

Multi-factor Authentication (MFA): Authenticator Phone (@aberdeen accounts)

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 email address 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 @aberdeen Microsoft account.

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 @aberdeen Microsoft Office 365 account.

You should set up two or more of these authentication methods:

- Use the Microsoft Authenticator app on a mobile device (recommended)
- Receive a code by text
- 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.

If you want to set up the Microsoft Authenticator app, please see our separate guide.

Set up an Authentication phone

Before you start, you will need:

- a phone – mobile or landline (home phone)
- a PC, Mac, or Tablet, open at a web browser
- a reliable internet connection



Set aside 10 minutes of uninterrupted time to work through this process.

You will be required to work on both your phone *and* PC, Mac, or Tablet during the setup.

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 @aberdeen email address* e.g. `j.bloggs2.18@aberdeen.ac.uk`
3. Enter your **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.

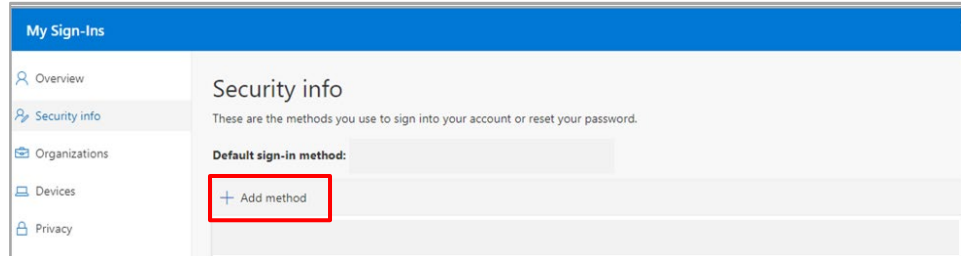
5. **Otherwise** the **My Sign-Ins** window will open.

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

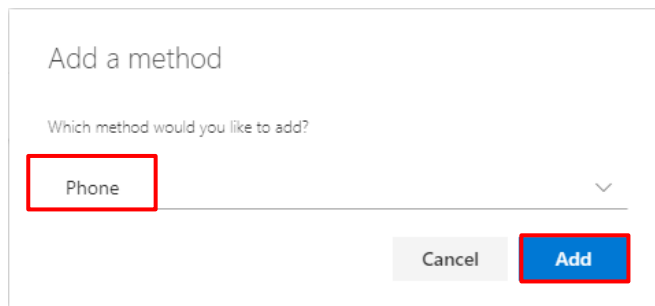
To be able to authenticate by receiving a notification (text or a call) to that phone, click on **Enable two-step notification** next to the number and follow the instructions from **step 8**.

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.

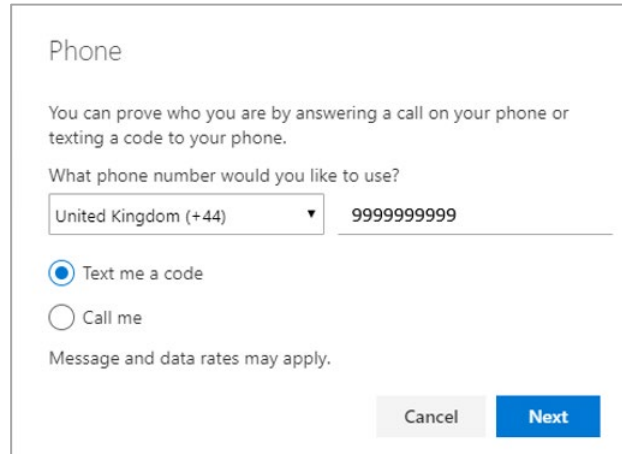
6. Click on **+ Add method**



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**.

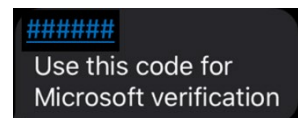
10. Click **Next**

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:

Phone

We just sent a 6 digit code to +44 9999999999 Enter the code below.

Enter code

[Resend code](#)

Back Next

- iii. Click **Next**
- iv. You should see a message to indicate you have registered your mobile phone as an authentication method.

Phone

✓ SMS verified. Your phone was registered successfully

Done

- 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:

Phone

We're calling +44 9999999999 now.

Back

On your mobile
or home phone

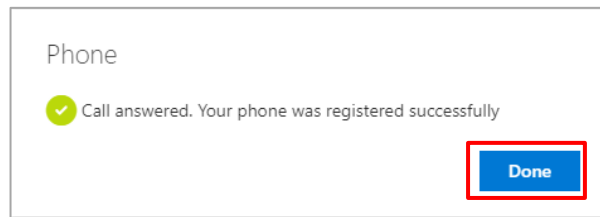


- ii. **Answer** your phone – a voice message will instruct you to press the **Hash** or **Pound** key to finish your verification.
- iii. Open or view your phone's **keypad**.
- iv. **Press #** - this is known as the hash, pound or number key on a phone.
- v. You should hear the message: "Your sign 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.

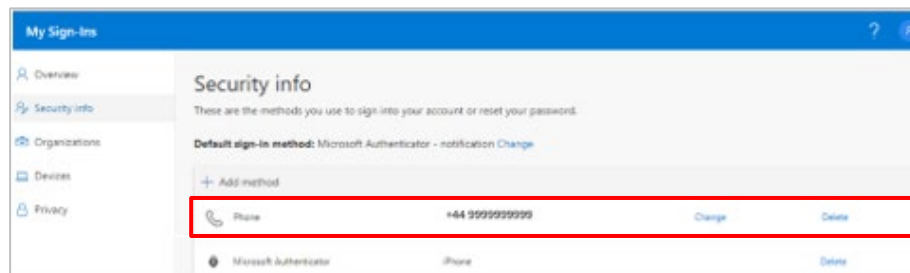


- viii. Click **Done** and carry on to step 11.

On your PC,
Mac or Tablet

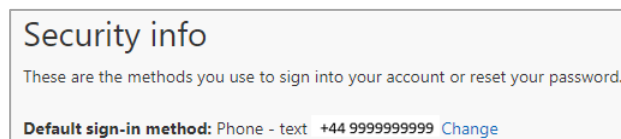


11. Your phone will now appear on the list of methods of authentication:

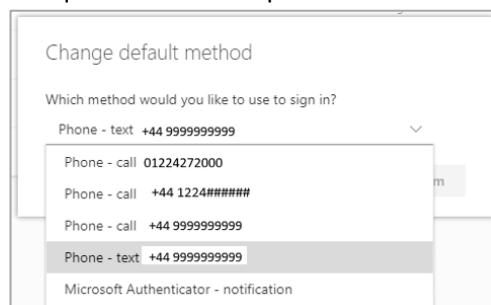


Note: If it is a mobile phone it will allow authentication by call or text, whichever way you chose to register it.

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.



At this point, we **strongly** recommend that you **set up a second method** of authentication. You can do this in the **My Sign-Ins** window:

1. Click on **+ Add method**
2. Choose **Alternate phone** and follow instructions below, *or* Choose **Authenticator app** and work through instructions in our separate [Microsoft Authenticator app guide](#).

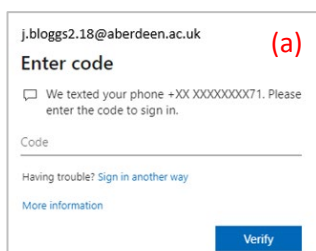
To set up an Alternate phone

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

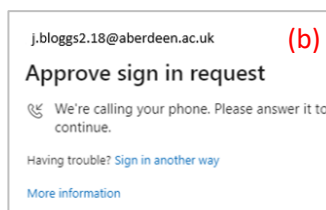
1. Open a browser and go to: <https://aka.ms/setupsecurityinfo>.
2. **Sign in** with *your @aberdeen email address*, e.g. j.bloggs2.18@aberdeen.ac.uk, and enter your **password** at the prompt.
3. In the **My Sign-Ins** window click on **+ Add method** (in the same way as above).
4. Choose **Alternate phone** as your method and click **Add**
5. 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.
6. Click **Next**
7. You will see a message that the Alternate phone is being called.
LEAVING THE MESSAGE OPEN, go to your phone, which you have registered.
8. **Answer** your phone – a voice message will instruct you to press the **Hash** or **Pound** key to finish your verification.
9. Open or view your phone's **keypad**.
10. **Press #** - this is known as the hash, pound or number key on a phone.
11. You should hear the message: "Your sign in was successfully verified".
12. **End the call and return to the browser on your PC, Mac, or Tablet.**
13. Click **Done** in the Phone window.
14. Your Alternate phone will now appear on the list of methods of authentication.

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 @aberdeen email address*, e.g. j.bloggs2.18@aberdeen.ac.uk
4. Enter your **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)



Dialog box (a) titled "Enter code" for user j.bloggs2.18@aberdeen.ac.uk. It contains a checkbox for "We texted your phone +XX XXXXXXXXX71. Please enter the code to sign in." and a text input field for the code. A "Verify" button is at the bottom right. Links for "Having trouble? Sign in another way" and "More information" are at the bottom left.



Dialog box (b) titled "Approve sign in request" for user j.bloggs2.18@aberdeen.ac.uk. It contains a phone icon and text: "We're calling your phone. Please answer it to continue." A "More information" link is at the bottom left.

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**.

What to expect after MFA is enabled on your account...

Help! I see a message saying my account is blocked! My email no longer works!

If you receive an email to say your account is blocked, or if your email/calendar no longer work on a smartphone, **don't panic!**

Your email account is not permanently blocked. It will be trying to connect using an old authentication method and we need it to use Modern Authentication as part of MFA.

To do this you can either:

- delete the account and set it up again, or
- install and use the Outlook app from the app store.

You will find guides to help you with this under the Help section below.

Already signed into Outlook?

If you were already signed into the Outlook app on a smartphone or tablet, or the Outlook desktop client on a personal computer, you will be required to **sign in again** with the extra step of authenticating.

From now on

Whether you use an email client or app, or Outlook Web Access (OWA) on any device, you will be asked to authenticate when you sign in to your @aberdeen email account, i.e. you will be prompted to:

- Enter *your* @aberdeen **email address** e.g. j.bloggs2.18@aberdeen.ac.uk
- Enter your **password**
- **Authenticate** by text or call

Further information and help

Use MyIT to report an issue with the IT Service Desk: <https://myit.abdn.ac.uk>

Configuration guides for email apps and clients

- [Office 365 email on iOS using Mail app](#)
- [Office 365 email on iOS using Outlook app](#)
- [Office 365 email on Android using Outlook app](#)
- [Office365 email on Mac using Apple Mail](#)