Southern Cross University

Multi-Factor Authentication at SCU

USER SETUP GUIDE

This is the Southern Cross University guide to MFA and Mobile Mail, showing you how to:

Set up the authenticator you'll need before you are enrolled, which only takes a few minutes.

Authenticating to MFA when your account is enrolled to confirm your identity. You will be occasionally asked to re-authenticate yourself.

Add your mobile number when your account is enrolled, if you don't have a smartphone.

SET UP THE MFA TOOLS

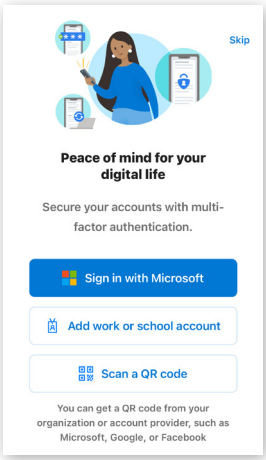
Before we enable MFA on your account, you will need to set up the Microsoft Authenticator App on your mobile device and register your SCU Account to the App, which is the most practical and straightforward way to use MFA with your University account.

The Authenticator is the most secure, easiest and fastest way to approve sign-ins. A single click is all you need to authenticate yourself, and then you can safely continue working.

01

On your mobile device, open the App Store or Play Store on your device, search for **Microsoft Authenticator** and install it.

For more information on Microsoft Authenticator app, visit the Microsoft Authenticator page on the **Apple App store**, or **Google Play store**.

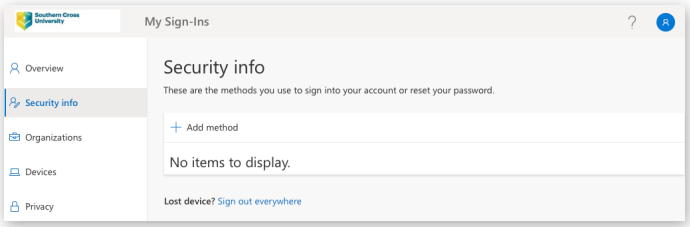


The Authenticator App will look like this.

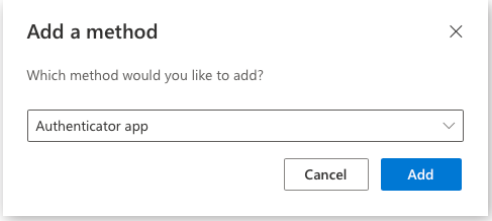
Please leave the Authenticator App and return to your computer now.

02

On your computer, open your browser to https://mysignins.microsoft.com/security-info, then click **Add method**.

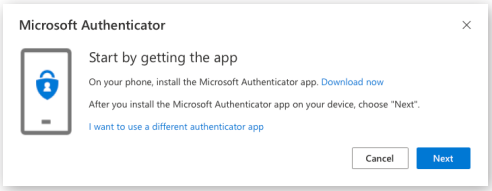


03



On the Add a method page, select **Authenticator app** from the drop-down list, and then select **Add**.

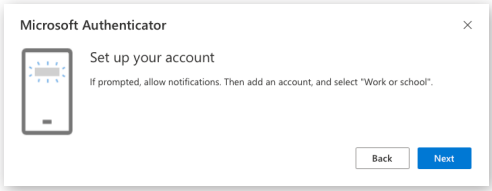
04



On the **Start by getting the app** page, ensure you have installed the Authenticator app on your mobile device, and then select **Next**.

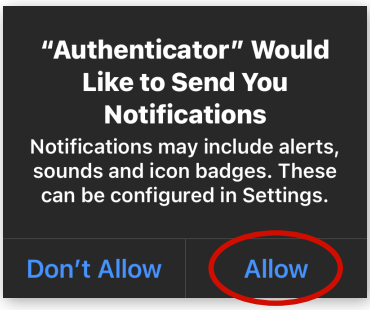
05

On your computer, remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device.

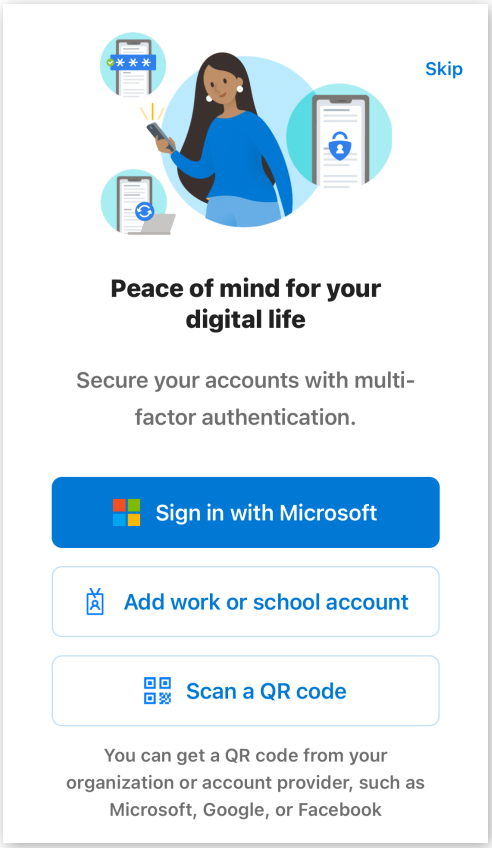


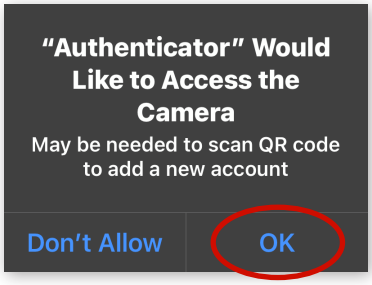
06

On your mobile device, open the Microsoft Authenticator app. Select **Allow** for Notifications if prompted so the app can alert you to log in.



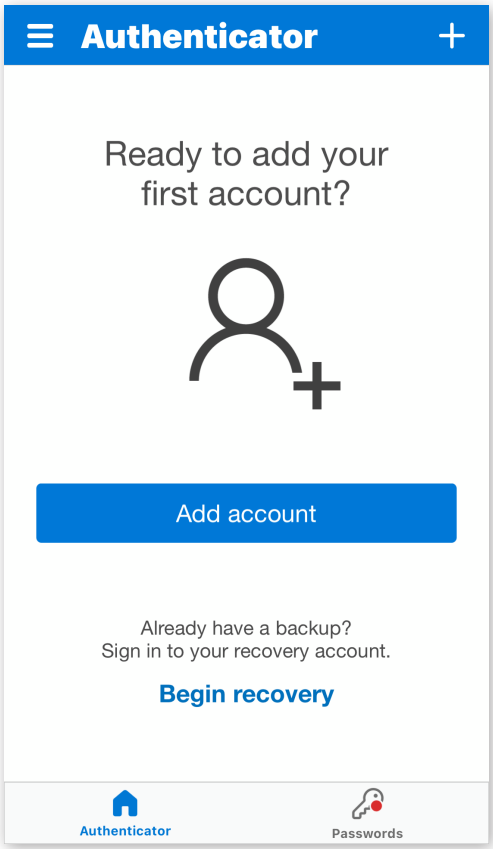
If this is the first time you've opened the app, Select **Scan a QR code**, then click **OK** on the Camera prompt to allow the app to scan the QR code during setup.

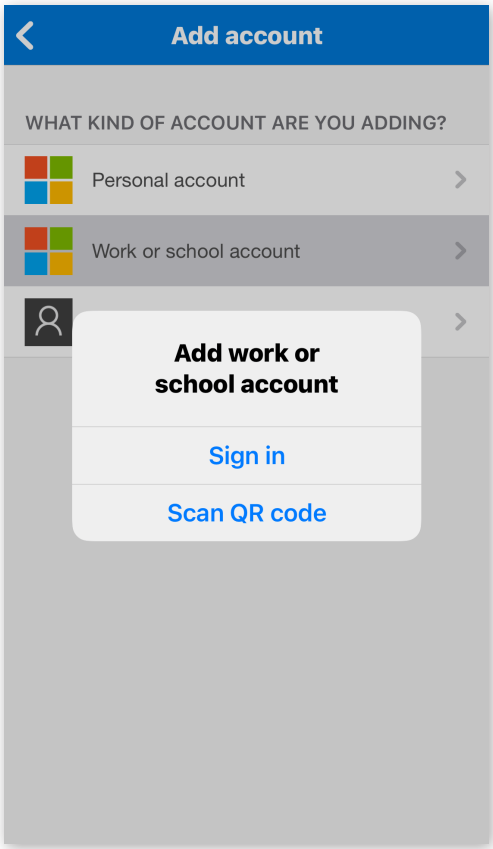




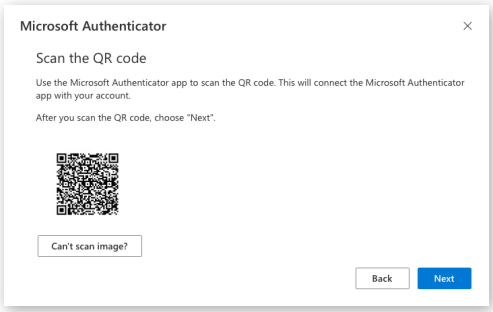
Please note: Some staff with older Android devices have reported that installing the 'Google Lens' app before the Microsoft Authenticator app has helped them scan the QR Code to set up their MFA more easily. Apple devices and newer Android devices are not affected this way.

If you have already opened the app previously, Select **Add account**, select **Work or school account** and click **Scan a QR code**.





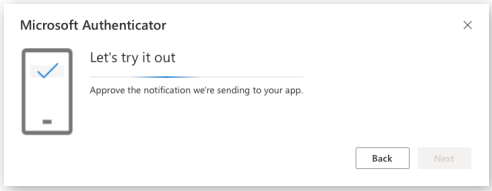
07



On your computer, return to the **Set up your account** page on your computer and select **Next**. Use your Mobile Device to scan the QR code page that appears on your computer. On the computer, select **Next**.

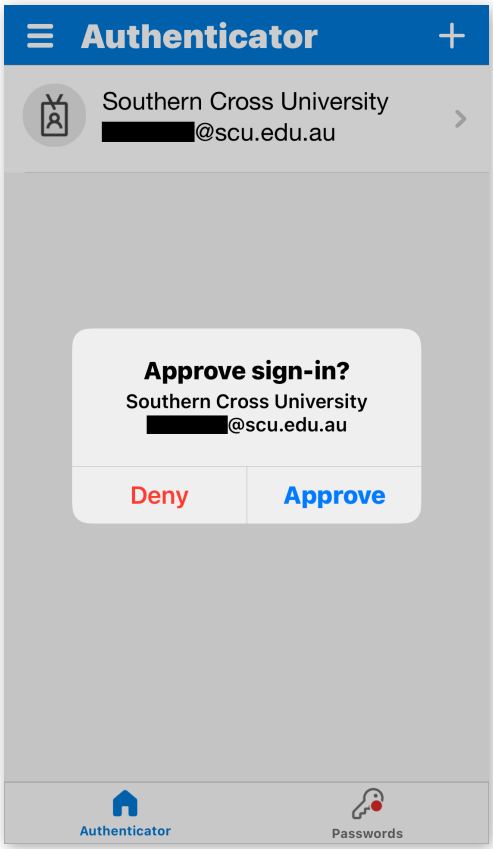
08

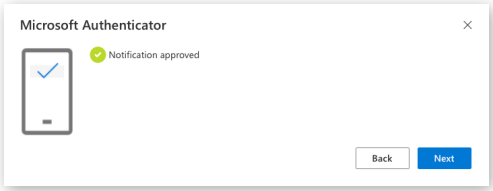
A notification is sent to the Microsoft Authenticator app on your mobile device to test your account connection.



09

On your mobile device, **approve** the notification in the Microsoft Authenticator app, and then select **Next**





Congratulations!

At this point, you have successfully registered for MFA at SCU.

Please note that you will not need to use the Authenticator App again until you are registered for MFA by Technology Services.

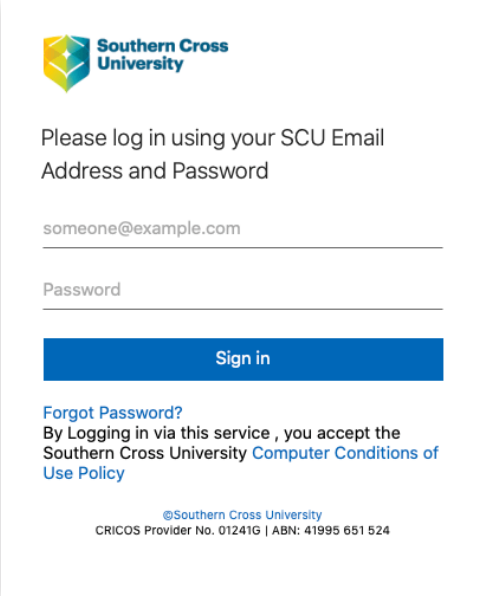
If you don't have a smartphone or do not want to install the Authenticator App, you may add your mobile number as your primary authentication method.

AUTHENTICATE TO MFA

You will need to Authenticate to MFA once you are enrolled and at various intervals after this point. The intervals will depend on what devices you use, your location, and what activities you are performing.

Technology Services will notify you of the date you will be enrolled in MFA, and the next time you log in after this date, you will need to use the Authenticator app to complete your MFA enrolment.

01

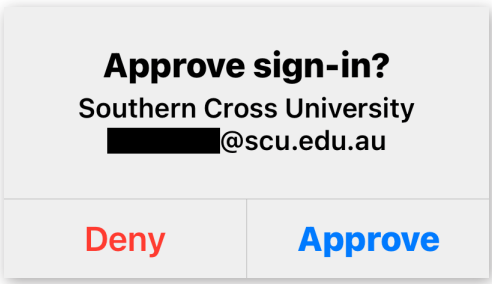


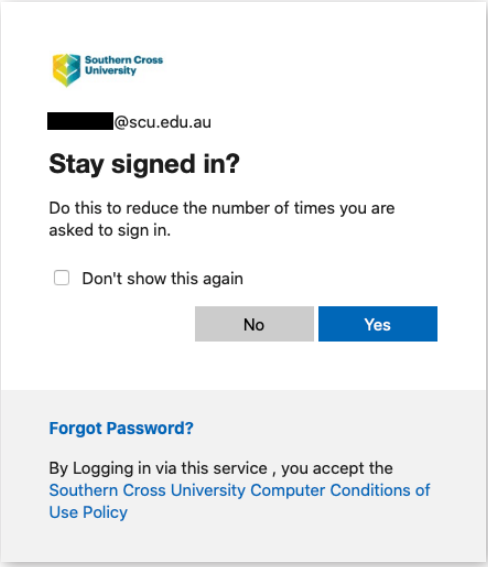
On your computer, on the first login after your MFA enrolment, go to https://email.scu.edu.au in a web browser on your computer and enter your credentials. After doing that, click **Sign in**.

02

On your mobile device, the Authenticator App will prompt you with **Approve sign-in?**. Click **Approve**, and you will be logged into your email.

Note that you may need to use your mobile devices' finger or face recognition to open the Authenticator; this provides an extra layer of biometric protection that makes this system extremely secure!





The next screen on your computer will be your SCU email Inbox.

You can elect to stay signed in if you check the **Don't show this again** checkbox and click **Yes**.

Please, only tick this on your work computer as it allows the computer to store your password, which is a potential security weakness on a shared or publicly accessed computer.

That's MFA!

You have used another factor to prove your identity to ensure the most secure way to protect the University and your data.

This simple process is all it takes to prevent almost all attacks with stolen credentials.

Cybersecurity is everyone's business, and by using MFA, you are actively helping the University fight phishing attacks, account takeovers, intellectual property and corporate information theft.

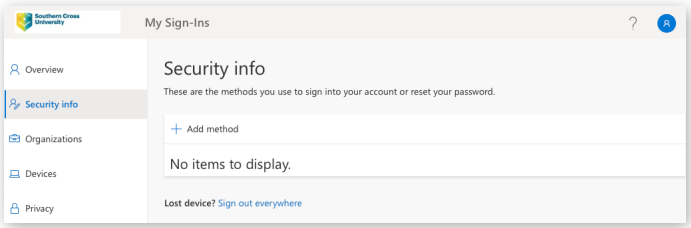
ADDING YOUR MOBILE NUMBER TO MFA

The University recommends that you add your mobile number to your University account as an alternate authentication method.

If you don't have a smartphone or do not want to install the Authenticator App, you can make your phone the default sign-in method.

Using a mobile number will send your mobile device an SMS code that you enter in your computer to authenticate, instead of the single click **Approve** of the Authenticator App.

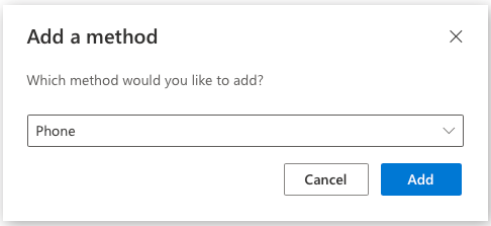
01



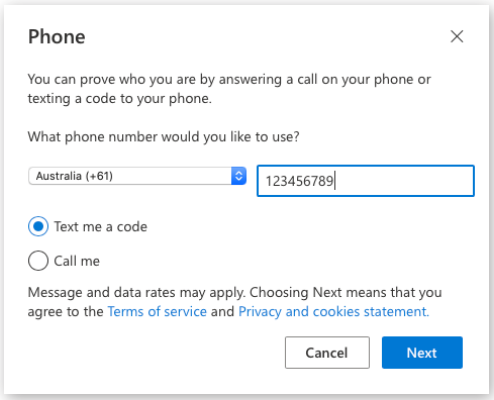
On your computer, open your browser to https://mysignins.microsoft.com/security-info, then click **Add method**.

02

Select **Phone** from the drop-down menu, and click **Add**.



03

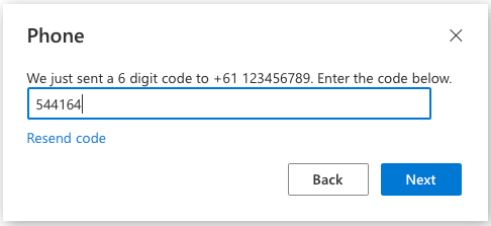


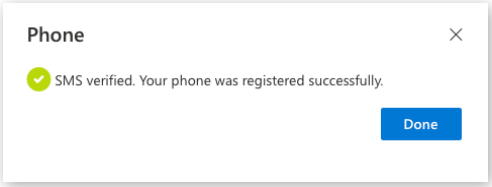
On the next page, select **Australia** as the country and enter your mobile number, making sure the **Text me a code** radio button is selected.

Please note you will need to leave out the leading zero (0) of your number, so if your phone number is 0123 456 789, you enter 123456789 (no spaces), then click Next.

04

You will receive a text from Microsoft - **Use verification code xxxxxx for Southern Cross University authentication**. Enter this code in the next window, and click **Next**.



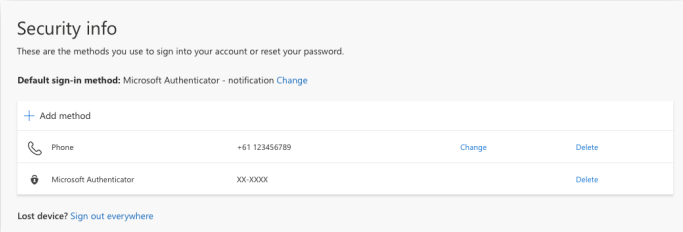


You have now registered to use SMS as the second factor for MFA at SCU.

MAKE YOUR PHONE THE DEFAULT SIGN-IN METHOD

If you want to use SMS instead of the Authenticator App to verify your identity when challenged, use these steps to make SMS your default method.

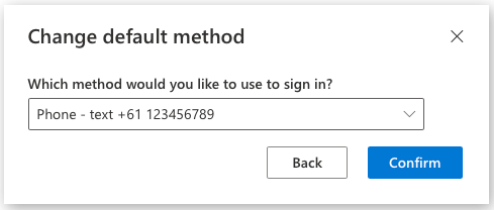
01



On the **Security info** page at https://mysignins.microsoft.com/security-info, next to the Default sign-in method information, select the **Change** link.

02

Select **Phone - text (your mobile number)** and click confirm. Your mobile phone (text) is now the default sign-in method.



That's it. Your mobile phone number is now the second factor, and you will receive an SMS code to verify your identity during an MFA login.