



Multi-Factor Authentication (MFA)

MFA with SMS setup guide

This document explains how to set up **Multi-Factor Authentication (MFA)** with SMS, allowing access to **Office 365** services (including **email**, **calendar** and **OneDrive**) from outside the University Network.

The SMS method is intended for situations where the Microsoft Authenticator app cannot be used, as it is considered less reliable and dependant on cellular signal strength.

Please consult the [Troubleshooting](#) section at the end of this document if you require assistance.

What do I need to set up MFA with SMS?

A device capable of receiving SMS messages (typically a mobile phone).

This will be your MFA device. Please have it with you when you wish to access Office 365 out with the University.



An internet connected PC or laptop.



Step 1

On your computer



Navigate to <https://aka.ms/mfasetup>.

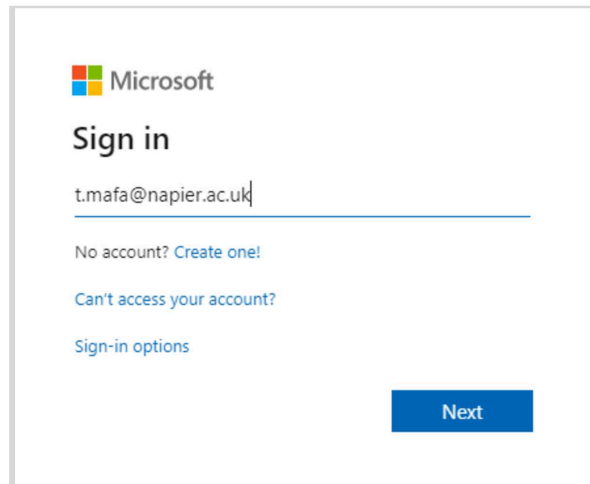
Sign in with your University **email address** and password.

Staff must not use their 4xxxxxxx number.

If prompted to stay signed in, select **Yes** if you trust the computer you are using.

You will be prompted to provide additional information.

Select **Next** to continue.



Microsoft

Sign in

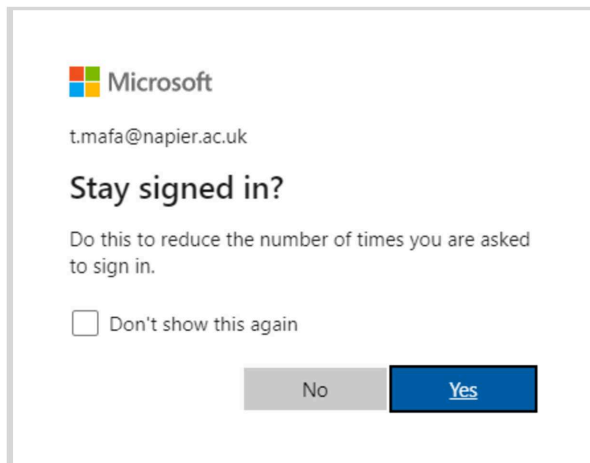
t.mafa@napier.ac.uk

No account? [Create one!](#)

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

[Sign-in options](#)

Next



Microsoft

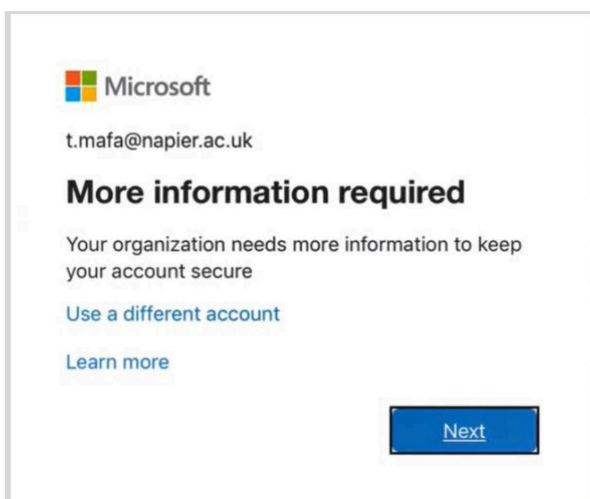
t.mafa@napier.ac.uk

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No **Yes**



Microsoft

t.mafa@napier.ac.uk

More information required

Your organization needs more information to keep your account secure

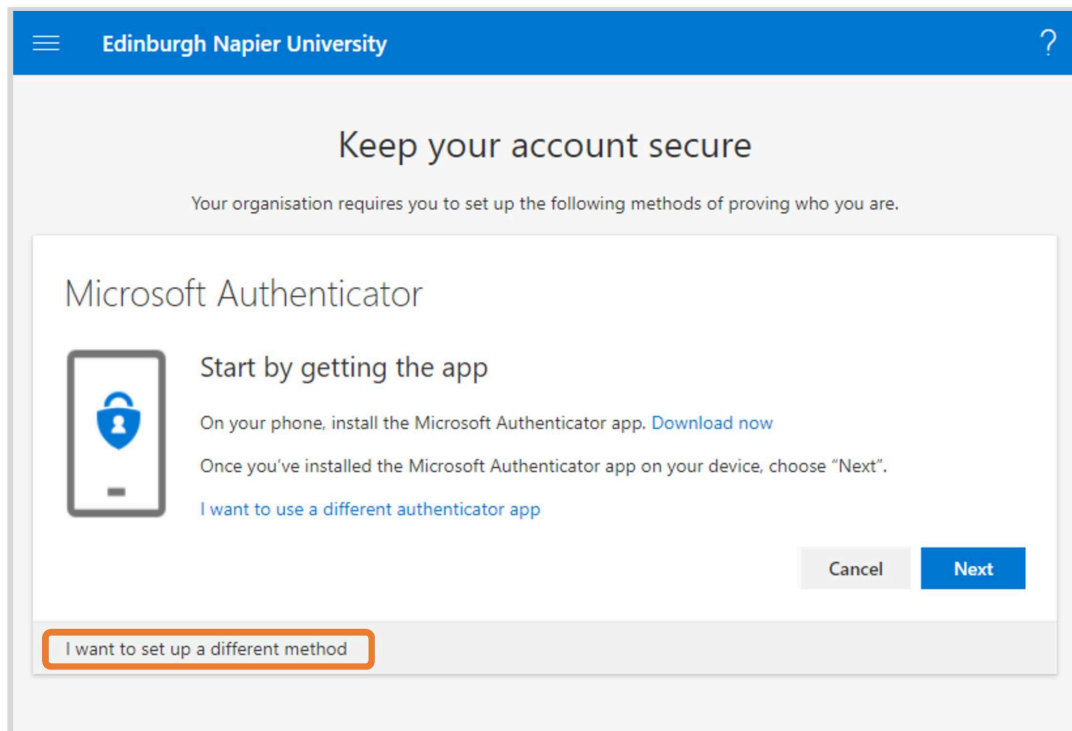
[Use a different account](#)

[Learn more](#)

Next

Step 2

To set up the SMS MFA method, select **I want to set up a different method.**



Step 3

Select **Phone** from the drop down menu which appears, then select **Confirm**.

The screenshot shows the Edinburgh Napier University account security setup interface. A modal dialog titled "Choose a different method" is open, prompting the user to select a method. The dropdown menu shows "Phone" as the selected option. The background screen displays "Keep your account secure" and "Your organisation requires you to set up the following methods of proving who you are." Below this, there's a section for "Microsoft Authenticator" with a "Start by getting" button. A "Next" button is visible at the bottom right of the main content area.

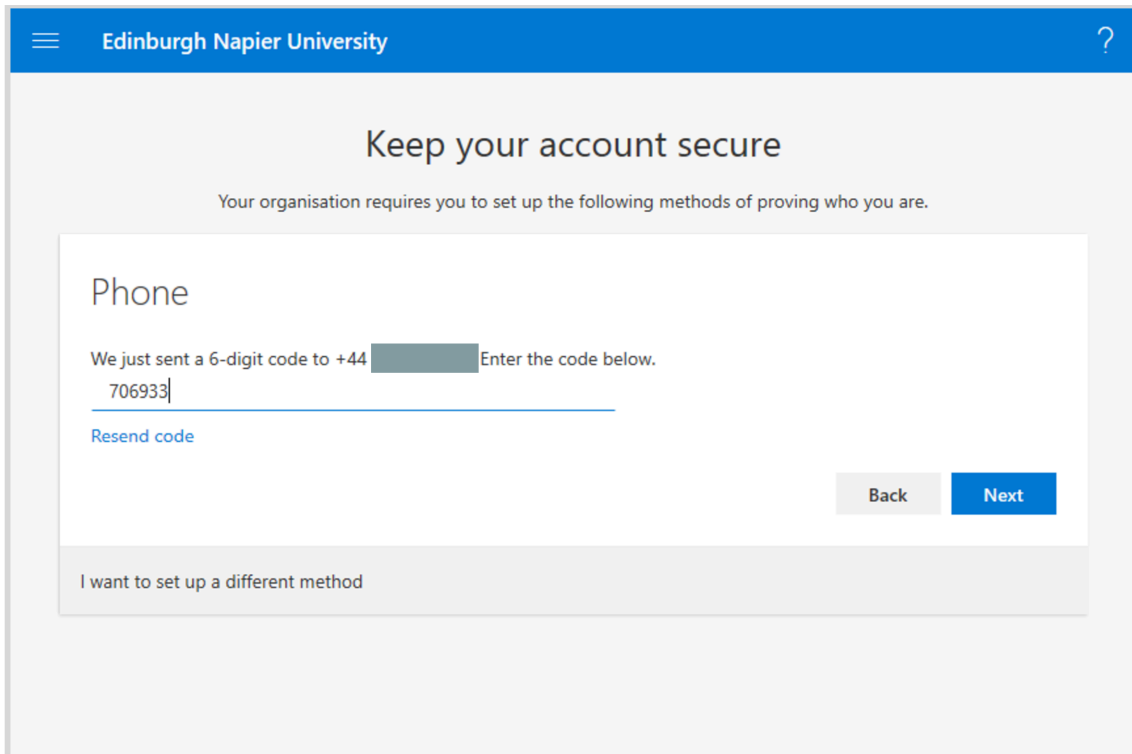
Step 4

Select your country code from the dropdown menu and enter your phone number. Select **Next**.

The screenshot shows the "Phone" step of the account security setup. The title "Phone" is at the top. Below it, the text says "You can prove who you are by texting a code to your phone." and "What phone number would you like to use?". There's a dropdown menu for the country code, currently set to "United Kingdom (+44)". To the right of the dropdown is a text input field for the phone number. Below the input field, there's a radio button labeled "Text me a code" which is selected. Below that, it says "Message and data rates may apply." A "Next" button is at the bottom right. At the bottom left, there's a link that says "I want to set up a different method".

Step 5

You will be sent a SMS message containing a 6 digit code. Enter it into the field provided and select [Next](#).



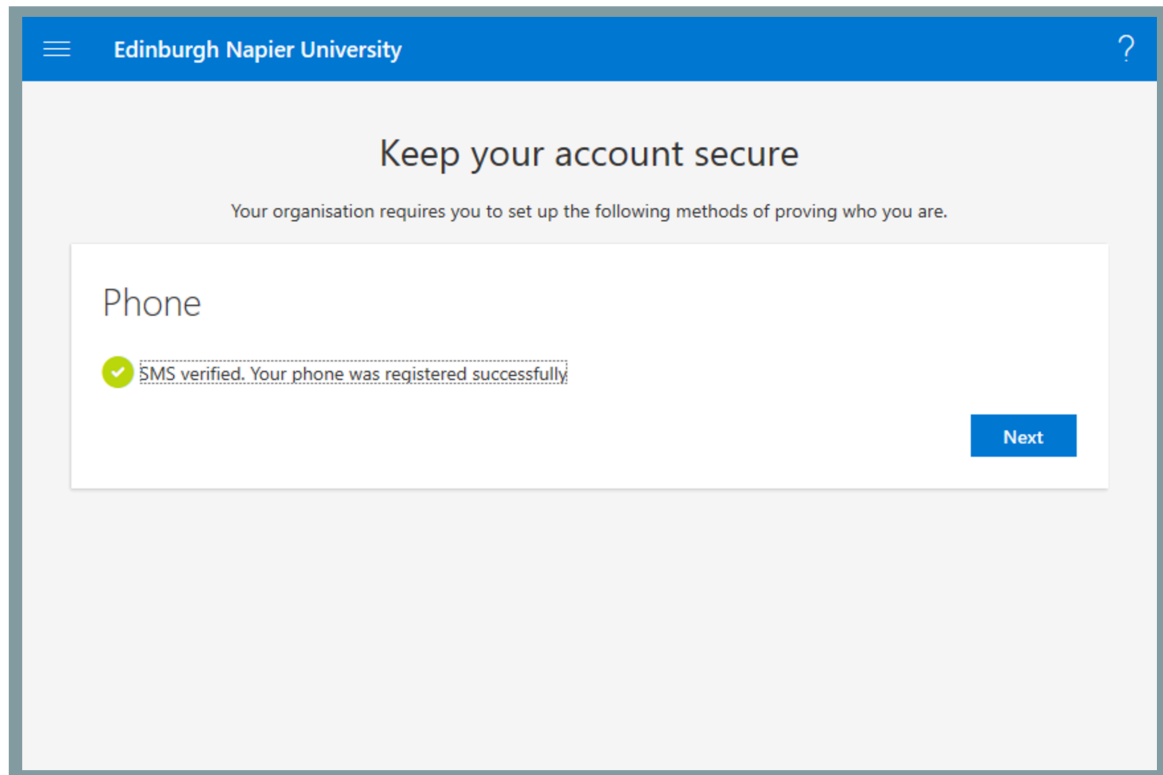
The screenshot shows a web interface for Edinburgh Napier University. At the top is a blue header with the university's name and a menu icon. Below the header, the main heading is "Keep your account secure". A subheading states: "Your organisation requires you to set up the following methods of proving who you are." The central part of the page is a white box titled "Phone". Inside this box, it says "We just sent a 6-digit code to +44 [redacted] Enter the code below." Below this, there is a text input field containing "706933". To the left of the input field is a blue link "Resend code". At the bottom right of the white box are two buttons: "Back" (grey) and "Next" (blue). At the bottom of the white box, there is a link "I want to set up a different method".



You will not be charged for any SMS messages sent to your phone. Be aware the message can be delayed if your phone signal is low. Sender name varies.

Step 6

You will receive a message indicating registration was successful, select **Next** to continue.

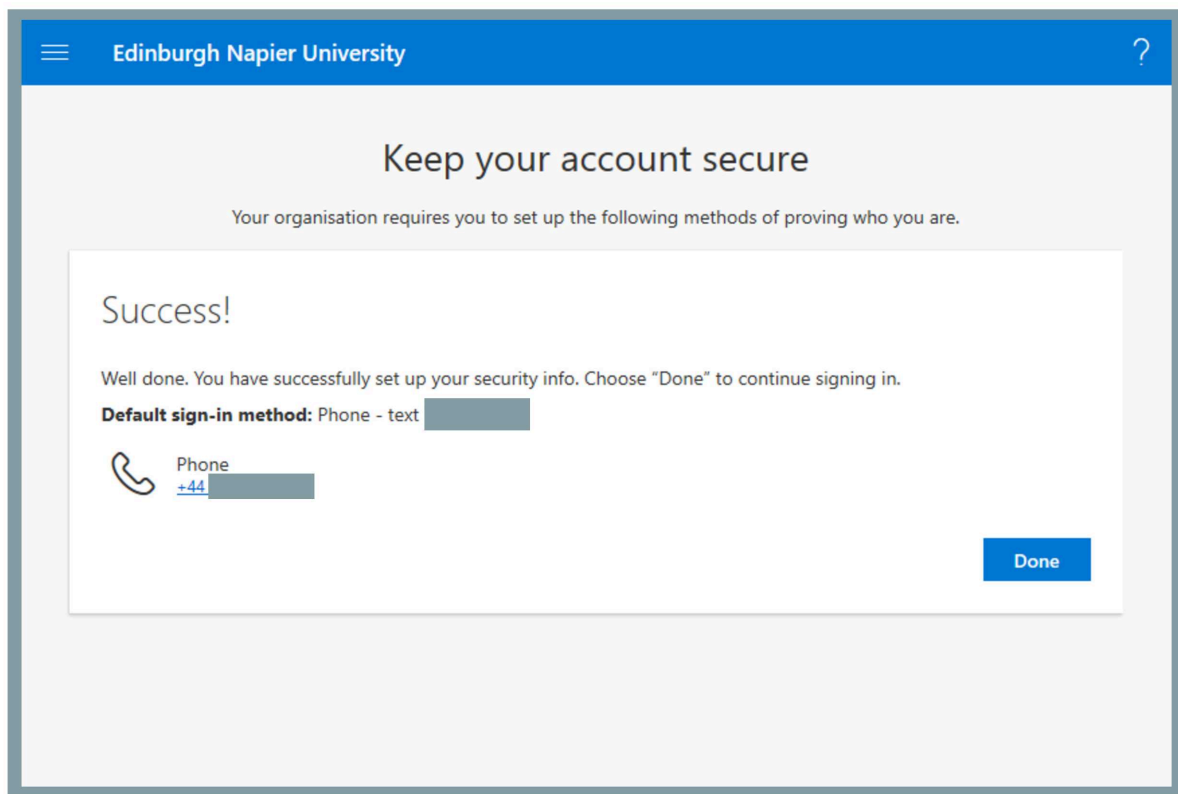


Stay safe in the future! You will only ever receive a SMS code like this when you have manually triggered its generation and are expecting one.

If you have received one out of the blue, it is an indication your account has been compromised! [Contact the IS Service Desk](#) immediately and request a **password reset**.

Step 7

Select **Done** to finish.



The screenshot shows a web interface for Edinburgh Napier University. At the top is a blue header with a hamburger menu icon, the text "Edinburgh Napier University", and a question mark icon. The main content area has a light gray background. It features a heading "Keep your account secure" and a subtext "Your organisation requires you to set up the following methods of proving who you are." Below this is a white box containing a "Success!" message, followed by the text "Well done. You have successfully set up your security info. Choose 'Done' to continue signing in." It then displays "Default sign-in method: Phone - text" with a grayed-out input field. Underneath is a phone icon, the label "Phone", a blue "+44" link, and another grayed-out input field. A blue "Done" button is located in the bottom right corner of the white box.

Edinburgh Napier University

Keep your account secure

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

Success!

Well done. You have successfully set up your security info. Choose "Done" to continue signing in.

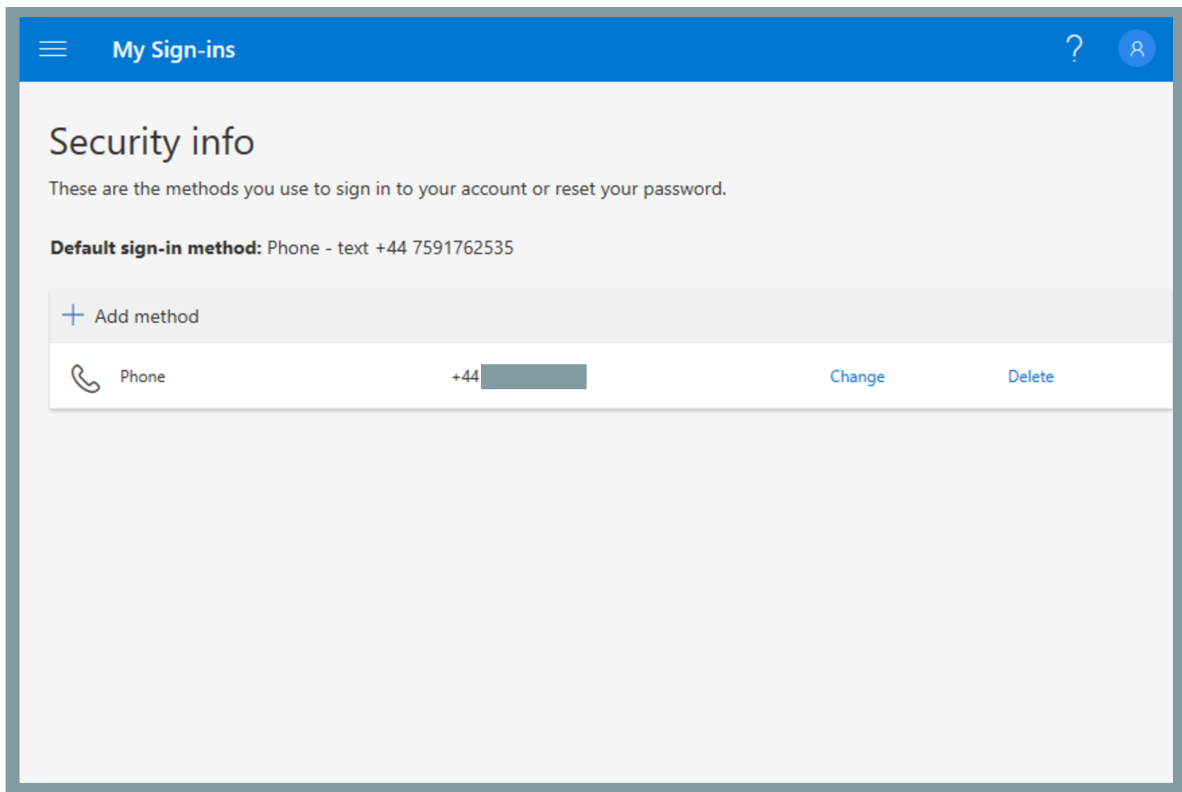
Default sign-in method: Phone - text

Phone [+44](#)

Done

Step 8

You will be taken to your security info page. Here you can manage your MFA settings and devices. You can access this in the future by navigating to <https://aka.ms/mfasetup>.




Troubleshooting

I didn't receive my SMS code?

SMS is reliant on your phone signal, so if you are in an area with no or low signal you might not receive it until you move to an area with a better signal.

It says I ran into a problem?

 We're sorry, we ran into a problem. Please choose "Next" to try again.

This can appear if the process isn't completed quickly enough (it times out for security reasons). It's best to start the process again from scratch. Close down the browser tab and go back to **Step 2**.

At Step 8 it says an unexpected error has occurred?

This is due to a conflict between your browser remembering a sign in using your 4xxxxxxx@napier.ac.uk and your email address. It doesn't indicate that MFA isn't working. You must sign out of the website from the top right dropdown, then clear your browser data. When you return to <https://aka.ms/mfasetup> it should display correctly.

Alternatively use a different browser to access this page in the future.

I've lost my device!

[Contact the IS Service Desk](#). They are able to reset your MFA settings so that you can set up MFA on a new device.

I do not wish to use a personal device for MFA, what can I do?

Please use a corporate mobile device to perform MFA if you have been provided with one. Otherwise, please use the [Virtual Desktop Service](#) or [Virtual Private Network](#) service to access Office 365.

If you are still having difficulty, please phone the **IS Service Desk** on **0131 455 3000** for assistance.