

# Microsoft Authenticator App

## User Setup Guide



# INTRODUCTION

## What is Microsoft Authenticator?

Microsoft Authenticator is a mobile device app that helps secure your online identity when accessing cloud services, such as Microsoft Office 365.

It does this by requiring you to prove your identity based on something you physically have (i.e. your phone) in addition to your username and password. This is referred to as Multi-Factor Authentication (MFA).

## Why do I need MFA?

Cyber criminals employ a range of methods for stealing online identities. Phishing scams are commonly used to steal usernames and passwords from unsuspecting users by having them log into a fake system that looks like Office 365 or other online service.

Once your credentials are stolen, cyber criminals can use them to access your online services, steal confidential information and email all your contacts to repeat the process.

With MFA enabled on your account, it is not possible for a cyber criminal to sign in with your username and password alone. They also require your mobile phone, which only you have.

## What is contained in these instructions?

The steps provided in this document explain how to set up the Microsoft Authenticator app on your smart phone. The screens shown are taken from an Apple iPhone, but the steps will be similar for Google Android and Windows Mobile devices.

## Disclaimer

These instructions are designed for to provide helpful information for Microsoft Multi-Factor Authentication and Authenticator app users. While organisations and their IT departments are free to distribute this document as-is, Magnitude 8 does not guarantee the accuracy of the contents at the time of use and will not be held responsible for damages caused by following these instructions. A customisable Microsoft Word version of this document can be requested via an enquiry on the Magnitude 8 web site at <https://www.magnitude8.com.au/contact>.

# SETUP INSTRUCTIONS

## Installing the Microsoft Authenticator App

The Microsoft Authenticator app is the easiest and preferred method for authenticating with Multi-Factor Authentication. You can install the app from the app store for your Apple iOS, Google Android or Windows Mobile device.

If you are viewing this document on your smart phone you can tap the links below to open in the app store.



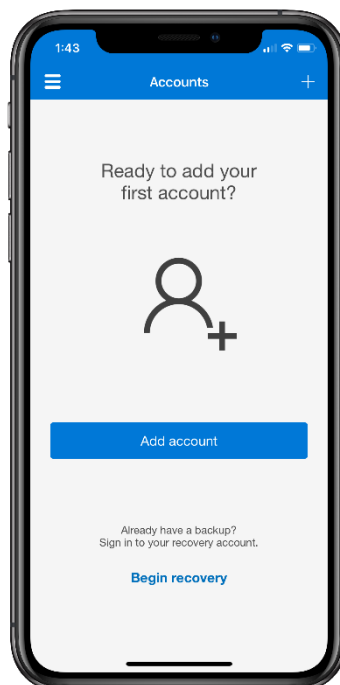
[Microsoft Authenticator app for Apple iOS Devices](#)

[Microsoft Authenticator app for Google Android Devices](#)

[Microsoft Authenticator app for Windows Mobile Devices](#)

*Note: If you don't have a supported device you won't be able to use the app to authenticate. Instead, you will need to receive a text message or call to your phone.*

Start the Microsoft Authenticator app and if you see the screen below you're ready to go!

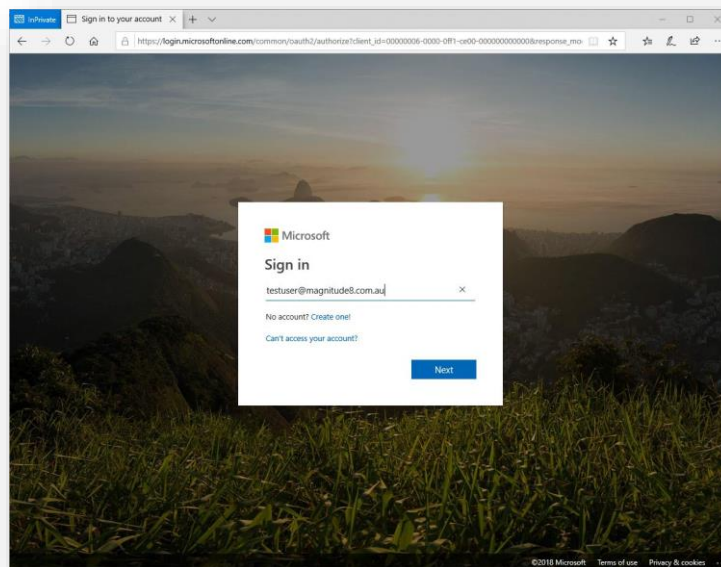


## Adding Your Office 365 Account

Before you begin this step, please ensure that the Microsoft Authenticator app is installed on your device. Once your IT department has enabled Multi-Factor Authentication for your account, you will be forced to set it up next time you log on.

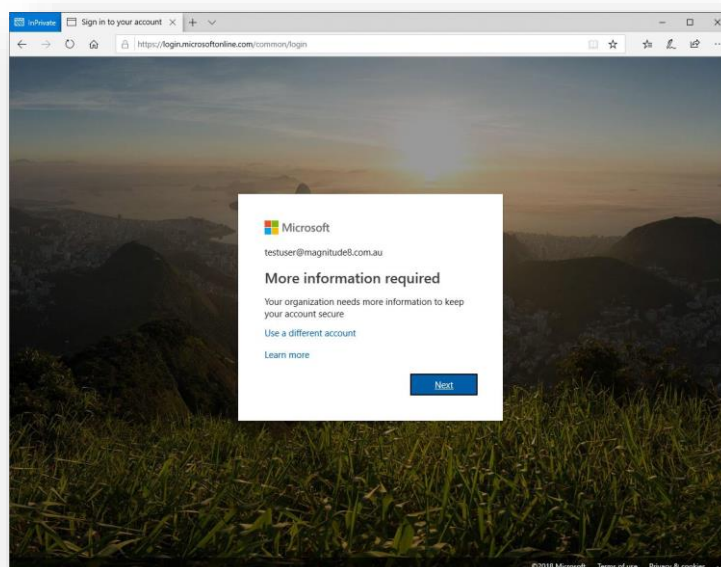
### 1. Sign in to Office 365

Go to <https://portal.office.com> and enter your login details and click Next to continue.



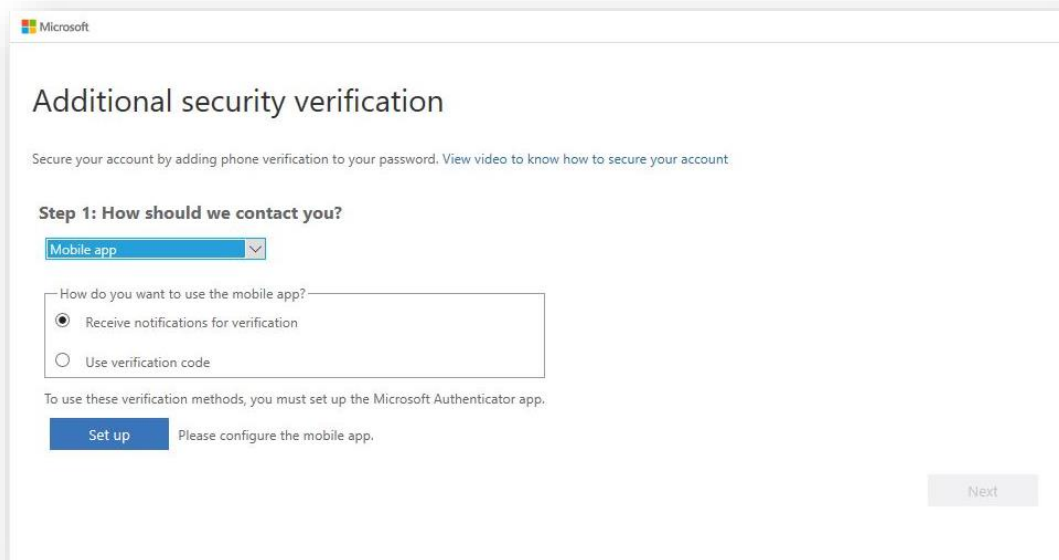
### 2. More information required

Click Next to continue.

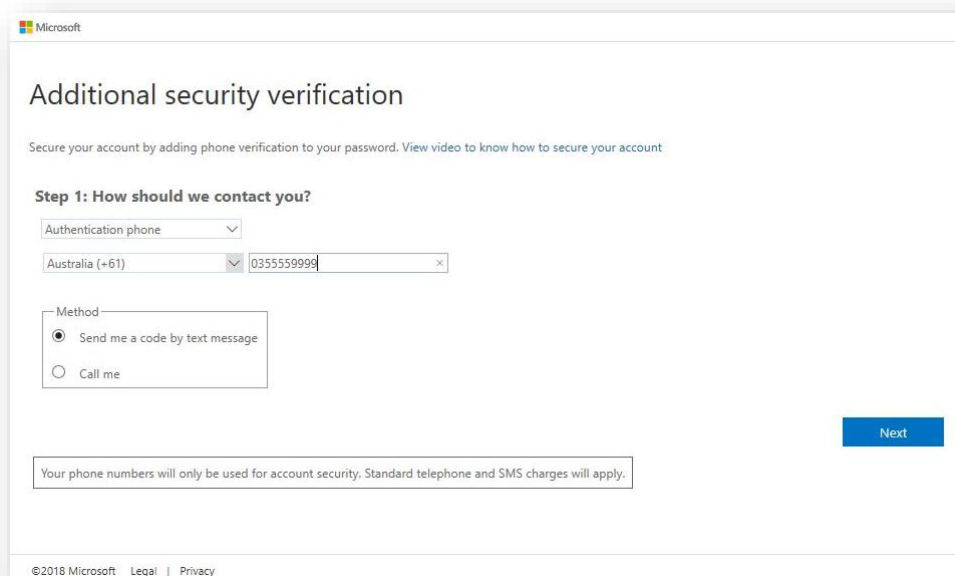


### 3. Additional security verification

On the Additional security verification screen choose Mobile App and tick the Receive notifications for verification option. Then click Set up to begin setting up the Microsoft Authenticator app.

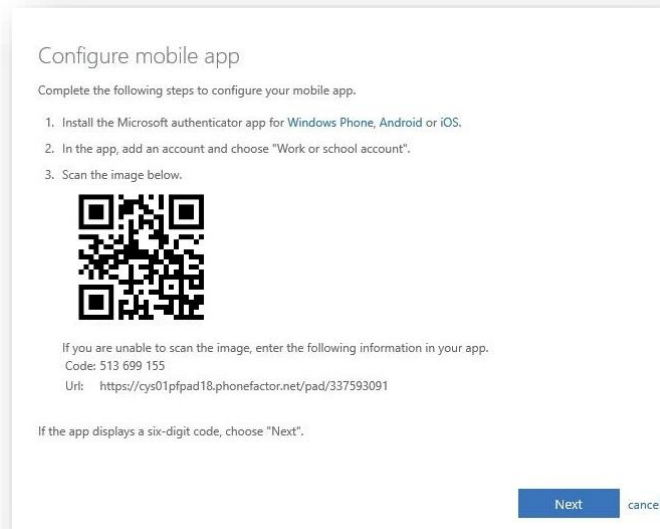


If you don't have a supported device you will need to select another authentication method, such as Authentication phone, which will send you an SMS code when you log on.



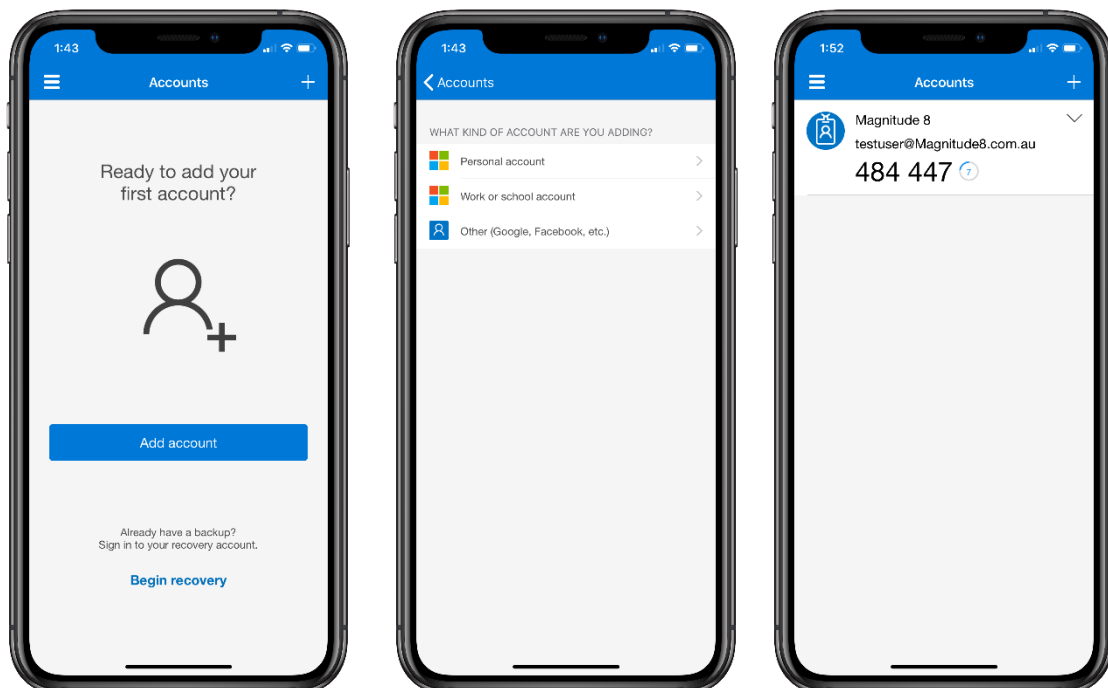
#### 4. Configure mobile app

Once you begin setting up, a QR code like the one below will appear on your screen.



#### 5. Add your account to Microsoft Authenticator

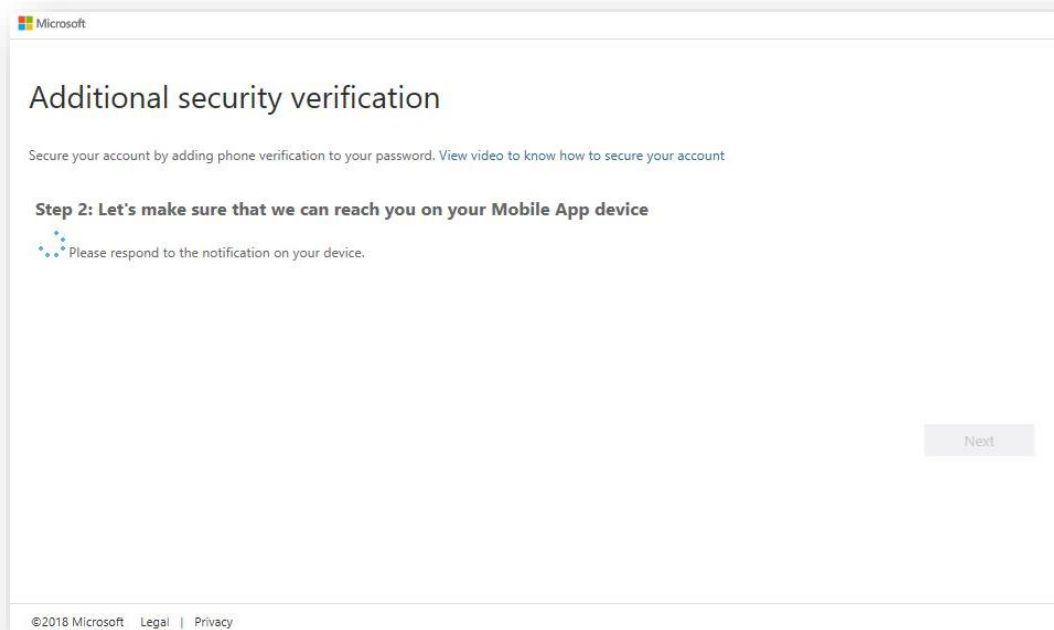
Start Microsoft Authenticator on your smart phone, tap the Add account button and tap on Work or school account. Point your smart phone camera to the QR code on your computer screen your account will be added to Microsoft Authenticator.



Your account should be displayed with a code that changes every 30 seconds. Click the Next button on your computer screen to continue.

## 6. Verify Microsoft Authenticator is working

An approval request will automatically be sent to your Microsoft Authenticator app.



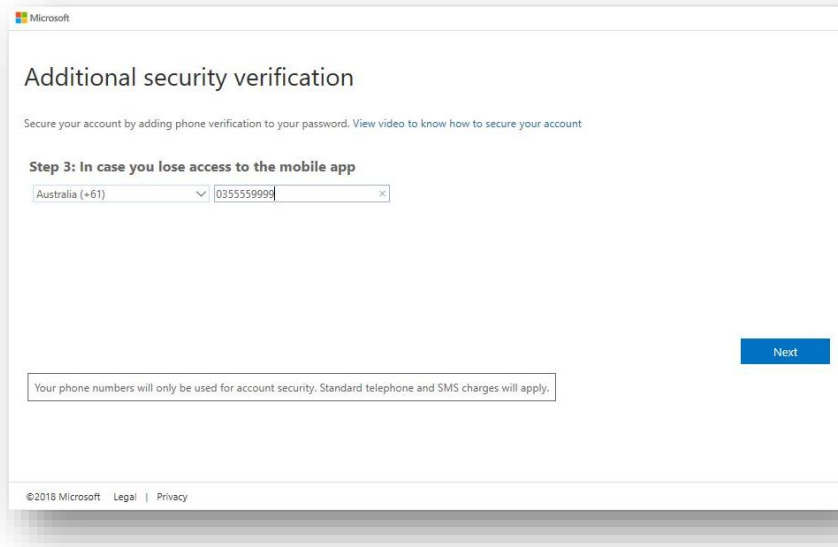
If your phone is locked or you are not using the Microsoft Authenticator app, you should receive a notification. Once you open the app, you will see a sign-in approval request.

Tap **Approve** on your phone screen to authenticate the login request.

*Important! Never approve a sign-in request that you receive unexpectedly. This may indicate that your account has been compromised. Tap **Deny** if you are not actively trying to sign in to your account and notify IT support if you have any concerns.*

## 7. Additional security verification

If the system administrator hasn't disabled other authentication methods, you will be able to set up a secondary method using an SMS. Just select your country code, enter your mobile phone number and click Next to continue.



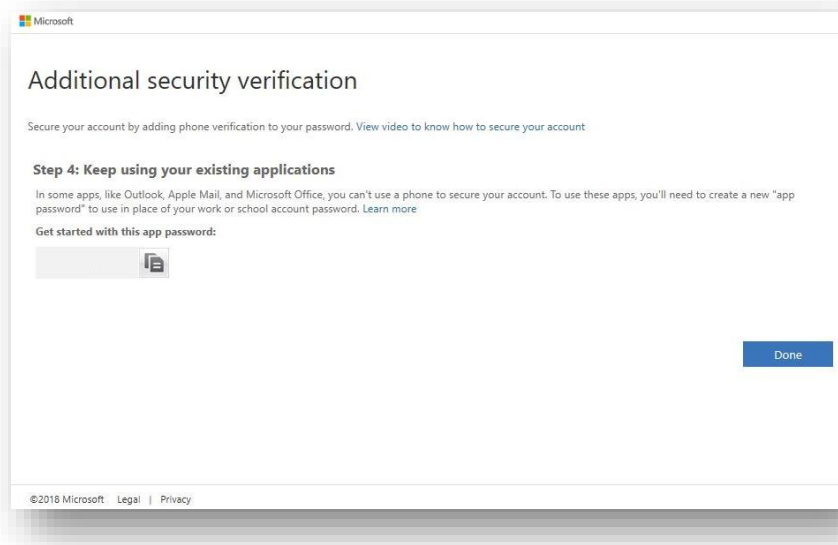
The screenshot shows the Microsoft 'Additional security verification' screen. The title is 'Additional security verification'. Below the title, it says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. The main heading is 'Step 3: In case you lose access to the mobile app'. There are two input fields: a dropdown menu for the country code, currently set to 'Australia (+61)', and a text input field for the phone number, containing '0355559999'. A blue 'Next' button is located on the right side. At the bottom, there is a small text box that says 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.' The footer contains '©2018 Microsoft Legal | Privacy'.

A secondary authentication method is useful if you ever lose access to the app, such as when you upgrade to a new phone.

If you lose access to the Microsoft Authenticator app and don't have a secondary authentication method, you will need to speak with IT support before you can log in again.

## 8. Complete the setup

Click Done on the last screen to complete the setup.



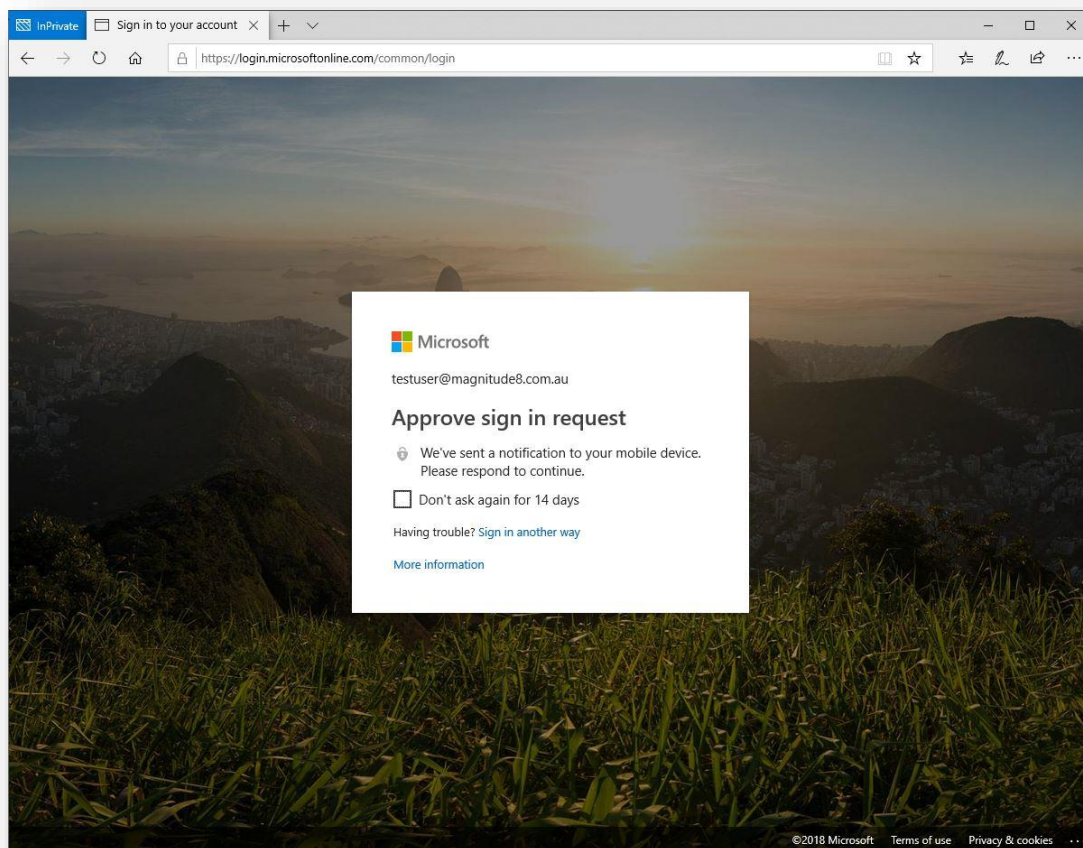
The screenshot shows the Microsoft 'Additional security verification' screen. The title is 'Additional security verification'. Below the title, it says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. The main heading is 'Step 4: Keep using your existing applications'. Below this, it says 'In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. Learn more'. There is a section titled 'Get started with this app password:' followed by a text input field and a small icon of a document with a lock. A blue 'Done' button is located on the right side. The footer contains '©2018 Microsoft Legal | Privacy'.



# SIGNING IN

Once your account has been set up with Multi-Factor Authentication you will need to use your phone to authenticate your sign in requests.

You may have the option to not require additional verification for a period between 14 and 60 days. If you use this device regularly, you can tick the box to not be prompted again.



You may receive similar prompts when accessing other Microsoft online services or systems that your IT department has integrated MFA.