Setting up One Time Password on a Mobile Phone

This guide is relevant if you have decided to set up Multi-Factor Authentication on your smart mobile device using a One Time Password.

One Time Passcode description and use.

- One Time Passcode is a random generation of 6 digits every 30 seconds, this is an alternative to using Push Notifications for Multi Factor Authentication.
- One Time Passcode can be setup to generate in the Microsoft Authenticator app following the below steps or Yubico software (this requires a hardware token, see Setup of Yubikey).
- Usage of One Time Passcode is often personal preference only, the most suitable use case is in areas of limited mobile network or Wi-Fi service where Push Notifications will timeout before approval.
- One Time Passcodes **do not** require a network connection to generate every 30 seconds once setup.
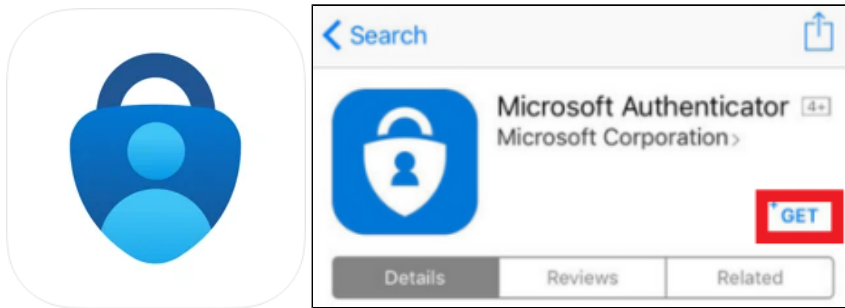
How to Install Microsoft Authenticator on a Smart Mobile Device

The Microsoft Authenticator is free software - only download the app from the official app store (use the links below) and make sure you install the app which is distributed by Microsoft Corporation. There are a number of fake apps which cost money or worst attempt to compromise your security.

iPhones

Navigate to the Apple App Store (App Store), and install Microsoft Authenticator:

https://itunes.apple.com/au/app/microsoft-authenticator/id983156458

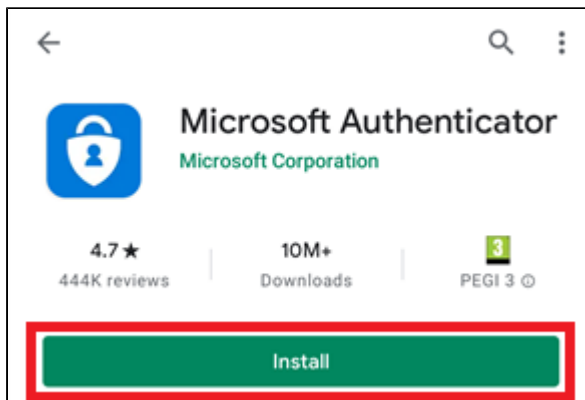**Android**

Navigate to the Google Play App Store (Play Store), and install Microsoft Authenticator:
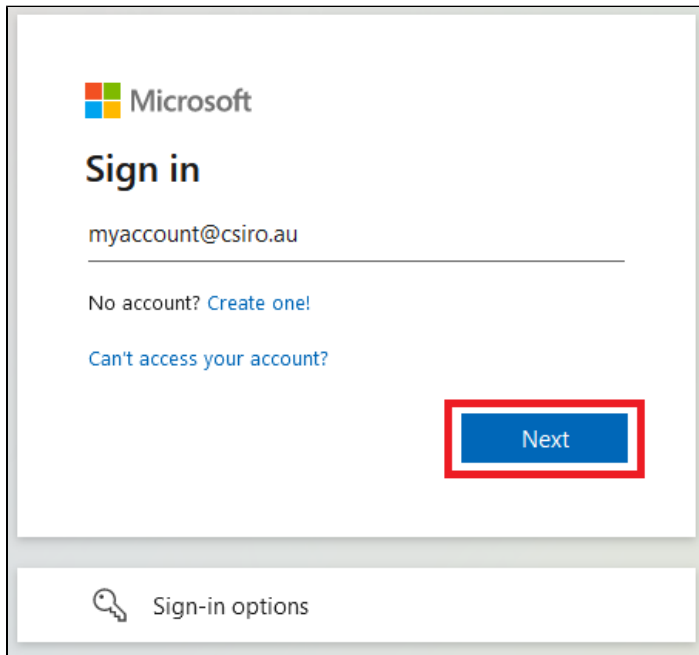
https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_AU

blocked URL

How to Configure your Smart Mobile Device for One Time Password Authentication

1. After installing Microsoft Authenticator, using a computer open a web browser and navigate to https://mfa.csiro.au
Once the page loads, enter your CSIRO login in the format of ident@csiro.au and click **Next**.

2. Click **Next** to start registration process.
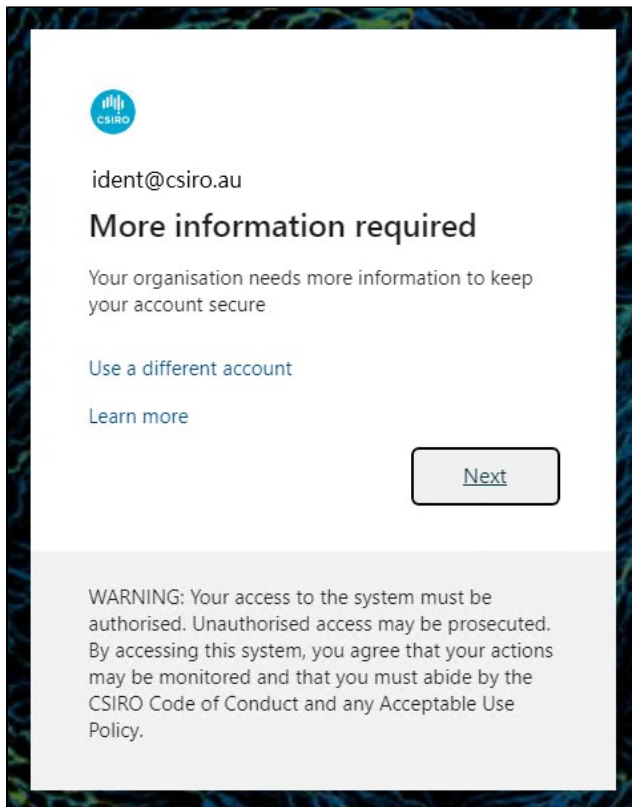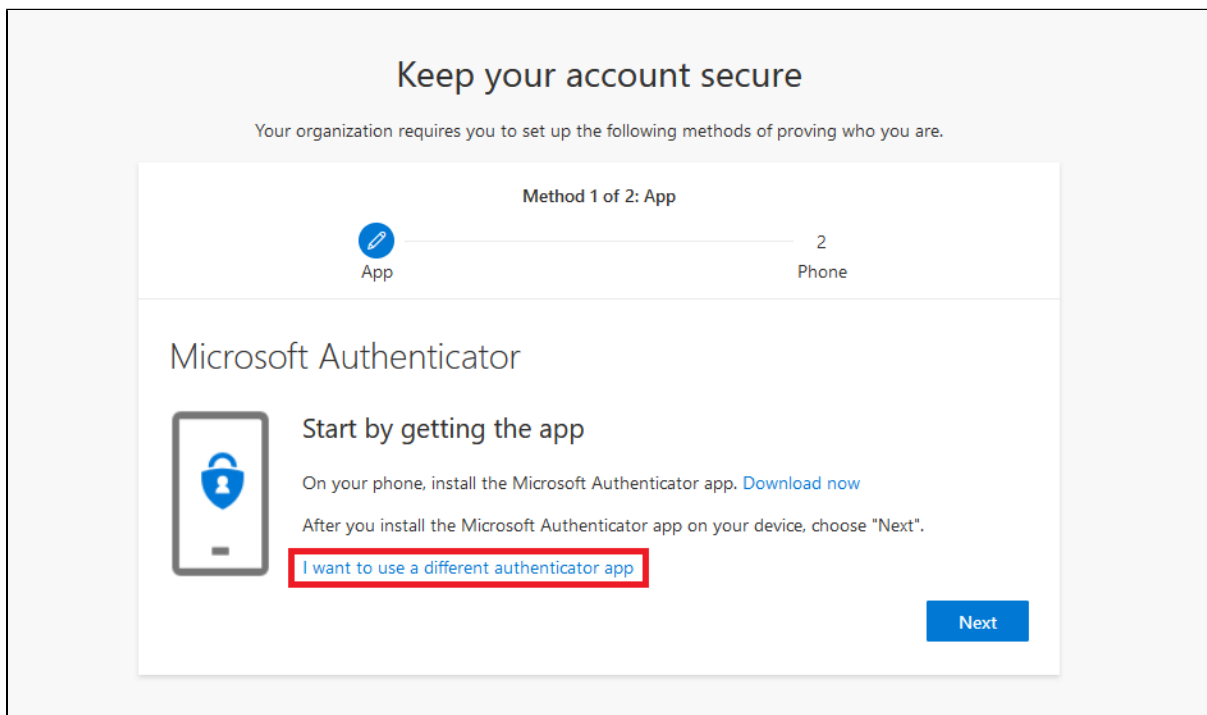
3. If you are setting up for the first time select **I want to use a different authenticator app** to configure the Authenticator app with OTP.

4. Open the Microsoft Authenticator app installed earlier on your mobile, If you don't already have an account set up in the Authenticator app, you'll see a large blue button **Add account**, otherwise select the plus icon, select **Add account**, select **Work or school account**, then **Scan a QR code**. Back on the website, Click **Next** when ready to scan the QR code.

5. Scan the QR code that will now be displayed in your browser window using the Microsoft Authenticator app, you should see something like the example below, then click **Next** when you see your account in the app.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.
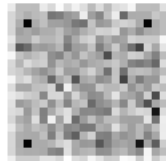
Method 1 of 2: App

● — 2
App   Phone

Authenticator app

Scan the QR code

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

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

[QR code image]

Can't scan image?

Back   Next

I want to set up a different method   Skip setup

6. After the QR code has been scanned you should see a One Time Password (OTP) in your Authenticator app, type this into the prompt as below and click **Next**.

7. One Time Password (OTP) using the Authenticator app has now been configured. **Note:** If you have not yet setup Self-Service Password Reset (SSPR) you will now be taken to compete the registration - Click **Next**, then click **I want to set up up a different method**. The pop-up 'Choose a different method' will appear, follow from step 3 on **Register for Self-Service Password Reset** to continue
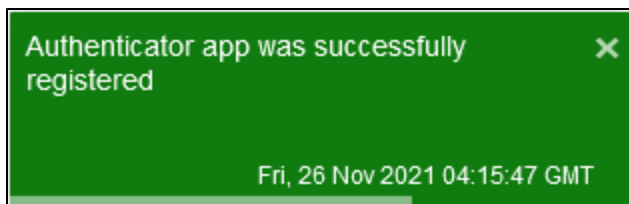
8. You will now be taken to your account Security info. Check the devices configured here, you should only have one of each **Microsoft Authenticator** and **Security questions** in the list, as below.
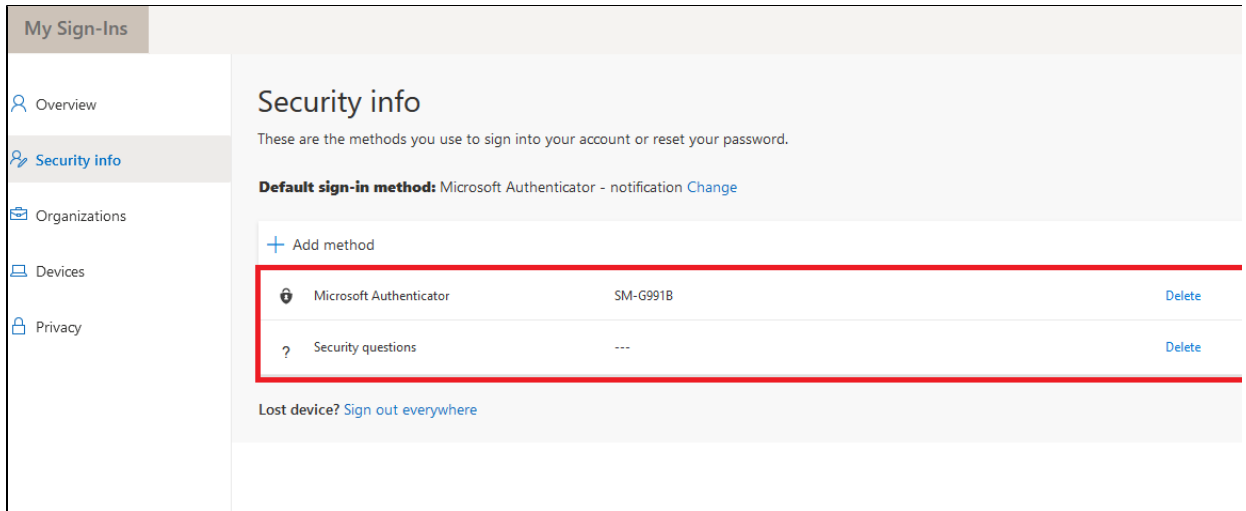
9. If you have more than one Microsoft Authenticator listed, usually from a previous device setup it is best practice to remove this. Select **Delete** on the device closest to the bottom of the list, refer to Removing Old MFA Verification Methods for more information on this.
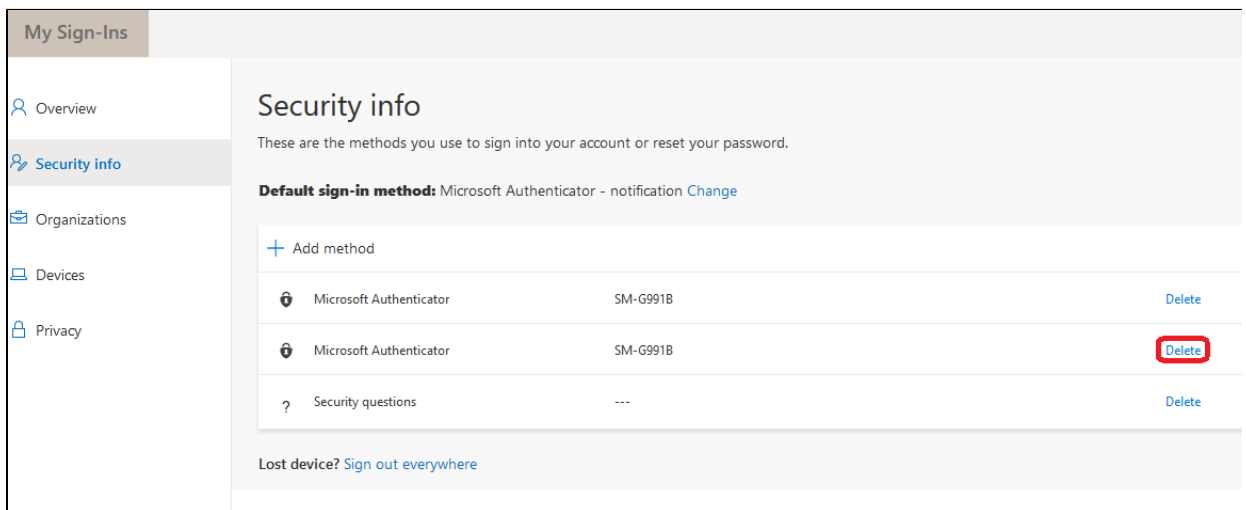
10. Close your browser window.

You are now set up to receive a One Time Password from your chosen mobile device. This means that every time Multi-Factor Authentication is required, you will need to open Microsoft Authenticator on your mobile device to get a One Time Password in order to authenticate.

What Does MFA Look Like?

Frequently Asked Questions

Changing Methods