

Office 365 Multi Factor Authentication Setup Guide

Applies to: Office 365 Applications/Remote Desktop & Applications

Prepared by: ICT



Contents

What is Multi-Factor Authentication?	2
Set Up Multi-Factor Authentication.....	2
Set up Multi Factor Authentication on a mobile device	3
Set up Multi factor Authentication Using a Desk/Home Phone	7
Troubleshooting.....	10
I have previously set up multi factor authentication but wish to change my method or add additional information	10
I have set up MFA but am unable to access resources.....	12
I have previously set up multi factor authentication but cannot receive notifications.....	12

What is Multi-Factor Authentication?

Multi-Factor Authentication (otherwise known as MFA or 'two-step verification') is a security feature included with Office 365 that protects your Office 365 account. MFA effectively makes it far more difficult for hackers to access your account, thus providing a further layer of protection for your data. MFA differs from using only a traditional username and password in that it also requires confirmation of the device that you are accessing your account from.

The two methods that are commonly used to prove your identity are your username and password along with a unique item that you have (e.g. mobile phone).

When logging in with MFA, you must supply your username/password AND additionally prove that you are in possession of a trusted device (i.e. phone.)

Due to the ongoing threat of internet based data breaches, it is a requirement at Concord College that MFA is enabled when accessing Office 365 enabled applications outside of the confines of the internal network to protect Staff and Student Office 365 linked user accounts. This means that you will be required to set up MFA if you are accessing Office 365 Creative Cloud/Office 365 applications and your new Office 365 mailbox from outside the college.

Set Up Multi-Factor Authentication

It is always recommended that a Mobile Phone or Android/Apple tablet device is used as your primary method of Multi Factor authentication.

If you DO have access to a mobile phone, please follow the instructions for 'Set up Multi Factor Authentication on a mobile device'

If you DO NOT have access to a mobile phone, please follow instructions for 'Set up Multi factor Authentication Using a Desk/Home Phone'

Set up Multi Factor Authentication on a mobile device

To set up Multi Factor Authentication for your Office 365 account:

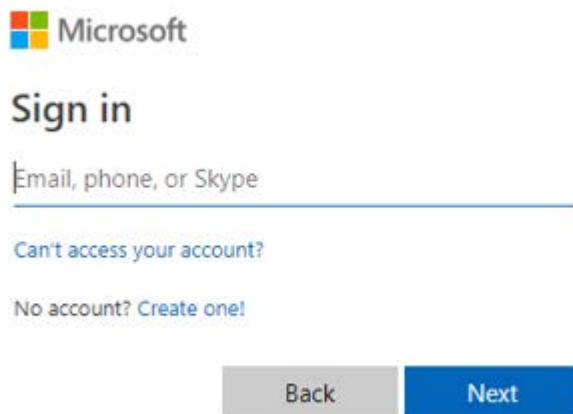
1. Please install the Microsoft Authenticator app from your supported AppStore on your mobile phone or mobile device. Below are direct links for the various supported platforms:

Android: <https://go.microsoft.com/fwlink/p/?LinkId=722778>

iOS: <https://go.microsoft.com/fwlink/p/?LinkId=722779>

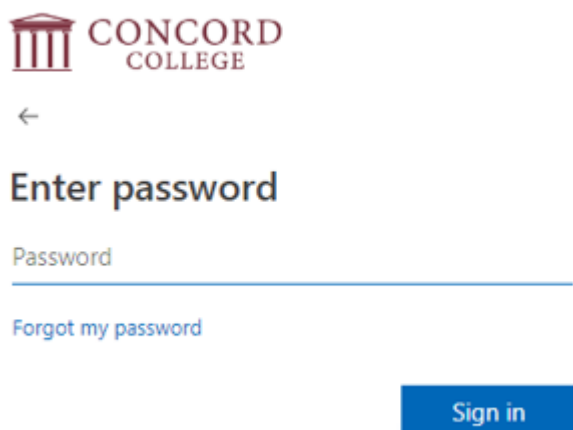
Windows Phone: <https://go.microsoft.com/fwlink/p/?LinkId=722777>

2. Open your web browser on your workstation/laptop/surface and go to <https://aka.ms/MFASetup>. Click 'Sign In'
3. Enter your Concord College email address and click 'Next'



The image shows the Microsoft sign-in interface. At the top left is the Microsoft logo. Below it is the text "Sign in". There is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "Can't access your account?" and "No account? Create one!". At the bottom are two buttons: a grey "Back" button and a blue "Next" button.

4. Please enter your usual network login password and click 'Sign In':



The image shows the Concord College sign-in interface. At the top left is the Concord College logo, which consists of a red building icon and the text "CONCORD COLLEGE". Below the logo is a left-pointing arrow. The main heading is "Enter password". There is a text input field with the placeholder text "Password". Below the input field is a link: "Forgot my password". At the bottom center is a blue "Sign in" button.

5. You will be redirected to the following page. Click Next:



More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

6. You will now see the Additional security verification/Multi Factor authentication setup page and have several options.

Choose **'Mobile App'** and select **'Receive notifications for verification'**. Click **'Set Up'**:

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

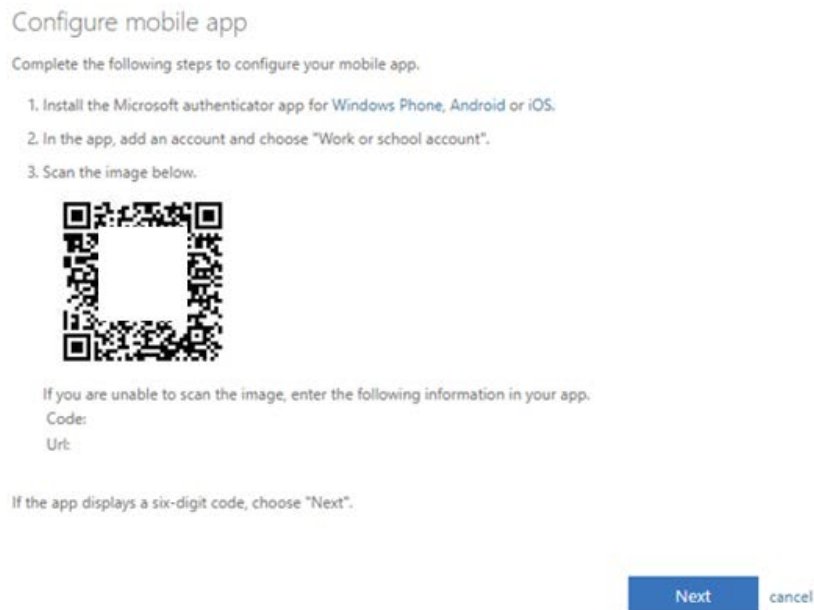
To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

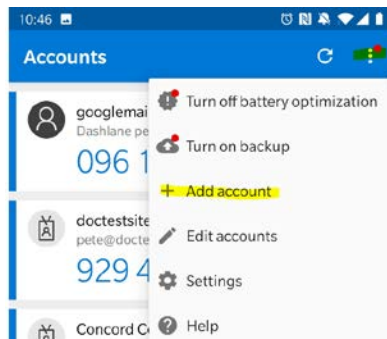
Mobile app has been configured.

Next

7. The following pop up box will appear, displaying a 'QR' code:



8. Open the Microsoft Authenticator app on your phone.
9. Tap + > Work or school account or choose 'Add account' from the options menu (on some devices you may need to access the 'Add account' option from the app menu:



Note: On first run, you may be also asked if you would like to add an account. Please skip this. It is important that you choose 'Work or school account' if presented with the option and that you do not select any other account type.

10. Use your phone to scan the QR square that is displayed on your computer screen.
11. Your account will be added automatically to the app and will display a six-digit code.
12. Switch back to your computer and click 'Next'.
13. Now wait for the 'Checking activation status' text to finish configuring your phone.
14. On your computer, ensure that 'Receive notifications for verification' is selected and click 'Next'.
15. Switch back to your phone and you'll see a notification for a new sign in.
16. Go to the Microsoft Authenticator app.
17. Tap Approve to allow it.

18. Back on the computer, follow any prompts that you might see such as adding a mobile number.

Note: It is recommended that you add a mobile number as this may be used as a secondary method of authentication. Click 'Finished' when complete.

CONCORD COLLEGE

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 3: In case you lose access to the mobile app

United Kingdom (+44)

Phone number can contain only the digits 0-9, dashes, spaces, full stops and parentheses.

[Finished](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft Legal | Privacy

19. You will now be redirected to an 'Additional Security verification web page'. You can add or amend details to this page as required and add further methods of Multi Factor Authentication as required. Once you are happy with the details entered you can safely close the window.

CONCORD COLLEGE

pk:1803scuser:1@concordcollege.org.uk | ?

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default:

Notify me through app

how would you like to respond?

Set up one or more of these options. [Learn more](#)

Authentication phone: United Kingdom (+44)

Office phone: Select your country or region Extension:

Alternative authentication phone: United Kingdom (+44) Phone number can contain only the digits 0-9, dashes, spaces, full stops and parentheses.

Authenticator app or Token: [Set up Authenticator app](#)

Authenticator app - ONEPLUS A5010: [Delete](#)

[Save](#) [Cancel](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

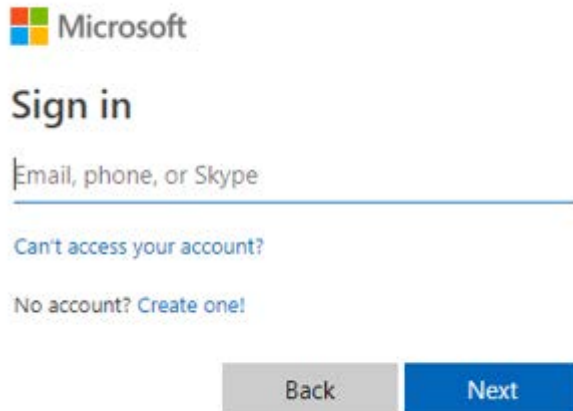
©2020 Microsoft Legal | Privacy

20. From now on, whenever you have a new sign in or add your Office 365 work or school account to an app, you'll open the Authenticator app on your phone and tap Approve.

If you have any issues setting up MFA you should contact the ICT department for further assistance.

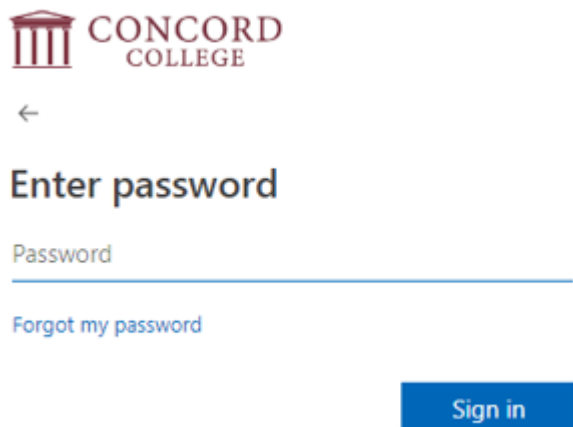
Set up Multi factor Authentication Using a Desk/Home Phone

1. Open your web browser and go to <https://aka.ms/MFASetup>. Click 'Sign In'
2. Enter your Concord College email address and click 'Next'



The image shows the Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the heading "Sign in". There is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "Can't access your account?" and "No account? Create one!". At the bottom are two buttons: a grey "Back" button and a blue "Next" button.

3. Please enter your usual network login password and click 'Sign In':



The image shows the Concord College sign-in page. At the top left is the Concord College logo, which consists of a red building icon and the text "CONCORD COLLEGE". Below the logo is a left-pointing arrow. The heading "Enter password" is centered. Below it is a text input field with the placeholder text "Password". Below the input field is a link "Forgot my password". At the bottom center is a blue "Sign in" button.

- You will be redirected to the following page. Click Next:



More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

- You will be presented with an 'Additional security verification page'
- In Step 1: How should we contact you?, choose **Authentication Phone**. Choose your region and enter your contact number. In the 'Method' section choose **Call me**

A screenshot of a web page titled "Additional security verification" for Concord College. The page includes a sub-header "Step 1: How should we contact you?". It features a dropdown menu for "Authentication phone" set to "United Kingdom (+44)", a text input field for a phone number, and a "Method" section with two radio button options: "Send me a code by text message" and "Call me", with "Call me" selected. A blue "Next" button is located at the bottom right. A footer note states: "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply." The footer also contains copyright information: "© 2020 Microsoft | Legal | Privacy".

- Click 'Next'
- You will now receive a phone call from the Microsoft Multi factor Authentication Center.
- Press the # key on your phone to approve.
- Click 'Finished'

11. You will now be presented with an 'Additional security verification' page. You may enter further details.in to this page to allow alternative multi factor authentication methods.

CONCORD COLLEGE

pk.1803scuser.1@concordcollege.org.uk

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
View video to know how to secure your account.

what's your preferred option?

We'll use this verification option by default.

Call my authentication phone nu

how would you like to respond?

Set up one or more of these options. [Learn more](#)

- Authentication phone
United Kingdom (+44) [Phone number field] Phone number can contain only the digits 0-9, dashes, spaces, full stops and parentheses.
- Office phone
Select your country or region [Country dropdown] [Phone number field] [Extension field]
- Alternative authentication phone
United Kingdom (+44) [Phone number field]
- Authenticator app or Token
[Set up Authenticator app](#)

Authenticator app - ONEPLUS A5010 [Delete](#)

[Save](#) [Cancel](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft [Legal](#) | [Privacy](#)

12. Click Save. Multi factor authentication setup is now complete.

If you have any issues setting up MFA you should contact the ICT department for further assistance.

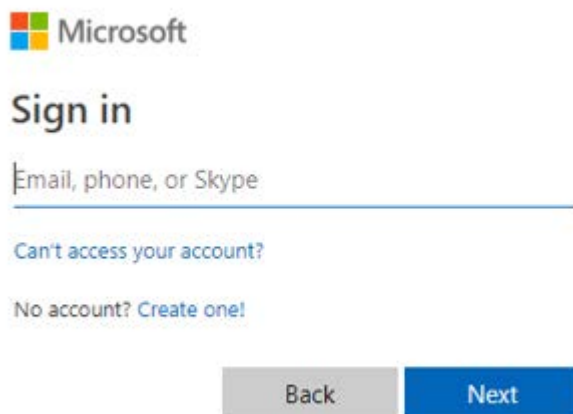
Troubleshooting

I have previously set up multi factor authentication but wish to change my method or add additional information

If you have previously set up MFA but would like to change your method to either notification via the Microsoft Authenticator app or receive a phone call, please follow the instructions below.

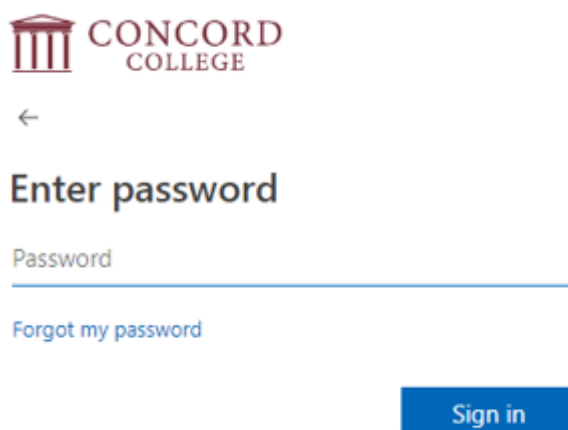
PLEASE NOTE: In order to access Office 365 applications(including Teams, OneNote) and remote desktop/applications, it is a requirement that you set up MFA to receive a notification to the Microsoft Authenticator app or receive a phone call

1. Open your web browser on your workstation/laptop/surface and go to <https://aka.ms/MFASetup>. Click 'Sign In'
2. Enter your Concord College email address and click 'Next'



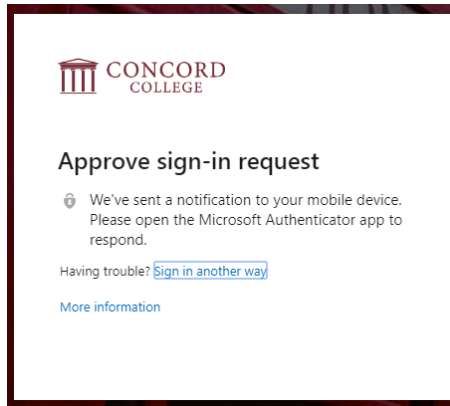
The image shows the Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the heading "Sign in". There is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "Can't access your account?" and "No account? Create one!". At the bottom of the form are two buttons: a grey "Back" button and a blue "Next" button.

3. Please enter your usual network login password and click 'Sign In':

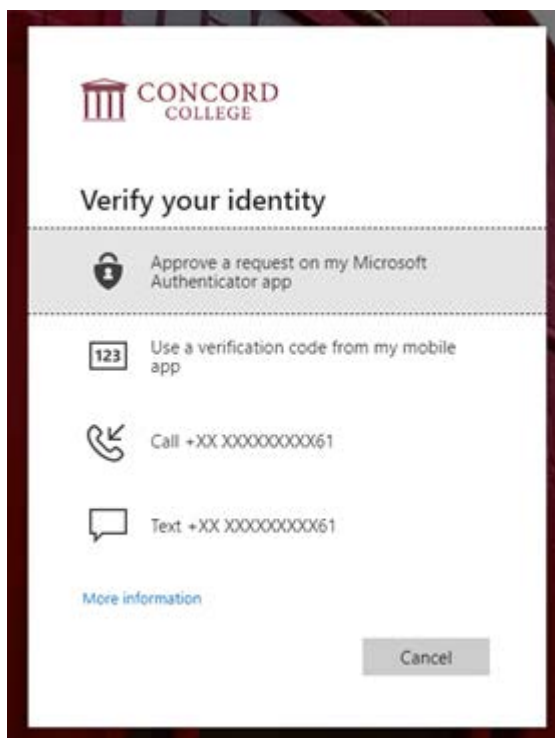


The image shows the Concord College login page. At the top left is the Concord College logo, which consists of a stylized building icon and the text "CONCORD COLLEGE". Below the logo is a left-pointing arrow. The heading "Enter password" is centered. Below it is a text input field with the placeholder text "Password". Below the input field is a link that says "Forgot my password". At the bottom right of the form is a blue "Sign in" button.

4. You will be prompted to approve your sign in request. Your approval will depend on how you originally set up Multi factor authentication.
 - a. If you previously set up approval via the Microsoft Authenticator app, you will be sent an MFA prompt to your phone.



- b. If you previously set up approval via a text to your mobile phone(or any other method), you can choose to receive a code another way



5. Once you have approved, you will receive the additional security verification page:

CONCORD COLLEGE

pk.1803sciuser.1@concordcollege.org.uk

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Call my authentication phone number

how would you like to respond?

Set up one or more of these options. [Learn more](#)

- Authentication phone: United Kingdom (+44) [Phone number field] [Extension field] Phone number can contain only the digits 0-9, dashes, spaces, full stops and parentheses.
- Office phone: Select your country or region [Phone number field] [Extension field]
- Alternative authentication phone: United Kingdom (+44) [Phone number field] [Extension field]
- Authenticator app or Token: [Set up Authenticator app](#)

Authenticator app - ONEPLUS A5010 [Delete](#)

[Save](#) [Cancel](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

© 2020 Microsoft Legal | Privacy

6. Please follow the instructions for 'Set up multi factor authentication' on a mobile device.

I have set up MFA but am unable to access resources

If you have previously set up multi factor authentication but are unable to access your resources, or MFA fails, it is likely that you do not have the correct multi factor authentication method setup.

Please follow the instructions in the troubleshooting section for 'I have previously set up multi factor authentication but wish to change my method or add additional information'

I have previously set up multi factor authentication but cannot receive notifications

This may occur if e.g you lose access to your mobile app or change your phone number. In this instance you should contact the ICT Helpdesk (helpdesk@concordcollege.org.uk) and they will reset your MFA status for you. You may then set up MFA as required using the instructions provided in this document.