

Multifactor Authentication

Introduction

Multifactor Authentication (MFA) is an additional security step to verify your identity when you log in to Federation applications and systems. This extra layer of security protects you and the university from unauthorised access.

Staff and students are required to have at least one MFA method: Microsoft Authenticator app or text messaging.

MFA Options	
Microsoft Authenticator app	Useful if you may not have internet access or the ability to receive text messages.
Text message	Useful if you prefer receiving a one-time code by SMS.

Instructions

The instructions below will guide you through setting up your preferred authentication method.

You can also watch one of our video tutorials to step you through:

- [Microsoft Authenticator app method](#)
- [Text message method](#)

Following setup, if you experience any issues relating to MFA or your login details you can get help through [the password portal](#) or by contacting IT Support on 03 5327 9999.

Microsoft Authenticator app method

The app is a handy method as it allows you to authenticate even if you're in a situation where don't have internet access or the ability to receive text messages.

Once your MFA is set up, view the [Receive a one-time passcode](#) guide for additional information on authenticating without internet access.

1. **On your mobile device:** download and install the Microsoft Authenticator app, based on your smart device operating system:

- Apple iOS: Go to the [App Store](#)
- Android: Go to [Google Play](#)

2. Once you have downloaded the authenticator app, navigate to [Microsoft My Signins](#)

3. Sign in with your university credentials (Staff username or Student ID and password)



Sign on with your FedUni Network Login

Student ID (or staff username)

Password

Sign in

Having trouble logging in or unsure of your username?
Please visit the [Passwords Self-Servicer Portal](#) for assistance.

4. On the 'Let's keep your account secure' screen, click **Next**



atest2@students.federation.edu.au

Let's keep your account secure

We'll help you set up another way to verify it's you.

[Use a different account](#)

[Learn more about verifying your identity](#)

Next

5. On the 'Install Microsoft Authenticator' screen, click **Next** (you should already have installed this on your device in step 1)

6. On the 'Now pair Authenticator with your account' screen, click **Pair your account to the app by clicking this link** (do NOT click the Next button).



← atest2@students.federation.edu.au

Now pair Authenticator with your account



When finished, come back to this setup experience.

Pair your account to the app by clicking this link.

[Show QR code](#)

[Set up a different way to sign in](#)

Next

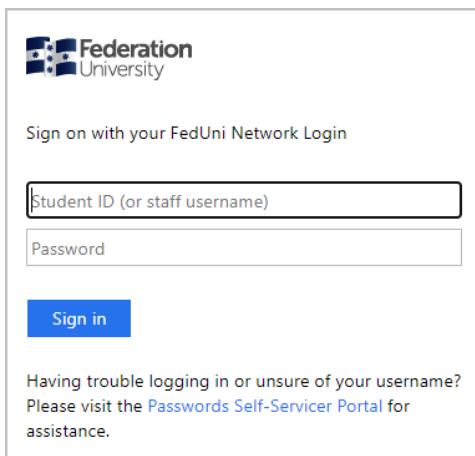
Your account will pair with Authenticator and be ready for use.

If you would also like to set up text message MFA as a back-up, follow the **text message method** section of the guide next.

Text message method

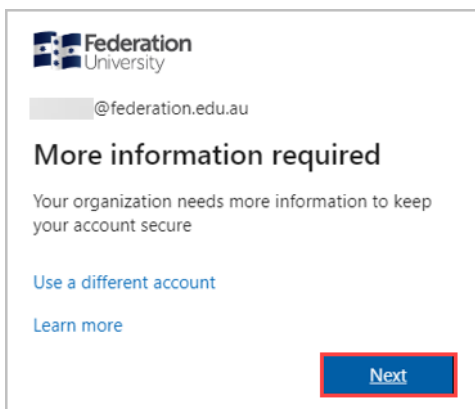
The other option is to receive a one-time code via text to authenticate. You can also [watch a video tutorial](#) to step you through this process.

1. Log into any Federation O365 online application (eg. [Outlook web-mail](#)) using your Federation credentials (Staff username or Student ID and password)



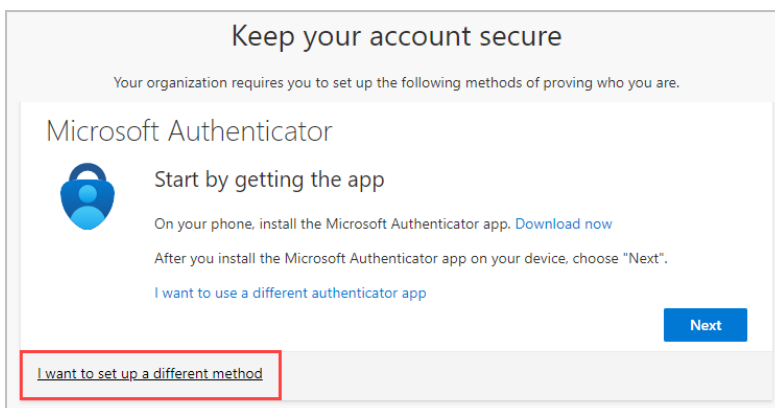
The login screen for Federation University. It features the university's logo at the top left. Below the logo, the text "Sign on with your FedUni Network Login" is displayed. There are two input fields: "Student ID (or staff username)" and "Password". A blue "Sign in" button is located below the password field. At the bottom, there is a link for users having trouble logging in, directing them to the Passwords Self-Service Portal.

2. You will be presented with the requirement to set up MFA. Select **Next**

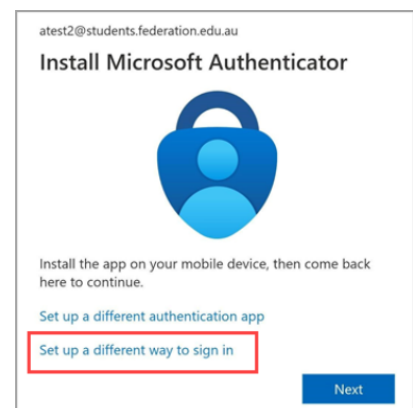


The "More information required" screen. It shows the user's email address as "@federation.edu.au". The heading "More information required" is followed by the text "Your organization needs more information to keep your account secure". There are two links: "Use a different account" and "Learn more". A blue "Next" button is at the bottom right.

3. Next, select **I want to set up a different method** in the bottom left of the screen. On a mobile device, this may read **Set up a different way to sign in** instead.

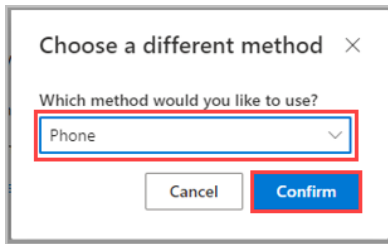


The "Keep your account secure" screen. It states "Your organization requires you to set up the following methods of proving who you are." The main heading is "Microsoft Authenticator". Below it, there is a blue shield icon and the text "Start by getting the app". Instructions follow: "On your phone, install the Microsoft Authenticator app. [Download now](#)" and "After you install the Microsoft Authenticator app on your device, choose 'Next'." There is a link "I want to use a different authenticator app" and a blue "Next" button. At the bottom left, a red box highlights the link "I want to set up a different method".

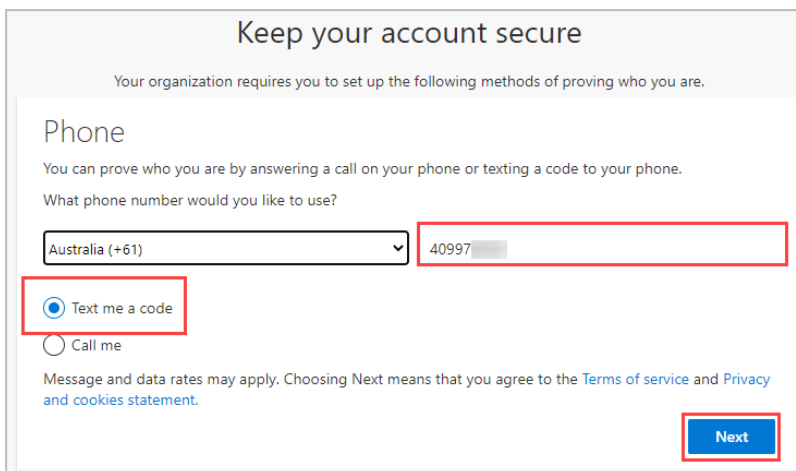


The "Install Microsoft Authenticator" screen. It shows the user's email address as "atest2@students.federation.edu.au". The heading is "Install Microsoft Authenticator" with a blue shield icon. Instructions say: "Install the app on your mobile device, then come back here to continue." There are two links: "Set up a different authentication app" and "Set up a different way to sign in". A red box highlights the "Set up a different way to sign in" link. A blue "Next" button is at the bottom right.

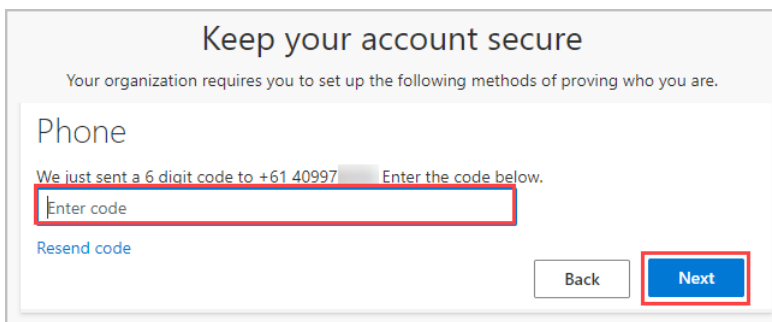
4. Select **Phone** from the drop-down list, then click **Confirm**



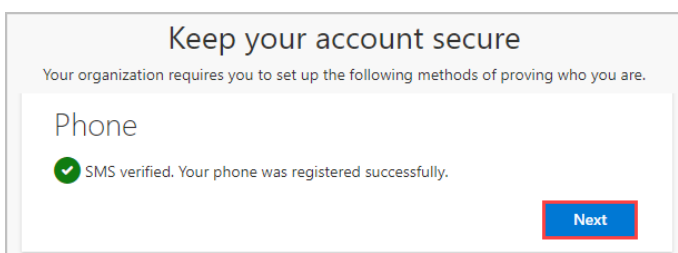
5. On the **Phone** page, enter the phone number for your mobile device, choose **Text me a code**, click **Next** and you will receive a text message.



6. **Enter the code** that you received in the text message and click **Next**.



7. You will receive confirmation of successful verification on your computer, select **Next**



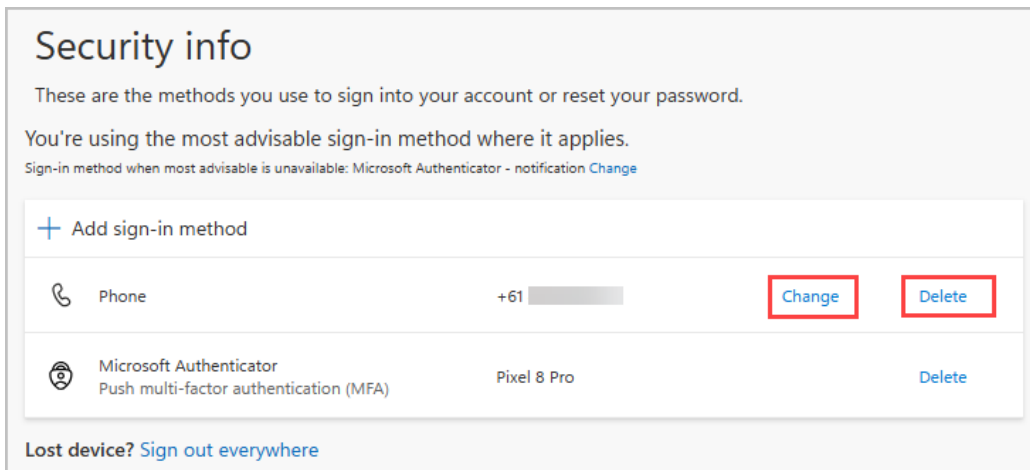
8. Your setup is now complete. Select **Done** to finalise and continue signing in.

If you would also like to set up MS Authenticator app MFA as a back-up, follow the **set up MS Authenticator** section of this guide.

Revise your MFA methods

Once setup, you can update your MFA methods at any time.

1. Log into [Microsoft My Account](#)
2. Click into the **Security Info** page from the left-hand menu
3. Click **Change** or **Delete** next to the method you wish you alter.



The screenshot shows the 'Security info' page in a Microsoft account interface. It includes instructions on how to use the methods to sign in or reset a password, a note about the most advisable sign-in method, and a list of current methods. The 'Phone' method is highlighted with a red box around its 'Change' and 'Delete' buttons. The 'Microsoft Authenticator' method is also listed with a 'Delete' button. A 'Lost device? Sign out everywhere' link is at the bottom.

Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification [Change](#)

[+ Add sign-in method](#)

	Phone	+61	Change	Delete
	Microsoft Authenticator Push multi-factor authentication (MFA)	Pixel 8 Pro		Delete

Lost device? [Sign out everywhere](#)

Please note: if you delete all methods, you will no longer be able to sign in to your Federation accounts.