Australian Government
Department of Defence
Chief Information Officer Group

VERA Security and Authentication

Help Guide

January 2025

Defending Australia and its National Interests
www.defence.gov.au

Contents

Overview

VERA document security level

VERA is Defence’s Microsoft Office 365 Cloud-based tool that is available in the Defence PROTECTED Environment (DPE) / DREAMS, and on authorised devices (Defence Protected Laptops, Defence Protected iOS Devices, and Personal laptops/computers). VERA delivers a capability to allow collaboration, file sharing, and the ability to support 'business as usual' in the Department of Defence in a secure environment.

Users are reminded:

- Accounts are provisioned by the Department of Defence for users with a valid Defence identity and email address.
- Users are not able to invite additional users to this platform.
- This platform is designed for Defence use only and should only contain materials of a rating of OFFICIAL, OFFICIAL:Sensitive and PROTECTED level.
- It should not be used as a replacement or alternative to DREAMS. Users are required to access business applications through the DPE or DREAMS platforms.
- Defence users can now access VERA with their ICT-activated DCAC. Password-less sign-in only requires connecting your DCAC to the device and entering the card PIN. For more information, please refer to Entra ID - Certificate-Based Authentication User Guide. This is the most preferred authentication method by the Department of Defence.
- Your Microsoft Authenticator app will need to be set up within the **PROTECTED** network such as **DREAMS**, **DPE** or from a **Defence PROTECTED Laptop.**
- If you are accessing VERA on **PROTECTED** devices e.g. iPhone/iPad, please setup the Microsoft Authenticator app on an alternate device e.g. personal phone to avoid access issues.
- DeepSeek products, applications or web services are not to be installed on devices used to access DREAMS or VERA.

VERA should be accessed through a Google Chrome or Microsoft Edge web browser, and through authorised personal devices. Please note documents and data exchanged to and from VERA can only occur within networks accredited up to PROTECTED. Documents can only be uploaded to and downloaded from VERA when accessing VERA on the DPE (including through DREAMS).

Personal device security settings

Ensure the personal device is password protected, has updated antivirus software, and the latest operating system security patches installed. In addition, for mobile devices (iOS and Android) please ensure:

- Users only install applications from trusted app stores; and
- VERA is not used on jailbroken iPhone or Android devices in developer mode.

What authentication and verification methods are available

The Department of Defence recommends passwordless authentication methods such as the DCAC smartcard, and the Microsoft Authenticator app because they provide the most secure sign-in experience.

Best: Passwordless	**Better:** Password and …	Phasing out: Password and …
Certificates Using your DCAC for Authentication This is the most preferred authentication method and your DCAC Smartcard is enabled for MFA by default.	Authenticator (Push Notifications) Microsoft Authenticator This works well with BYOD or if you do not work regularly in the Defence zone 3 or higher facilities.	Voice Add Skype phone call option The phone call authentication is planned to be removed. Please use your DCAC for authentication instead.

Entra ID Certification based Authentication

Defence users can now access VERA with their ICT-activated DCAC. Password-less sign-in only requires connecting your DCAC to the device and entering the card PIN. Using your DCAC for MFA will improve security and ensure that Defence remains compliant with industry best practices, and ISM and DSPF requirements.

This is the most preferred authentication method by the Department of Defence.

Using your DCAC for VERA / Entra ID Authentication

Follow the steps in this document Entra ID - Certificate-Based Authentication User Guide to use DCAC to sign into VERA.

Microsoft Authenticator Installation

How to install Microsoft Authenticator

Microsoft Authenticator is an application used for multi factor authentication (MFA) when logging into VERA.

MFA is not required when logging into VERA through a DPE terminal or DREAMS session.

MFA is required when logging into VERA outside of the DPE/DREAMS (e.g. through a BYOD (personal) device).

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 VERA, follow the steps on section of how to add a VERA account to an already installed Microsoft Authenticator on your mobile device to set up. Your Microsoft Authenticator app will need to be set up within the PROTECTED network such as DREAMS**,** DPE or from a Defence PROTECTED Laptop.

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 or set the phone call method as an alternative authentication method.

How to install Microsoft Authenticator on BYOD iOS device

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

1. On your iOS device, click and open App Store

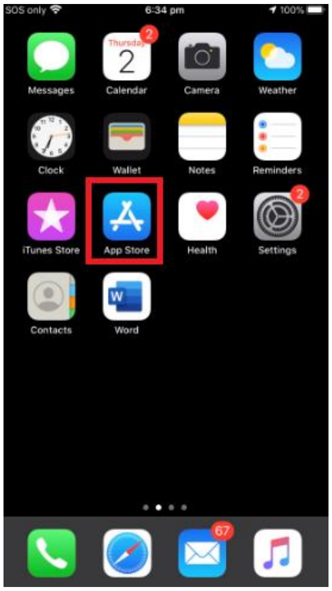


Image 1

2. In App Store, go to Search bar and enter ‘Microsoft Authenticator’, and click on Get to install the app (image 2).

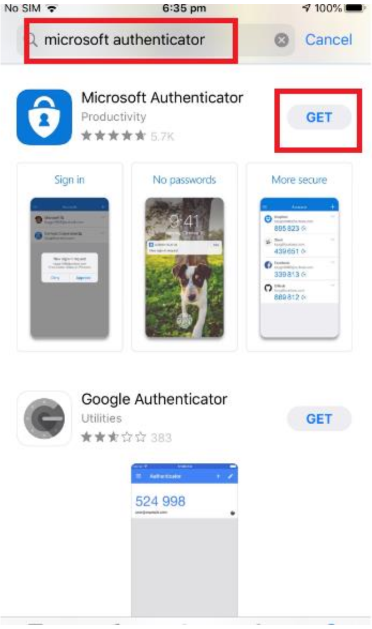


Image 2

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

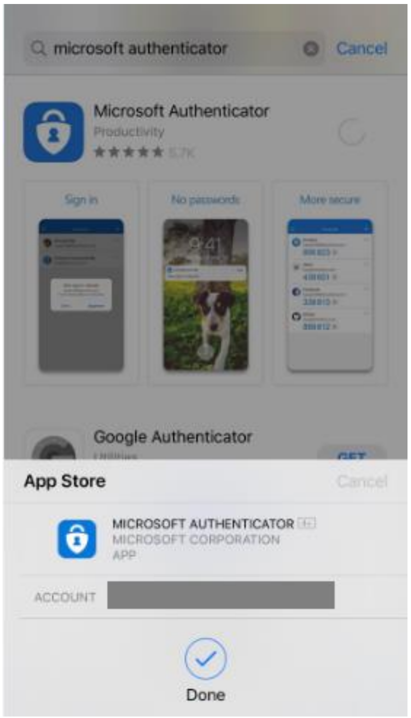


Image 3

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

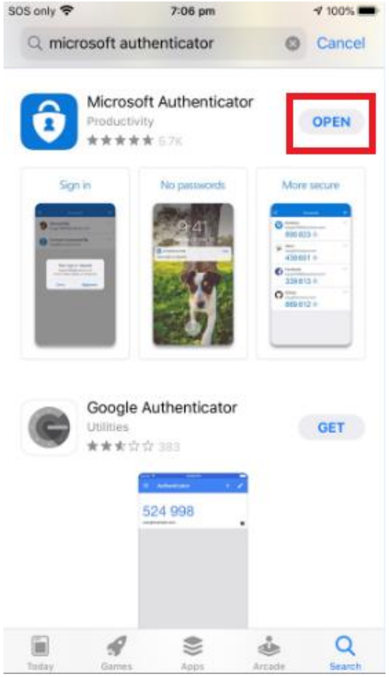


Image 4

5. You can find the app on the main screen (Image 5)

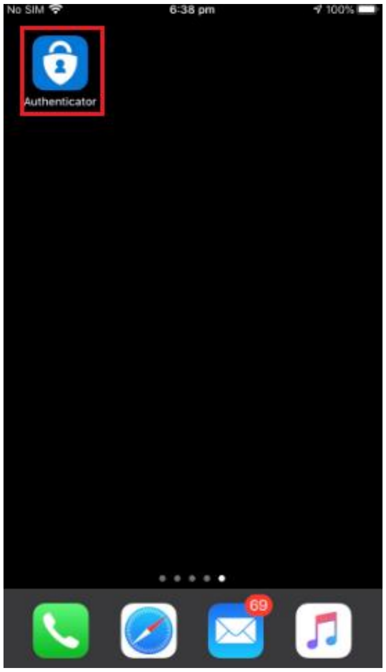
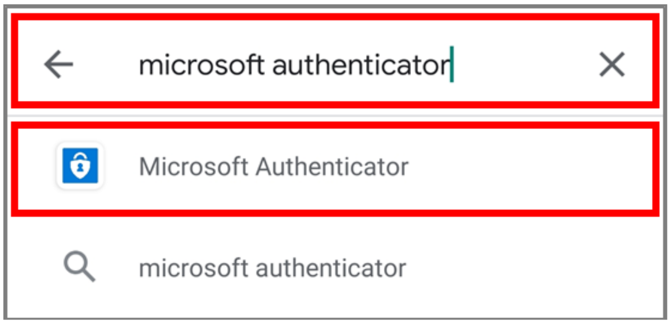


Image 5

How to install Microsoft Authenticator on BYOD 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 (**Image 1**);



microsoft authenticator

Image 1

2. **Click** Install (**Image** 2);

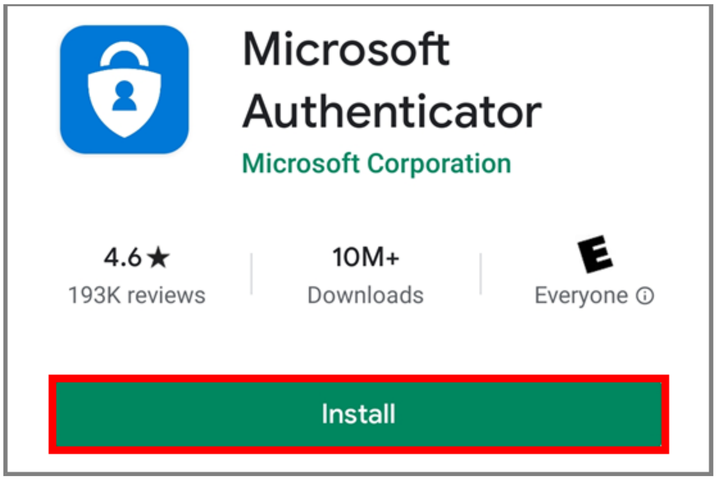


Image 2

3. Once installed, **click** Open to launch the Microsoft Authenticator app (**Image 3**);

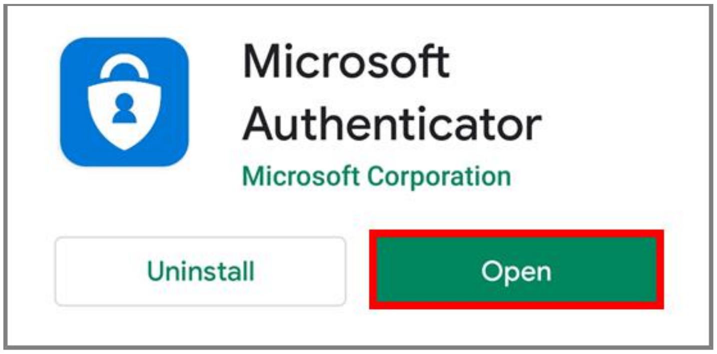


Image 3

4. You can locate the app on main screen (Image 4)

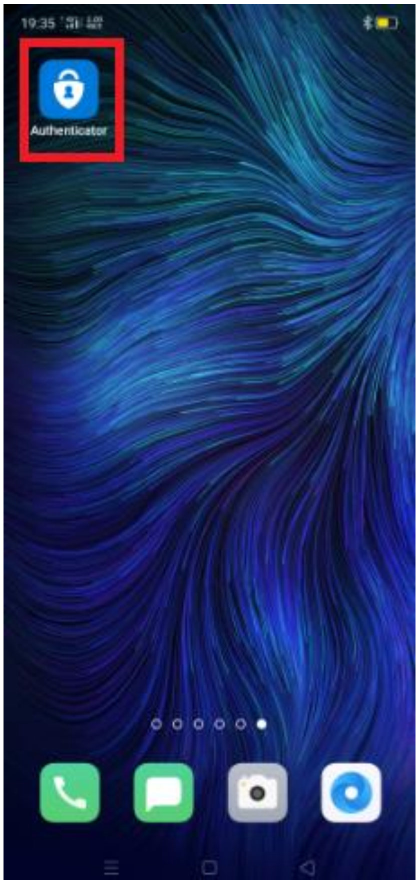


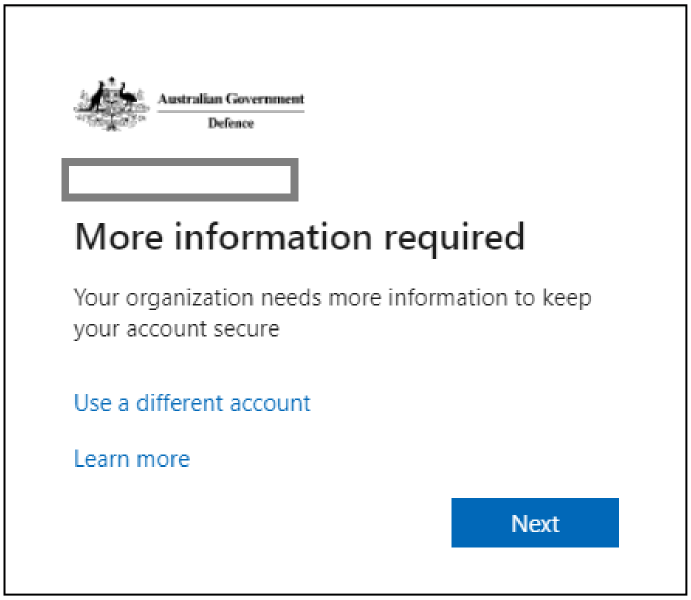
Image 4

Microsoft Authenticator Setup

Microsoft Authenticator is an application used for multi factor authentication (MFA) when logging into VERA. MFA is not required when logging into VERA through a DPE terminal or DREAMS session. MFA is required when logging into VERA outside of the DPE/DREAMS (e.g. through a BYOD (personal) device).

MFA set up can only be completed through a DPE terminal or DREAMS session. This includes your first time setting up MFA or if you require an MFA reset.

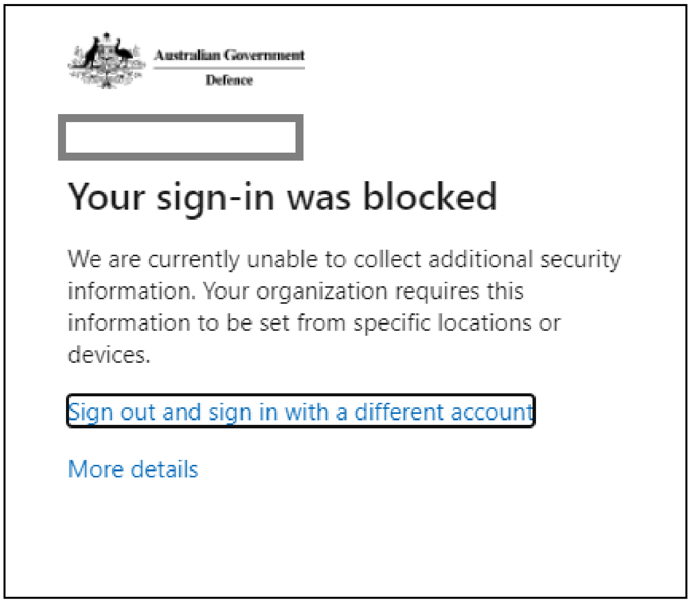
If MFA has not been set up prior to external VERA login, your sign-in will be blocked and you will be unable to access VERA outside of the DPE/DREAMS (**Image 1** and **Image 2).** If you are not able to set up your MFA via the DPE/DREAMS, you will not be able to access VERA externally.



[redacted]

More information required

Your organization needs more information to keep your account secure



[redacted]

Your sign-in was blocked

We are currently unable to collect additional security information. Your organization requires this information to be set from specific locations or devices.

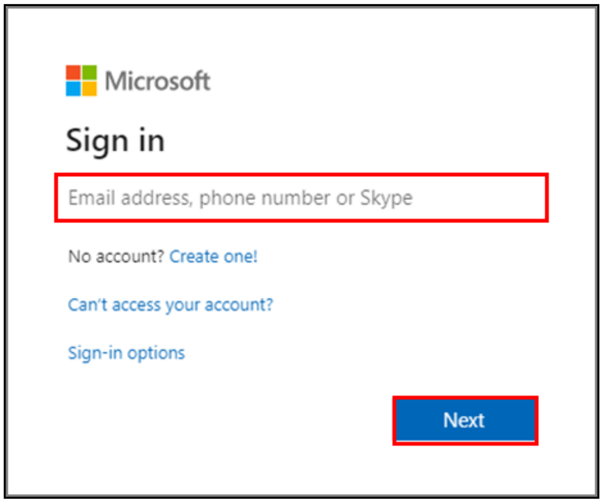
Image 1 and Image 2

How to setup Microsoft Authenticator for VERA

Follow the steps in this section to setup Microsoft Authenticator for VERA

1. Through a DPE Terminal or DREAMS session, **navigate** to https://mysignins.microsoft.com/security-info.

2. **Enter** your full Defence email address. **Click** *Next* (**Image 16**).



Microsoft

Sign in

Email address, phone number or Skype

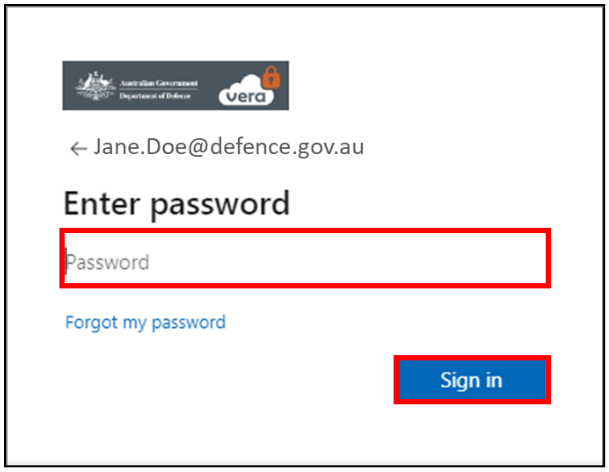
No account? Create one!

Can't access your account?

Sign-in options

Image 16

3. **Enter** your DPE password. **Click** *Sign in* (**Image 17**).



← Jane.Doe@defence.gov.au

Enter password

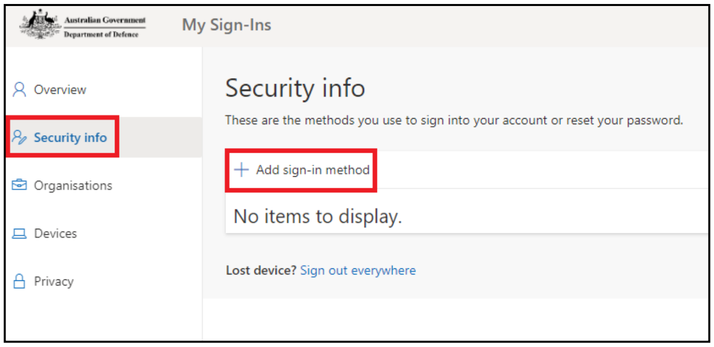
Password

Forgot my password

Image 17

4. Once within the My Sign-ins page, **select** the *Security info option.*

5. **Select** *Add sign-in method* (**Image 18**).



Security info

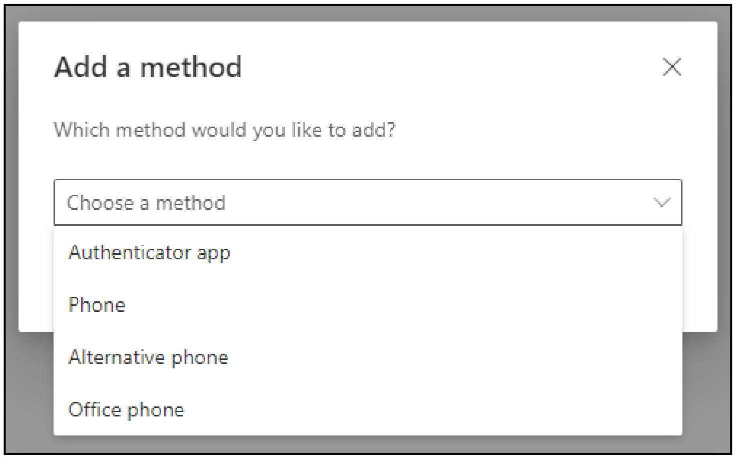
These are the methods you use to sign into your account or reset your password.

No items to display.

Lost device? Sign out everywhere

Image 18

6. In the *Add a method* window, **select** either *Authenticator app, Phone, Alternative phone* or *Office phone* and **select** *Add* **(Image 19)**.

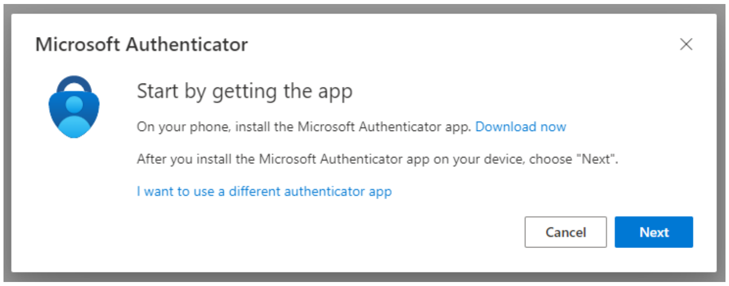

Add a method

Which method would you like to add?

Image 19

7. The following steps describe if you have selected the *Authenticator app* option:

   Download the Microsoft Authenticator app or if you have already installed the app on your device, **select** *Next* (**Image 20**).


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

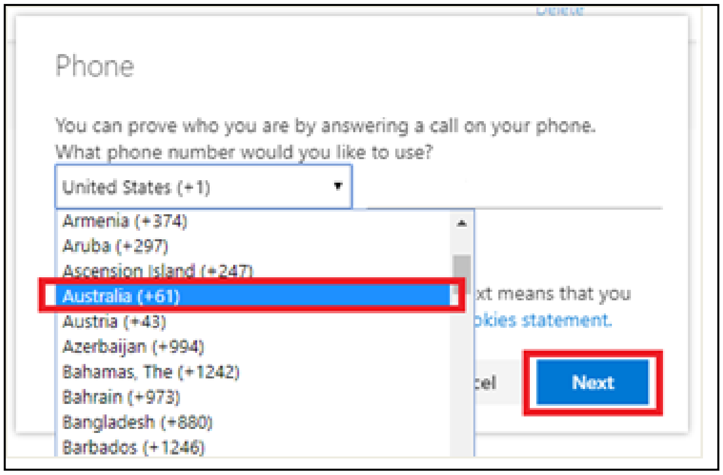
Image 20

Note: If you select either of the phone call options, you will receive a call from Microsoft (via a US phone number) to confirm your authentication. Follow the prompts within the phone call to confirm your MFA.

If you choose to enable your desk/office phone e.g. Skype phone number as an additional form of multi factor authentication, please ensure that your office number is correct when entered and on the VERA My Sign-ins page.

To activate your unique Skype phone number, please refer to [Skype for Business](#).

The phone number must be formatted with the correct country code in the dropdown menu (for example, for Australia, +61) and phone number entered correctly (**Image 21**). Incorrect phone numbers will lead to a failure of the phone number verification process (not receiving a verification call). **Click** *Next* (**Image 21**).



Phone

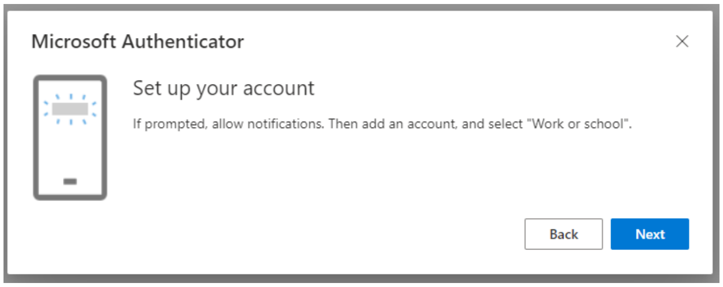
You can prove who you are by answering a call on your phone.
What phone number would you like to use?

United States (+1)

Image 21

8. The following steps describe if you have selected the *Authenticator app* option:

   Follow the prompt to set up your Microsoft Authenticator app, and then **select** *Next* (**Image 22**).



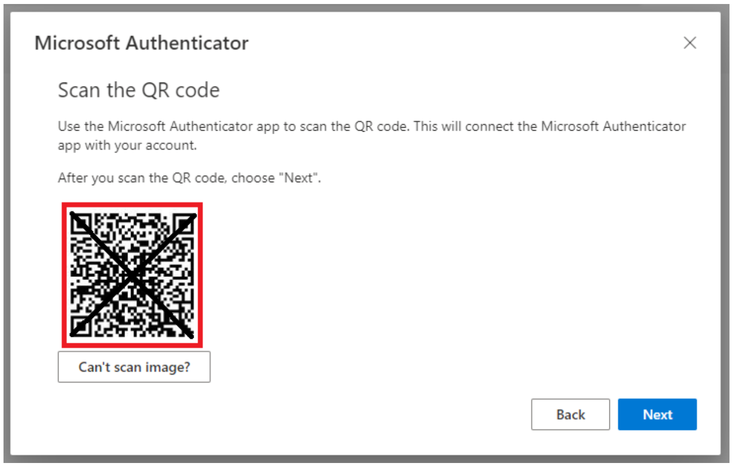
Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Image 22

9. Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app to your account. Once you have scanned the QR code, **select** *Next* (**Image 23**).



Microsoft Authenticator

Scan the QR code

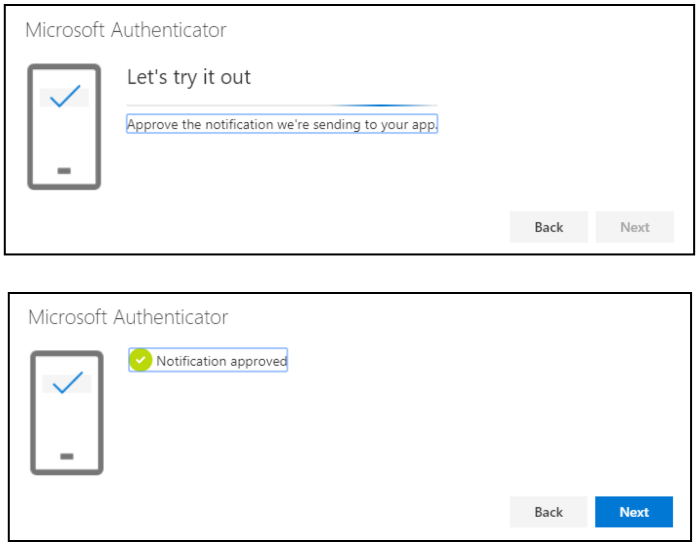
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

Image 23

10. You will be prompted on your mobile device and the webpage to *approve* the new account (**Image 24**). **Select** *Approve* when prompted in the mobile app.

    When the *Notification approved* message appears on the webpage, **select** *Next*.



Microsoft Authenticator

Let's try it out

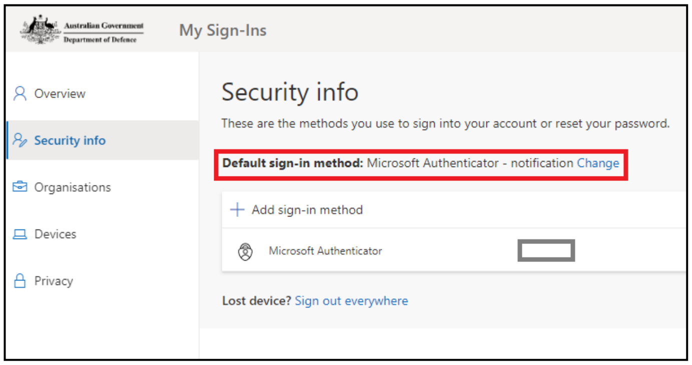
Approve the notification we're sending to your app.

Microsoft Authenticator

Notification approved

Image 24

11. You will now be able to see your default sign-in method on the *Security Info* page and login to VERA externally (**Image 25).**



Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

Lost device? Sign out everywhere

Image 25

How to setup Microsoft Authenticator for a new phone

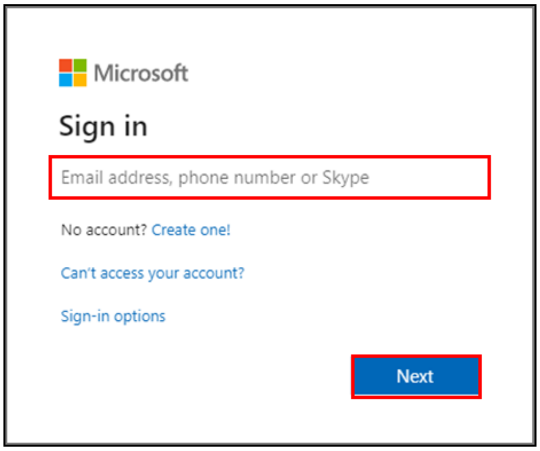
This document provides steps to take if you obtain a new phone and are using VERA currently on your old phone.

Note: Attempting to login to VERA prior to deleting your account from your old mobile will result in technical difficulties. Your Microsoft Authenticator will need to be set up within the **PROTECTED** network such as **DREAMS**, **DPE** or from a **Defence PROTECTED Laptop.**

Remove VERA account on your old phone

Follow the steps in this section to remove the VERA account from your old phone.

1. **Navigate to** https://account.activedirectory.windowsazure.com/proofup.aspx
2. **Enter** your Defence email address. Click ***Next*** (Image 1);



Microsoft

Sign in

Email address, phone number or Skype

No account? Create one!

Can't access your account?

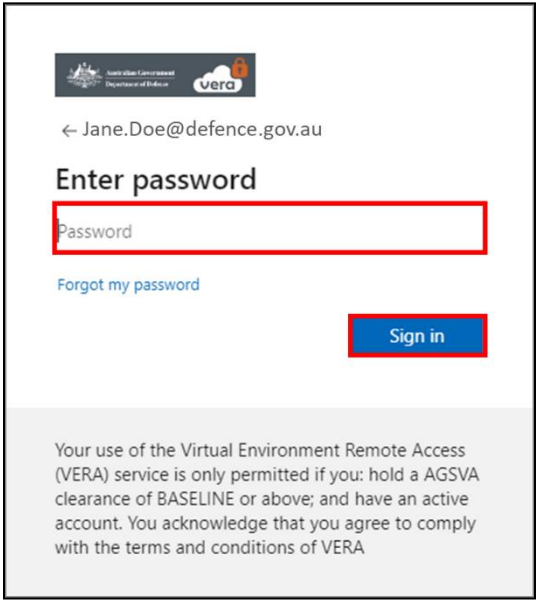
Sign-in options

Next

Image 1

3. **Enter** your Defence password. Click **Sign in** (**Image 2**);

   Note: You may need to enter the authenticator code from your old phone.



← Jane.Doe@defence.gov.au

Enter password

Password

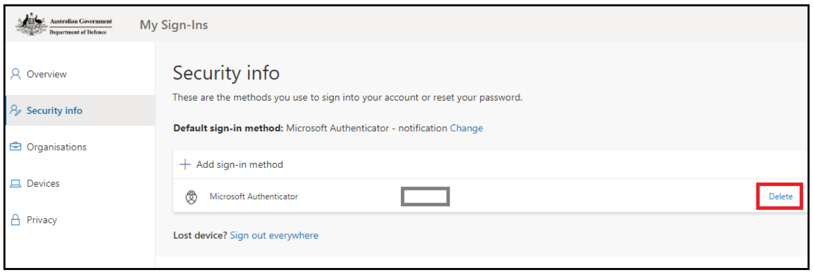
Forgot my password

Sign in

Your use of the Virtual Environment Remote Access (VERA) service is only permitted if you: hold a AGSVA clearance of BASELINE or above; and have an active account. You acknowledge that you agree to comply with the terms and conditions of VERA

Image 2

4. **Delete** the authenticator app associated with your old phone **(image 3).**



Australian Government
Department of Defence

My Sign-Ins

- Overview
- Security info
- Organisations
- Devices
- Privacy

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

+ Add sign-in method

Microsoft Authenticator Delete

Lost device? Sign out everywhere

Image 3

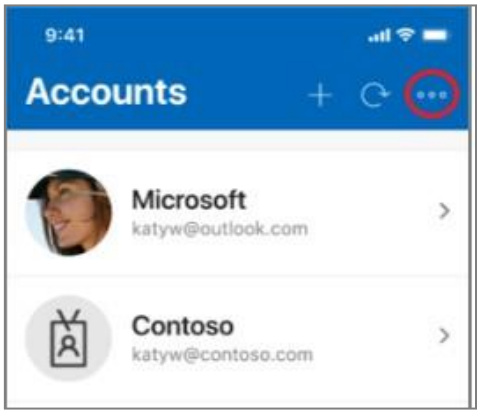
5. Open the **Microsoft Authenticator** app on your mobile device **(Image 4)**.

Image 4

6. If your old phone is an **Android device**, **click** the three dots up the top right and select ‘Edit Accounts’ **(Image 5)**.

7. Press the red X button next to your relevant Defence account.

8. If your old phone is an iOS device, tap on the account tile for the account you would like to remove from the app.



9:41

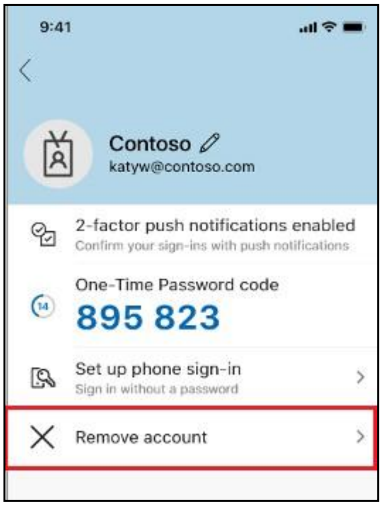
Accounts

Microsoft
katyw@outlook.com

Contoso
katyw@contoso.com

Image 5

9. **Tap** the ‘Remove Account’ option to remove the account from the app **(Image 6)**.



9:41

Contoso
katyw@contoso.com

2-factor push notifications enabled
Confirm your sign-ins with push notifications

One-Time Password code
895 823

Set up phone sign-in
Sign in without a password

Remove account

Image 6

Setup Microsoft Authenticator account on your new phone after removal from the old phone

To set up Microsoft Authenticator account on your new phone after removal from the old phone, follow the help guide how to setup Microsoft Authenticator on your mobile device from step 1 at section of ‘How to setup Microsoft Authenticator for VERA’.

Updating your Microsoft Authenticator options

This document provides steps to take if you would like to update your multi factor authentication (MFA) options.

Note: If you require a MFA device reset (e.g. lost your MFA device), you will need to recomplete the set-up process through a DPE terminal or a DREAMS session.

Add phone call Multi Factor Authentication option

Follow the steps in this section to phone call multi factor authentication option in Microsoft Authenticator.

Please note that phone call authentication is planned to be removed as a sign-in option. Please use your DCAC to complete multifactor sign-in.

1. **Login** to VERA.
2. **Select** the *App Launcher* button located at the top, in the left-side toolbar (**Image 1**).

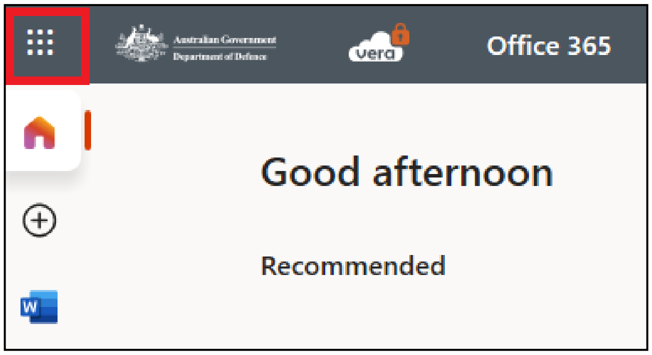


Image 1

3. **Select** the *All apps* button and then **select** the *Authentication* app icon (**Image 2**).

   Note: You can also directly access the *Authentication* app through the link: https://mysignins.microsoft.com/security-info.

   If you use this link to directly access the authentication process, you may need to sign-in once again. Before logging in, you may be prompted to enter an authentication code from your Microsoft Authenticator app on your mobile device.

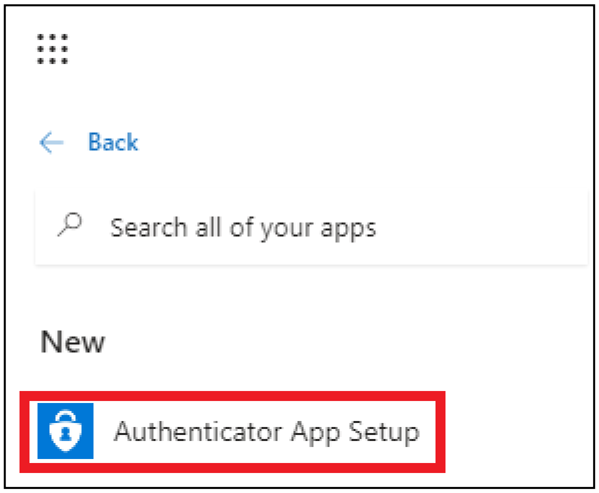
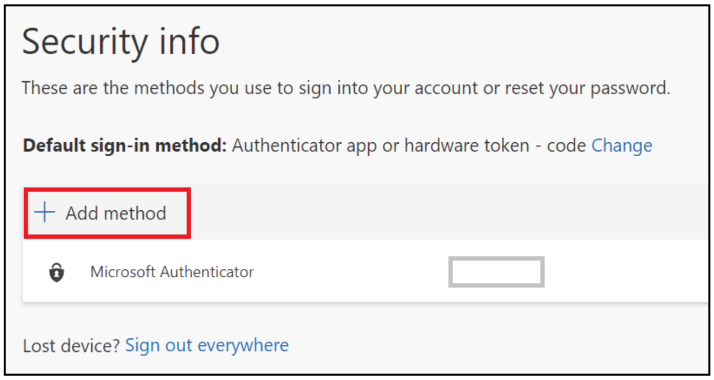


Image 2

4. Once within the My Sign-ins page, **select** *Add method* (**Image 3**).



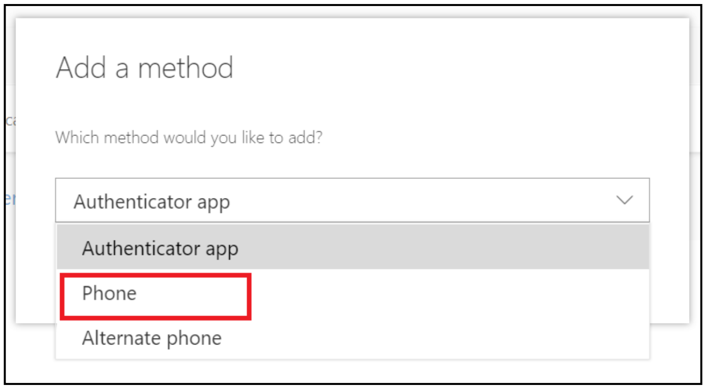
Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Authenticator app or hardware token - code Change

Image 3

5. In *Add a method*, **select** *Phone* (**Image 4**).



Add a method

Which method would you like to add?

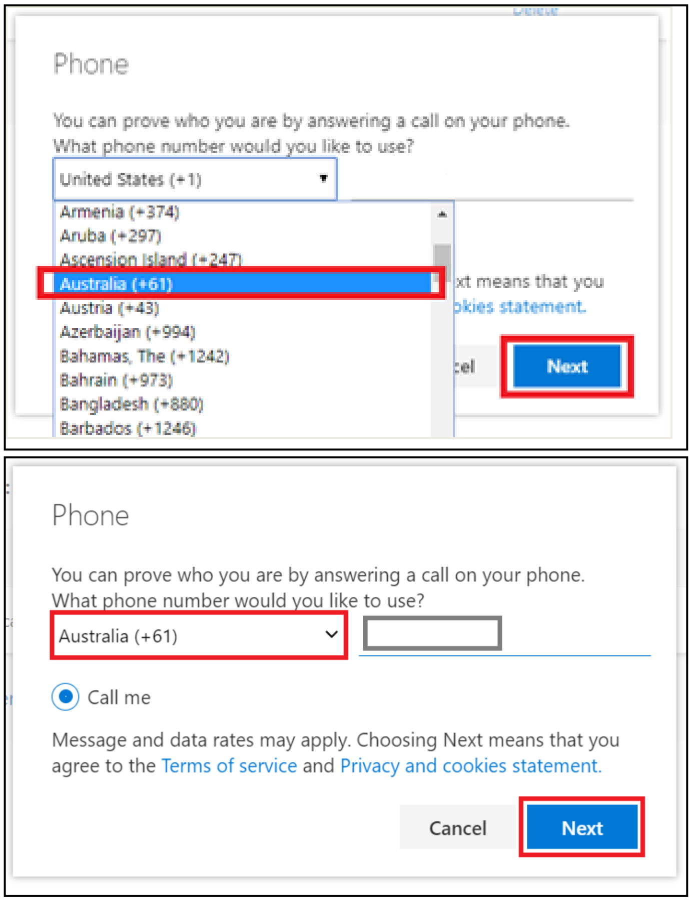
Image 4

6. In *Phone*, **set** the *country code* to *Australia (+61)* and **add** your preferred number for authentication.

   This phone number includes personal mobile phones and desk/office phones.

   Note: If you choose to enable your desk/office phone as an additional form of multi factor authentication, please ensure that your office number is correct when entered and, on the VERA, My Signins page.

   The phone number must be formatted with the correct country code in the dropdown menu (for example, for Australia, +61) and phone number entered correctly (**Image 5**). Incorrect phone numbers will lead to a failure of the phone number verification process (not receiving a verification call). **Click** *Next* (**Image 5**).



Phone

You can prove who you are by answering a call on your phone.
What phone number would you like to use?

Phone

You can prove who you are by answering a call on your phone.
What phone number would you like to use?

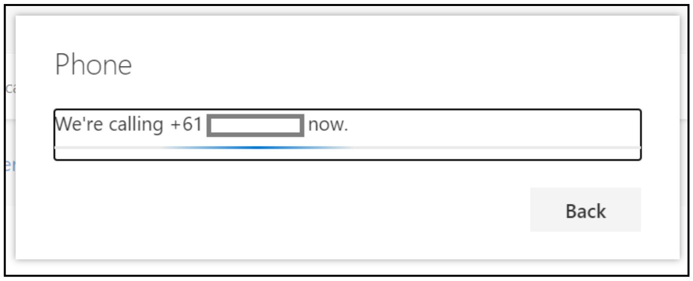
Australia (+61)

● Call me

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

Image 5

7. Microsoft will then call the designated number from a US phone number, to confirm and verify the MFA option (**Image 6**).



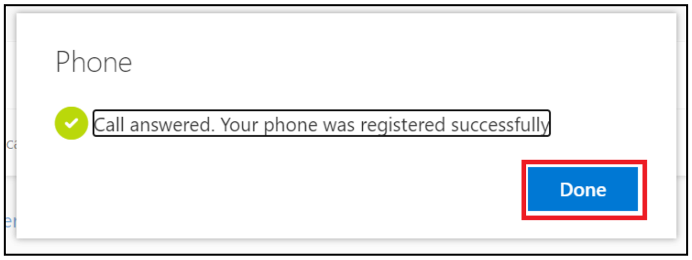
Phone

We're calling +61 now.

Image 6

8. Answer the phone call and follow the prompts stated over the call to confirm and verify the MFA option (by pressing the '#' key on your keypad)

   Once you successfully confirm the authentication option, you will see (**Image 7**). **Select** *Done.*

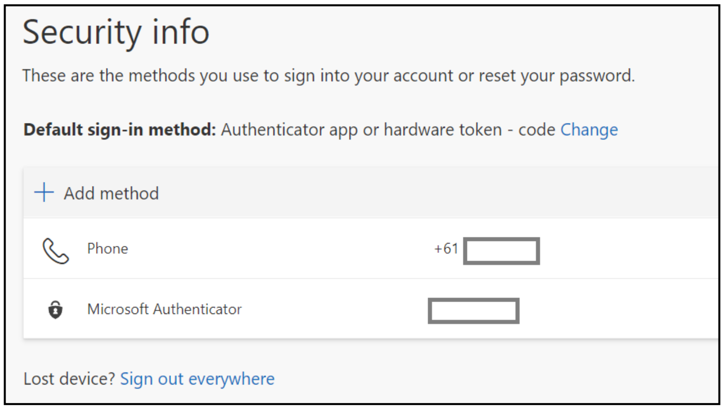


Phone

✓ Call answered. Your phone was registered successfully

Image 7

9. You will be returned to the *Security info* page, and see the addition of the MFA call option (**Image 8**).



Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Authenticator app or hardware token - code Change

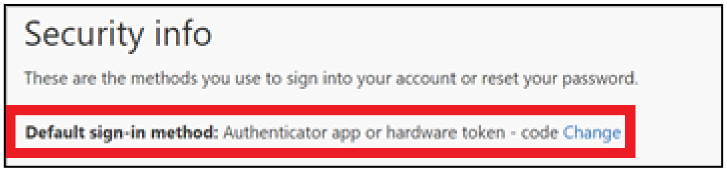
Phone	+61 [redacted]
Microsoft Authenticator	[redacted]

Lost device? Sign out everywhere

Image 8

10. To then set the phone call option as your *Default sign-in method*, **select** *Change* (**Image 9**).

    In *Change default method***, select** the phone call option and then *Confirm* (**Image 10**).

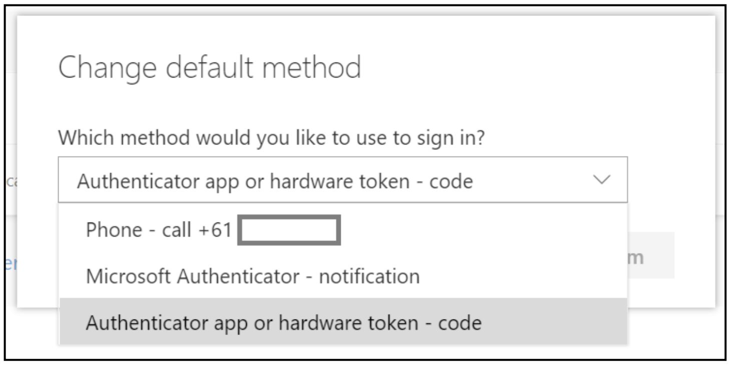


Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Authenticator app or hardware token - code Change

Image 9



Change default method

Which method would you like to use to sign in?

Authenticator app or hardware token - code

- Phone - call +61 [redacted]
- Microsoft Authenticator - notification
- Authenticator app or hardware token - code

Image 10

Switch between Multi Factor Authentication options in Microsoft Authenticator

Follow the steps in this section to switch between multi factor authentication options in Microsoft Authenticator.

1. Through a DPE terminal or DREAMS session, **login** to VERA.

2. **Select** the *App Launcher* button located at the top, in the left-side toolbar (**Image 11**).

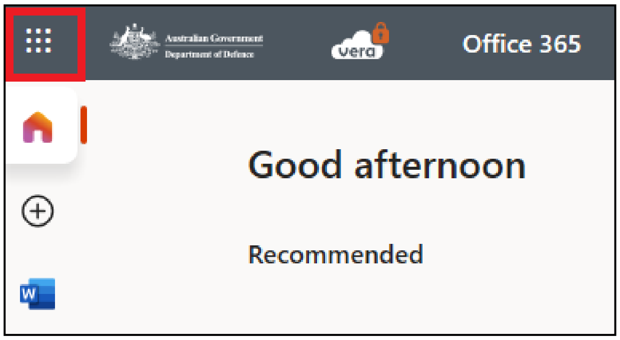


Image 11

3. **Select** the *All apps* button and then **select** the *Authentication* app icon (**Image 12**).

   Note: You can also directly access the *Authentication* app through the link: https://mysignins.microsoft.com/security-info.

   If you use this link to directly access the authentication process, you may need to sign-in once again. Before logging in, you may be prompted to enter an authentication code from your Microsoft Authenticator app on your mobile device.

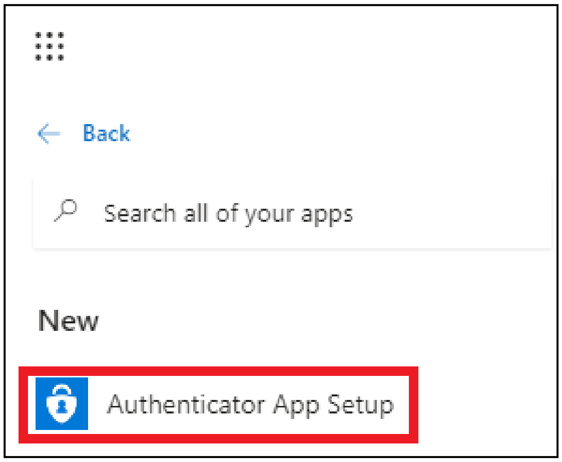
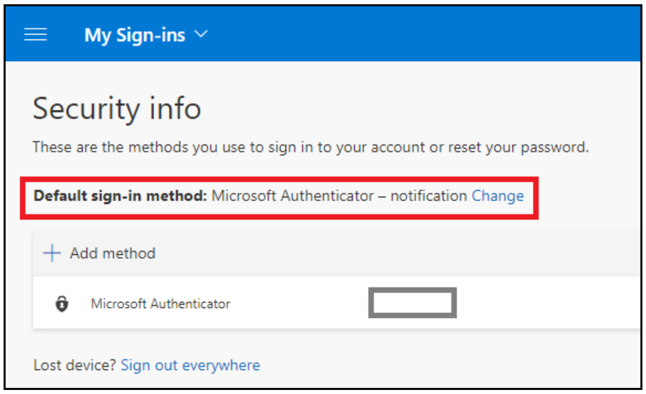


Image 12

4. Once within the My Sign-ins page, **select** *Change* found next to *Default sign-in method* (**Image 13**).



These are the methods you use to sign in to your account or reset your password.

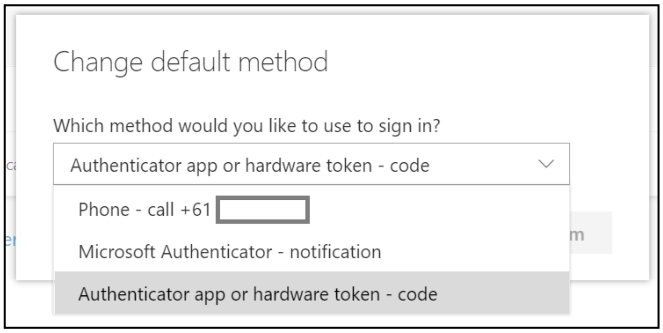
Default sign-in method: Microsoft Authenticator – notification Change

Lost device? Sign out everywhere

Image 13

5. In *Change default method*, select your preferred MFA options, and then *Confirm* (**Image 14**).

   Note: MFA methods available for selection require the method to be set up prior to changing the default method.



Change default method

Which method would you like to use to sign in?

Authenticator app or hardware token - code

Phone - call +61 [redacted]
Microsoft Authenticator - notification
Authenticator app or hardware token - code

Image 14

VERA and Records Management

All Defence personnel are responsible for creating, capturing, controlling and disposing of Defence records in accordance with the Defence Records Management Policy. VERA does not integrate with Objective meaning users are responsible for ensuring Defence records are exported and uploaded to Objective to meet the requirements of the Defence Records Management Policy.