

Setting up Push Notifications on a Mobile Phone

This guide is relevant if you have decided to set up Multi-Factor Authentication on your [smart mobile device using push notifications](#).

✔ If you setup Push Notifications you can also use One-Time Password (OTP) option on the Microsoft Authenticator app when you have **no internet connection**.

You do not need to setup OTP to use this method if you have setup push notifications – tap your CSIRO ident on the Microsoft Authenticator app to see the six-digit 'One-time password code'.

Visit [What does it look like](#) for instructions.

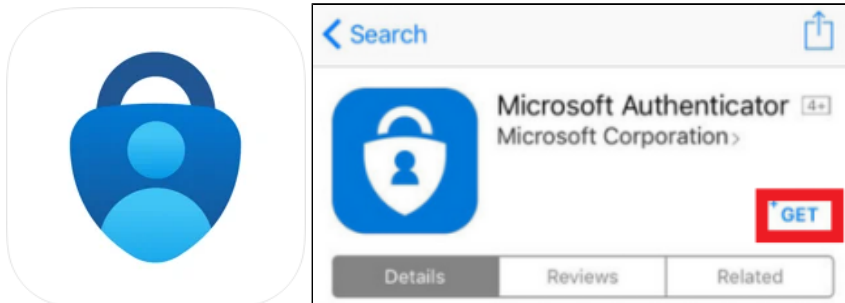
How to Install Microsoft Authenticator on a Smart Mobile Device

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.

iPhone

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

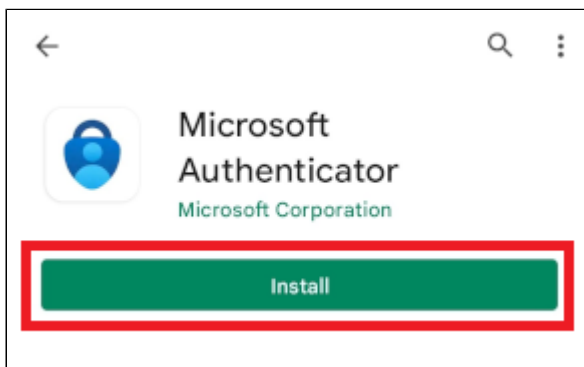
<https://itunes.apple.com/au/app/microsoft-authenticator/id983156458>



Android

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

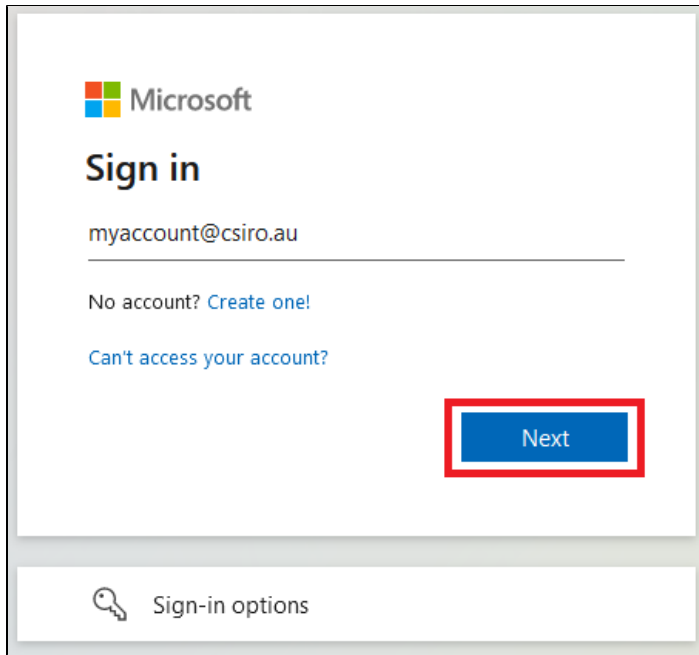
https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_AU



blocked URL

How to Register for Multi-Factor Authentication (MFA) with Push Notifications

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**.



Microsoft


Sign in

myaccount@csiro.au

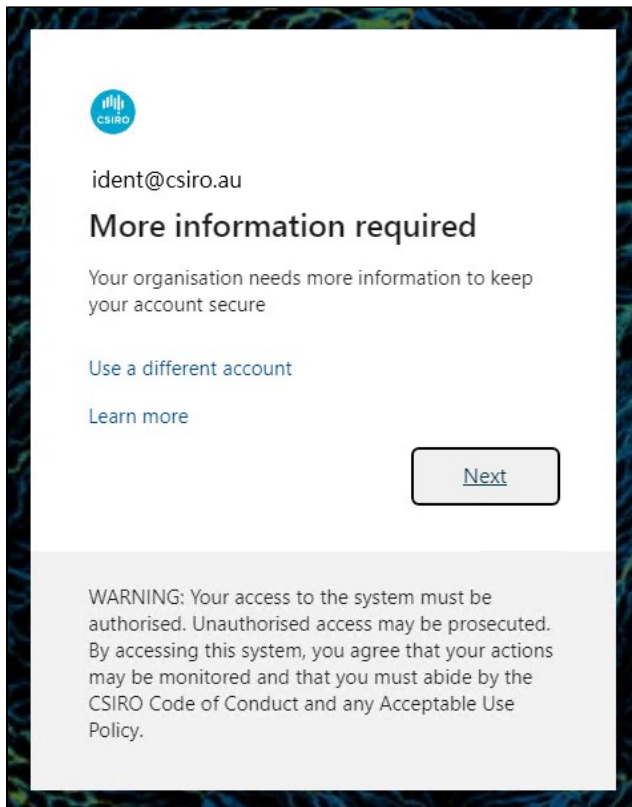
No account? [Create one!](#)

[Can't access your account?](#)

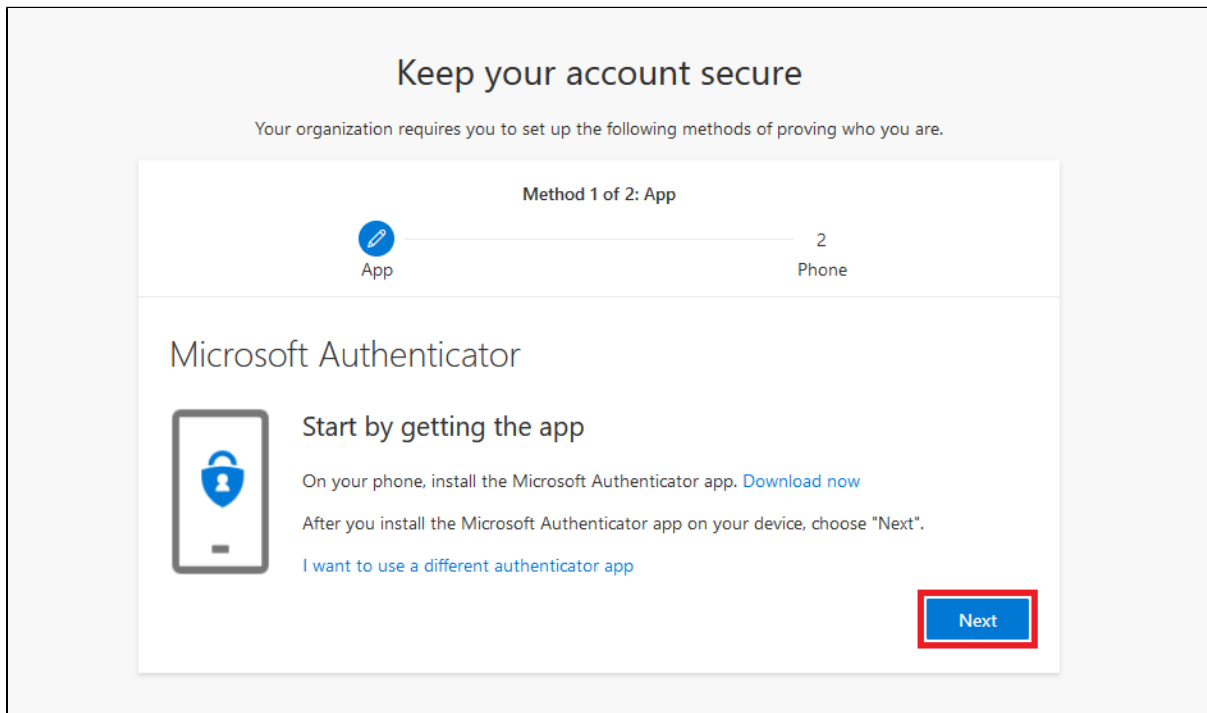
Next

 Sign-in options

2. Click **Next** to start registration process.



3. On the next page you will be given the option to setup your Microsoft Authenticator app, click **Next** to continue.



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**, and then select **Work or school account**. Click **Next** when ready to scan the QR code.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator



Set up your account

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

Back

Next

5. Scan the QR code displayed in your browser window using the Microsoft Authenticator app, as shown in the below example.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App



App

2

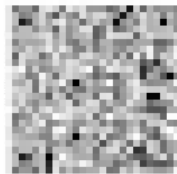
Phone

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".



Can't scan image?

Back

Next

6. Approve the notification by entering the highlighted number into the MS Authenticator application and clicking **Yes** that appears on the phone and click **Next** once approval is detected (Step 7).



Please note: the number highlighted below will be unique to you and will be different on any subsequent registrations.

Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Method 1 of 2: App

App Questions

Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

34

7. MFA with Push Notifications is now setup. **Note:** If you have not yet setup [Self-Service Password Reset \(SSPR\)](#) you will now be taken to complete the registration - Click **Next**, then click **I want to set 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


Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

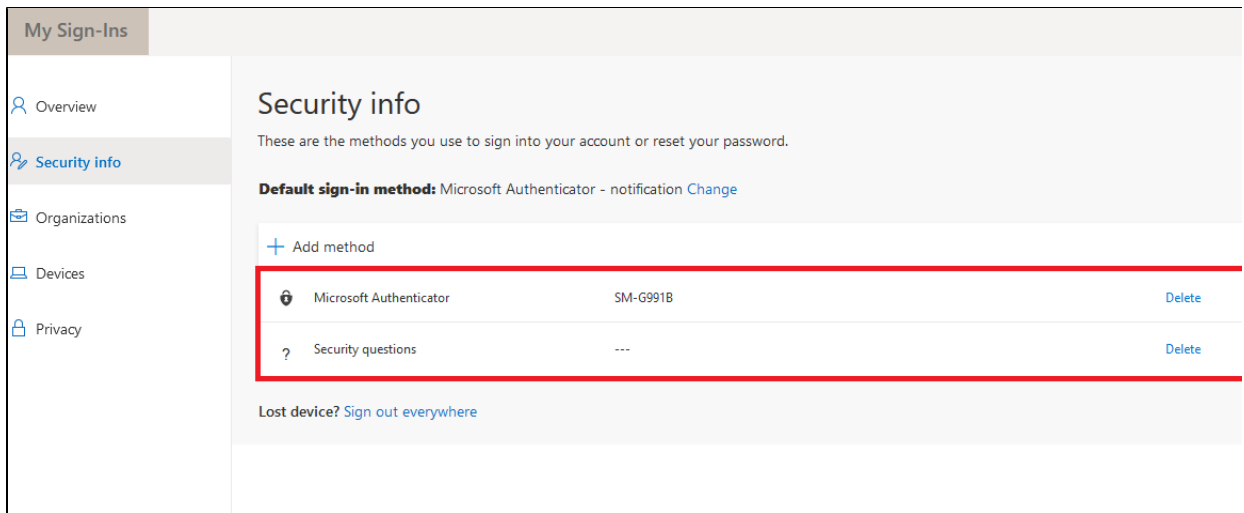
Method 1 of 2: App

App 2
Phone

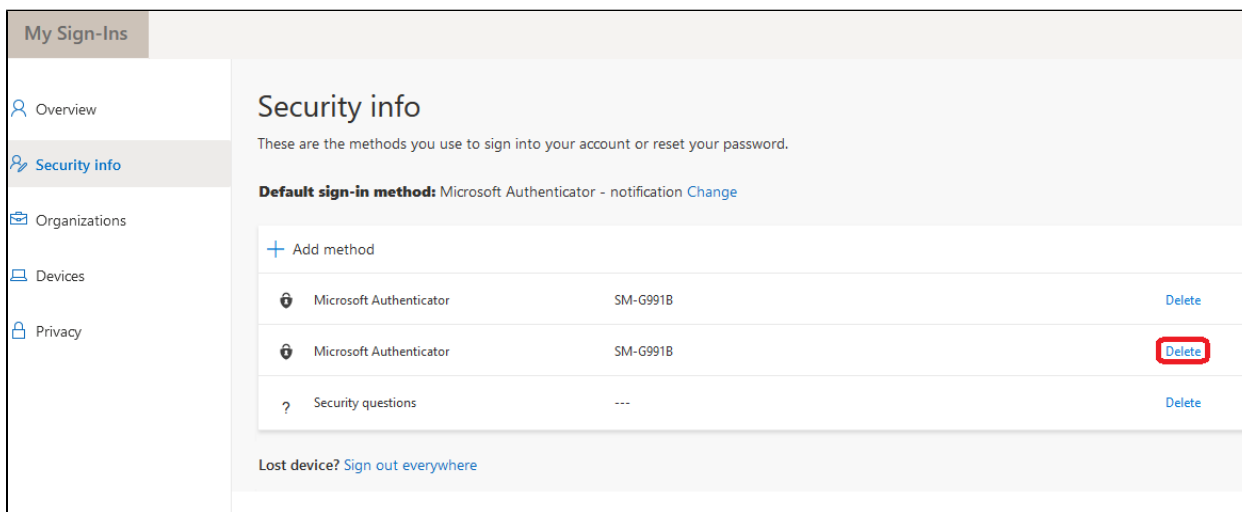
Microsoft Authenticator

 ✔ Notification approved

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 per below.



9. If you have more than one Microsoft Authenticator listed, usually from a previous device setup it is best practice to remove this. First **refresh** the page in your browser, then once the list has loaded again, 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 push notifications through your mobile phone. This means that every time Multi-Factor Authentication is required, you will need to select 'approve' or 'deny' on your mobile phone to authenticate.



**What Does MFA
Look Like?**



**Frequently Asked
Questions**



Changing Methods