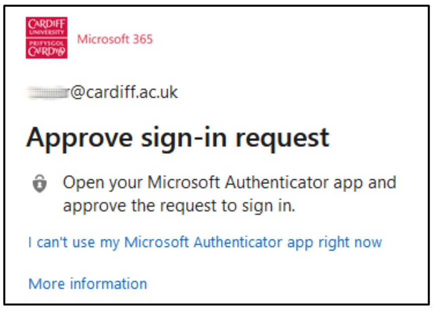
Using MS authenticator app to verify log in

Complete Multi-Factor Authentication (MFA) using the Microsoft Authenticator app that was previously installed and set up on your smartphone.

Being notified

1. When trying to use Microsoft Office 365, either through a web browser, mobile app, or desktop application, you might be prompted to complete MFA before being allowed to access your account.
2. Before the MFA prompt, you might be prompted to log in to Office365. If you are, do so as normal using your Cardiff University email address and password.
3. You will be notified that this sign-in attempt needs further approval through MFA, and that Microsoft have sent a notification to the smartphone upon which you previously set up the Microsoft Authenticator app.



Microsoft 365

[redacted]@cardiff.ac.uk

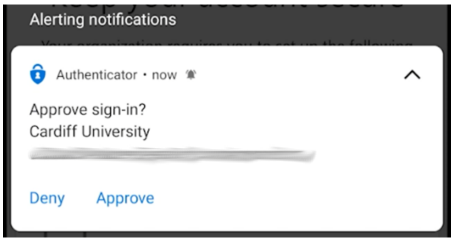
Approve sign-in request

Open your Microsoft Authenticator app and approve the request to sign in.

I can't use my Microsoft Authenticator app right now

More information

4. Your smartphone should then show a pop-up notification (or message on the lock screen), from the Microsoft Authenticator app, asking you to **Approve** or **Deny** the login attempt.

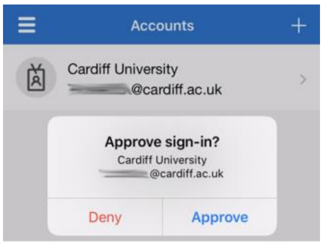


Alerting notifications

Authenticator • now

Approve sign-in?
Cardiff University
[redacted]

Deny Approve



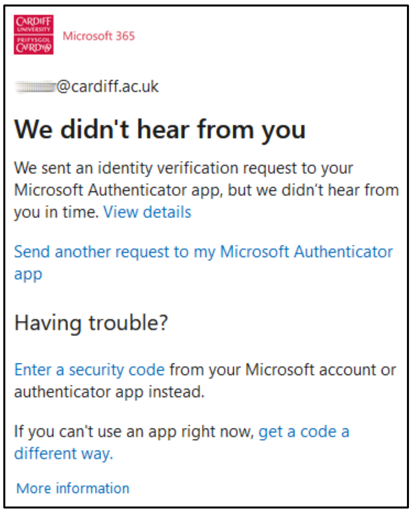
Accounts

Cardiff University
[redacted]@cardiff.ac.uk

Approve sign-in?
Cardiff University
[redacted]@cardiff.ac.uk

Deny Approve

5. If the Microsoft Authenticator app lock is active, you will need to enter your smartphone unlock code, or biometric (such as fingerprint or face recognition) before your response will be accepted.
6. If for some reason you are not able to respond to the notification in a timely manner, you will be offered another chance by clicking **Send another request to my Microsoft Authenticator app.**



[redacted]@cardiff.ac.uk

We didn't hear from you

We sent an identity verification request to your Microsoft Authenticator app, but we didn't hear from you in time. View details

Send another request to my Microsoft Authenticator app

Having trouble?

Enter a security code from your Microsoft account or authenticator app instead.

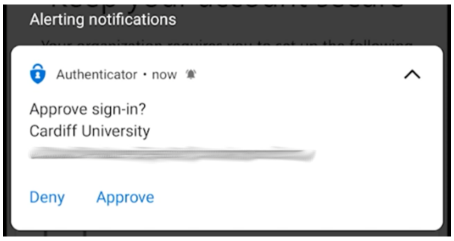
If you can't use an app right now, get a code a different way.

More information

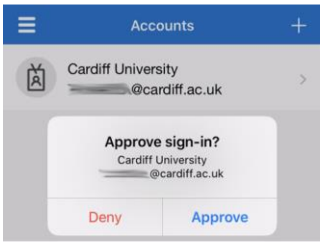
Approving or denying

Approving

1. Approving the sign-in attempt is a simple as tapping the **Approve** button on the pop-up notification.



Approve sign-in?
Cardiff University
[redacted]



Cardiff University
[redacted]@cardiff.ac.uk

Approve sign-in?
Cardiff University
[redacted]@cardiff.ac.uk

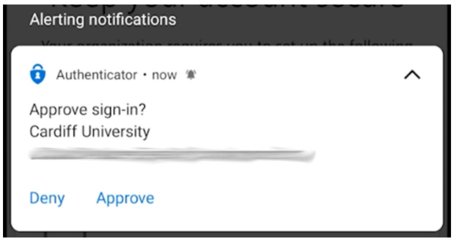
2. If the pop-up notification has disappeared, open the Microsoft Authenticator app on your smartphone, and it should display the prompt again.
3. Once you have tapped **Approve**, the pop-up notification should disappear from your smartphone, and the **Approve sign-in** request message should disappear from the web browser, mobile app, or desktop application, you were using – giving you access to your Office 365 account as intended.

   Please note: If you receive an MFA alert to confirm sign-in, but it is not you signing-in, it is possible someone is trying to illegally access your account. Do not approve the login, this ensures your account remains secure.

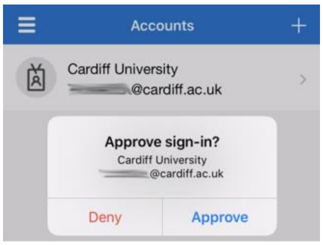
   If you receive multiple MFA alerts that are not you, it might be an indication that someone is trying to hack into your account. In this situation, please report this to the IT Service Desk who will investigate.

Denying

1. If it is not you attempting to sign-in, **Deny** the sign-in attempt to keep your account safe. Denying the sign-in attempt is as simple as tapping the **Deny** button on the pop-up notification.



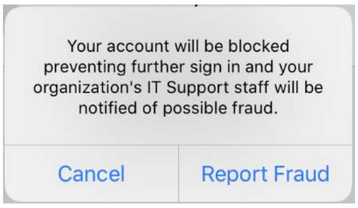
Approve sign-in?
Cardiff University
[redacted]



Cardiff University
[redacted]@cardiff.ac.uk

Approve sign-in?
Cardiff University
[redacted]@cardiff.ac.uk

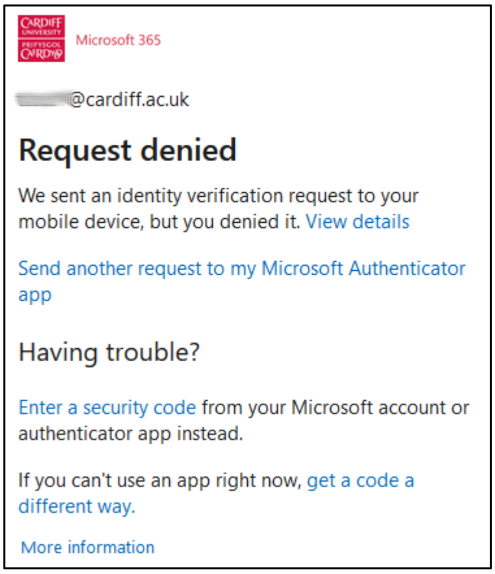
2. If the pop-up notification has disappeared, open the Microsoft Authenticator app on your smartphone, and it should display the prompt again.
3. Once you have tapped **Deny**, the pop-up notification on your smartphone will be replaced with a new pop-up notification asking you if you want to Report Fraud. In most circumstances it is sufficient to tap **Cancel.**



Your account will be blocked preventing further sign in and your organization's IT Support staff will be notified of possible fraud.

Please note: If you receive multiple MFA alerts that are not you, it might be an indication that someone is trying to hack into your account. In this situation, we advise that you either "Report Fraud" or contact the IT Service Desk who will investigate

4. The **Approve sign-in request** message on the web browser, mobile app, or desktop application, you were using will update to reflect that MFA was denied



Microsoft 365

[redacted]@cardiff.ac.uk

Request denied

We sent an identity verification request to your mobile device, but you denied it. View details

Send another request to my Microsoft Authenticator app

Having trouble?

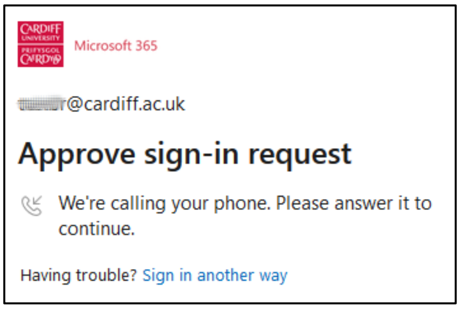
Enter a security code from your Microsoft account or authenticator app instead.

If you can't use an app right now, get a code a different way.

More information

Picking as an alternate method

1. If you are prompted to complete MFA using your default method, and instead you want to use the Microsoft Authenticator app that you have previously set up, you can click on **Sign in another way.** Or click on the left-pointing arrow found to the left of your email address



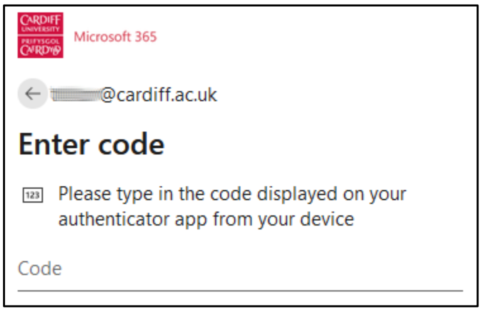
Microsoft 365

[redacted]@cardiff.ac.uk

Approve sign-in request

We're calling your phone. Please answer it to continue.

Having trouble? Sign in another way



Microsoft 365

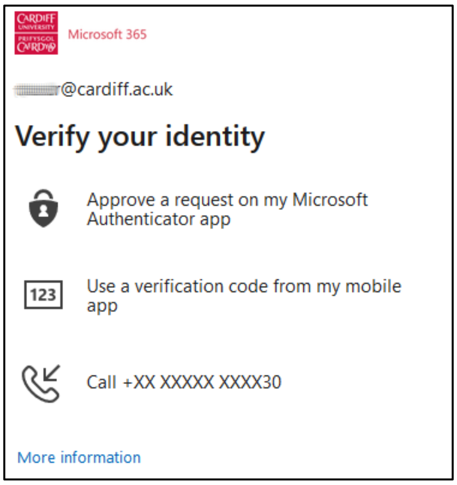
← [redacted]@cardiff.ac.uk

Enter code

Please type in the code displayed on your authenticator app from your device

Code

2. You will then be presented with a set of options on how to complete MFA. The exact options will depend upon which MFA methods you have previously configured.



Microsoft 365

[redacted]@cardiff.ac.uk

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Call +XX XXXXX XXXX30

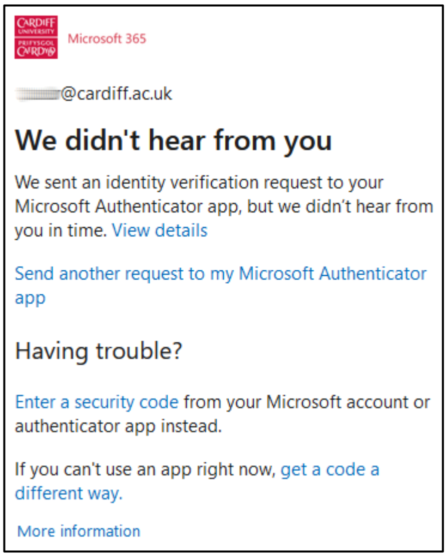
More information

Important: It is highly recommended that you set up several methods of completing MFA to ensure you can still access your account should you encounter difficulties with one of the methods.

3. To use the Microsoft Authenticator app, click on **Approve a request on my Microsoft Authenticator app** You can now complete MFA as described starting at the **Approving** section of this page

Using codes (including offline)

1. If you encounter an issue completing MFA using the Microsoft Authenticator app notifications, including if you do not have a connection to the internet, you can opt to use a verification code from the app instead. If you have encountered an issue, click on **Enter a security code**, otherwise click on **Sign in another way**, or click on the left-pointing arrow found to the left of your email address



Microsoft 365

[redacted]@cardiff.ac.uk

We didn't hear from you

We sent an identity verification request to your Microsoft Authenticator app, but we didn't hear from you in time. View details

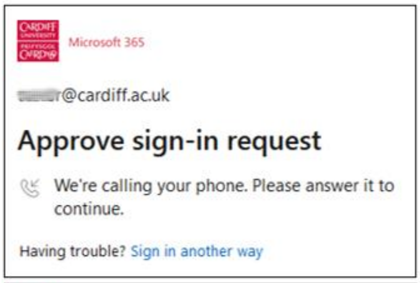
Send another request to my Microsoft Authenticator app

Having trouble?

Enter a security code from your Microsoft account or authenticator app instead.

If you can't use an app right now, get a code a different way.

More information



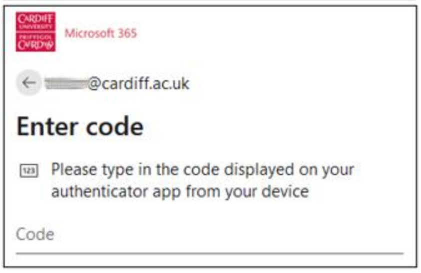
Microsoft 365

[redacted]r@cardiff.ac.uk

Approve sign-in request

We're calling your phone. Please answer it to continue.

Having trouble? Sign in another way



Microsoft 365

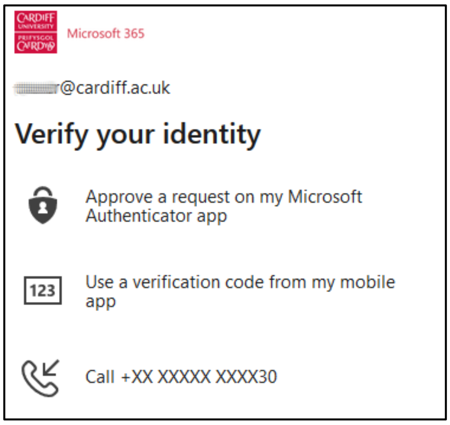
← [redacted]@cardiff.ac.uk

Enter code

Please type in the code displayed on your authenticator app from your device

Code

2. You will then be presented with a set of options on how to complete MFA to select between. The exact options will depend upon which MFA methods you have previously configured. Click on **Use a verification code from my mobile app**



Microsoft 365

[redacted]r@cardiff.ac.uk

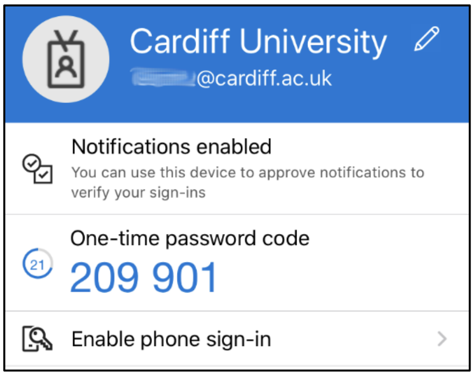
Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Call +XX XXXXX XXXX30

3. On your smartphone, open the Microsoft Authenticator app, and tap into your Cardiff University account. You will see a six-digit code entitled **One-time password code** displayed on screen which is replaced every 30 seconds. **Take note of the code displayed.**



Cardiff University

[redacted]@cardiff.ac.uk

Notifications enabled

You can use this device to approve notifications to verify your sign-ins

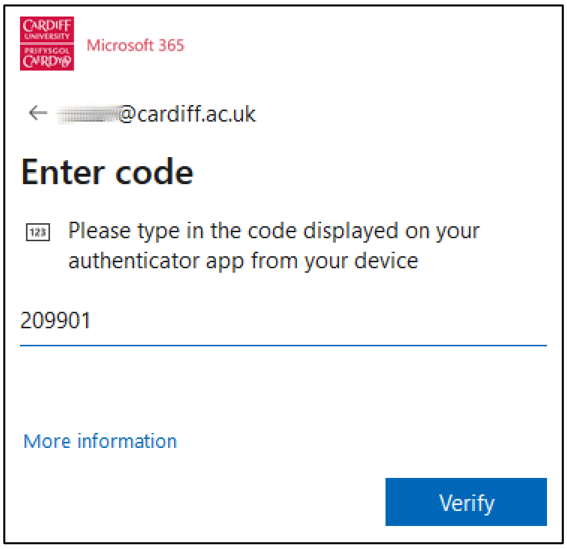
One-time password code

21

209 901

Enable phone sign-in

4. Enter the six-digit code into the popup message on the web browser, mobile app, or desktop application, you were using that prompted for MFA. Then click **Verify.**


Microsoft 365

← [redacted]@cardiff.ac.uk

Enter code

Please type in the code displayed on your authenticator app from your device

209901

These six-digit one-time password codes generated by the Microsoft Authenticator app on your smartphone will function correctly even if your smartphone does not have an active data connection at the time. Therefore, they are a valid mechanism for using the Microsoft Authenticator app offline.

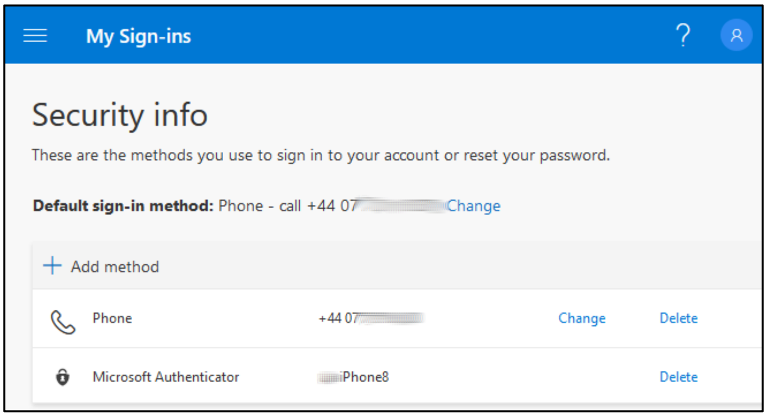
You need to enter the code and click Verify before the 30 seconds shown on the Microsoft Authenticator app expires, or the code will be invalid, and you will need to try again.

5. The **Enter code** message should disappear from the web browser, mobile app, or desktop application, you were using – giving you access to your Office 365 account as intended.

Setting as default method

If you have configured another MFA method (such as an automated phonecall or a different authenticator application) as your default method, you can alter this to make the Microsoft Authenticator app the default.

1. To start the process, use a web browser to navigate to https://aka.ms/mfasetup
2. You will be prompted to log in to Office365 using your Cardiff University email address and password. You might be challenged to complete MFA using one of the methods you have already set up.
3. After successfully logging in, you will be taken to the **My Sign-ins** page where you can review the MFA methods you have already set up so far. Next to **Default sign-in method**: click on **Change.**



My Sign-ins

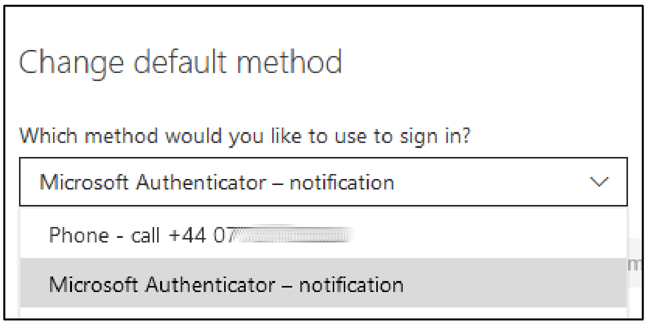
Security info

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

Default sign-in method: Phone - call +44 07[redacted] Change

Phone	+44 07[redacted]	Change	Delete
Microsoft Authenticator	[redacted]iPhone8		Delete

4. Pick **Microsoft Authenticator – notification** from the list of options.



Change default method

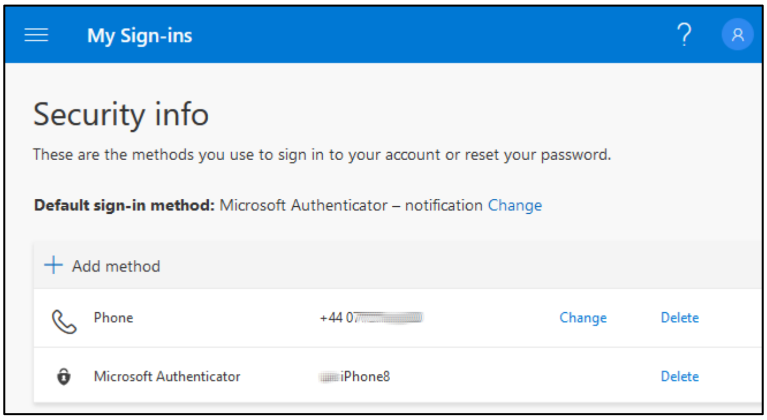
Which method would you like to use to sign in?

Microsoft Authenticator – notification

Phone - call +44 07[redacted]

Microsoft Authenticator – notification

5. The default sign-in method will now show **Microsoft Authenticator – notification.**



My Sign-ins

Security info

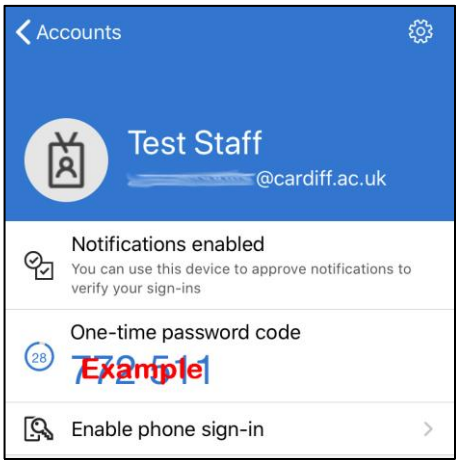
These are the methods you use to sign in to your account or reset your password.

Default sign-in method: Microsoft Authenticator – notification Change

Phone	+44 07[redacted]	Change	Delete
Microsoft Authenticator	[redacted]iPhone8		Delete

Renaming and removing your account

1. If you want to rename the entry for your account within the Microsoft Authenticator app, open the app on your smartphone, tap into your Cardiff University account, and then tap on the **cog icon** in the top right hand corner of the screen.



Accounts

Test Staff

[redacted]@cardiff.ac.uk

Notifications enabled

You can use this device to approve notifications to verify your sign-ins

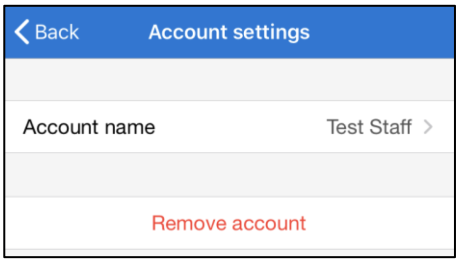
One-time password code

28

772 511 Example

Enable phone sign-in

2. Tap **Account name** to be able to enter a new description for how the app will refer to the account. Note this only affects how the Microsoft Authenticator app lists this account on your smartphone.



Back Account settings

Account name Test Staff

Remove account

3. If you need to remove this account from the Microsoft Authenticator app completely (for example because you need to undertake set up again on this or a different smartphone) tap on **Remove account**. If you understand the consequences of continuing (see note below), and are happy to proceed, tap as appropriate to confirm.

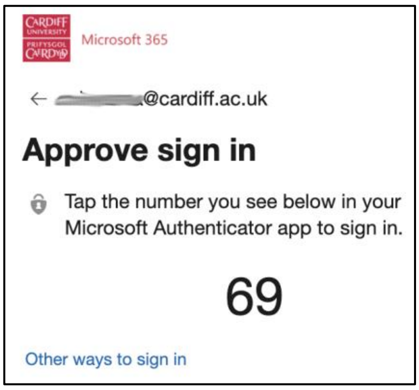
Important: Before you remove your account from the app, ensure that either you have set up the Microsoft Authenticator app on another smartphone and confirmed that it is functioning correctly with your account, or that you have other methods of completing MFA already set up and confirmed as working.

Otherwise you will find that you cannot complete MFA and will be locked out of your account.

Exiting phone sign-in

Important: Phone sign-in has not been configured and enabled at Cardiff University. If you accidentally activate this function, it will change your MFA experience, but will not operate correctly and will result in errors.

1. If your MFA prompt asks you to tap a corresponding two-digit number on the Microsoft Authenticator app, or if you receive an error message indicating that Your company policy requires that you use a different method to sign in, then you need to deactivate **Phone sign-in.**



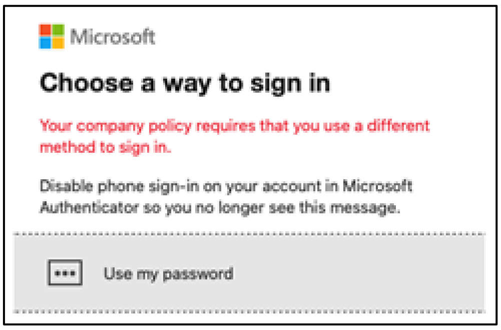
← [redacted]@cardiff.ac.uk

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

69

Other ways to sign in



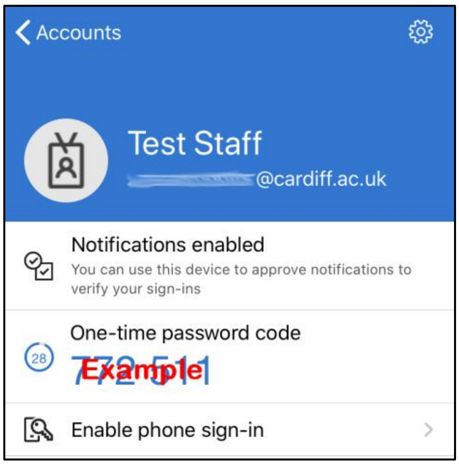
Choose a way to sign in

Your company policy requires that you use a different method to sign in.

Disable phone sign-in on your account in Microsoft Authenticator so you no longer see this message.

Use my password

2. Open the Microsoft Authenticator app on your smartphone and tap into your Cardiff University account. Then tap **Disable phone sign-in** and **confirm.**
3. The app should now show **Enable phone sign-in**, indicating that phone sign-in has been successfully disabled.



Test Staff

[redacted]@cardiff.ac.uk

Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

Example

Enable phone sign-in