Multi-factor Authentication (MFA): Authenticator Phone

What is Multi-factor Authentication?

Multi-factor Authentication (MFA) is an approach to online security that requires you to provide more than one type of authentication for a login or other transaction.

Also known as 'Two-step Verification', MFA adds an extra layer of protection to your account and is used on a regular basis for many online transactions such as banking, shopping, or PayPal.

MFA requires you to authenticate using:

1. **Something you know:** your username and password
2. **Something you have**: a trusted device, such as your mobile phone, on which to receive and respond to verification requests

You must complete both authentication steps in order to access your University Microsoft account when off campus or on eduroam.

Setting up Multi-factor Authentication

Multi-factor Authentication is fast becoming essential to secure cloud-based services. For this reason, you are required set up MFA on your University Microsoft Office 365 account.

You can set up one or more of these authentication methods:

- Use the Microsoft Authenticator app on a mobile device (recommended)
    - If you would prefer to install and use the Microsoft Authenticator app on your mobile device, please see our separate guide for setting this up.
- Receive a code by text[1]
- Receive a call by phone

This user guide steps you through setting up your **Phone** as a method of authentication.

This could be a mobile phone or a landline phone, e.g. home phone.

Set up an Authentication phone

Can I use my office phone?

Although your office phone number is listed, it is preferable to set up another phone such as your mobile or home phone.

This ensures that if you need to sign in to Office 365 away from the campus network or at home, you have the means to receive the authentication code.

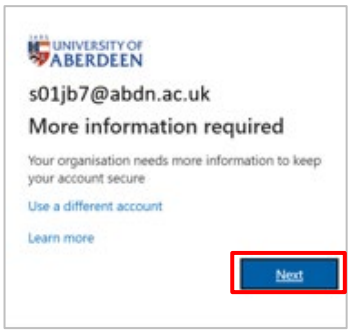
[1] Some services such as SSH gateway will not accept the entry of a code. If you use these services, please make sure you set up the Authenticator app and/or phone call as methods of authentication and set one of these as your default.

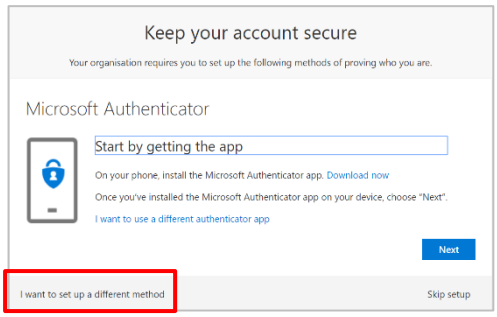
To set up first Phone

On your PC, Mac or Tablet

1. Open a browser and go to: https://aka.ms/setupsecurityinfo
2. **Sign in** with *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
3. Enter your University **password** at the prompt

4. ***If*** you are prompted that *Your organisation needs more information to keep your account secure* click **Next.**

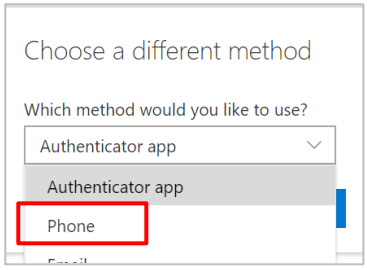




Click **I want to set up a different method** at the prompt to set up the Microsoft Authenticator app.

Choose **Phone** from the drop-down options.

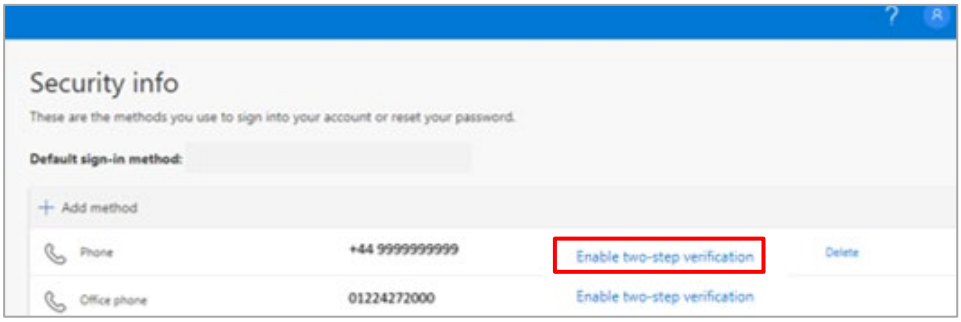
Skip to step 8.



5. ***Otherwise*** the **My Sign-Ins** window will open.

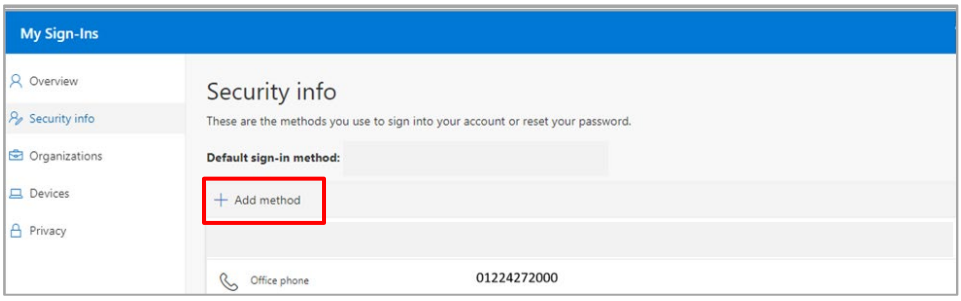
   Note: If you have registered a phone for SSPR (Self Service Password Reset), the details of this phone will already be listed.

   To be able to authenticate by receiving a notification (text or a call) to that phone, click on **Enable two-step notification** next to the number and follow the instructions from **step 8**.

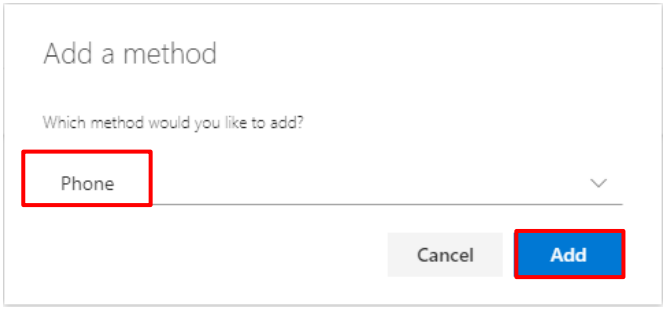


If there are no phones listed continue to **step 6** to set up your first **Phone.** If you choose to register a *mobile phone* you will have the options to receive a text or call.

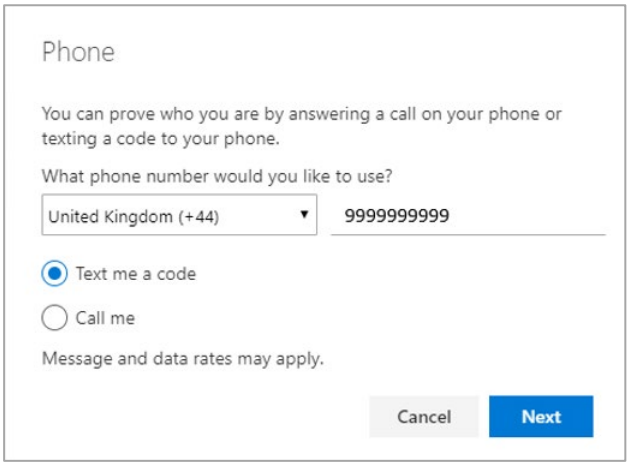
6. Click on **+ Add method**



7. Choose **Phone** as your method and click **Add**



8. In the **Phone** window, enter the details of your phone, on which you want to receive notification, i.e. **country code** (from the drop-down) and **phone number**.

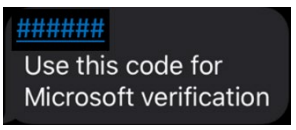


9. Choose Text me a code or Call me.
10. Click **Next**

On your mobile phone

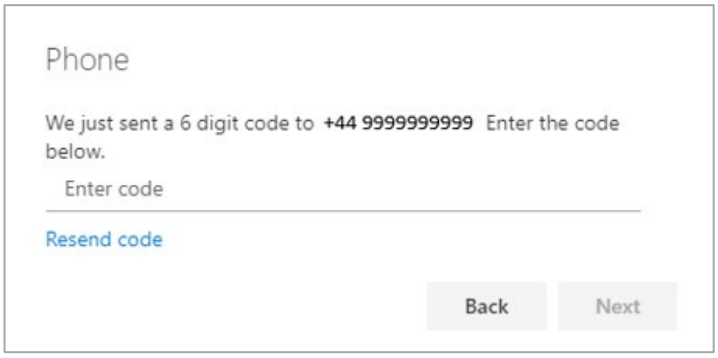
If you chose **Text me a code**

i. You will receive an SMS message to your mobile phone from SmsVerify similar to this:



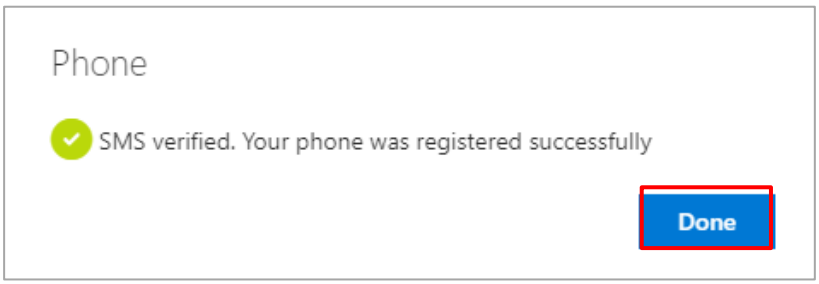
On your PC, Mac or Tablet

ii. **Enter** this 6-digit code in the window that appears on screen on your PC, Mac or Tablet:



iii. Click **Next**

iv. You should see a message to indicate you have registered your mobile phone as an authentication method.

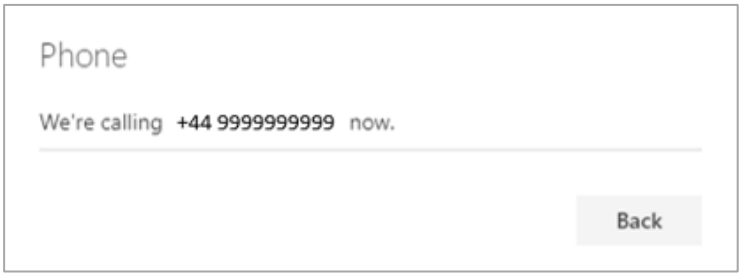


v. Click **Done** and **go to Step 11** below.

On your PC, Mac or Tablet

If you chose **Call me**

i. You will see the following message and receive a call to your phone, which you have registered:



On your mobile or home phone

ii. **Answer** your phone – a voice message will instruct you to press the **Hash** or **Pound** key to finish your verification.

iii. Open or view your phone's **keypad**.

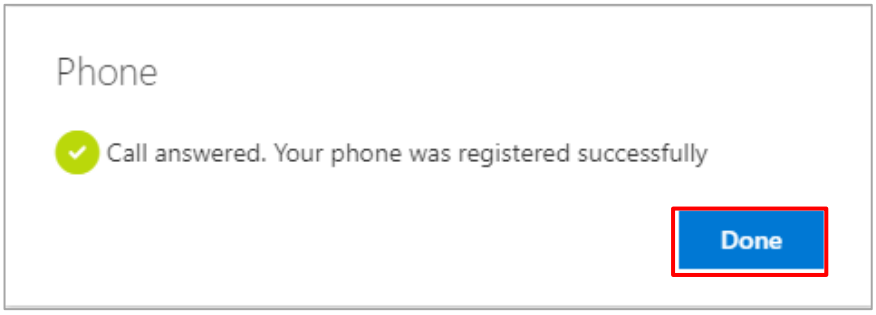
iv. **Press #** - this is known as the hash, pound or number key on a phone.

v. You should hear the message: "Your sign in was successfully verified".

vi. **End the call and return to the browser on your PC, Mac or Tablet.**

On your PC, Mac, or Tablet

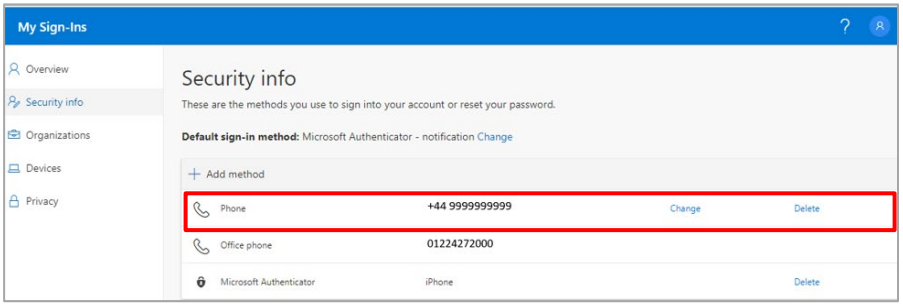
vii. You should see a message to indicate you have registered your mobile phone as an authentication method.



viii. Click **Done** and carry on to step 11.

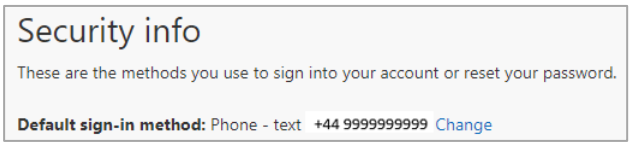
On your PC, Mac, or Tablet

11. Your phone will now appear on the list of methods of authentication:

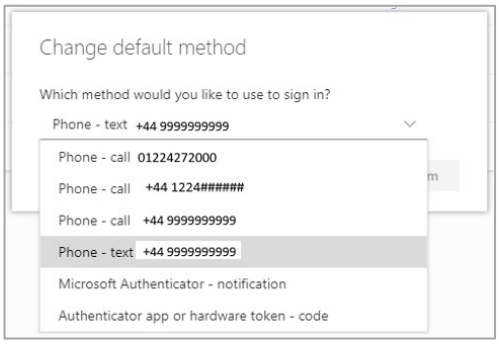


Note: If it is a mobile phone it will allow authentication by call or text, whichever way you chose to register it.

12. At top of the **My Sign-Ins** window, under **Security Info**, you will see what has been set as your **Default sign-in method** – for example **Phone – text**, as shown below.



13. Click **Change** to see other options and to select a different default sign-in method if required – for example **Phone – call**.



Note: If you have also set up the Microsoft Authenticator app, we recommend you set that as the Default sign-in method.

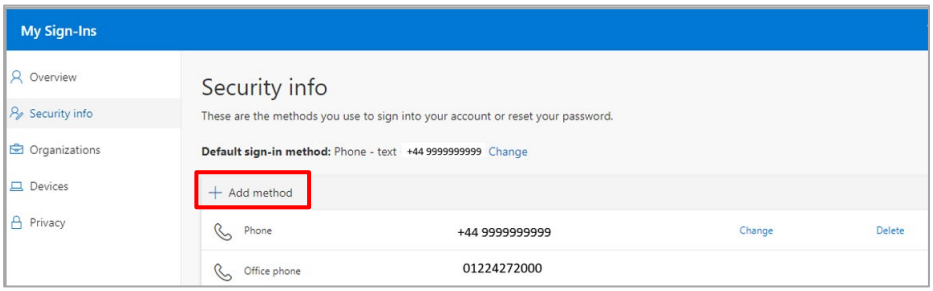
14. Now **go to Page 8** and follow the **Testing** Instructions

To set up an Alternate phone

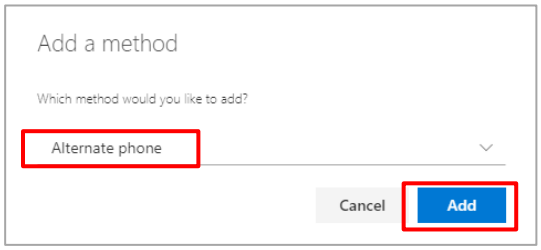
You can only set up one Phone to receive texts, but you can set up an Alternate phone to receive calls.

On your PC, Mac or Tablet

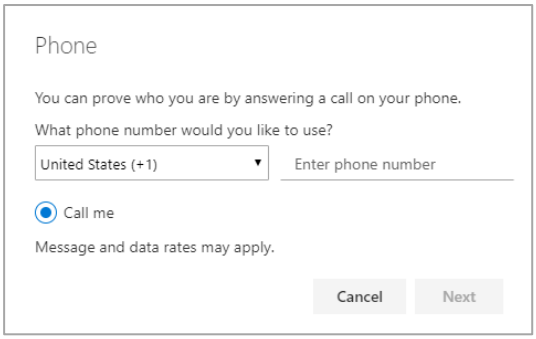
1. To add another, Alternate phone, click on **+ Add method**



2. Choose **Alternate phone** as your method and click **Add**

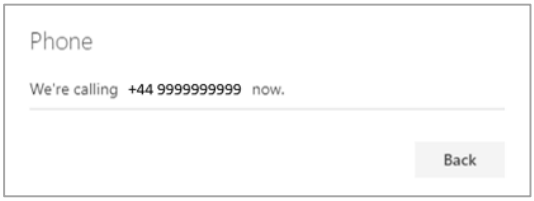


3. In the **Phone** window, enter the details of your phone, on which you want to receive notification, i.e. **country code** (from the drop-down) and **phone number**.



Note: You can only receive calls to an Alternate phone.

4. Click **Next**
5. You will see the following message:



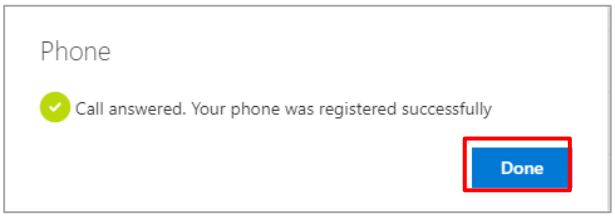
6. **LEAVING THE MESSAGE OPEN, go to your phone, which you have registered.**

On your mobile or home phone

7. **Answer** your phone – a voice message will instruct you to press the **Hash** or **Pound** key to finish your verification.
8. Open or view your phone's **keypad**.
9. **Press #** - this is known as the hash, pound or number key on a phone.
10. You should hear the message: "Your sign in was successfully verified".
11. **End the call and return to the browser on your PC, Mac or Tablet.**

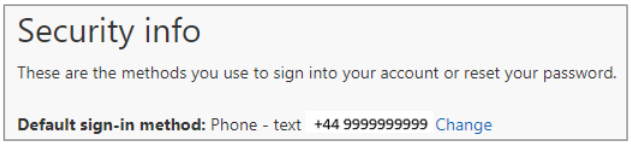
On your PC, Mac or Tablet

12. Click **Done** in the Phone window.

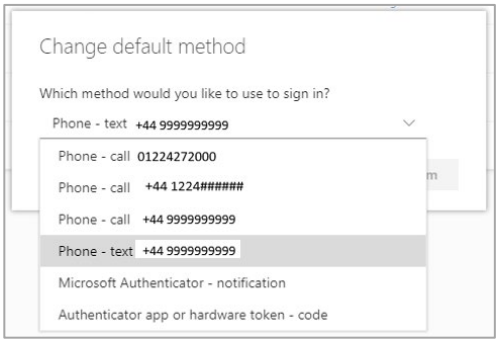


13. Your Alternate phone is now listed as a method of notification.

14. At top of the **My Sign-Ins** window, under **Security Info**, you will see what has been set as your **Default sign-in method** – for example **Phone – text**, as shown below.



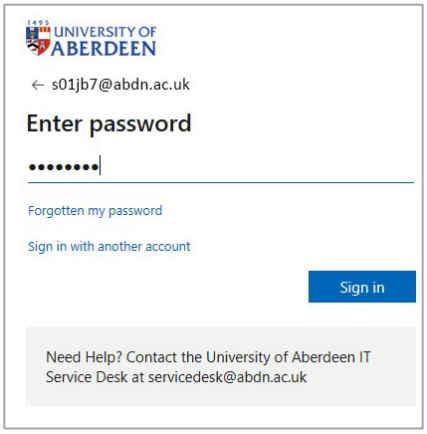
15. Click **Change** to see other options and to select a different default sign-in method if required – for example **Phone – call**.



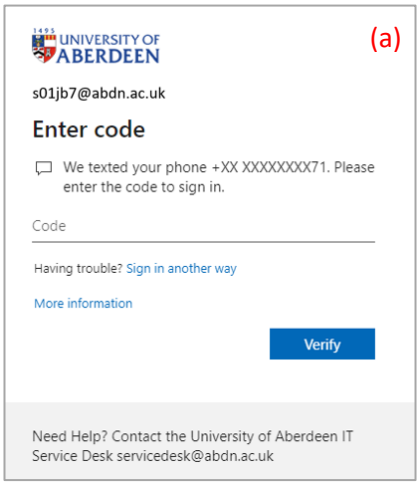
Note: If you have also set up the Microsoft Authenticator app, we recommend you set that as the Default sign-in method.

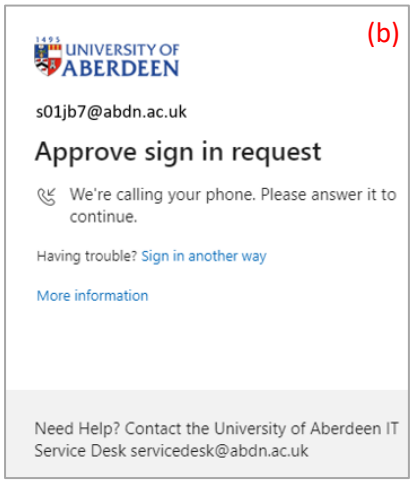
Testing authentication

1. In a browser on your PC, Mac or Tablet go to https://aka.ms/setupsecurityinfo
2. If you are already signed in, go to your Profile picture and choose **Sign out**.
3. **Sign in** again with *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
4. Enter your University **password** at the prompt



5. If prompted to stay signed in, click **No**.
6. From the menu on the left, click **Security Info**.
7. You will see an action briefly on screen followed by one of the dialogs shown below.
   - If you chose **Text** as the default sign-in method, a code will be sent to your mobile phone. Enter this in the box provided on screen and click **Verify**. (a)
   - If you chose **Call** as the default sign-in method, you will receive a call. Answer this and follow the instructions using your phone's keypad. (b)





8. The sign-in to your account is complete.

If the authentication method offered is not suitable or convenient at that time, you can choose **Sign in another way**. You will be presented with a list of all the authentication methods you have set up, from which you can choose an alternative.

9. When you have completed the set up and testing of authentication methods go to the profile icon at top right and choose **Sign Out**.

After you have set up Multi-factor Authentication…

What to expect on campus

You will see no difference when using the Outlook desktop client, OWA, SharePoint or Office 365 online on your desktop computer or on a University laptop when connected via direct access or uoa-corporate.

However, a device connected using *eduroam* is regarded as 'off campus'.

What to expect at home or off campus

If you were already signed into Office 365 apps – e.g. Outlook or OneDrive – on a smartphone or tablet, or the Outlook desktop client on a personal PC, you will be required to sign in again with the extra step of authenticating.

When you sign in to OWA, SharePoint, or Office 365 online you will be asked to authenticate, i.e. you will be prompted to:

- Enter *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
- Enter your University **password**
- Authenticate by text or call

Further information and help

If you have any questions or concerns contact the Service Desk: https://myit.abdn.ac.uk