is updated to the latest version to avoid the "Your browser is not supported or up-to-date" error message during setup.

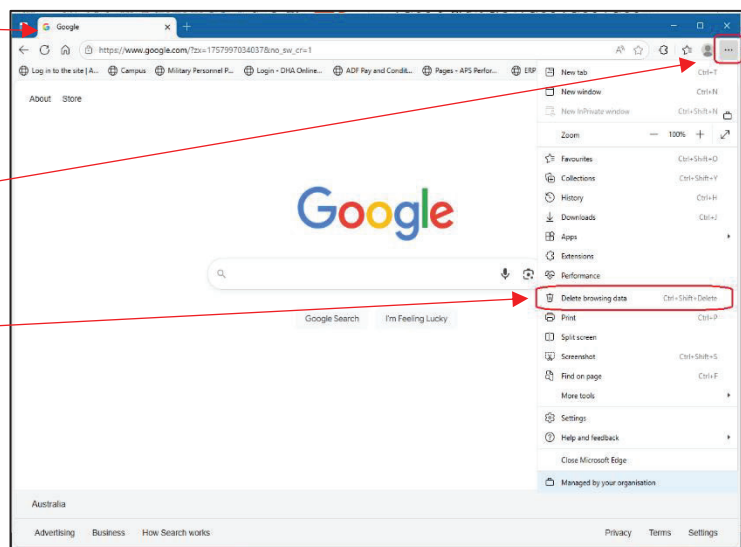
Recommended Browsers: Microsoft Edge, Google Chrome, and Mozilla Firefox are generally recommended for their compatibility with MFA processes.

Check for Interfering Components: Make sure the Microsoft Edge WebView2 Runtime is up-to-date if you're using it.

Clear Browser Data

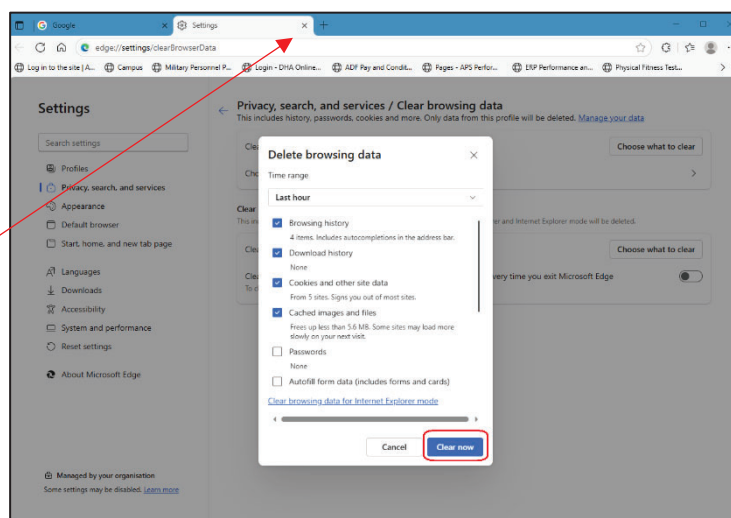
Clear Cache and Cookies: Sometimes, issues with MFA can be resolved by clearing your browser's cache and cookies.

1. Open web browser, in this instance I am using Google
2. Select [...] which will drop down menu
3. Select Delete Browsing Data



4. Select **Clear Now**, this will initiate and complete the clearing of browser's cache and cookies the

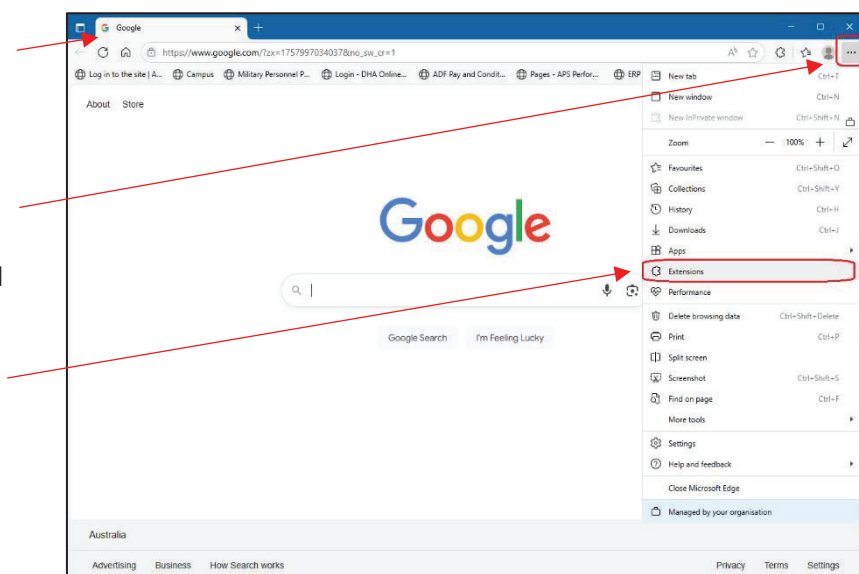
5. You can now close your web browser and commence login



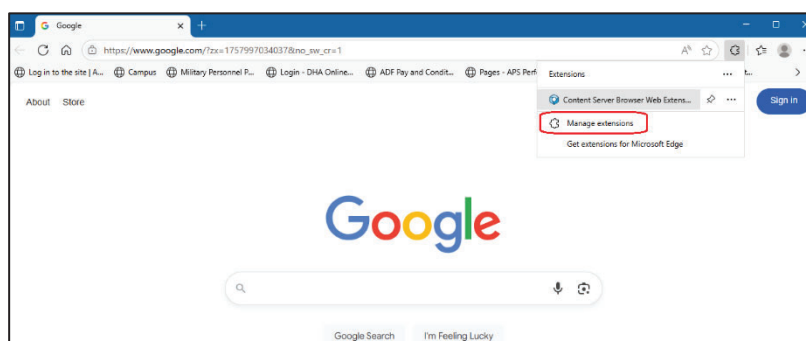
Check for Browser Extensions

Disable Extensions: Some browser extensions can interfere with the MFA process. Try disabling them to see if the issue is resolved. [This example uses Microsoft Edge](#)

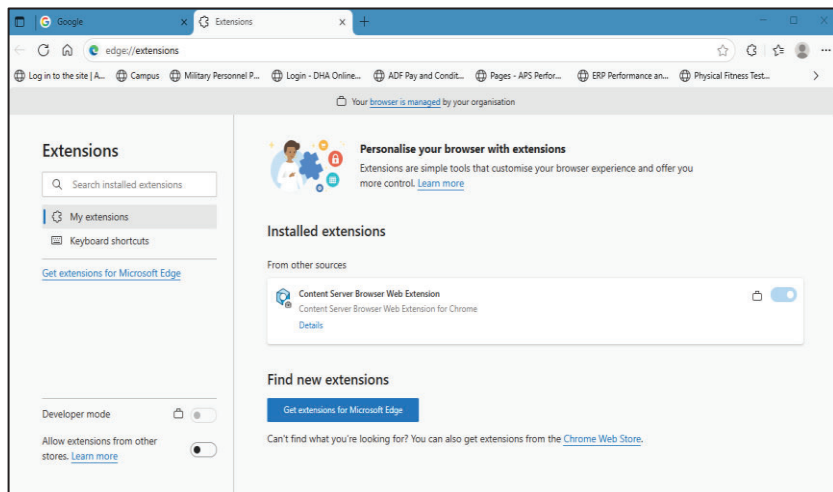
1. Open web browser, in this instance I am using Google
2. Select [...] which will drop down menu
3. Select Extensions



4. Select Manage Extensions



5. Manage Extension from the homepage
6. Once actioned, you can now close your web browser and commence login



I don't remember my username. What do I do now?

Ask your unit staff they will be able to provide it to you.

How do I reset my password?

You can use the self-serve [password reset](#) by Microsoft

Remember, the only question left is the one you're about to ask! Don't hesitate to reach out.. Enjoy!