Australian Government
Department of Defence
Chief Information Officer Group

VERA Security and Authentication

Help Guide

July 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. This is the most preferred authentication method by the Department of Defence.
- Your Microsoft Authenticator app is optional. It can only 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 set up the Microsoft Authenticator app on the same PROTECTED iOS devices 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.

Recommended: Passwordless	Password and …
	
Using your DCAC for Authentication	Microsoft Authenticator
This is the most preferred authentication method and your DCAC Smartcard is enabled for MFA by default.	This works well with BYOD or if you do not work regularly in the Defence zone 3 or higher facilities.

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.

Microsoft Authenticator app is **optional** when logging into VERA outside of the DPE/DREAMS (e.g. through a BYOD (personal) device), as your DCAC card is an approved authentication method that has been automatically setup for you to access VERA.

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 use your DCAC card as an alternative authentication method.

How to install Microsoft Authenticator on 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)

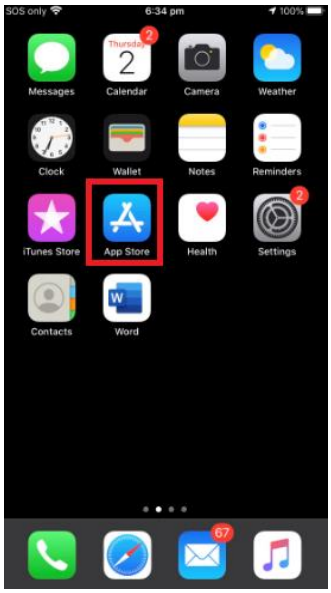

Image 1

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

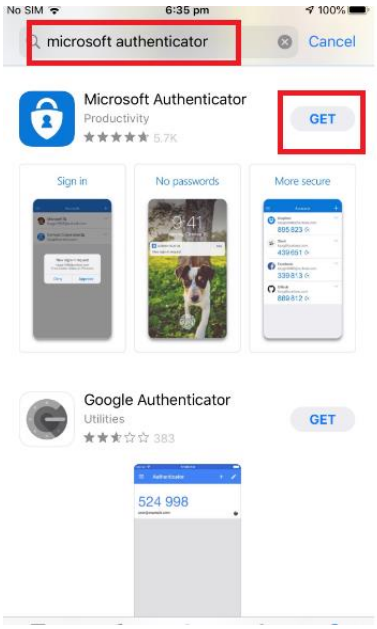

Image 2

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).

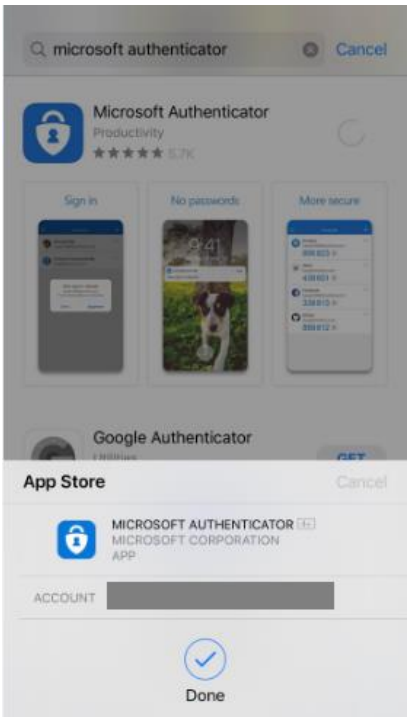

Image 3

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

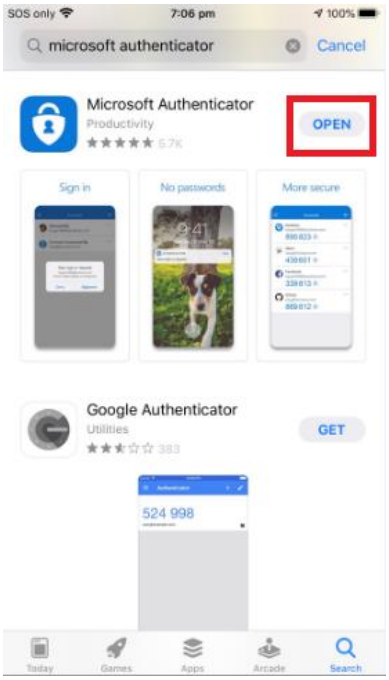

Image 4

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

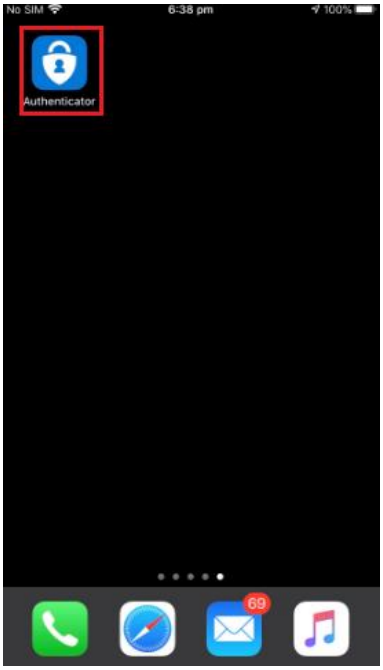

Image 5

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 6**);

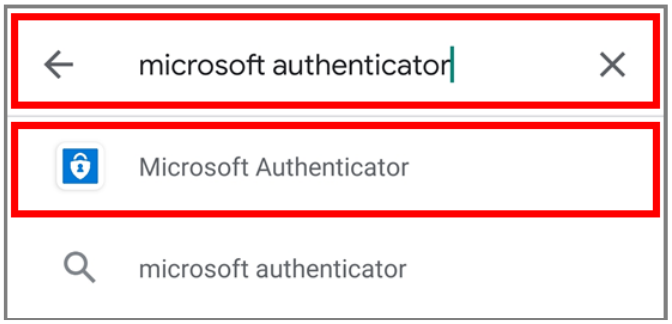

Image 6

2. **Click** Install (**Image** 7);

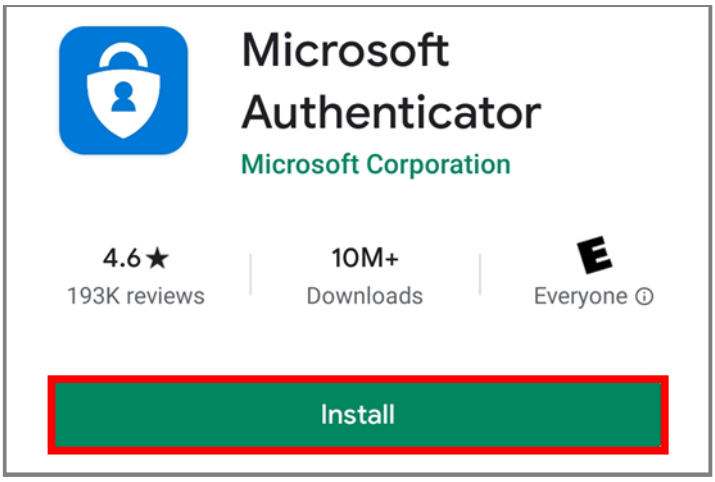

Image 7

3. Once installed, **click** Open to launch the Microsoft Authenticator app (**Image 8**);

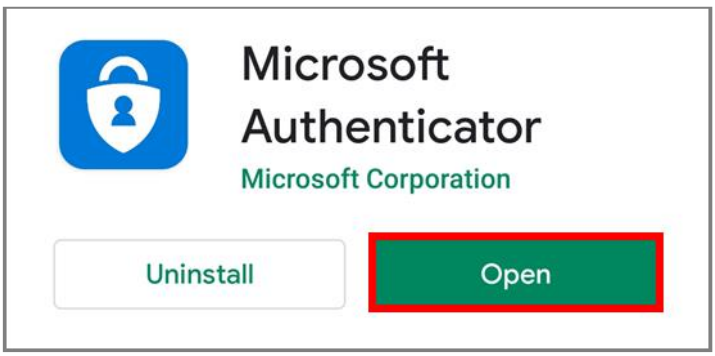

Image 8

4. You can locate the app on main screen (Image 9)

Image 9

Microsoft Authenticator Setup

How to setup Microsoft Authenticator for VERA

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.

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 10**).

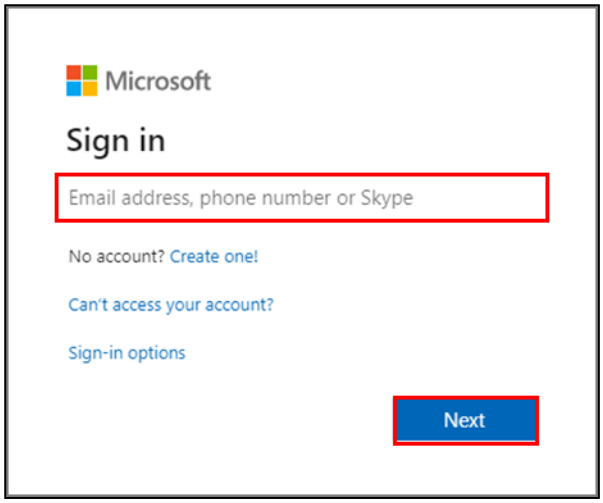

Image 10

3. **Enter** your DPE password. **Click** *Sign in* (**Image 11**).

Image 11

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

5. **Select** *Add sign-in method* (**Image 12**)**.**

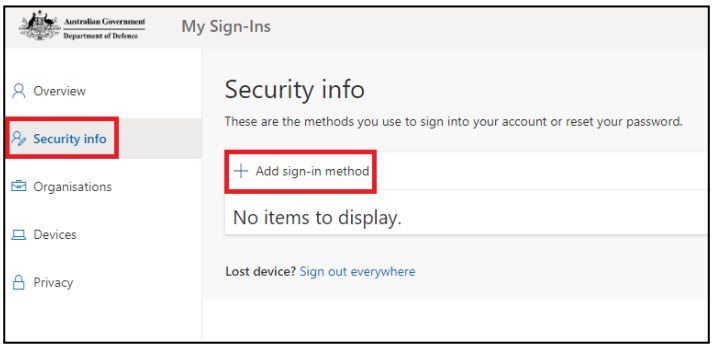

Image 12

6. In the *Add a method* window, **select** *Microsoft Authenticator* **(Image 13)**.

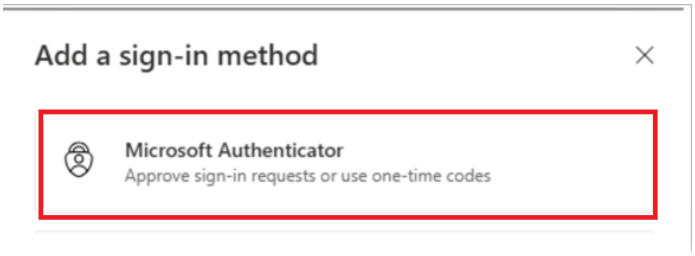

Image 13

7. **Download** the Microsoft Authenticator app or if you have already installed the app on your device, **select** *Next* (**Image 14**).

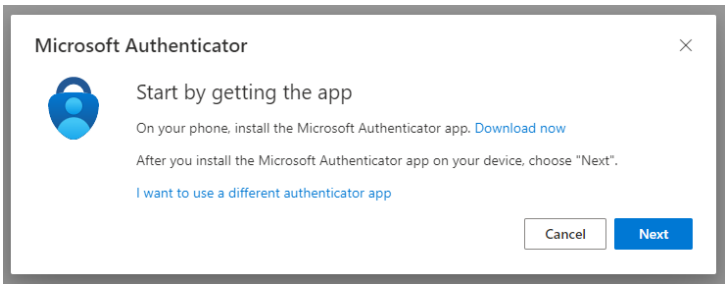

Image 14

8. Follow the prompt to set up your Microsoft Authenticator app, and then **select** *Next* (**Image 15**).

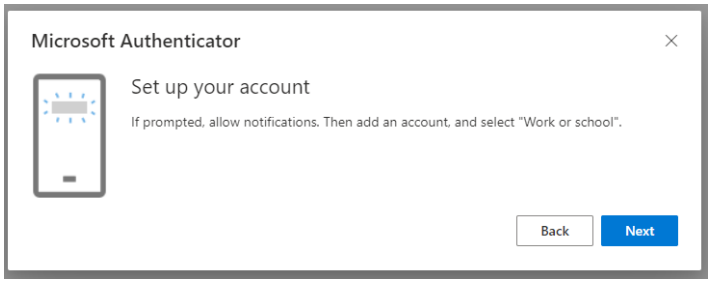

Image 15

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 16**).

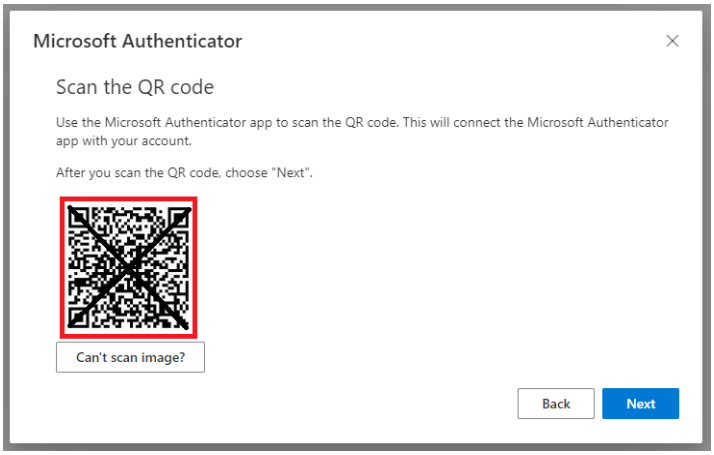

Image 16

10. You will be prompted on your mobile device and the webpage to *approve* the new account (**Image 17**). **Select** *Approve* when prompted in the mobile app.

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

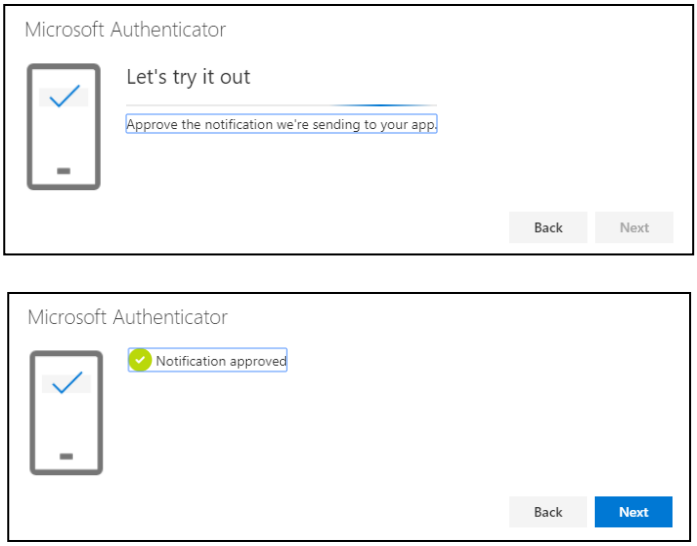

Image 17

11. You will now be able to see your default sign-in method on the *Security Info* page and login to VERA externally (**Image 18).**

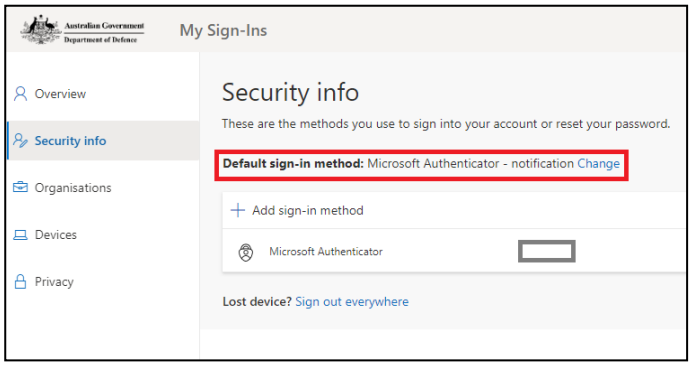

Image 18

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 19);

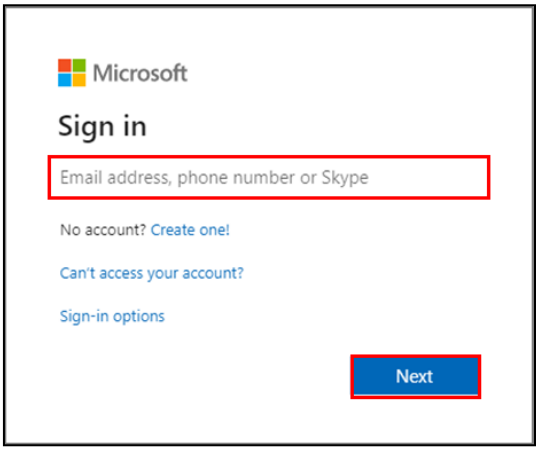

Image 19

3. **Enter** your Defence password. Click **Sign in** (**Image 20**);

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

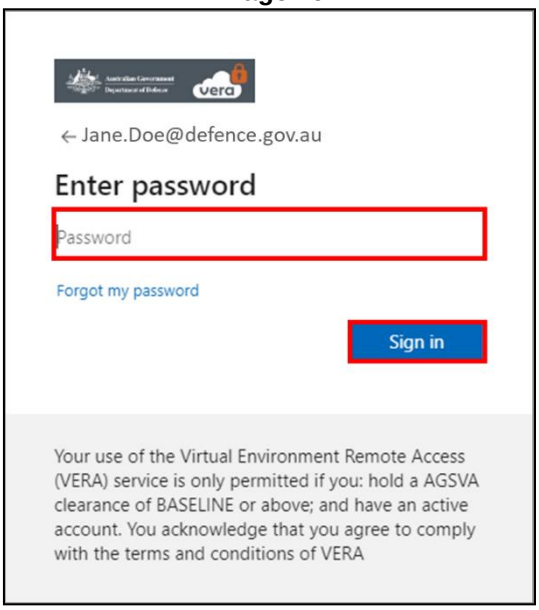

Image 20

4. **Delete** the authenticator app associated with your old phone **(image 21).**

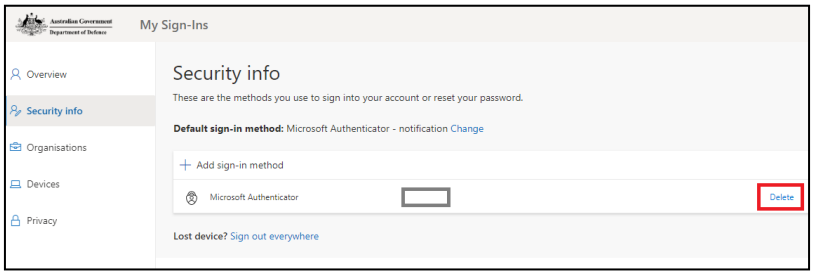

Image 21

5. Open the **Microsoft Authenticator** app on your mobile device **(Image 22)**.

Image 22

6. If your old phone is an **Android device**, select the Defence account and find the 'Setting' option **(Image 23)**.

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

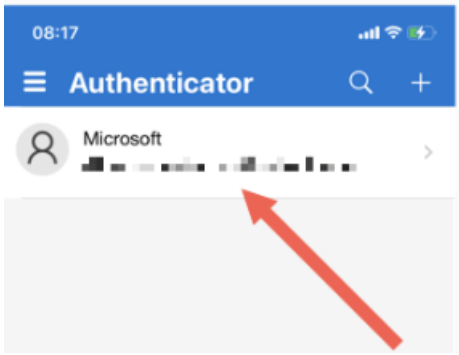

Image 23

8. **Tap** the 'Remove Account' option to remove the account from the app **(Image 24)**.

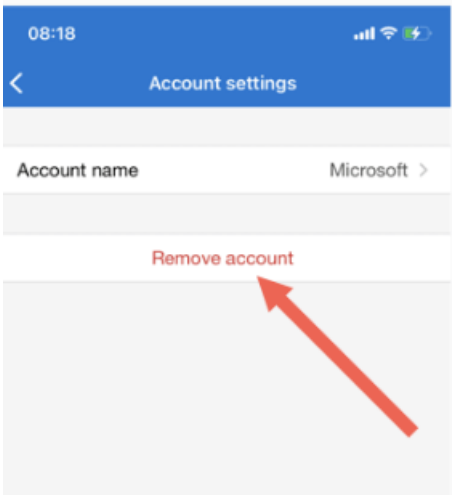

Image 24

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'.

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.