



# Multi-factor authentication methods for returning students

When you use the Student Desktop application, only two authentication methods work:

1. The mobile authentication app
2. receiving an automated phone call

If you are using the web link, Student Desktop will work with any authentication method.

You only need to do this set up once.

The steps below will detail out how to set your authentication methods. Select one method and click on it.


## Contents

Method 1 – authentication phone call.....	1
Method 2 – authentication app .....	4

## Method 1 – authentication phone call

Follow this link: [Register for MFA here](#)

When you log on to your Office 365 account, you'll receive a prompt for more information. Click **Next**:



ashanks@sruc.ac.uk

### More information required

Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

If you have already logged on in the past, you may see the option below to select an account, choose the appropriate SRUC account:



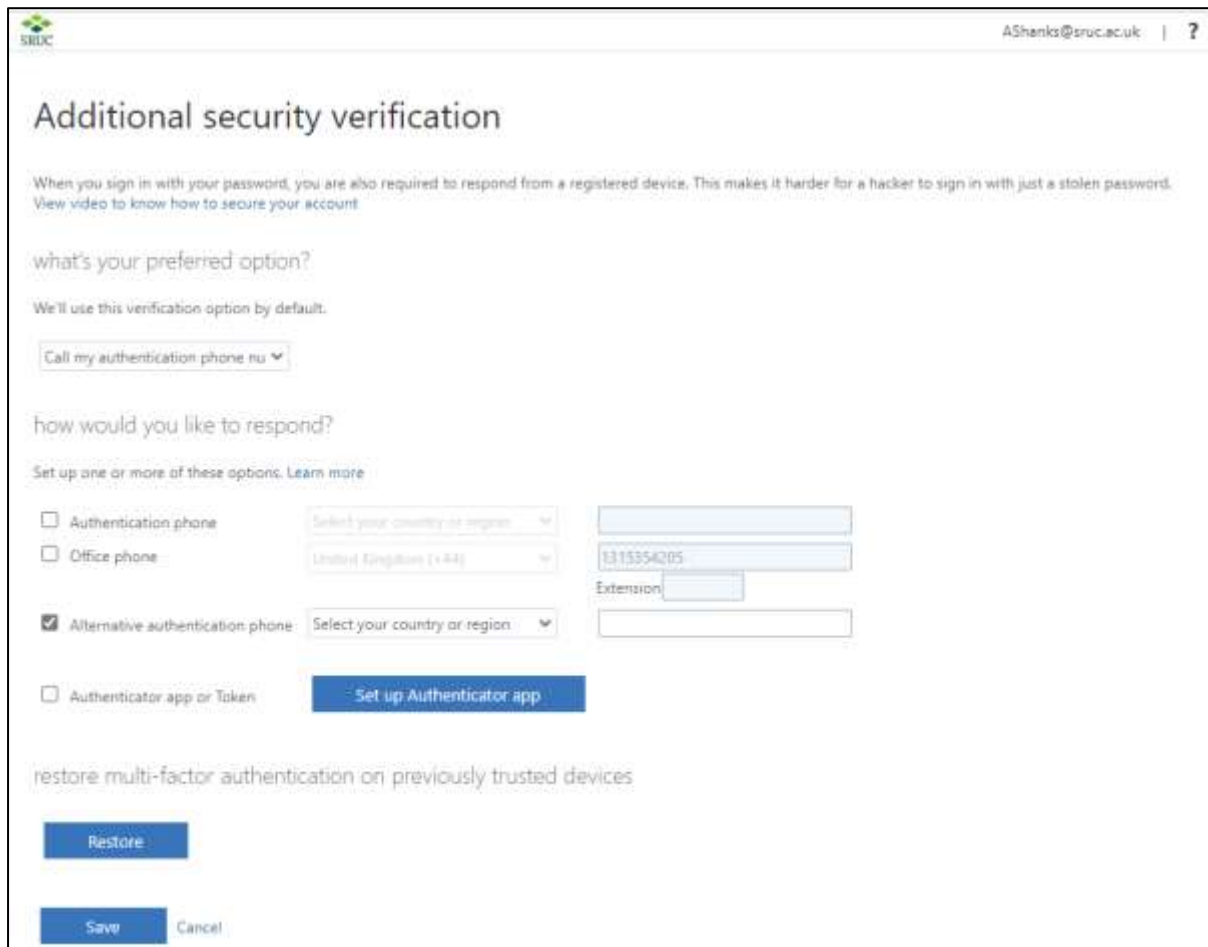
### Pick an account

---



Anne Shanks  
AShanks@sruc.ac.uk  
Connected to Windows

The next screen you should see is this:



The screenshot shows a web interface for 'Additional security verification'. At the top left is the SRUC logo, and at the top right is the email address 'AShanks@sruc.ac.uk' with a help icon. The main heading is 'Additional security verification'. Below it is a paragraph explaining that a registered device is required for sign-in and a link to 'View video to know how to secure your account'. The section 'what's your preferred option?' has a dropdown menu currently set to 'Call my authentication phone number'. Below this, the text 'We'll use this verification option by default.' is shown. The section 'how would you like to respond?' includes a link 'Set up one or more of these options. Learn more'. There are four options: 'Authentication phone' (unchecked), 'Office phone' (unchecked), 'Alternative authentication phone' (checked), and 'Authenticator app or Token' (unchecked). The 'Alternative authentication phone' option is expanded, showing a 'Select your country or region' dropdown set to 'United Kingdom (+44)', a phone number field containing '1315354205', and an 'Extension' field. A blue button 'Set up Authenticator app' is also visible. At the bottom, there is a 'restore multi-factor authentication on previously trusted devices' section with a 'Restore' button, and 'Save' and 'Cancel' buttons at the very bottom.

Under **What's your preferred option**, click the drop down and choose **Call my authentication phone number**.

Next, make sure **Authentication phone** is ticked and your phone number is in the field next to it.

Click **Save**.

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) 0123456789

☐ Office phone Select your country or region

☐ Alternative authentication phone Select your country or region

☐ Authenticator app or Token Set up Authenticator app

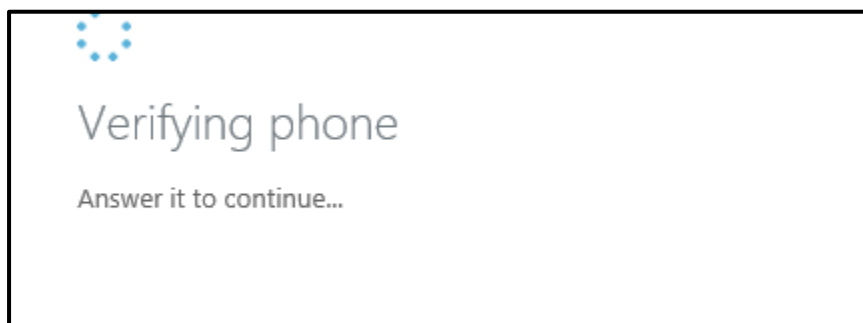
Authenticator app - emma\_gunning's iPhone Delete

restore multi-factor authentication on previously trusted devices

Restore

Save Cancel

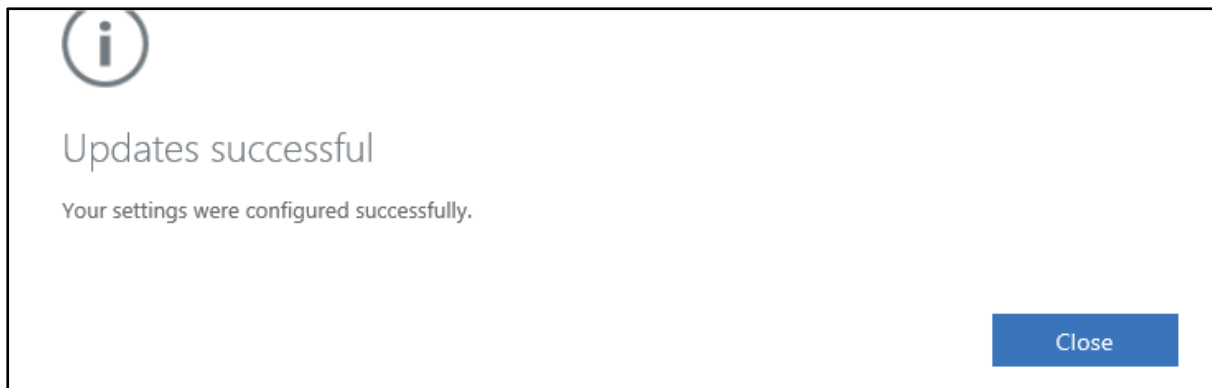
On your PC screen you will see a prompt that it is verifying and to answer the call:



When you answer your phone, you will hear an automated message asking you to press the hash # key to verify.

Press the # key on your keypad. The automated call will say it was successful then say goodbye.

On your screen you will see a message to say it's successful. Click **Close** once finished.



## Method 2 – authentication app

**Follow the instructions below if you want to use the authentication app to authorise logon.**

Before you start, you will need:

- An Android or iOS device such as a smartphone or tablet
- Access to a computer with internet access

If you do not have a smartphone but have another suitable phone to receive a call, you will need to follow “method 1” above.

### Register

On your PC, follow this link: [Register for MFA here](#)

Log on to your account using the format [studentnumber@sruc.ac.uk](#) and your password. For example, [S12345667@sruc.ac.uk](#)

You will then receive a prompt for more information. Click **Next**:



ashanks@sruc.ac.uk

## More information required

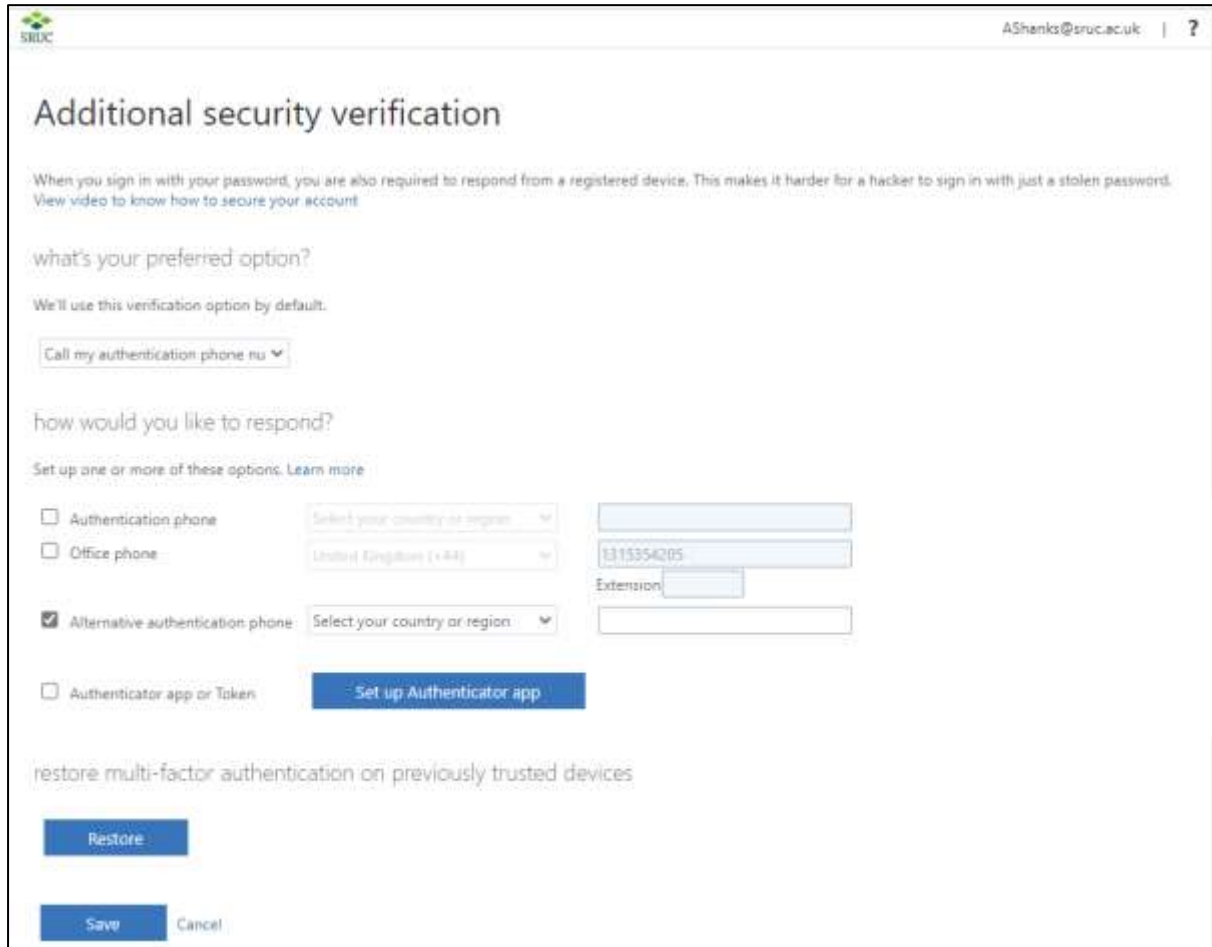
Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

The next screen you should see is this:



The screenshot shows the 'Additional security verification' page for a SRUC account. The page title is 'Additional security verification'. Below the title, there is a message: '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'. The page is divided into two main sections: 'what's your preferred option?' and 'how would you like to respond?'. In the 'what's your preferred option?' section, there is a dropdown menu with 'Call my authentication phone number' selected. In the 'how would you like to respond?' section, there are four options: 'Authentication phone' (unchecked), 'Office phone' (unchecked), 'Alternative authentication phone' (checked), and 'Authenticator app or Token' (unchecked). The 'Alternative authentication phone' option is selected, and there are input fields for 'Select your country or region' (United Kingdom (+44)), 'Phone number' (1315354205), and 'Extension'. There is a 'Set up Authenticator app' button. At the bottom, there is a 'restore multi-factor authentication on previously trusted devices' section with a 'Restore' button. At the very bottom, there are 'Save' and 'Cancel' buttons.

SRUC AShenks@sruc.ac.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
- ☐ Office phone    
Extension
- ☒ Alternative authentication phone
- ☐ Authenticator app or Token [Set up Authenticator app](#)

restore multi-factor authentication on previously trusted devices

[Restore](#)

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

This is where you set up your authentication method.

Under the option: **What's your preferred option?** choose "Notify me through the app"

**Additional security verification**

When you sign in with your password, you are also required to respond  
[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 ▼

- Call my authentication phone number
- Text code to my authentication phone number
- Call my office phone number
- Notify me through app
- Use verification code from app or token

☐ Authentication phone

☐ Office phone

Under the option: **How would you like to respond?** select the box next to “Authenticator app or Token” and then click on the button “Set up Authenticator App”

**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

☐ Office phone

☐ Alternative authentication phone

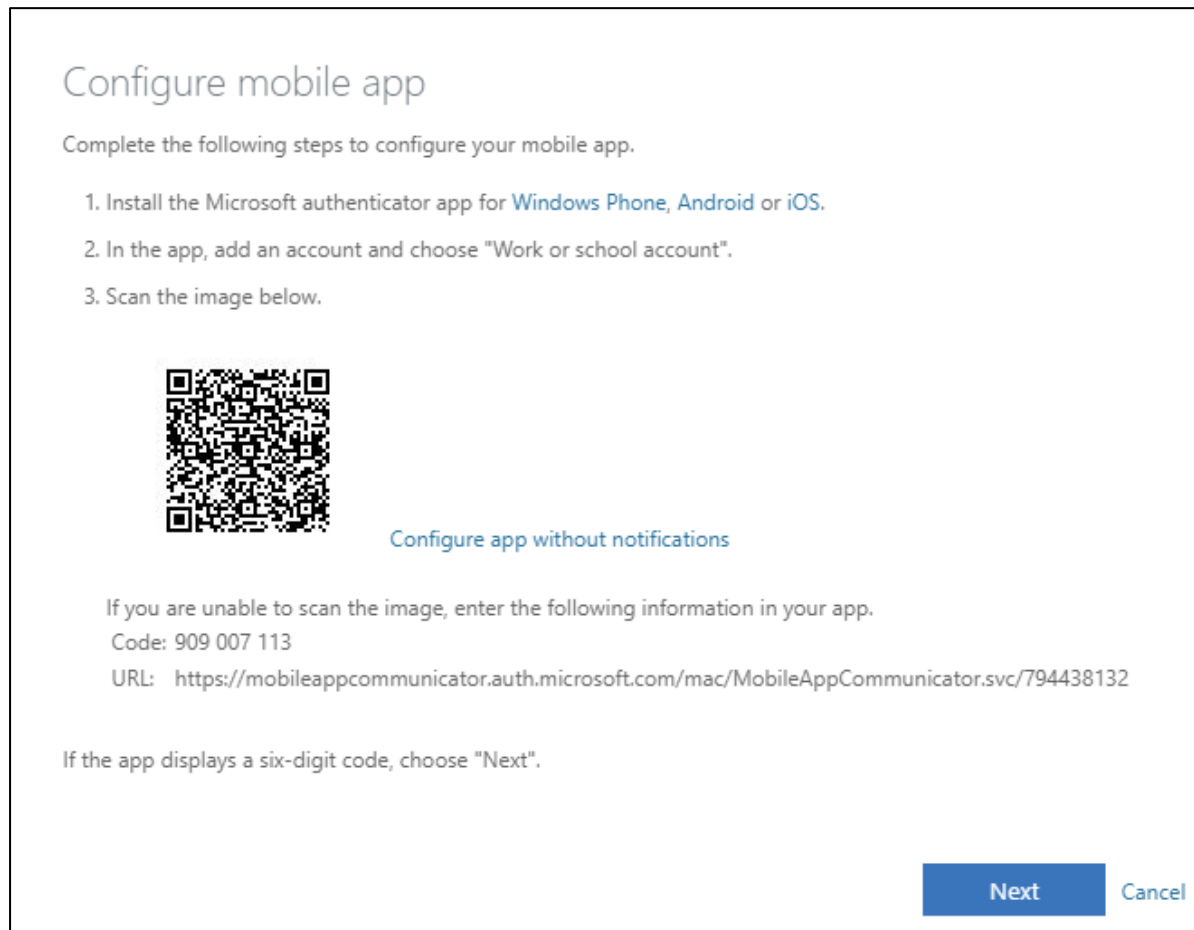
☒ Authenticator app or Token

restore multi-factor authentication on previously trusted devices

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



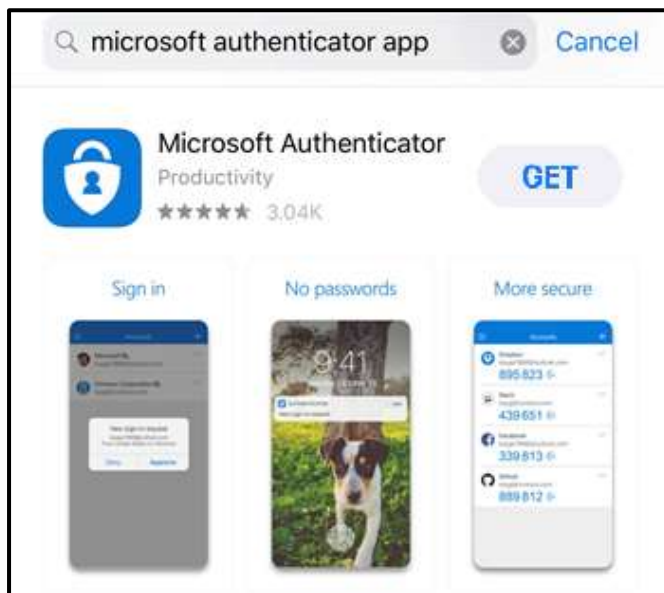
You should now see a screen similar to this:



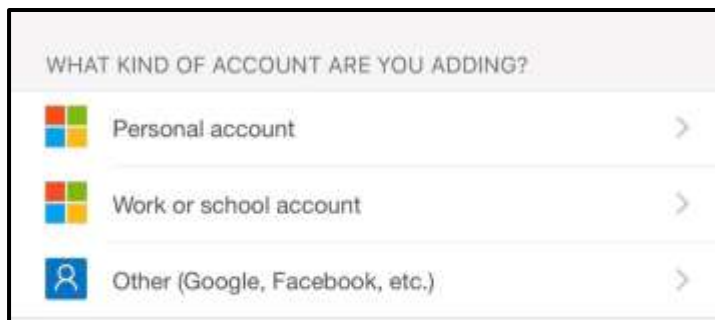
**Please note – the above graphic (QR Code) is an example only. Do not try to scan it. You need to scan the QR code that appears on the web page**

At this point you need to switch to your mobile device. The steps below tie in with the steps in the screenshot on the previous page.

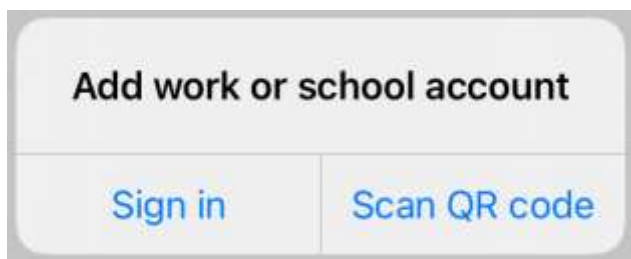
1. Install the app. On your phone, go to App store or Play store and search for **Microsoft Authenticator App**



2. Once installed, open the app. You may see this screen, if so, select **Work or School account**



The app will use the mobile's camera (it may prompt you for permission to access)



3. Hold the mobile up to the QR code (The barcode-looking square on your workstation screen). If you don't have a camera on your mobile, you can manually enter the code on your screen into the app



If you are unable to scan the image, enter the following information in your app.

Code: 734 893

URL: <https://cys01eupad07.eu.phonefactor.net/pad/8576i>

Once accepted, the authenticator will show your username along with a 6-digit number which changes every 30 seconds. At this stage, you don't need to do anything with these 6 digit numbers.



SRUC

████████@sruc.ac.uk

917 289



After those three steps, go back to your PC and Select **Next** on the screen:

### Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.

Code: 909 007 113

URL: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/794438132>

If the app displays a six-digit code, choose "Next".

Next

Cancel

You may see the screen below on your PC:

## Additional security verification

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

**Step 2: Let's make sure that we can reach you on your Mobile App device**

Please respond to the notification on your device.

You should now see the popup for you to **Approve** or **Deny** on your mobile phone:

