Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

Multi-Factor Authentication

User guide

23 October 2026

ICT Partner portal
021 8084367

Stellenbosch UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

forward together
sonke siya phambili
saam vorentoe

Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

How to use the guide

1. Select the topic (on the left)
2. Complete the steps as required

Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

What is Multi-Factor Authentication (MFA)?

When you sign into your account, (a process we call "authentication") you're proving to the service e.g. SUNFin or SUNStudent, that you are who you say you are.

Traditionally that's been done with a username and a password. Unfortunately, that's not a very good way to do it and that is why Microsoft 365 has added a way for your account to be more secure called Multifactor Authentication.

When you sign into your account you will need a second factor to prove who you are. A factor in authentication is a way of confirming your identity when you try to sign in. The three most common factors are:

Something you know – like a password.
Something you have – like a smartphone and authenticator application or a secure USB key (hardware token).
Something you are – like a fingerprint or facial recognition.

Multifactor Authentication therefore gives you access to applications, services or products and secure you and the University against username and password theft.

We recommend that you use the Microsoft Authenticator application as your default method of authentication.

Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

What must I do?

1. Connect to the Wi-Fi or to mobile data on your mobile device
2. Have a Smart Mobile device where you can download the Authenticator application
3. Your Smart Mobile device should have the following minimum requirements:

   a. **Microsoft Authenticator:**
      - Android: v8
      - iOS/iPadOS: v15

   b. **To setup passkeys on Microsoft Authenticator :**
      - Android: v14
      - iOS/iPadOS: v17

   c. **Google Authenticator:**
      - Android: v5
      - iOS/iPadOS: v15 *(iPhone 6S and later)*

4. A mobile number belonging to you and is not shared with anybody
5. Select an authentication method:

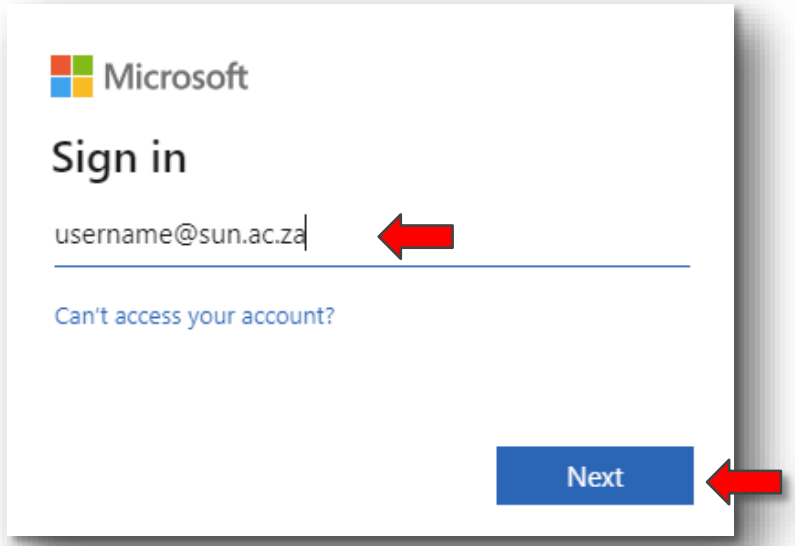
   a. **An Authenticator Application *(preferred method)***
   b. **Hardware Token**
      - Requires motivation from your Departmental Head
      - You will have to purchase the hardware token

NB: You only need to register once to use MFA for SU services requiring MFA

Microsoft Authenticator Application 1/15 30 Easy steps

IMPORTANT: *Some of the Huawei mobile devices are incompatible with the Microsoft Authenticator Application. If the Microsoft Authentication application is not available on the Huawei App Gallery, you will have to use the Google Authenticator Application as your method of authentication.*

1. On your computer, open **MFA Setup**.
You will be prompted to sign in with your Stellenbosch University credentials. First type in your ***SU email address*** and click **Next**.

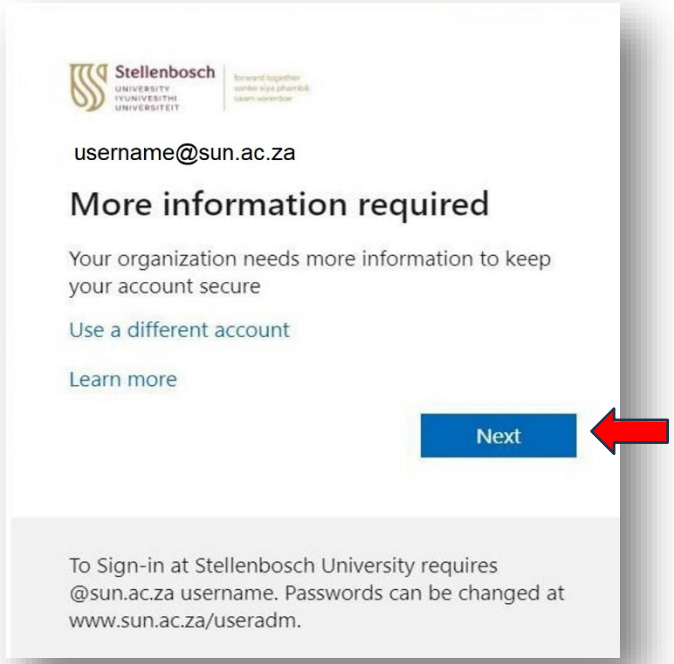


2. Enter your ***SU password*** and click **Sign in**.

Microsoft Authenticator Application

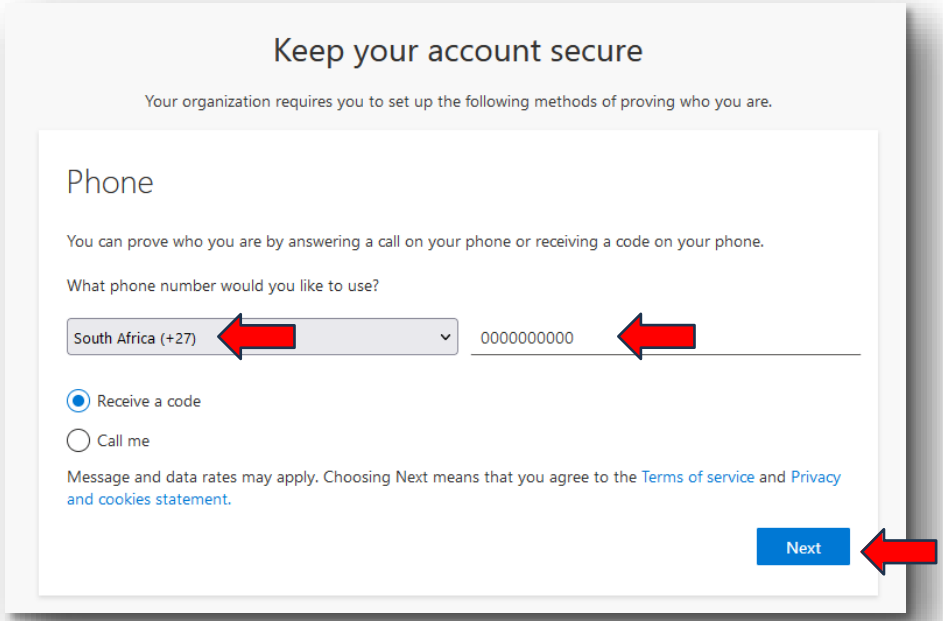
You will be requested to enable additional security on your account. Click **Next** to proceed.

If you don't see the screen below, you are already registered for MFA and don't need to do anything further.



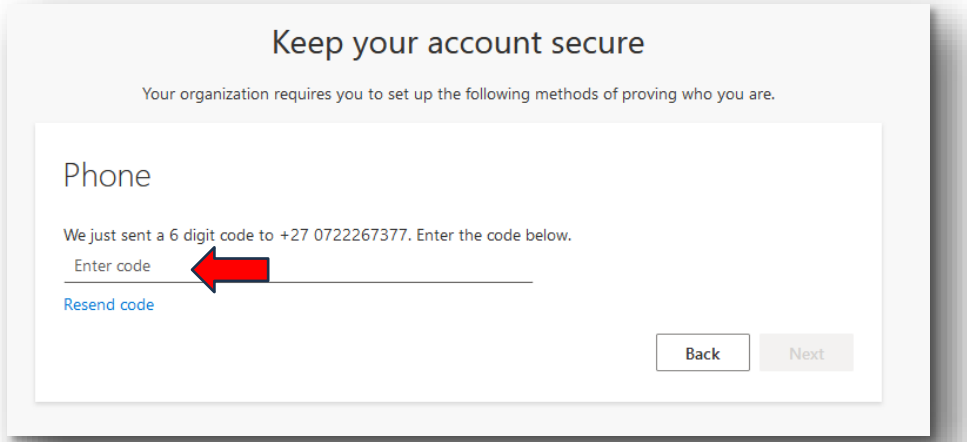
4. Select the correct country and type in the cell phone number of the mobile device you will be using for MFA authentication and click on **NEXT**.

An SMS with a Code will be sent to the cellphone number you have indicated in the below image.

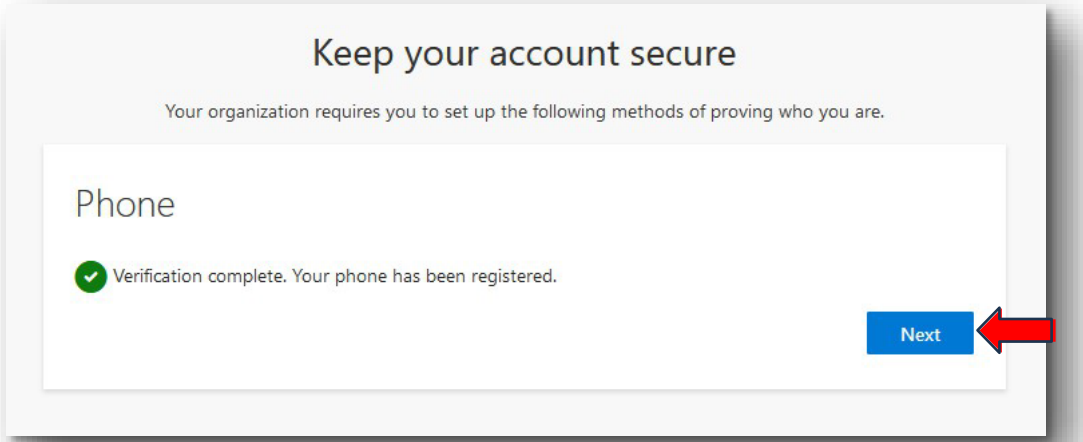


Microsoft Authenticator Application

5. Enter the code that was received via SMS in the space provided and click on **Next.**

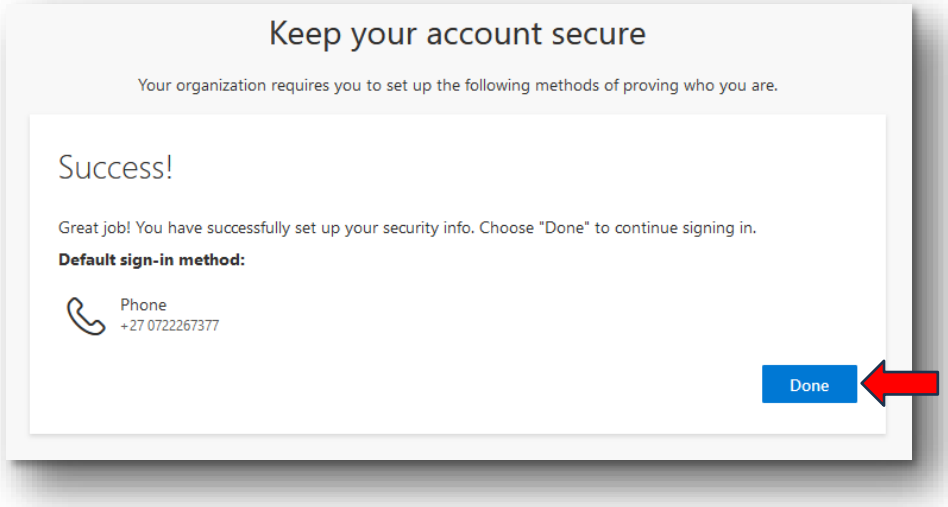


6. The verification of your mobile device is completed. Click on **Next.**

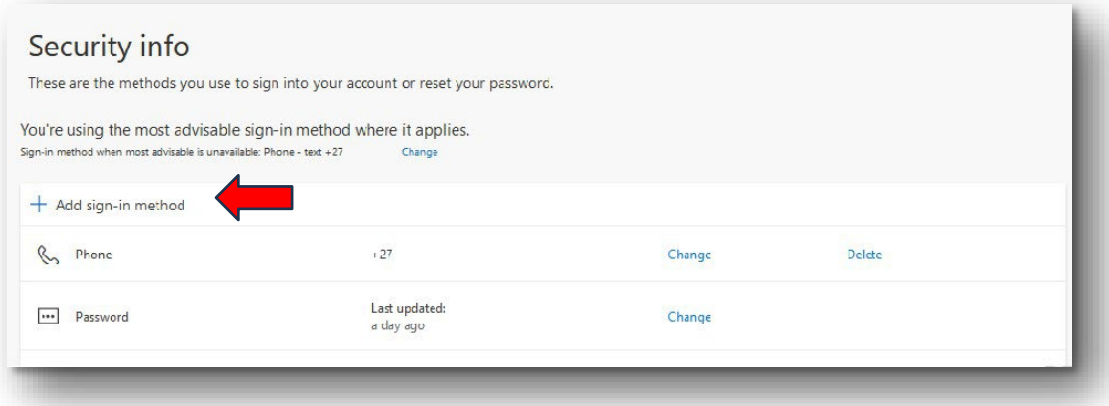


Microsoft Authenticator Application 4/15 30 Easy steps

7. Your mobile device is now registered for MFA. Click on **Done**.

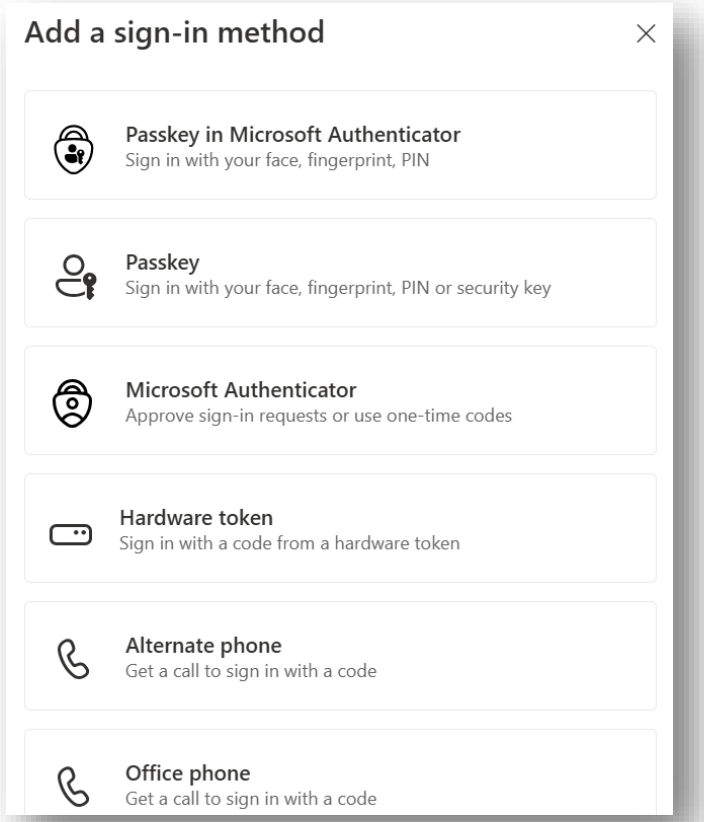


8. Your internet browser will display the below security info. You will now have to click on **Add sign-in method** to add the Microsoft Authenticator Application as a method.



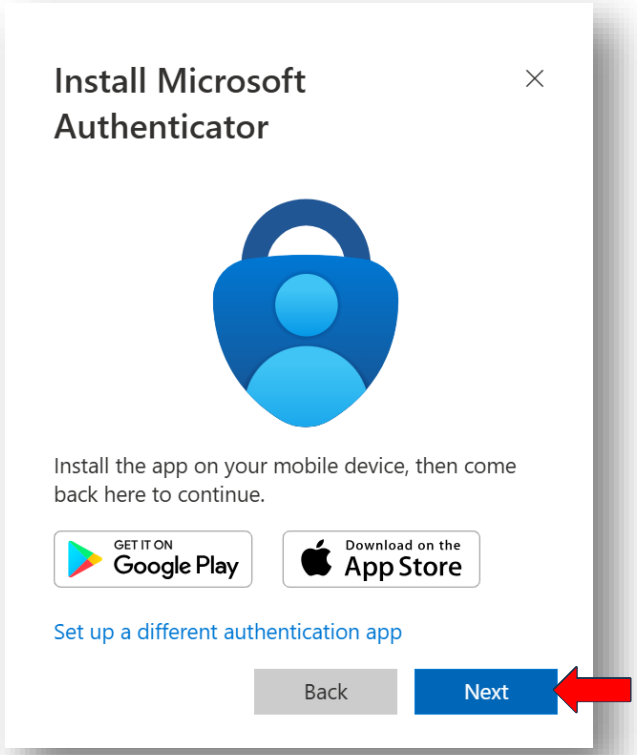
Microsoft Authenticator Application

9. Select the Authenticator app method and click on **Add**.



10. You are now requested to download and install the Microsoft Authenticator application on your cellphone.

Follow the installation steps on the next slides.



Microsoft Authenticator Application

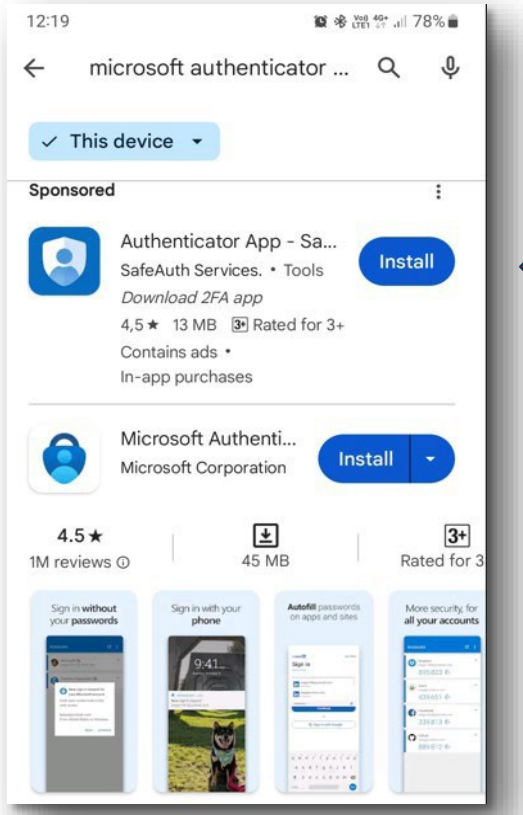
11. Open the relevant Application store on your mobile device and search for the Microsoft Authenticator Application.

Huawei devices are incompatible with the Microsoft Authenticator but can use the Google Authenticator Application.

Android Phone

iPhone

12. **Please make sure that you select the correct application:** Microsoft Authenticator Application. Tap on **Install**.

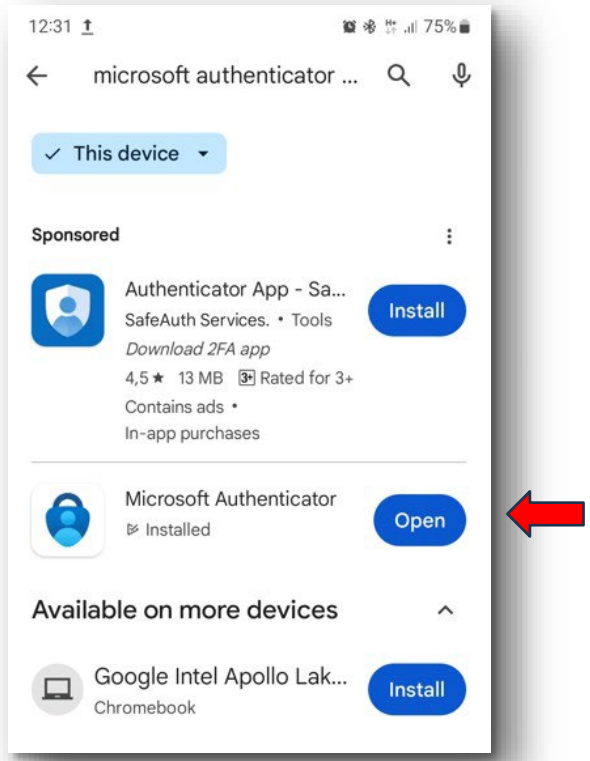


NOT THIS ONE

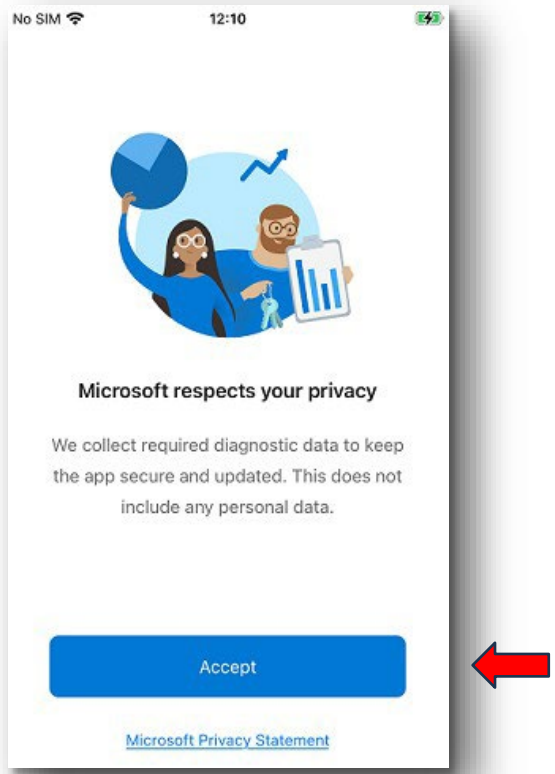
THIS IS THE APP TO INSTALL

Microsoft Authenticator Application

13. Once the application installation is completed, tap on **Open**.

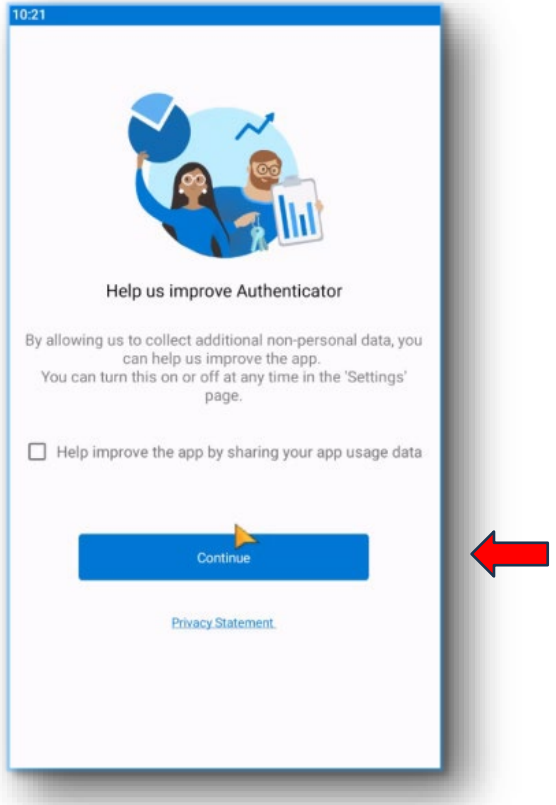


14. Allow the app to send notifications and click on **Accept** at the Privacy statement**.**

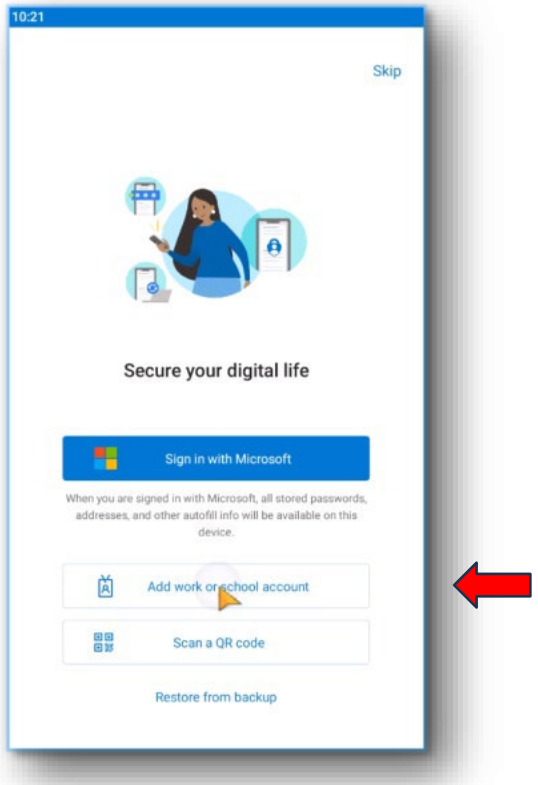


Microsoft Authenticator Application

15. Click on **Continue**.

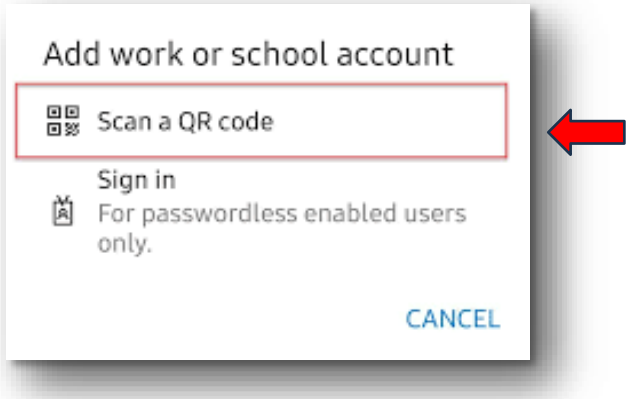


16. Click on **Add work or school account.**



Microsoft Authenticator Application 9/15 30 Easy steps

17. Select **Scan a QR code.**

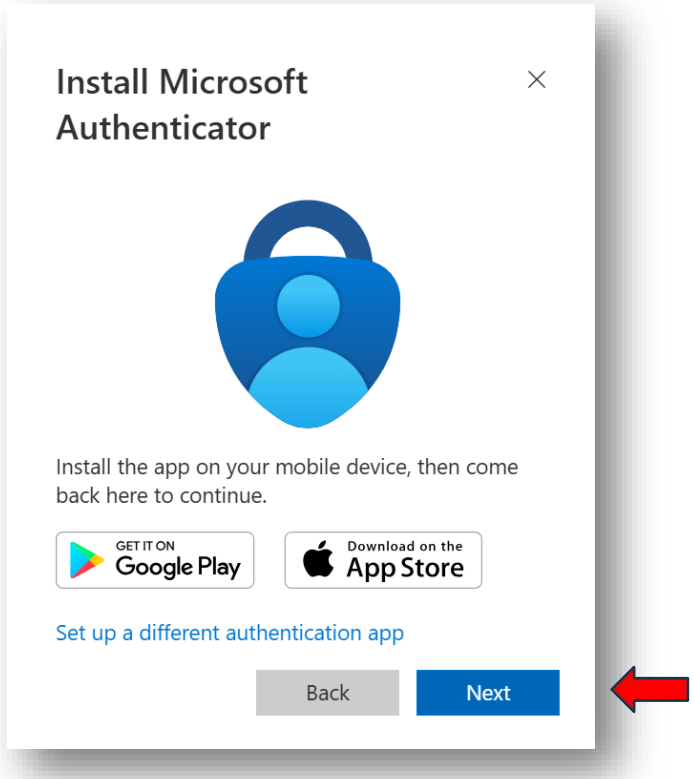


18. Click on **While using this app**. Your mobile device is now ready to scan the QR code.

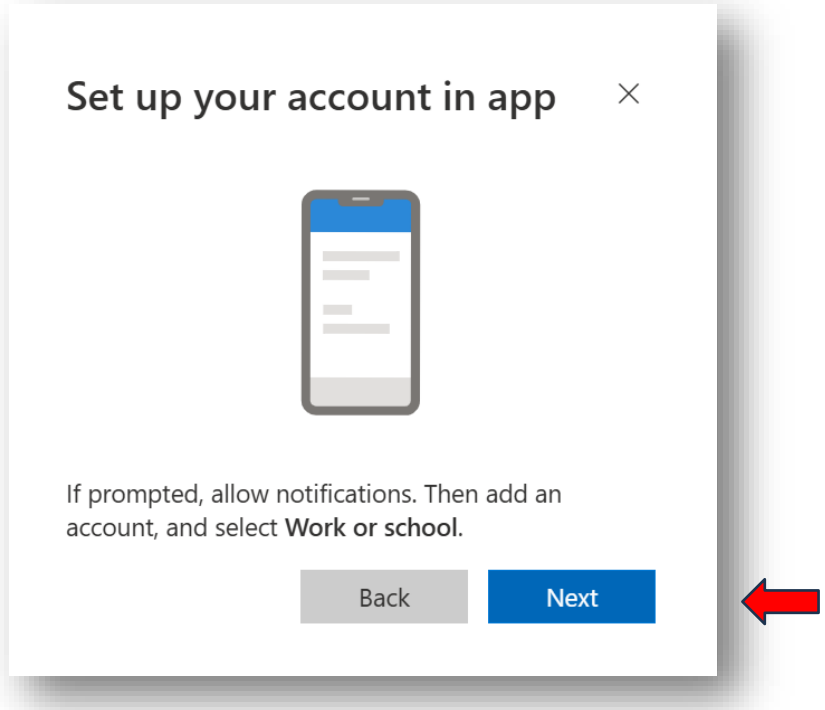
Now go back to your browser on your computer.

Microsoft Authenticator Application

19. Once you are back in the browser, click on **Next** *(on your mobile device).*

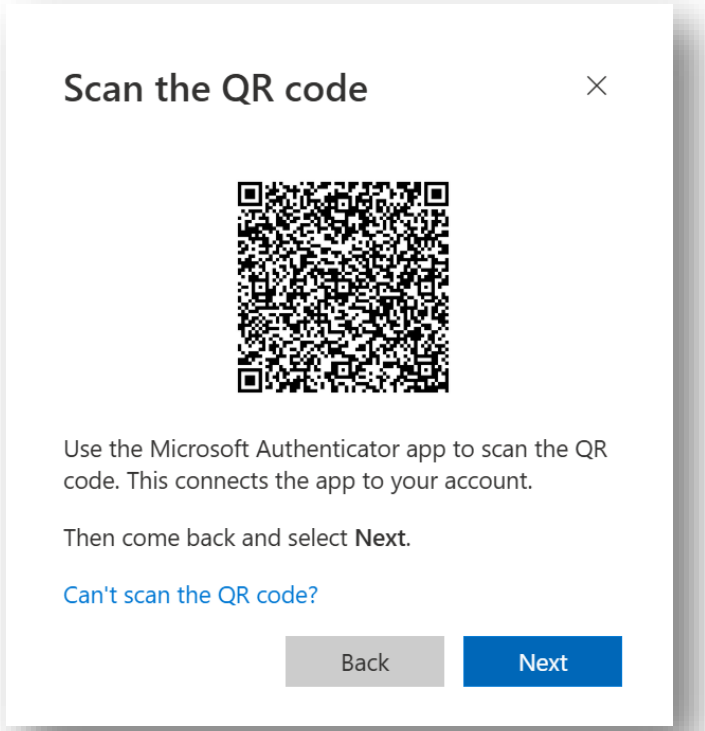


20. Click on **Next** to setup your account.



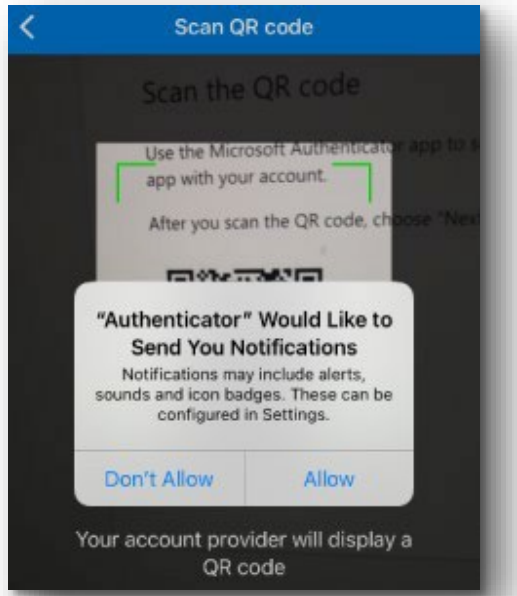
Microsoft Authenticator Application

21. A QR code will display on your computer.
DO NOT click on Next yet.



22. Position the camera of your mobile device over the QR code displaying **on your desktop.**

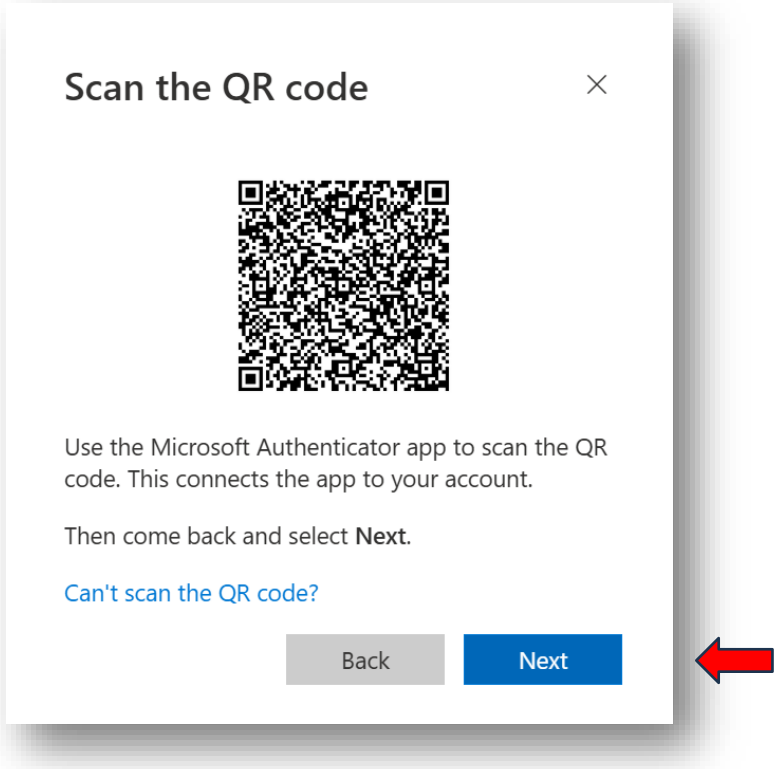
Click on **Allow** to be able to receive the next notifications.



Microsoft Authenticator Application 12/15 30 Easy steps

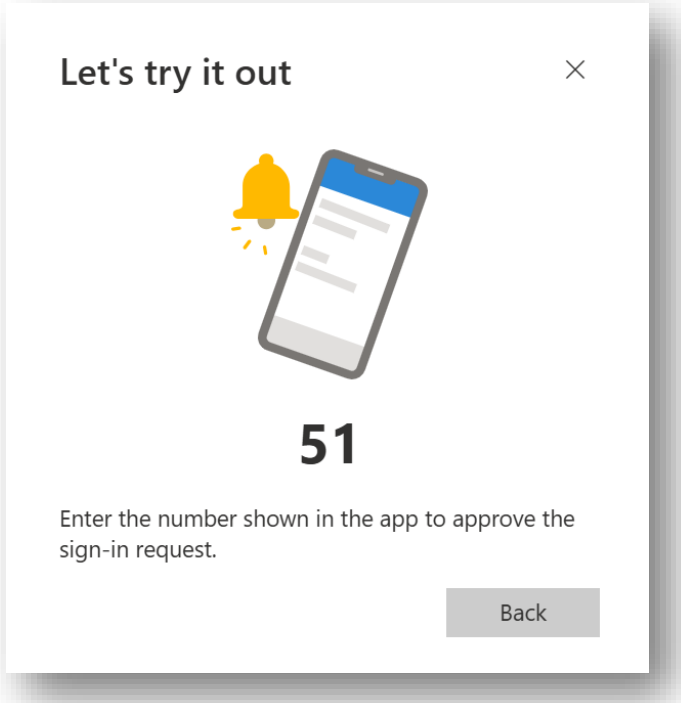
23. Your account will now show in the Microsoft Authenticator Application *(on your mobile device).*

24. Go back to your browser on your computer and click on **Next.**

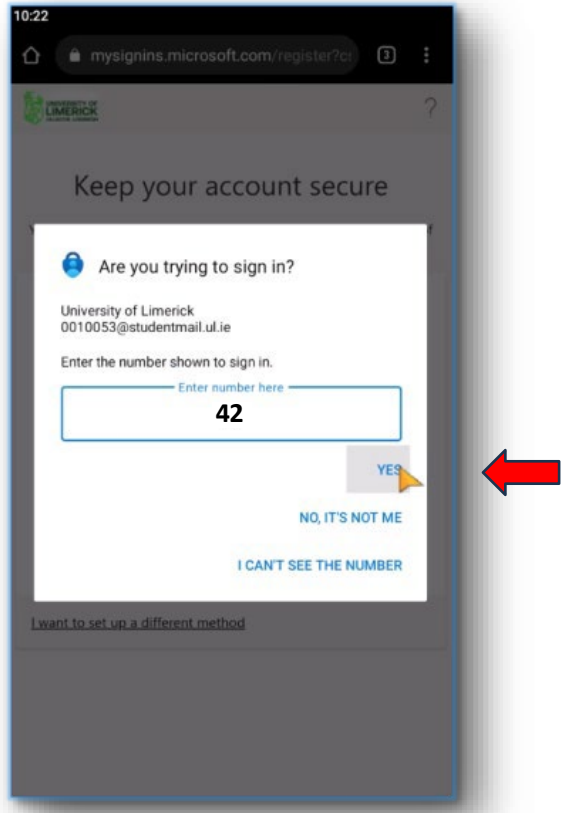


Microsoft Authenticator Application

25. A notification is sent to your mobile device.

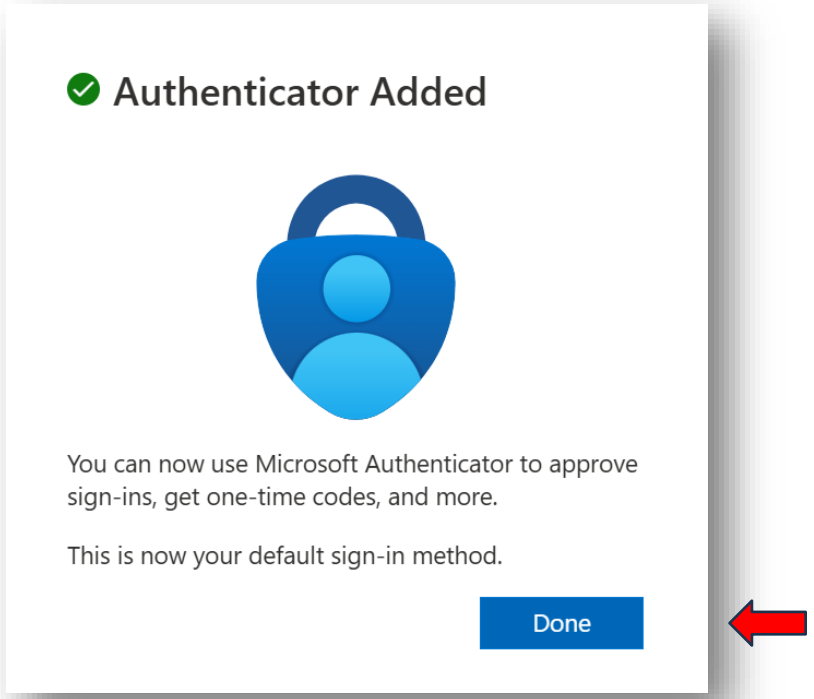


26. Enter the number on your mobile device that was sent from the browser and click on **Yes** to sign in.

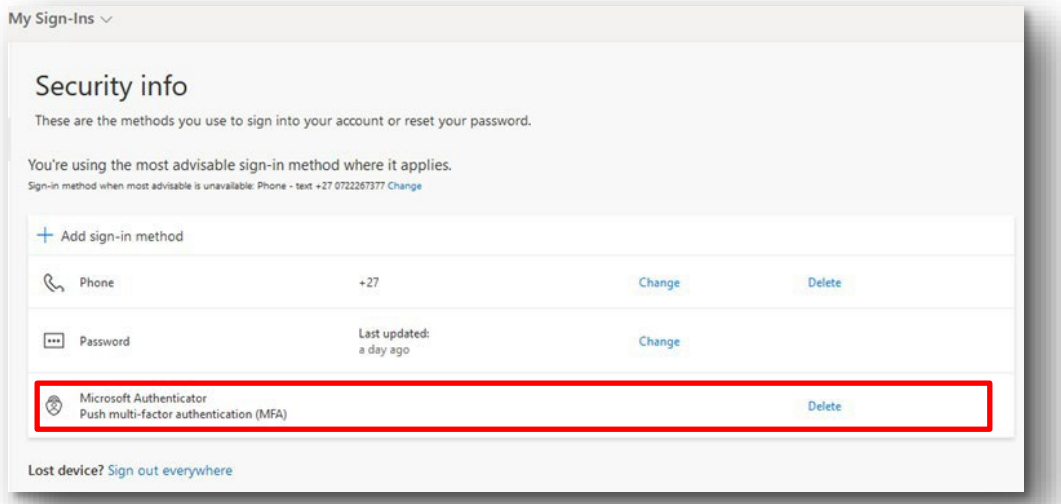


Microsoft Authenticator Application 14/15 30 Easy steps

27. The notification was approved, click on **Done**.



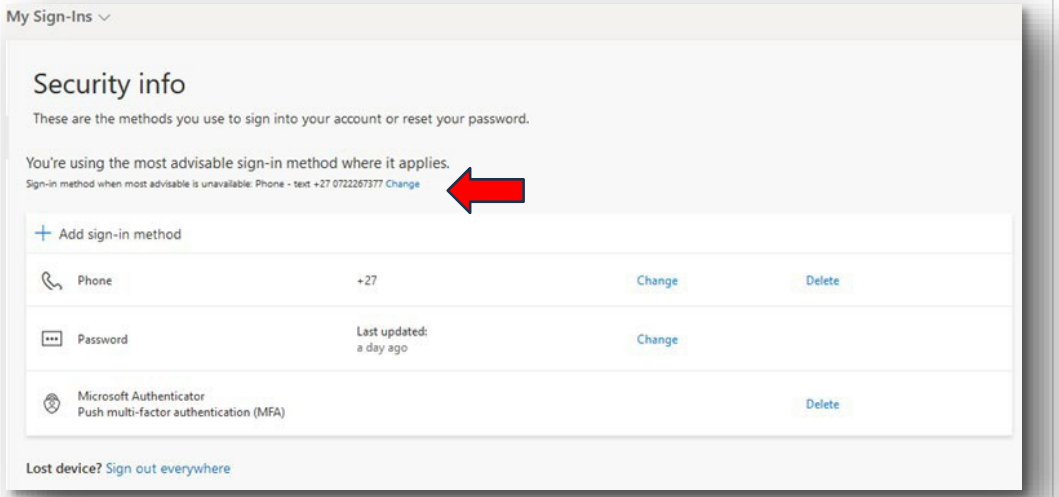
28. The Microsoft Authenticator Application is now added as a method as shown in your browser.



Microsoft Authenticator Application 15/15 30 Easy steps

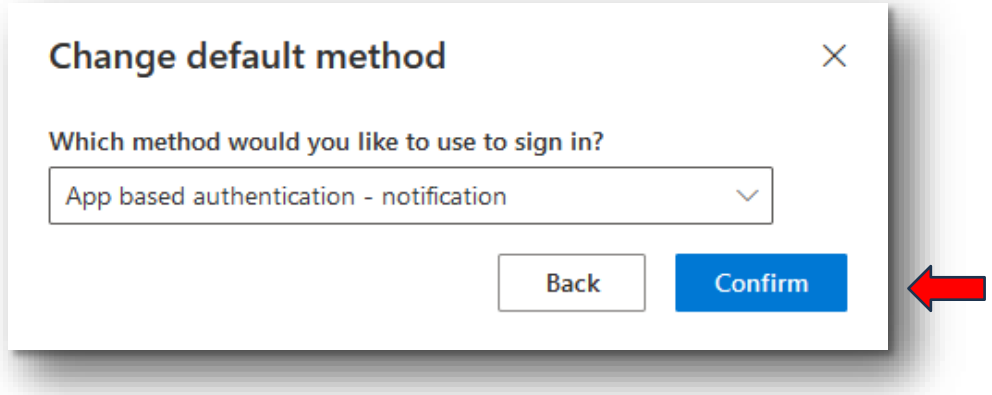
29. The last step is to make the Microsoft Authenticator Application your default method of authentication.

In your browser where your methods shows, Click on **Change**.



30. Select the **App based authentication – notification,** click on **Confirm** close the browser.

You are now ready to authenticate with the Microsoft Authenticator Application when requested.



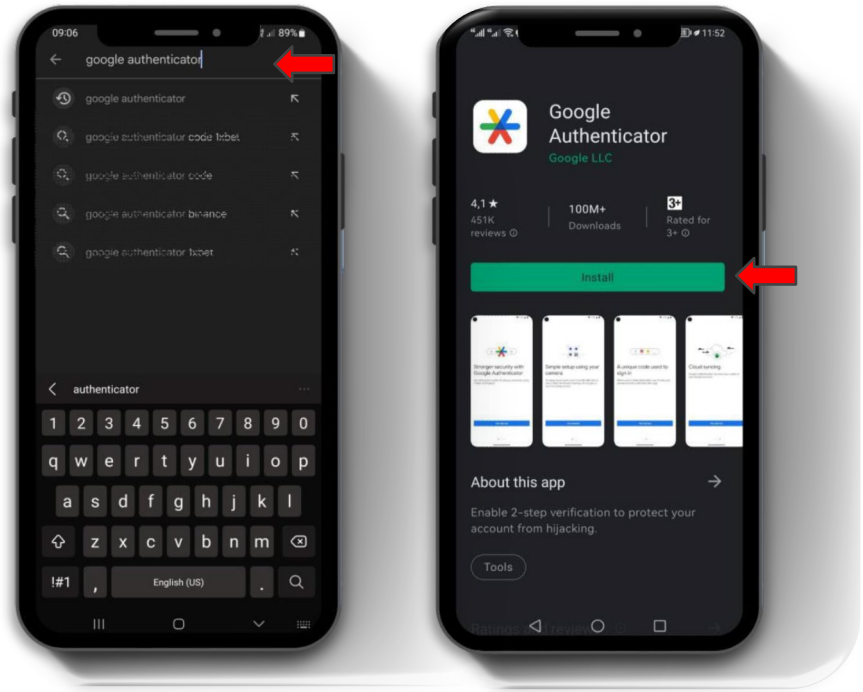
Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

Prerequisites to the Google Authenticator Application

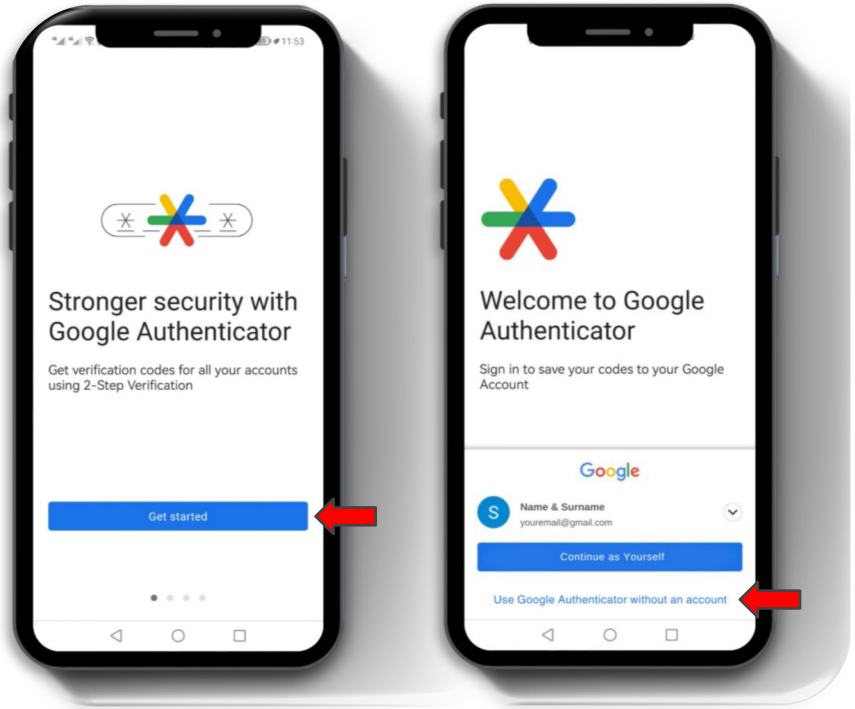
1. An active Gmail address (Google Account). Follow the link to create a new Google Account.
2. Have the GBox application already downloaded from the app store and installed on your smart mobile device.

Google Authenticator Application 1/8 16 Easy steps

1. Google Authenticator app can be found in the app store on the relevant phone. Click on **install**.
(If you cannot find Google authenticator on the app store, install GBox first.)



2. Click on **Get started** and select **Use Authenticator without an account.**

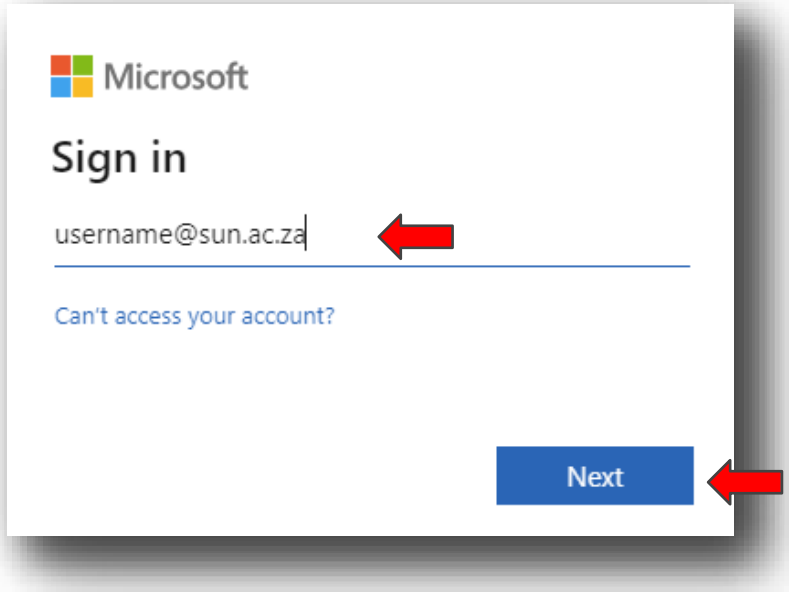


Google Authenticator Application 2/8 16 Easy steps

Your app is not complete, verify via your old method of authentication.

3. On your computer, open the browser and go to https://mysignins.microsoft.com.

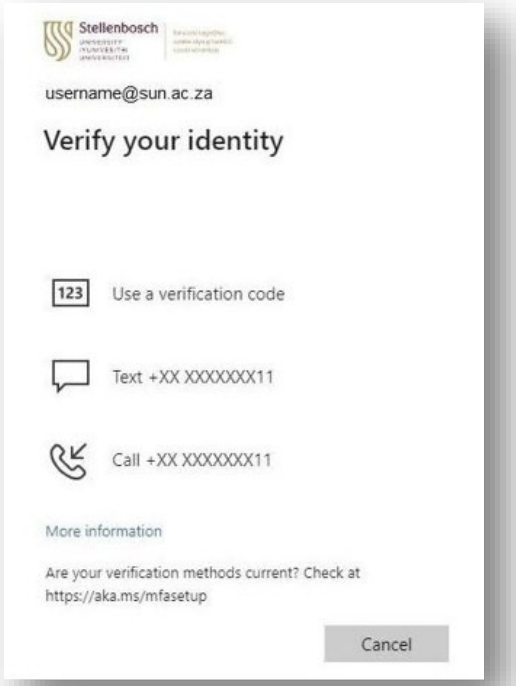
You will be prompted to Sign in with your Stellenbosch University credentials. First type in your email address and click on **Next**.



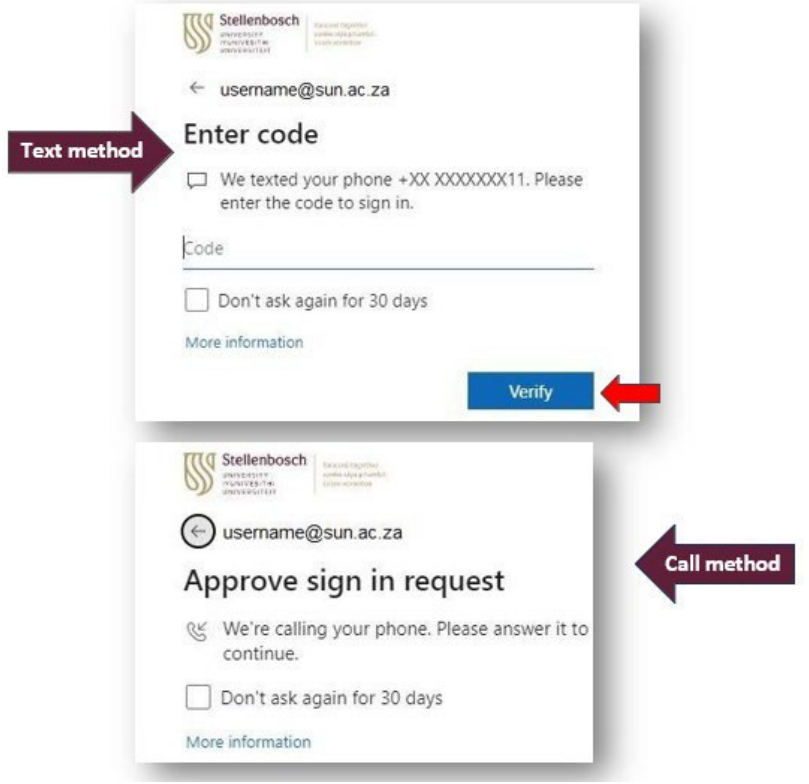
4. You will then be prompted to enter your password and click on **Sign in.**

Google Authenticator Application

5. You will now be requested to verify your identity via Text or Call. Use your current method.



6. Below is the result if you either choose the **Text or Call** method.



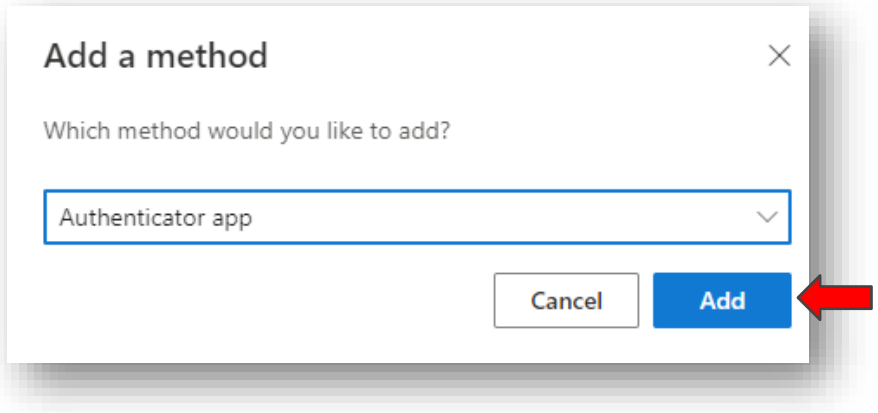
Google Authenticator Application

7. Select **Yes** if it is your OWN device .

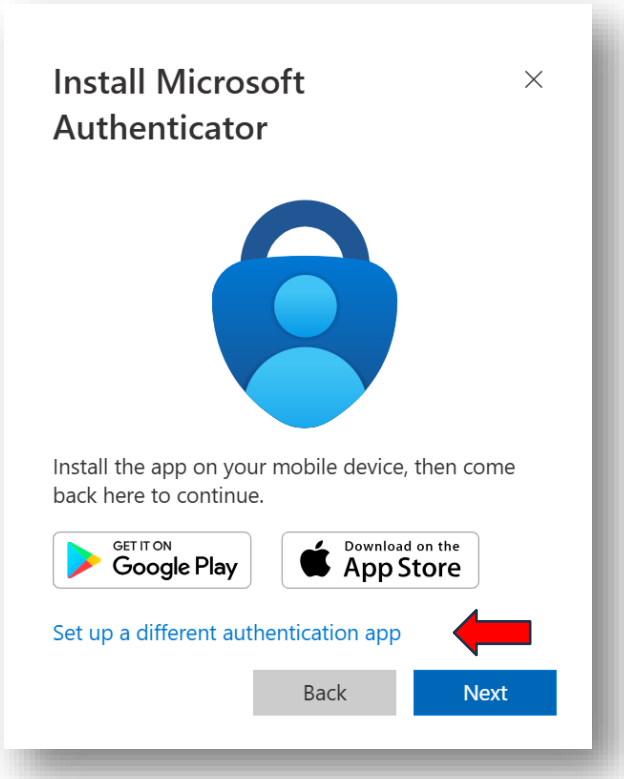
8. In the left menu, select **Security info**. Click on **+ Add sign-in method.**

Google Authenticator Application 5/8 16 Easy steps

9. Choose Authenticator app and click on **Add**.

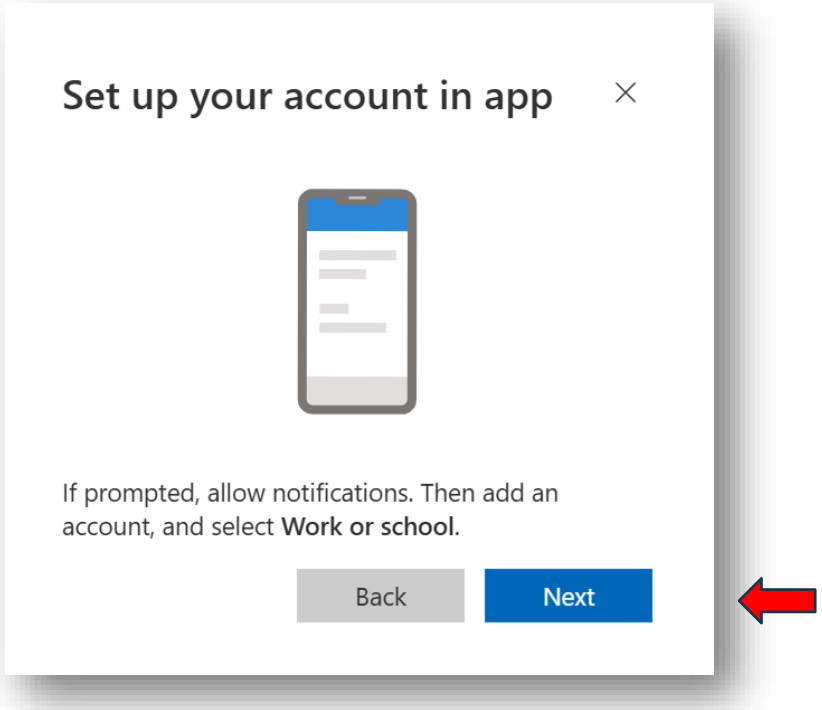


10. Click on **I want to use a different authenticator app.**



Google Authenticator Application 6/8 16 Easy steps

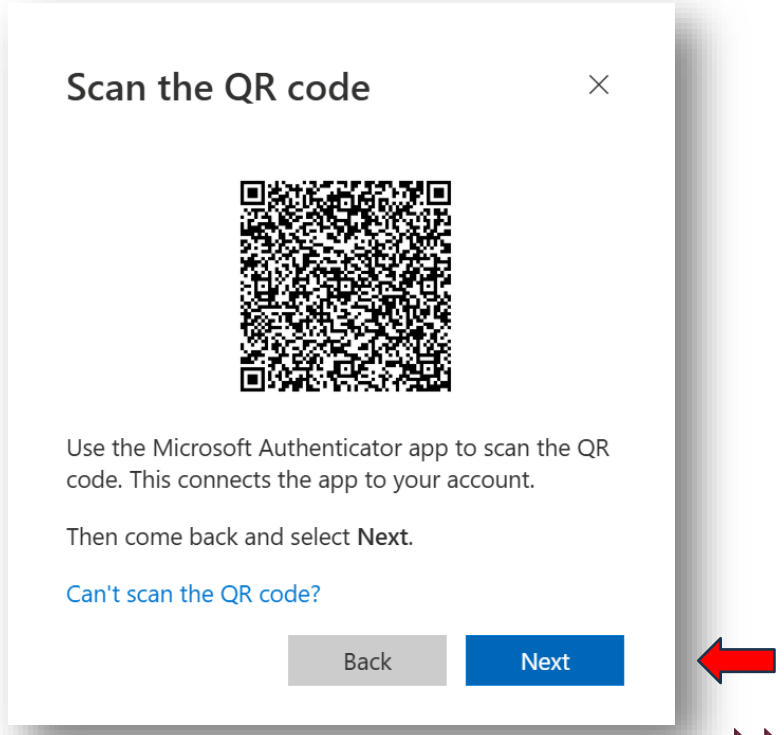
11. Select **Next**.



12. Open the Google Authenticator app on your phone and use your phone to scan the QR code shown on your computer.

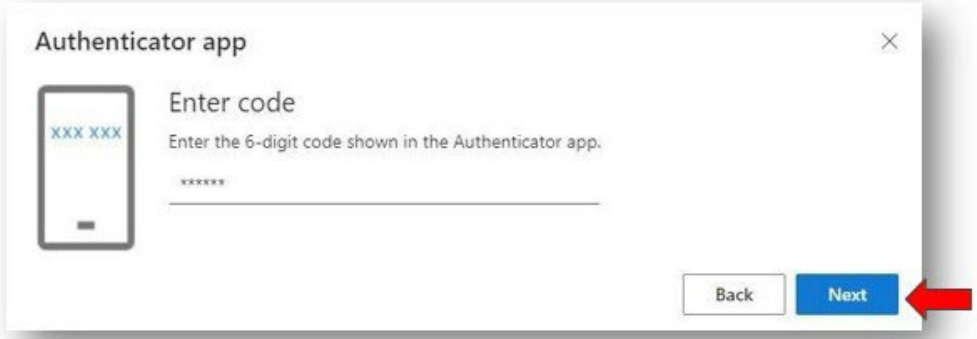
On your mobile device, click on + to add an account and scan the QR code with Google Authenticator.

Select **Next** on your computer.



Google Authenticator Application 7/8 16 Easy steps

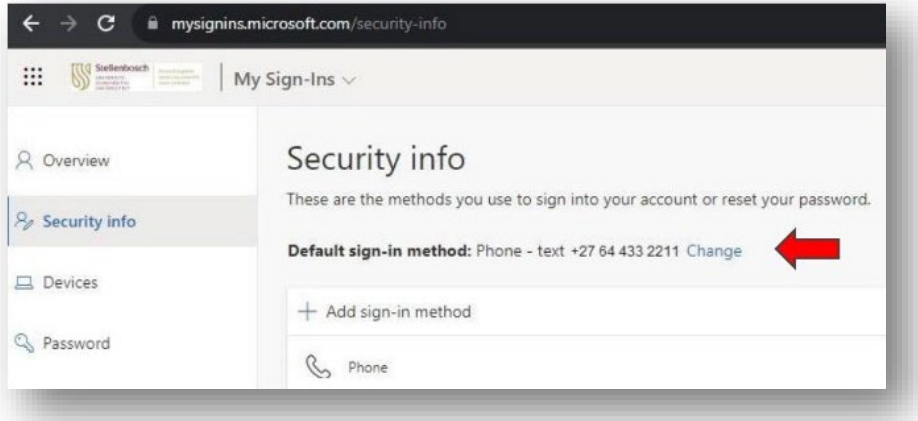
13. Enter the 6-digit code from the Google Authenticator app and click **Next**.



14. *Although you added the authentication method, you still must change the default sign-in method.*

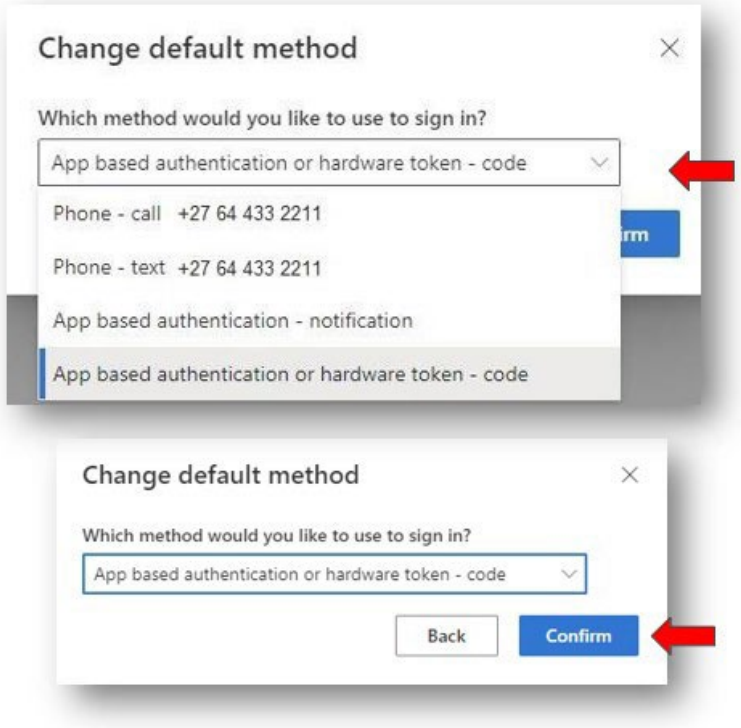
Go back to the Security Information on the https://mysignins.microsoft.com page to change your sign in method.

Next to Default sign-in method, click on **Change**.

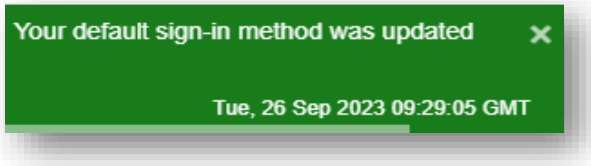


Google Authenticator Application 8/8 16 Easy steps

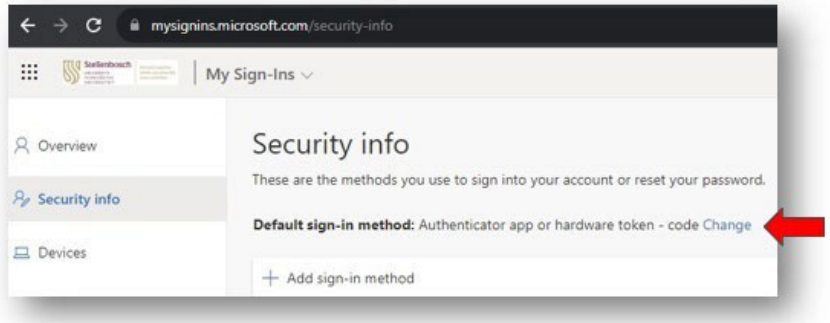
15. Left click on the drop-down menu and see all the available methods.
Select **App based authentication or hardware token - code** and click Confirm.



16. You will see a notification in the top right corner of your computer screen to confirm the change of the default sign-in method.



The default sign-in method has changed to the Authenticator application or hardware token - code



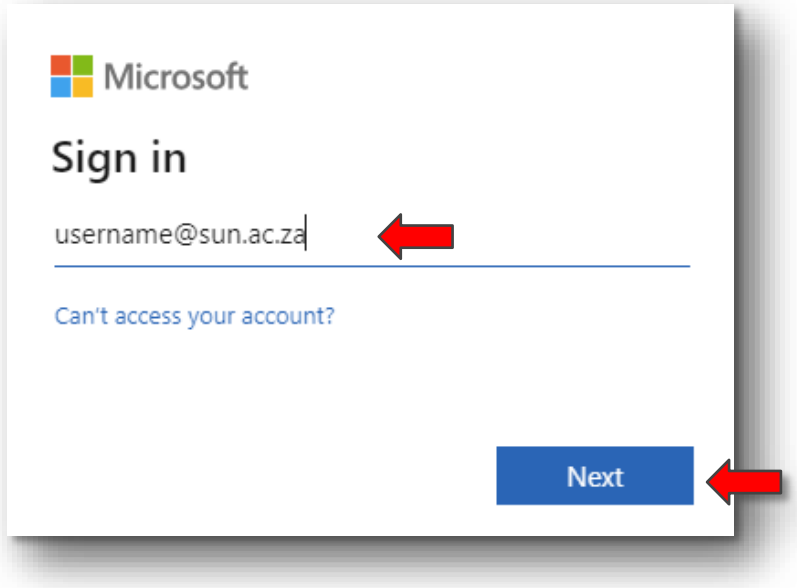
Your MFA should now be successfully setup using the Authenticator application.

Hardware Token

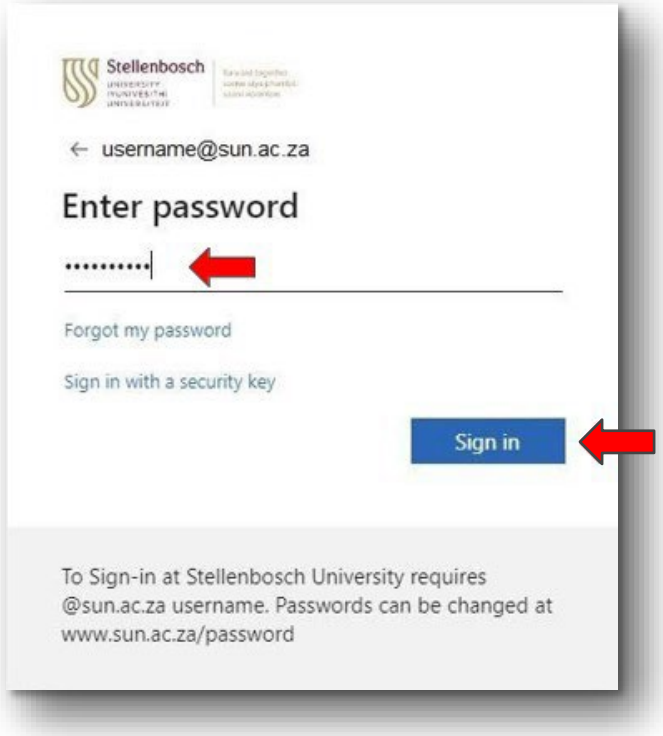
24 Easy steps

IMPORTANT: *You must be enabled to use a FIDO key with your university credentials. Log a request on the ICT Partner Portal to be enabled.*

1. On your computer, open the **MFA Setup**.
You will be prompted to sign in with your Stellenbosch University email address and click on **Next**.



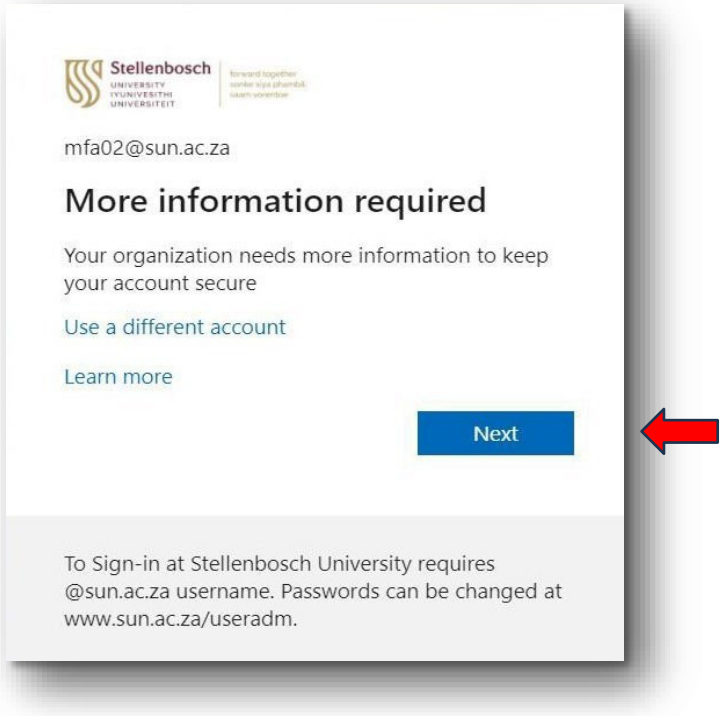
2. Enter your password and click **Sign in**.



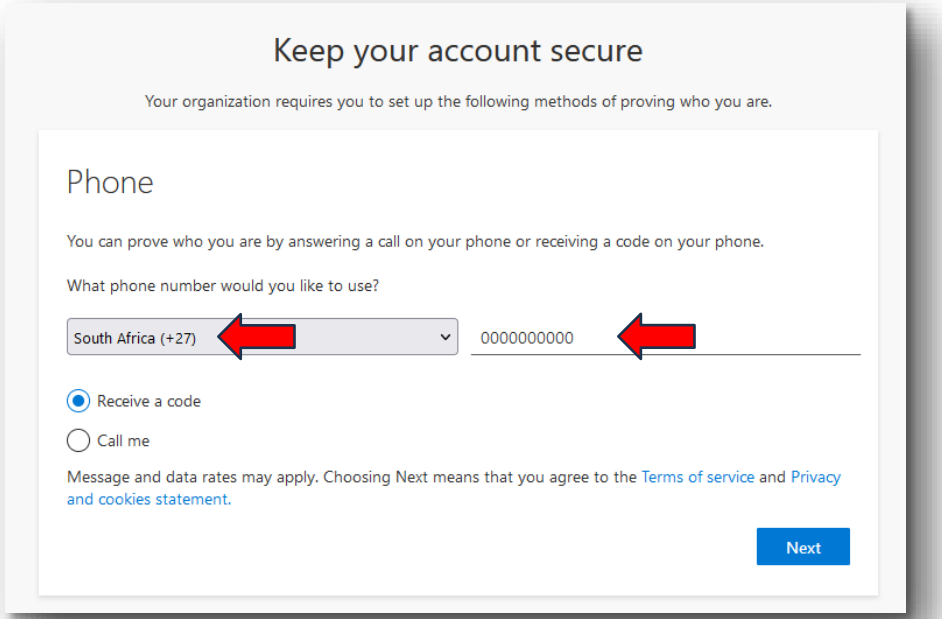
Hardware Token

3. You will be asked to enable additional security on your account. Click **Next** to proceed to step 4.

If you do not see the below screen, you are already registered for MFA and do not need to do any further steps.

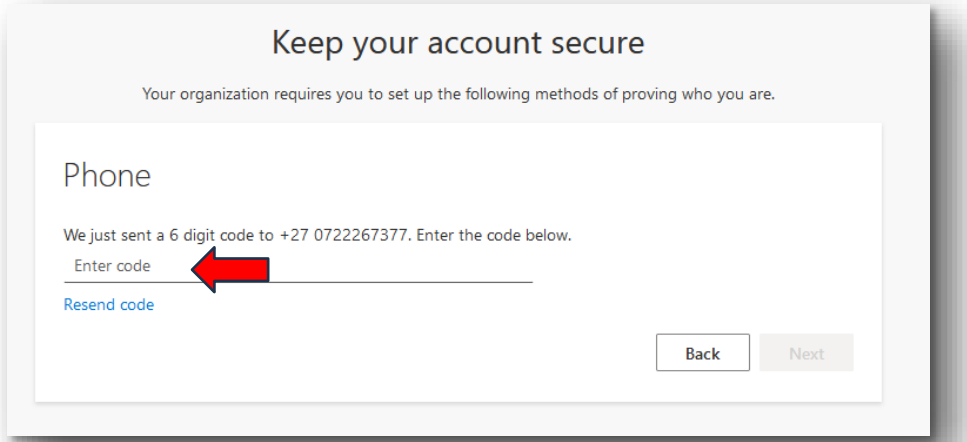


4. Enter your mobile number and click **Next**.

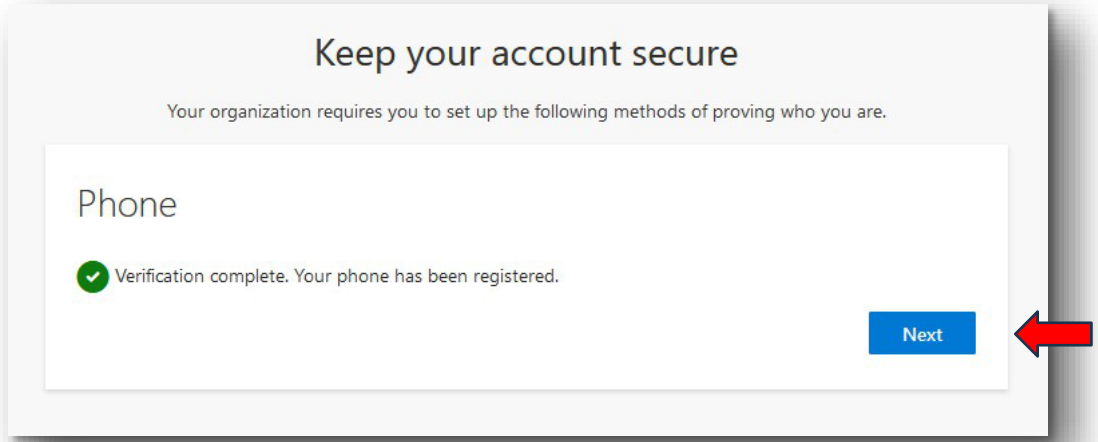


Hardware Token

5. A verification code will be sent to your mobile device. Enter the code and select **Next**.

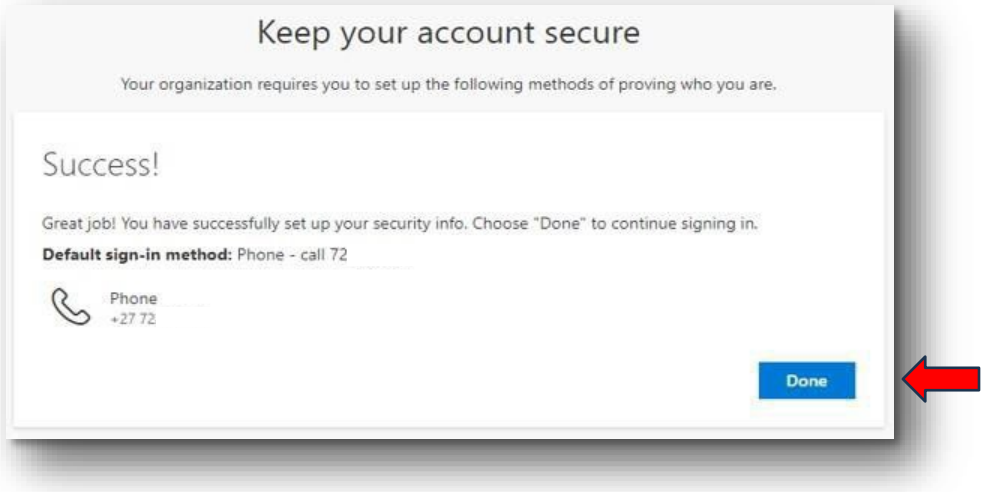


6. Click **Next** when the code has been verified.



Hardware Token

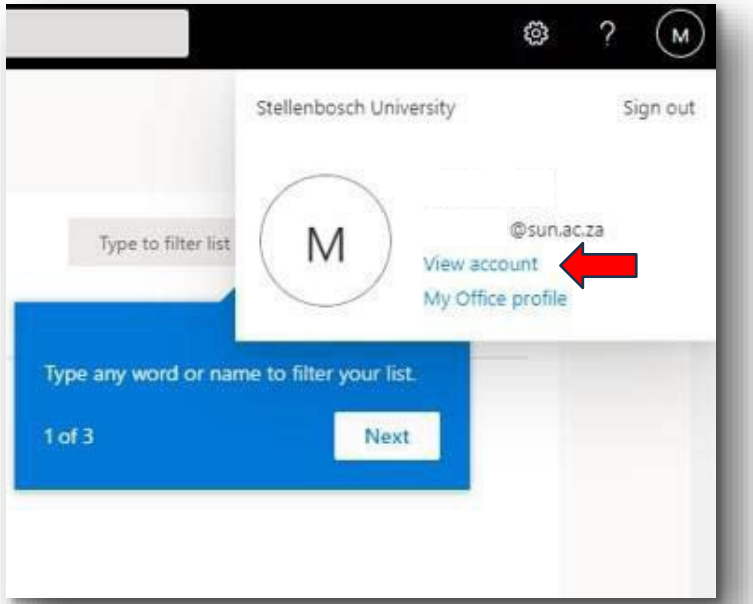
7. Your mobile number has been successfully added as an authentication method. Click **Done**.



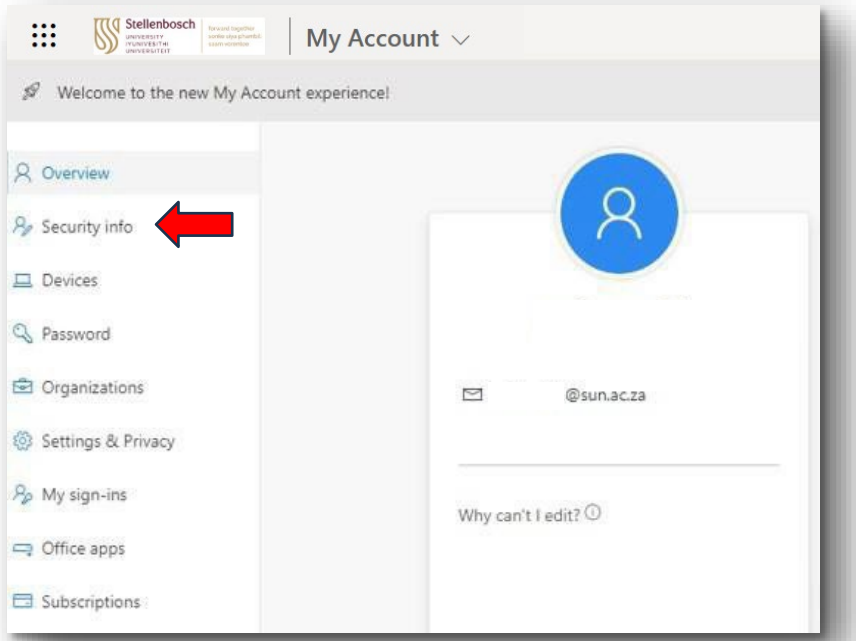
8. When asked if you want to stay signed in, click **No**.

Hardware Token

9. Once signed into your Stellenbosch University account, Select the icon in top right-hand corner and select **View account.**

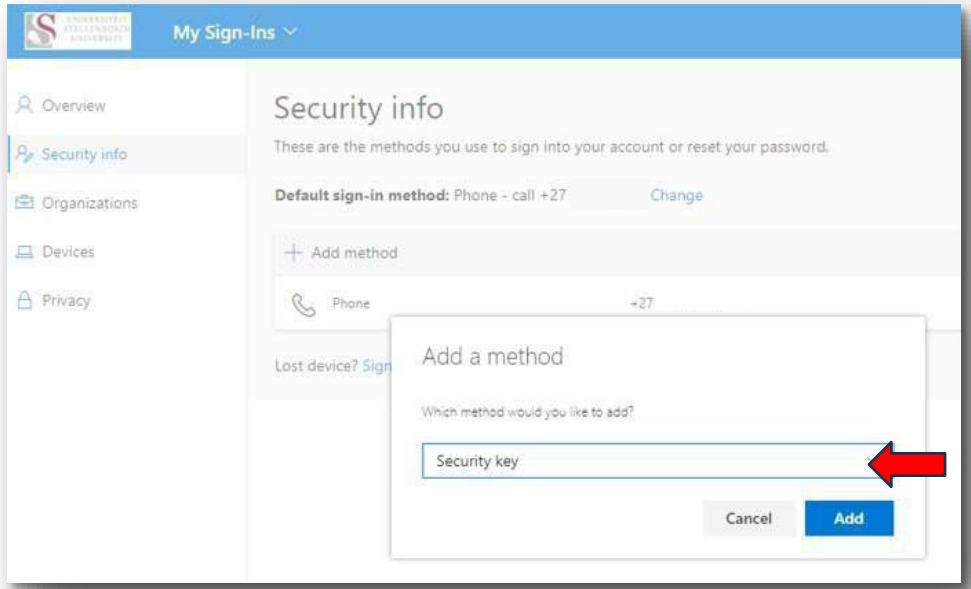


10. You will be directed to https://myaccount.microsoft.com. Select **Security Info**.



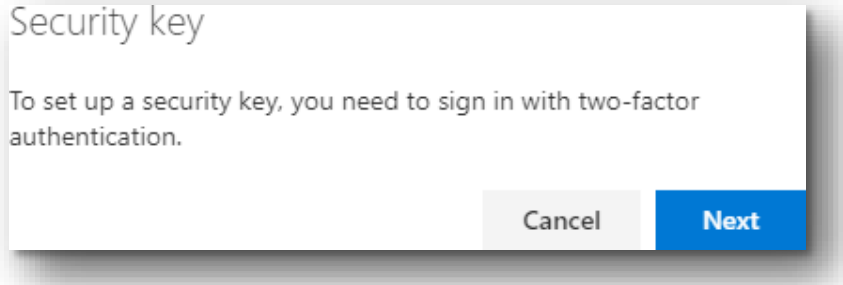
Hardware Token

11. Select **Add a Method** and select **Security Key** from the drop- down menu. Click **Add**.



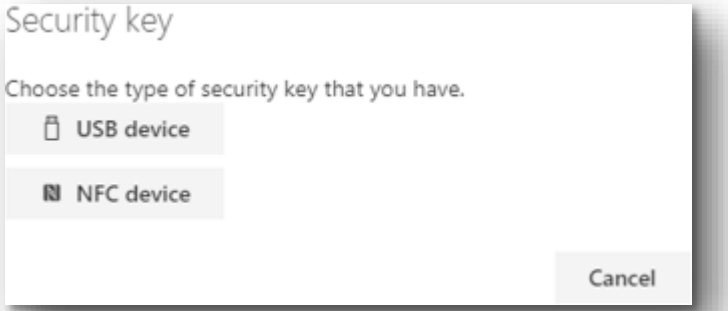
12. You will be prompted again to authenticate. Depending on your method, you will either receive a phone call or a SMS.

Follow the prompts.

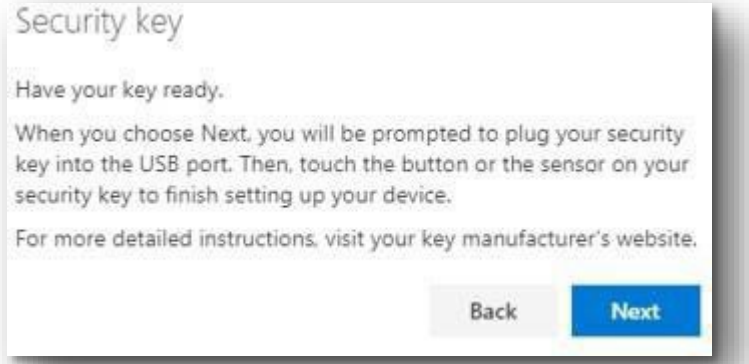


Hardware Token

13. Select your type of security key.
In this example we will use a USB device option.

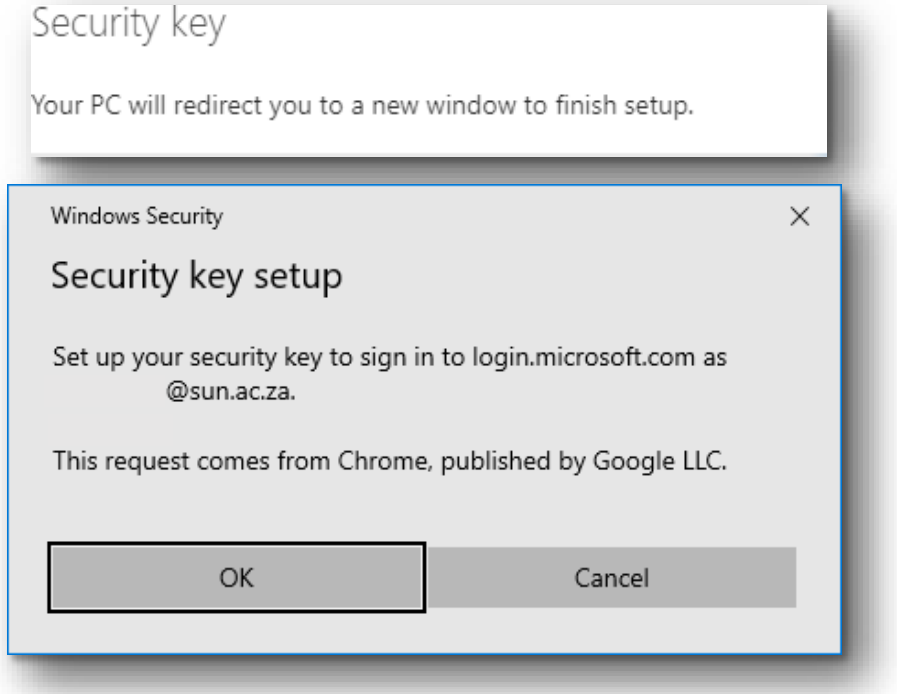


14. Have your key ready and click **Next**.



Hardware Token

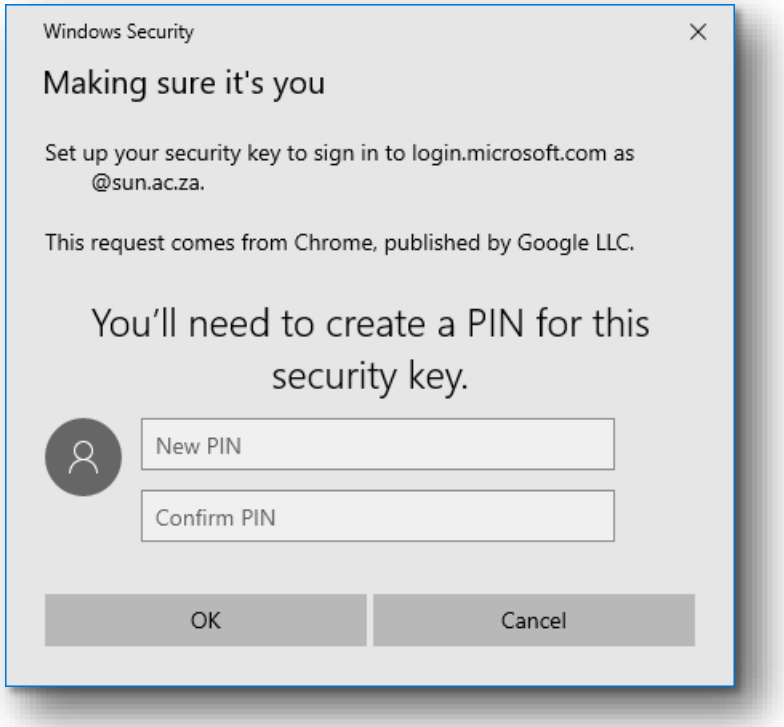
15. Follow the prompts and click **OK** when prompted.



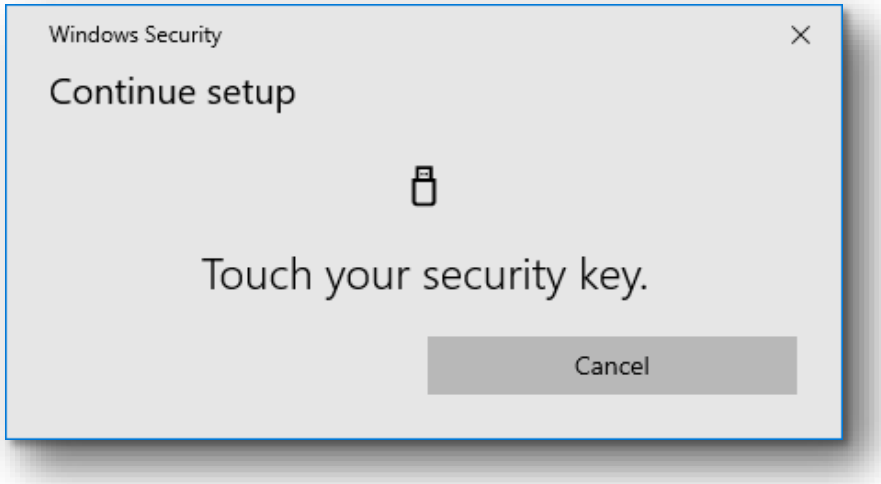
16. You will need to create a PIN for the security key. Enter one and click **OK.**

Hardware Token

17. You will need to create a PIN for the security key. Enter one and click **OK**.

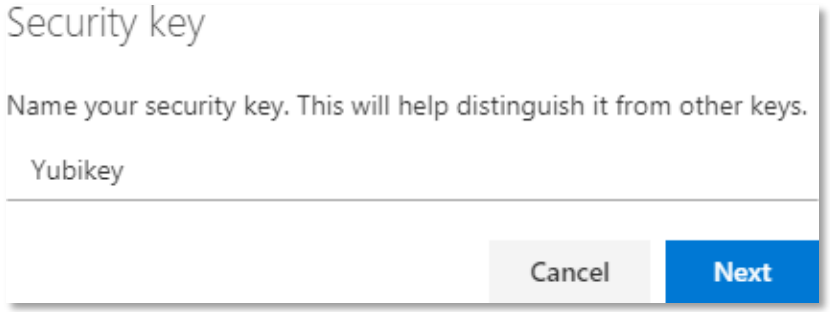


18. You will be requested to touch the security key.

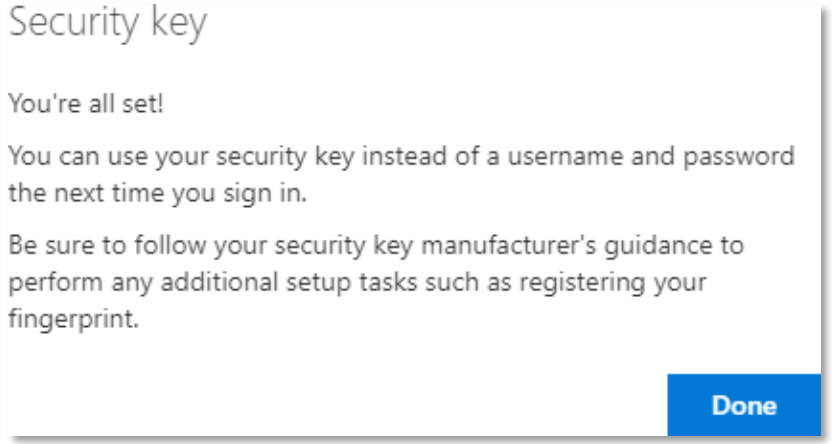


Hardware Token

19. Once the device has been verified, you will be prompted to give your key a name.

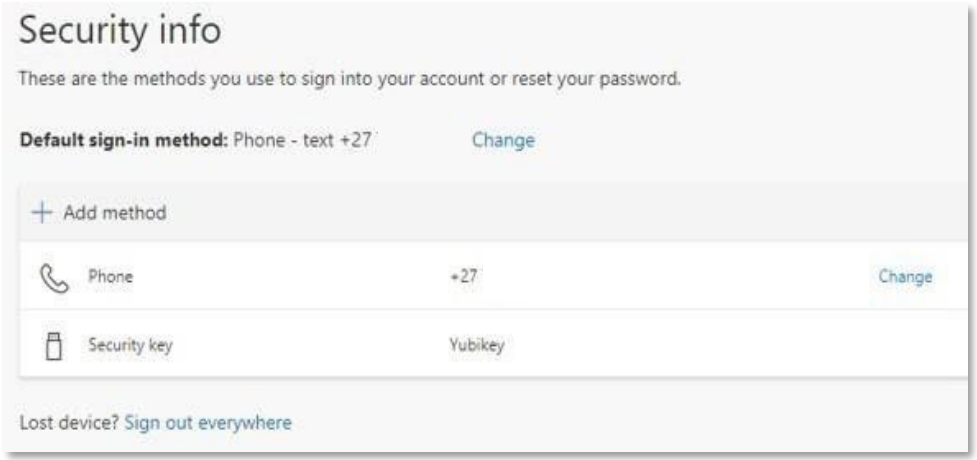


20. You're all set. Click **Done**.

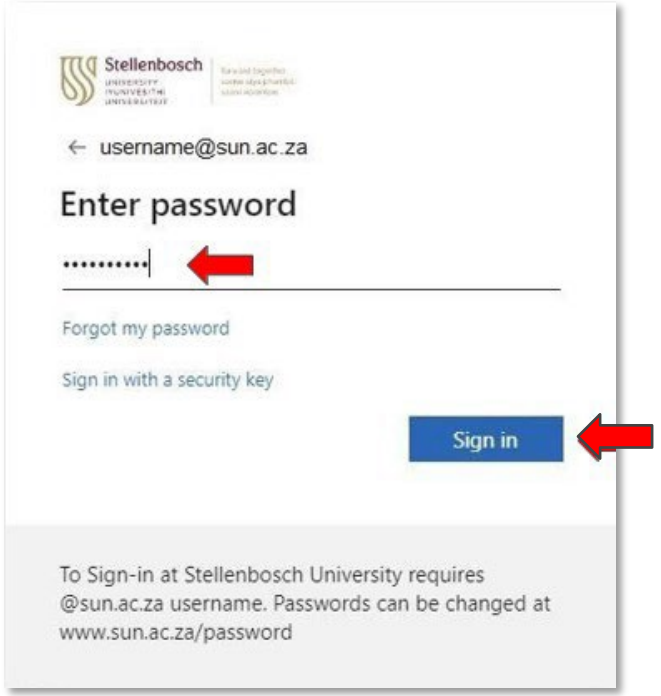


Hardware Token

21. The newly added security key will be listed among your allowed sign-in methods.



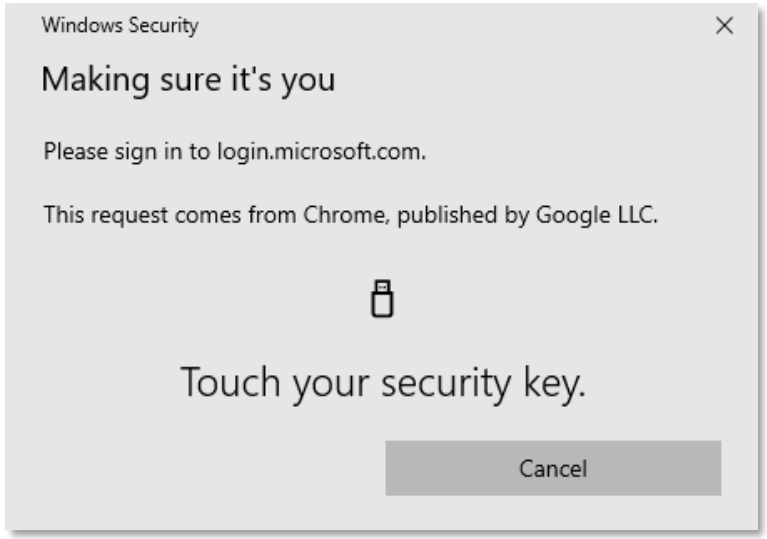
22. When you are prompted to enter the password, you can simply insert the hardware token (security key) in the USB port and click on **Sign in**.



Hardware Token

23.

Touch the key on the allocated spot as before.



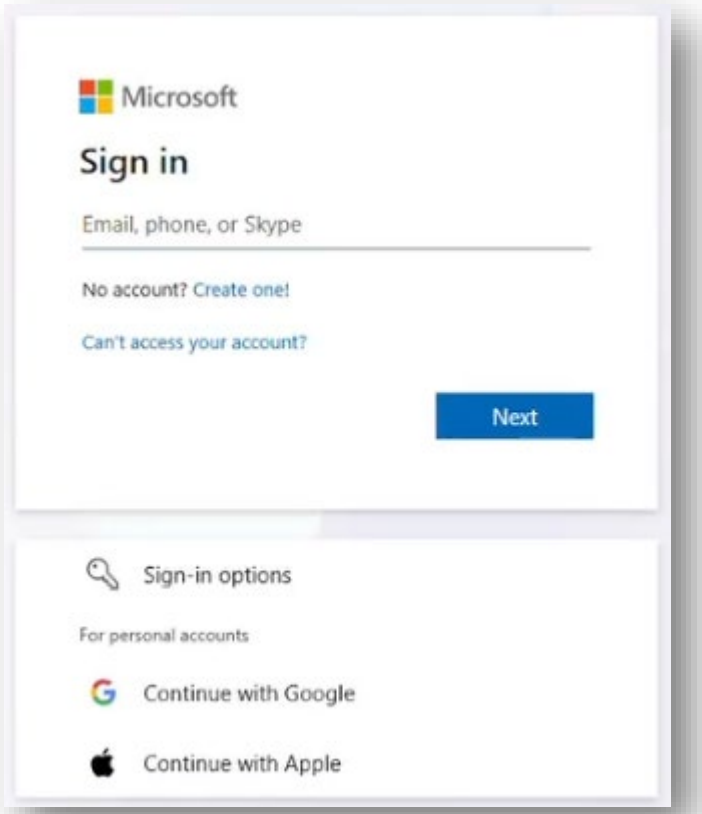
24.

All set, you are now signed in using a security key!

SMS/Voice to Authenticator app 1/4 8 Easy steps

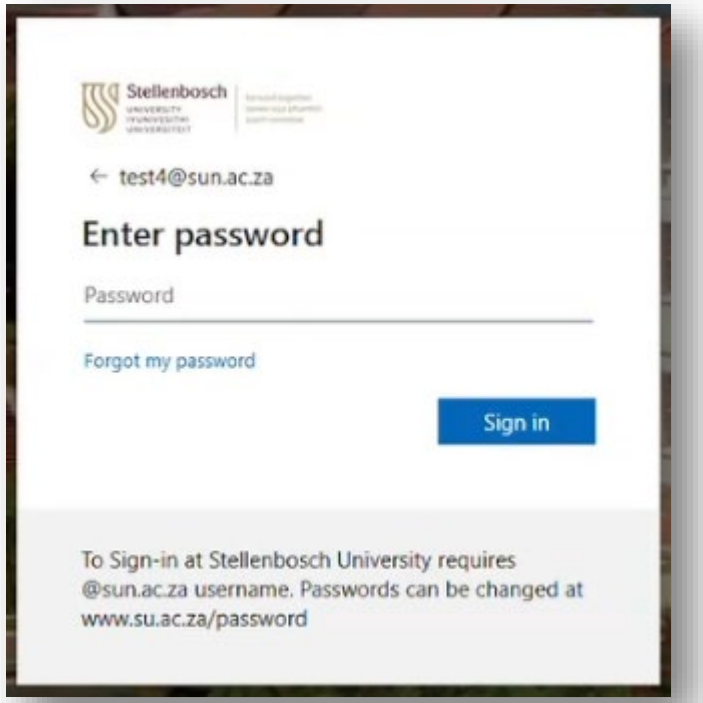
Steps for users who are still using SMS and Voice as authentication method when using Microsoft applications.

1. Sign in with your **SU email address** and click **Next**.



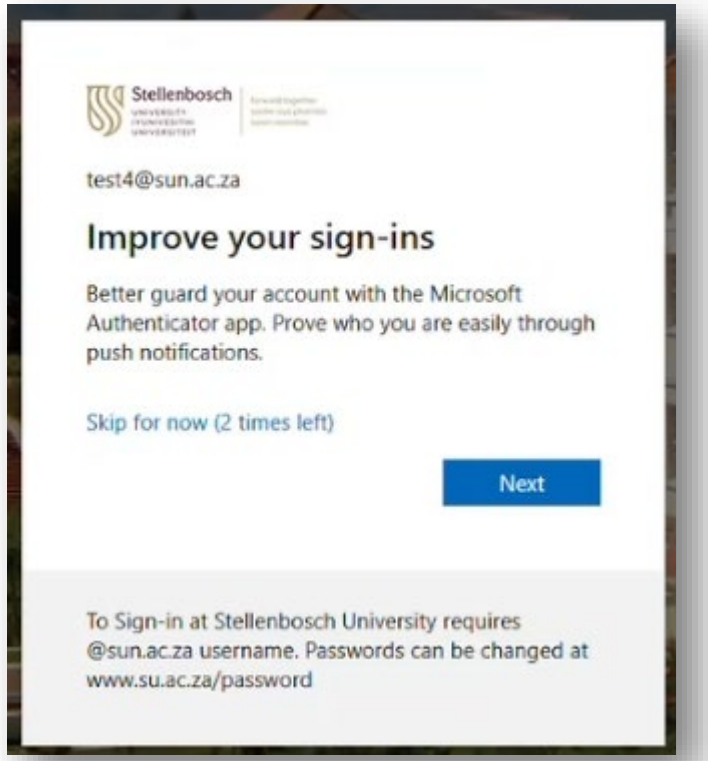
If you do not have access to this screen, go to the MFA Setup portal.

2. Enter your **password** and click **Sign in**.

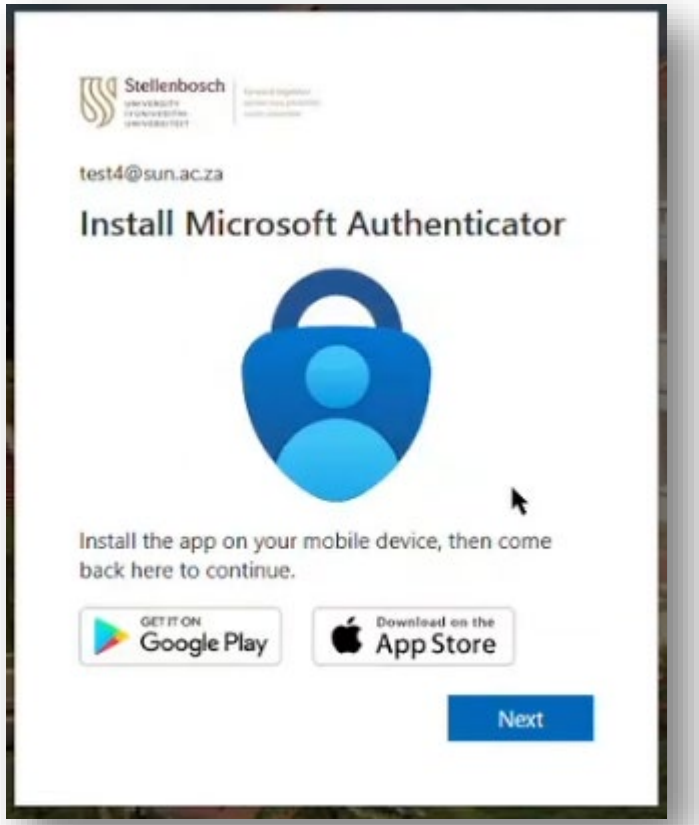


SMS/Voice to Authenticator app 2/4 8 Easy steps

3. You will be prompted with the below screen to improve your sign-in method. **Click next.**

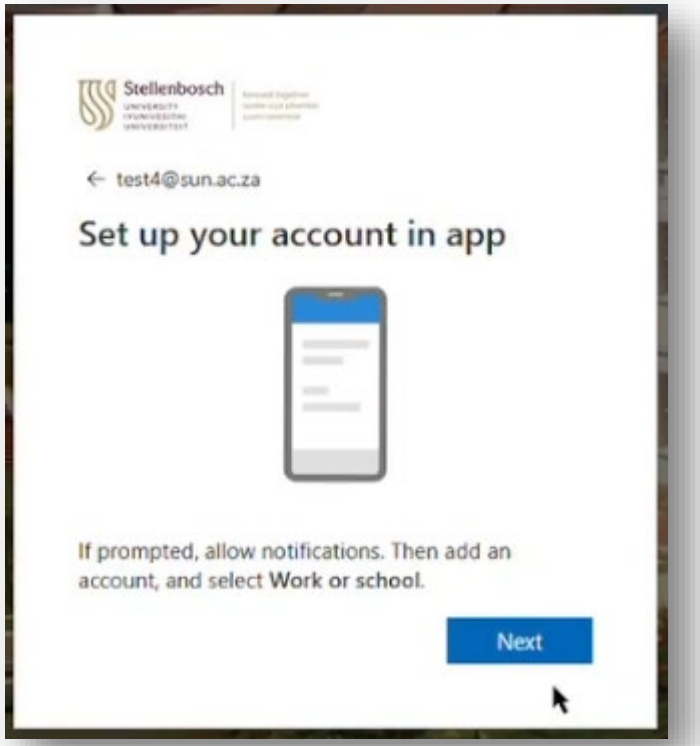


4. You will be prompted to install the Authenticator application on your cell phone. Click **Next**.

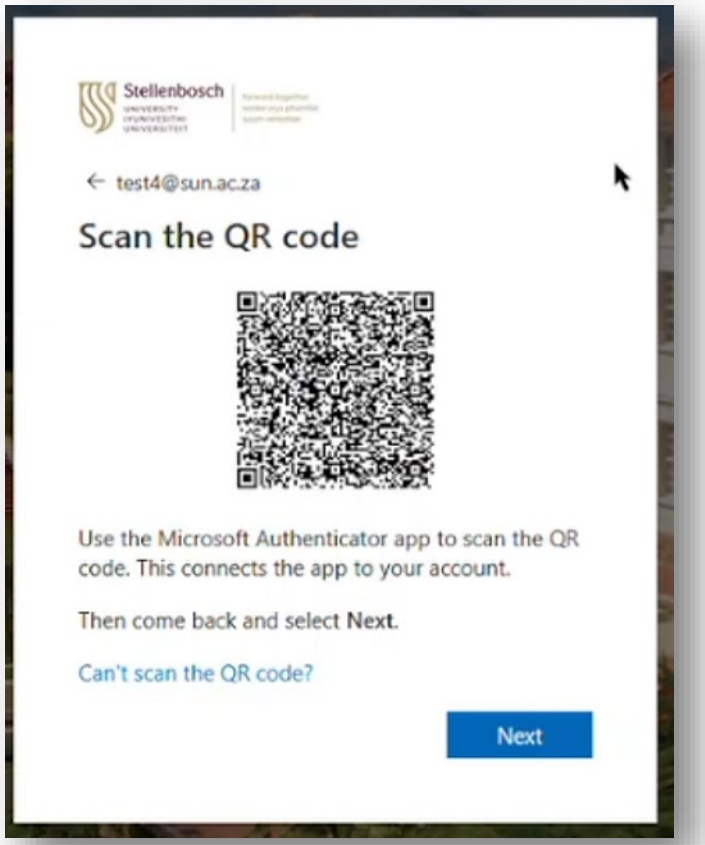


SMS/Voice to Authenticator app 3/4 8 Easy steps

5. Your account will now be added to the Microsoft Authenticator application. Click **Next**.

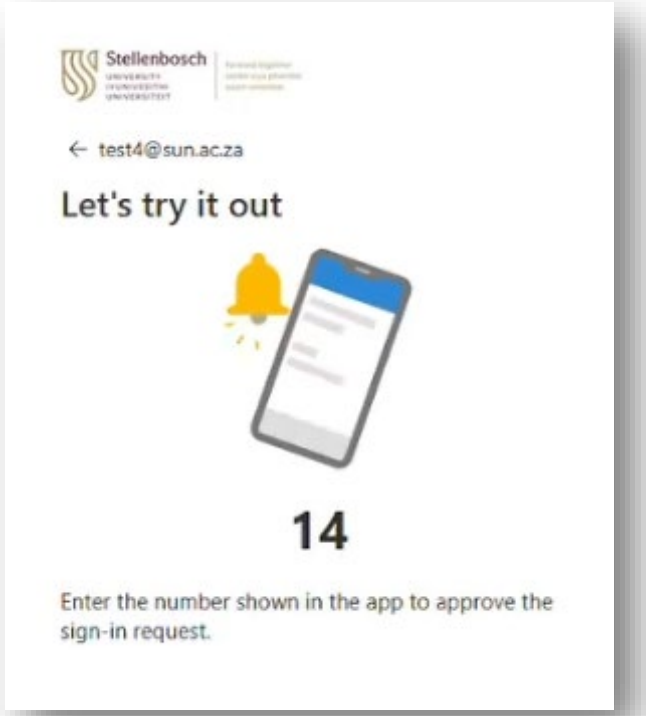


6. Scan the QR code as shown on your computer screen with your cell phone. Click **Next**.

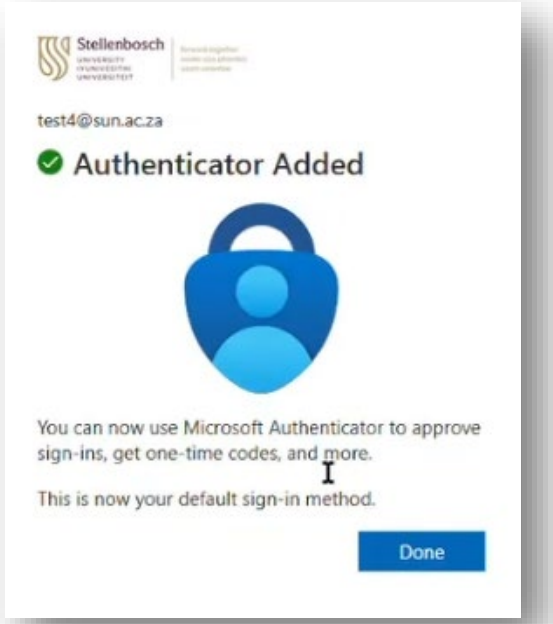


SMS/Voice to Authenticator app 4/4 8 Easy steps

7. Type the number that is displayed on your computer screen into the prompt on your cell phone:



8. As soon as you entered the number on your phone the prompt on your computer screen will change to Authenticator Added. Click on **Done**.



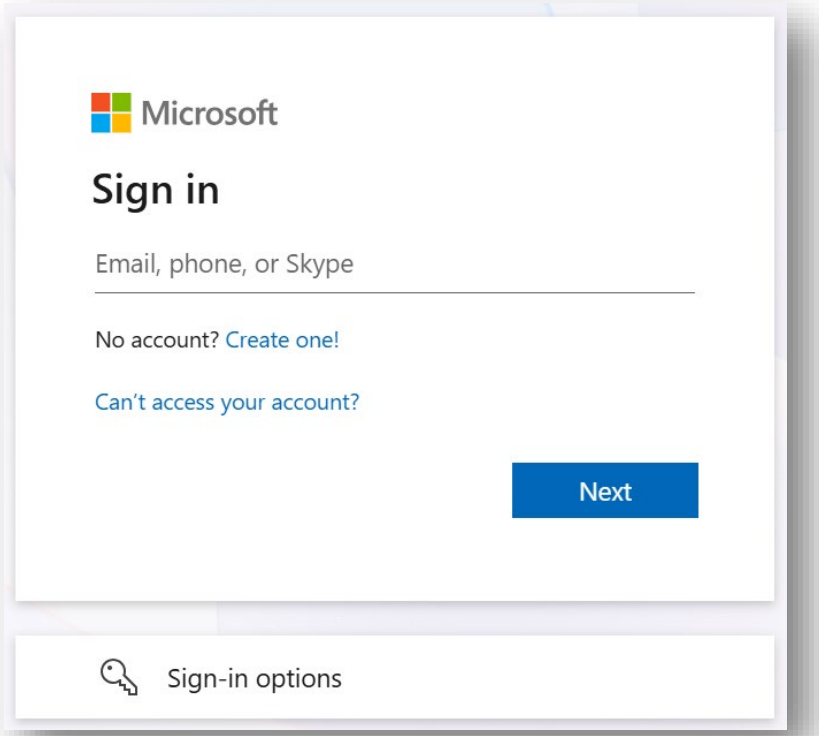
You are now signed in with the Microsoft Authenticator application into the Microsoft program that requested you to authenticate for instance Teams or Outlook. From now on going forward you will be prompted on the Microsoft Authenticator application on your cell phone to authenticate when necessary instead of an SMS or a voice call.

Passkeys

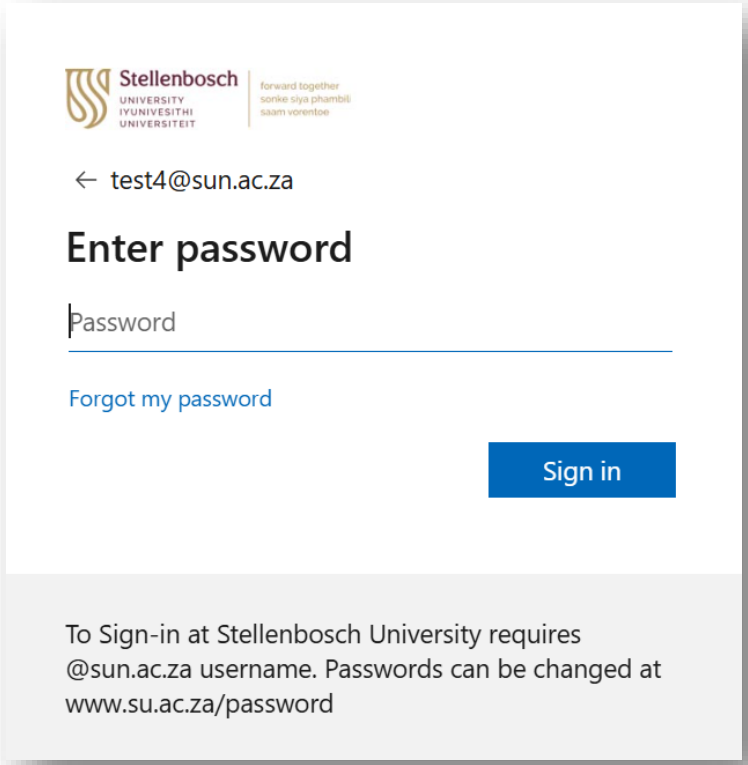
11 Easy steps

IMPORTANT: *Your MS Authenticator App must be on the latest version and device screen lock must be enabled.*

1. Sign in with your **SU email address** and click **Next**.

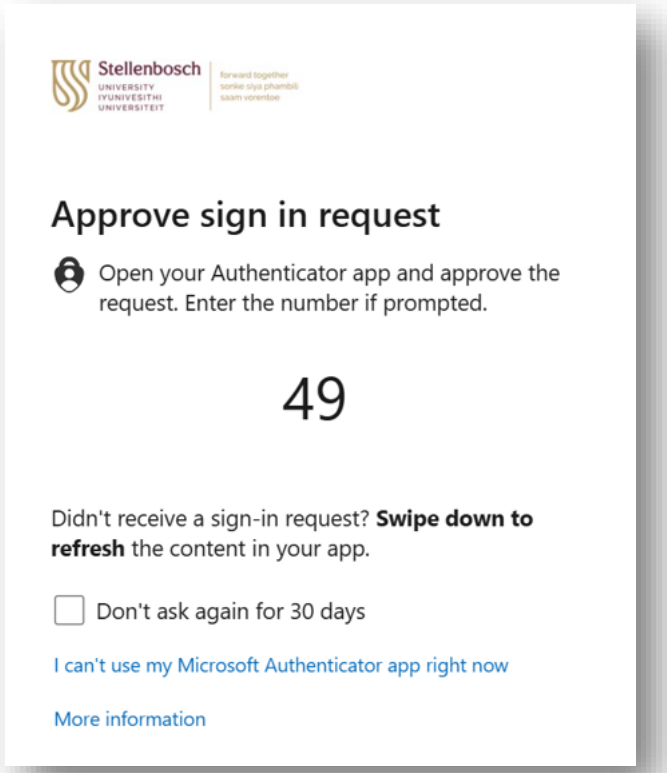


2. Enter your **password** and click **Sign in**.

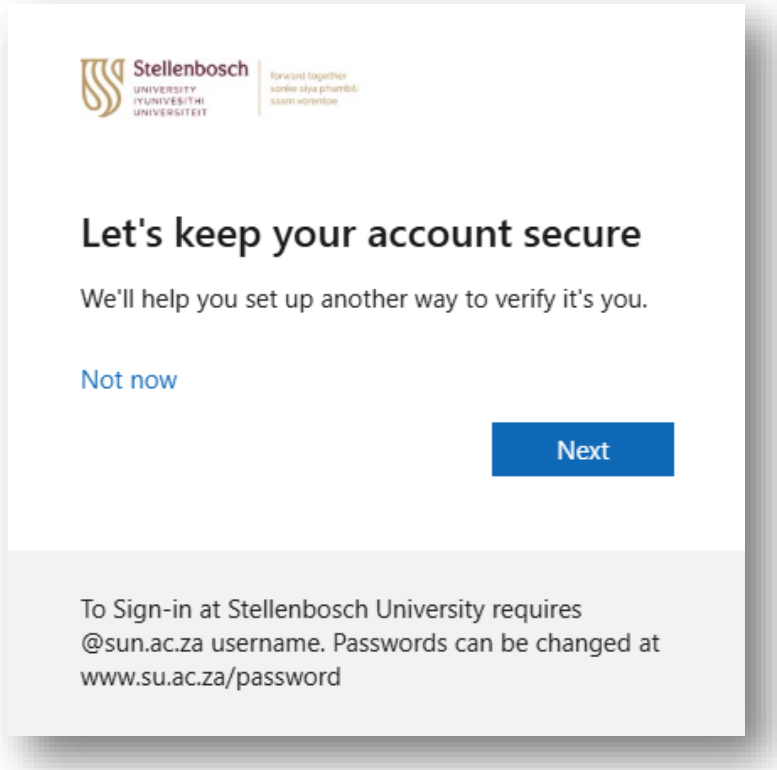


Passkeys

3. Click on the **Microsoft Authenticator notification** on your **mobile device** and enter the **number displayed on the screen.**

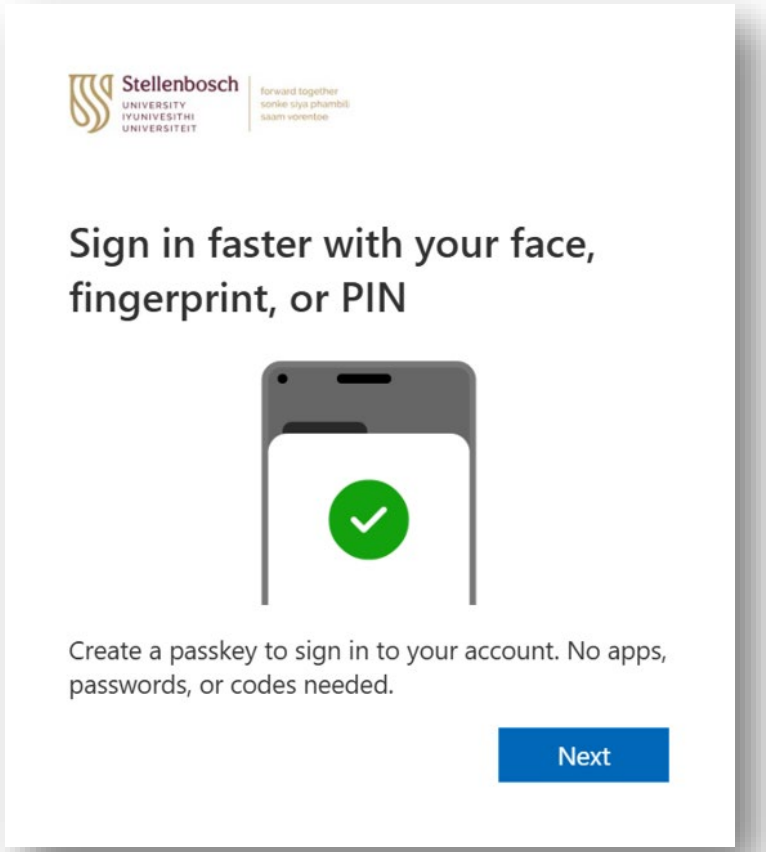


4. Select **Next**.

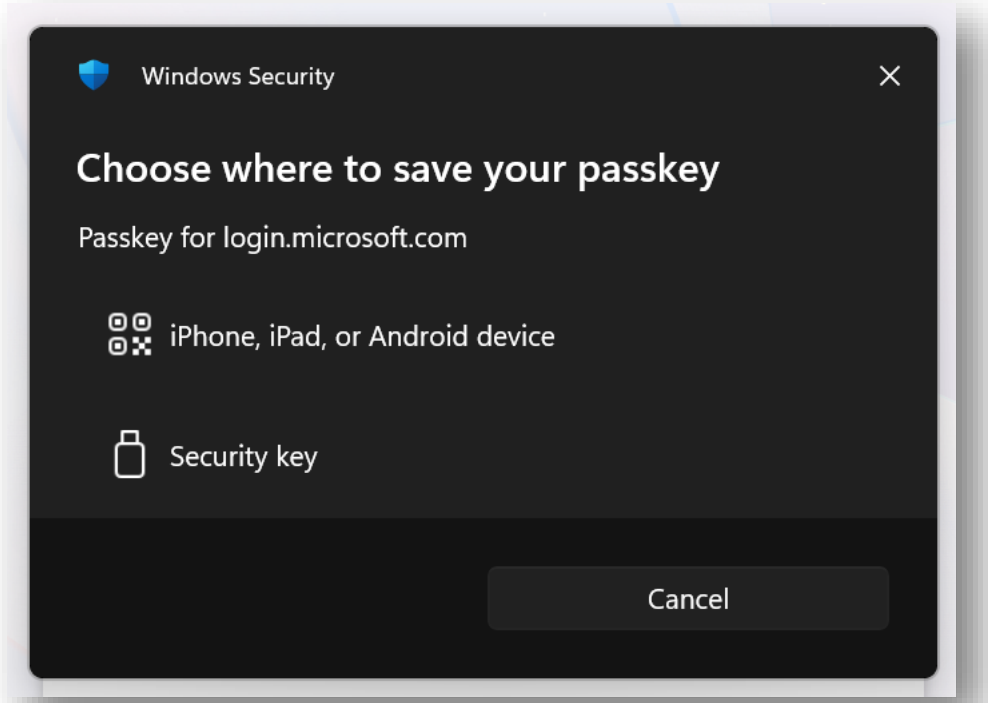


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

5. Select **Next**.



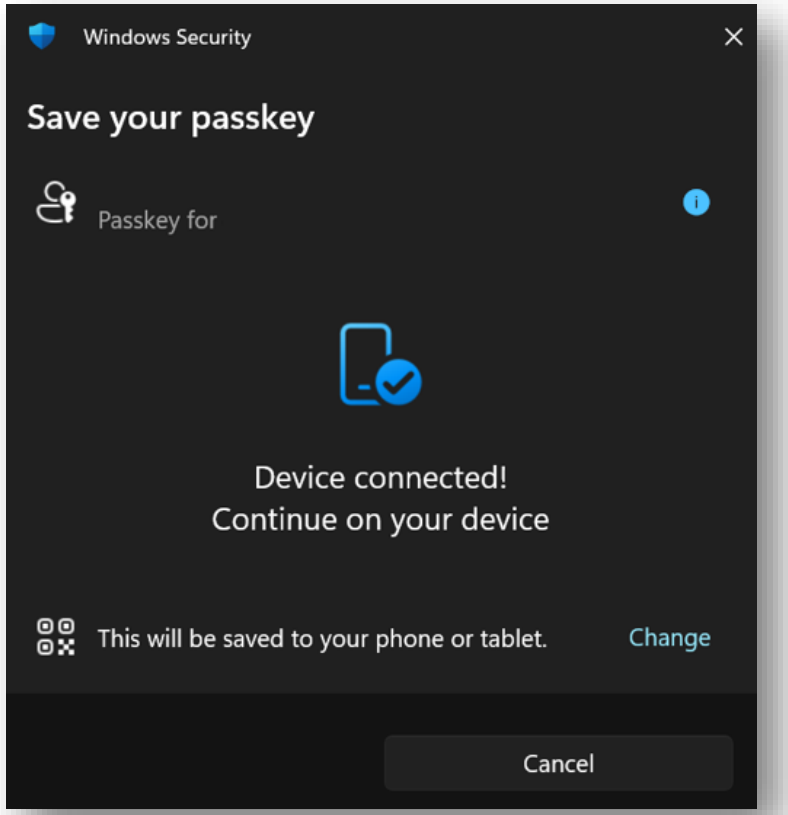
6. Click on the **iPhone, iPad, or Android device** option.



Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

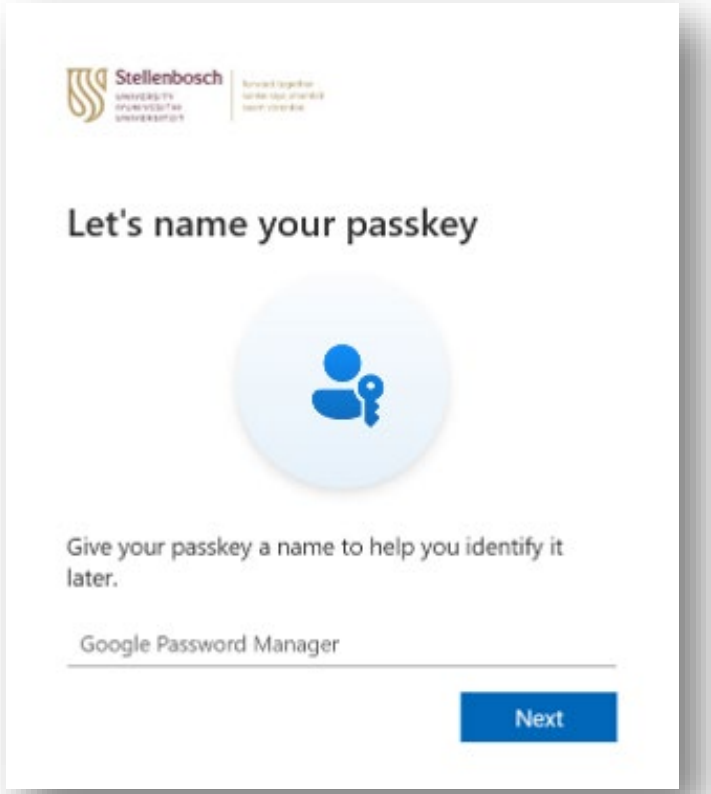
7. Open the camera on your mobile device and scan this QR code.

8. On your mobile device select **Create Passkey**.

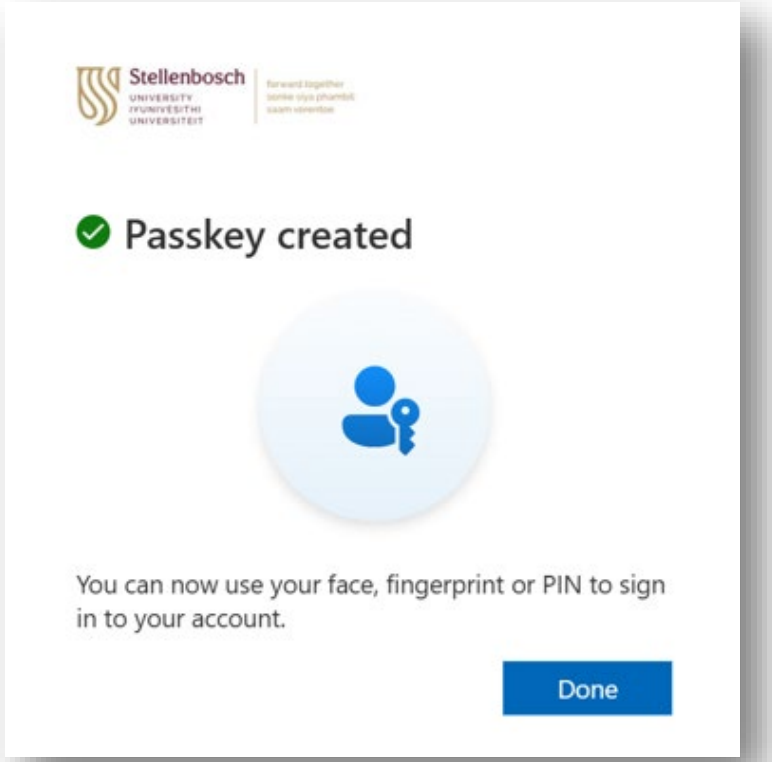


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

9. Type in a name for your passkey.

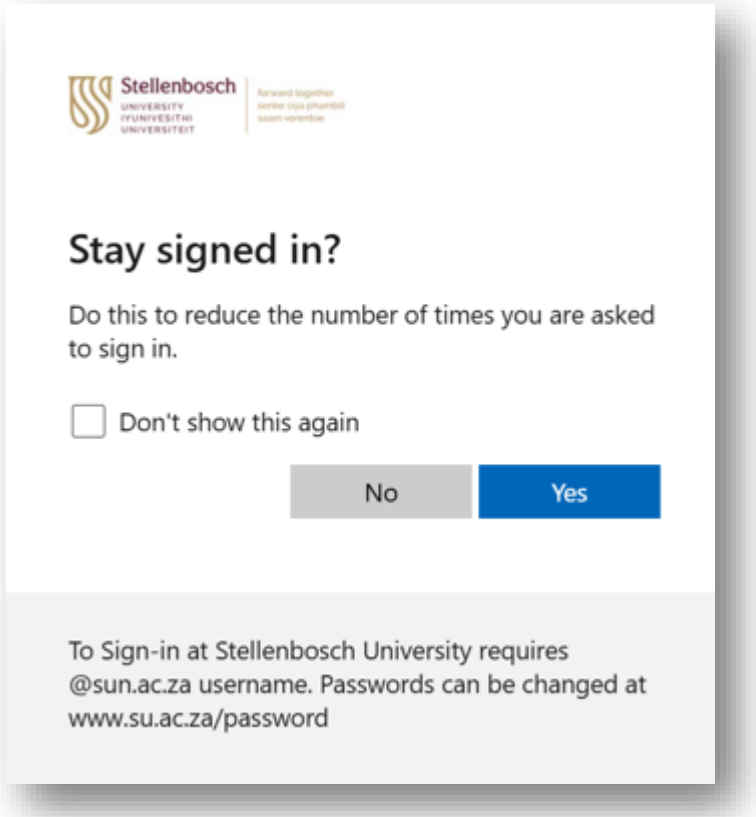


10. Enter your **password** and click **Sign in**.



Passkeys 6/6 11 Easy steps

11. Type the number that is displayed on your computer screen into the prompt on your cell phone:



Frequently Asked Questions

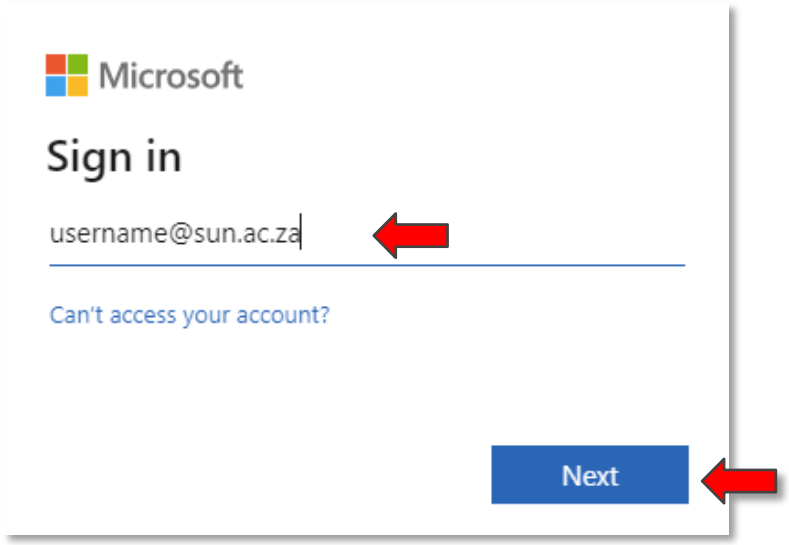
1. How do I add a second authentication method? ..... Click here
2. How do I change my default sign-in authentication method? ..... Click here
3. How do I install GBox? ..... Click here
4. How do I change from SMS/Voice method to the Microsoft Authenticator app..... Click here

Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

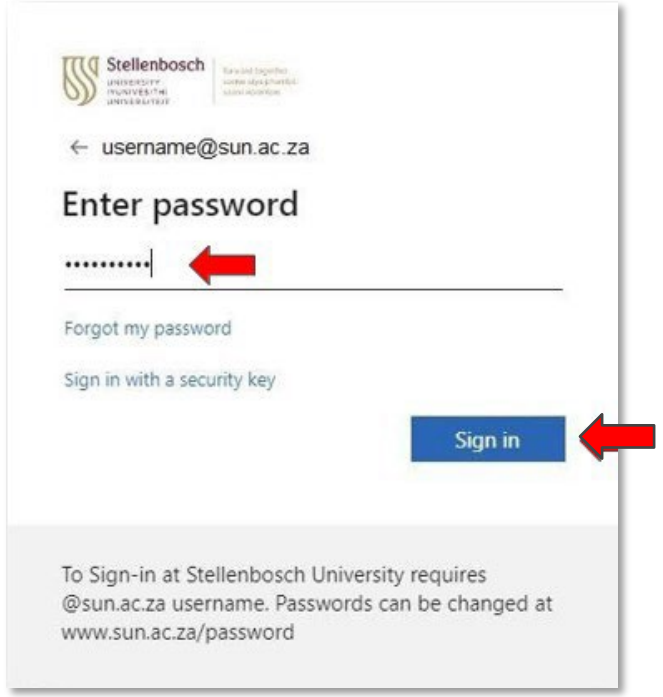
How do I add a second authentication method?

1. On your desktop, open your browser and type the following address: https://mysignins.microsoft.com.

   You will be prompted to sign in with your Stellenbosch University email address. Click **Next**.

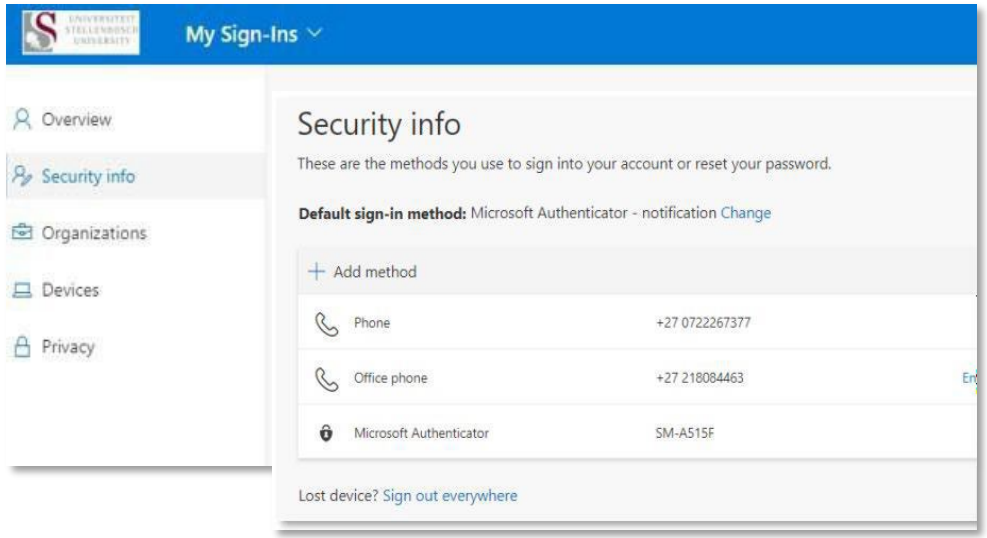


2. Enter your password and click **Sign in**.



FAQ: 2/2 4 Easy steps

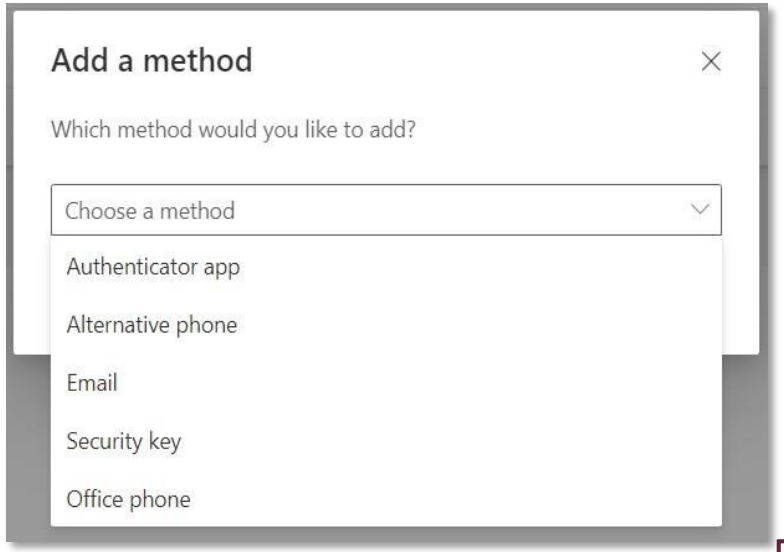
3. Once signed in, your Security Info will display with all the authentication methods you have registered. Left click on **Add method**.



4. Left click on the drop-down menu, select the method you want to add and click on **Add**.

We recommend the **Microsoft Authenticator** Application as a method.

Follow the steps for the chosen method as indicated in the steps provided in this document.

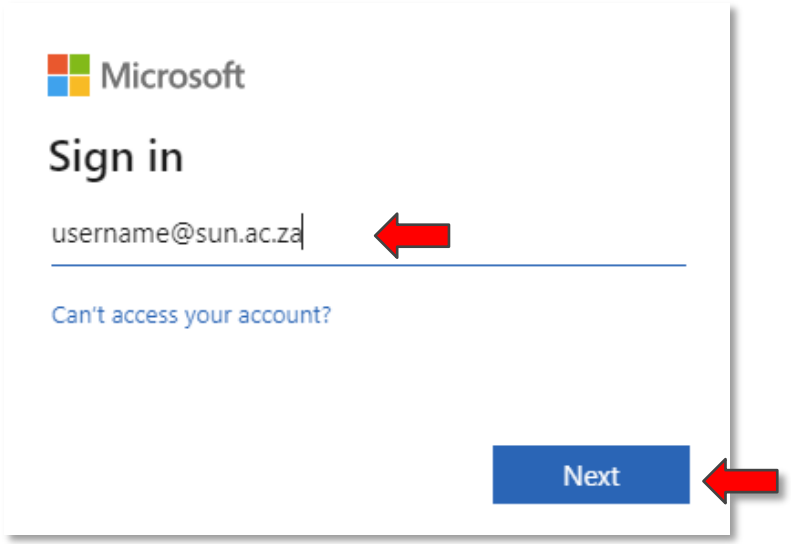


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

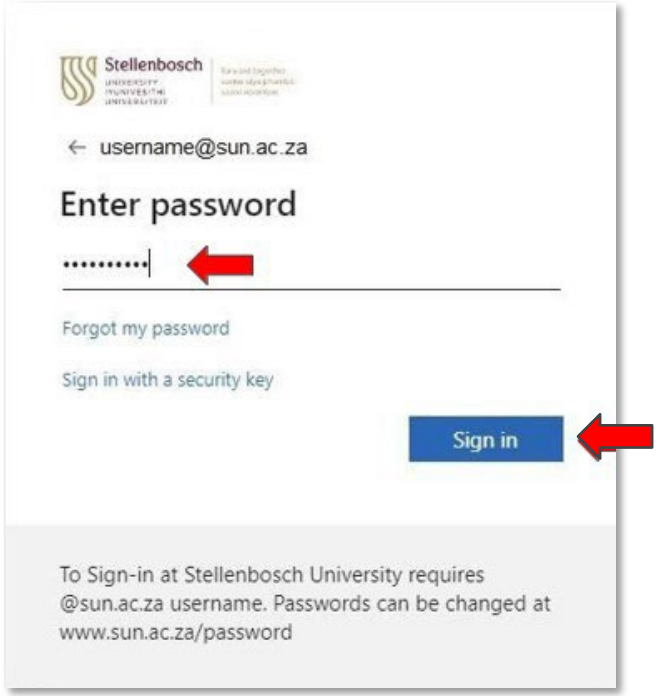
How do I change my default authentication method?

1. On your desktop, open your browser and type the following address: https://mysignins.microsoft.com.

   You will be prompted to sign in with your Stellenbosch University email address. Click **Next**.

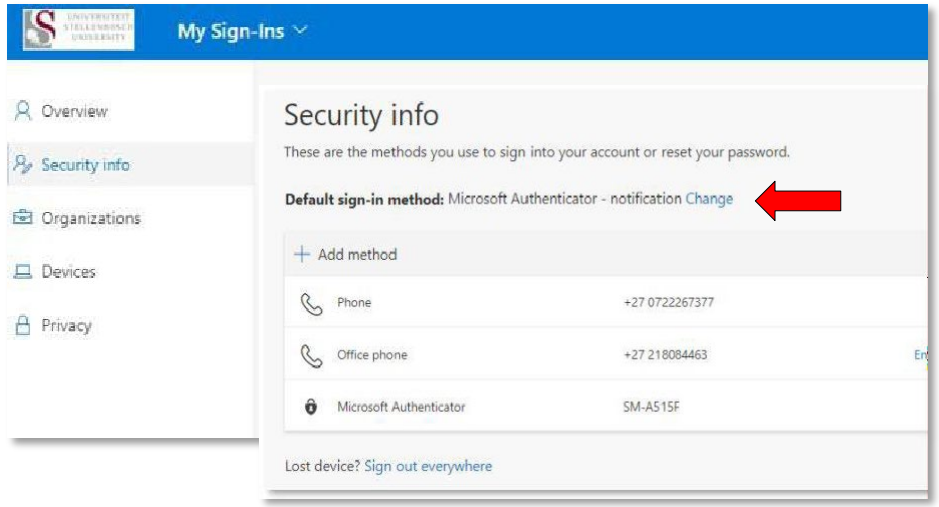


2. Enter your password and click **Sign in.**

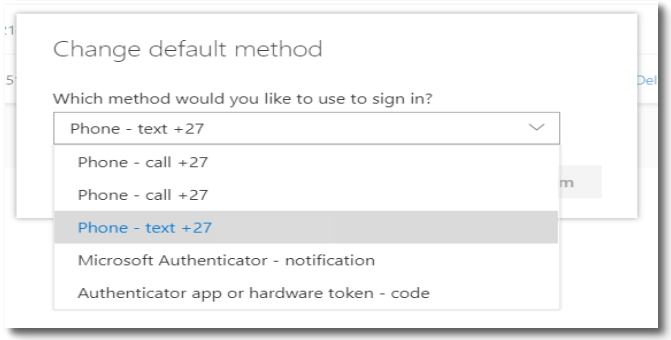


FAQ: 2/2 4 Easy steps

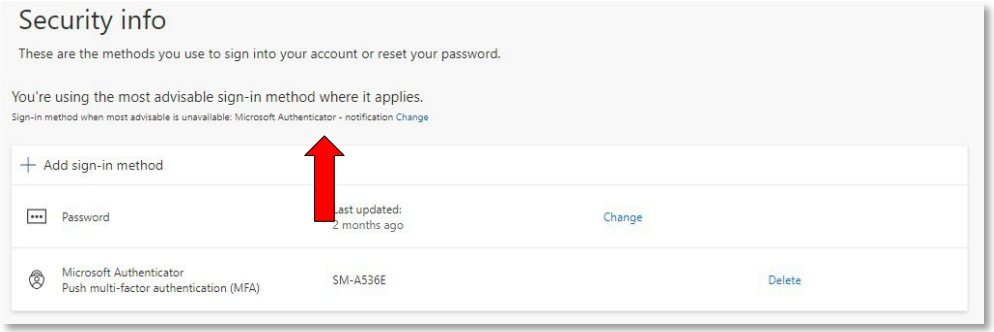
3. Once signed in, your Security Info will display with all the authentication methods you have registered. Left click on **Change**.



4. Left click on the drop-down menu and see all the available methods. Select the method of your choice and click **Confirm**.



Your new default method will display here:

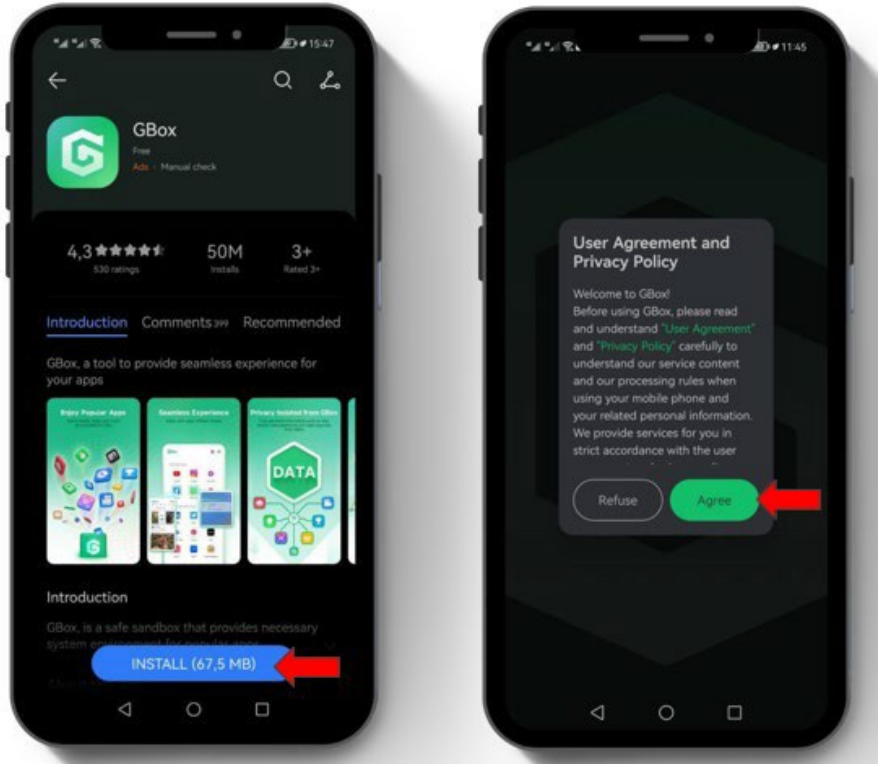


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

How do I install GBox?

1. In your app store, search for Gbox and click on **Get Gbox.**

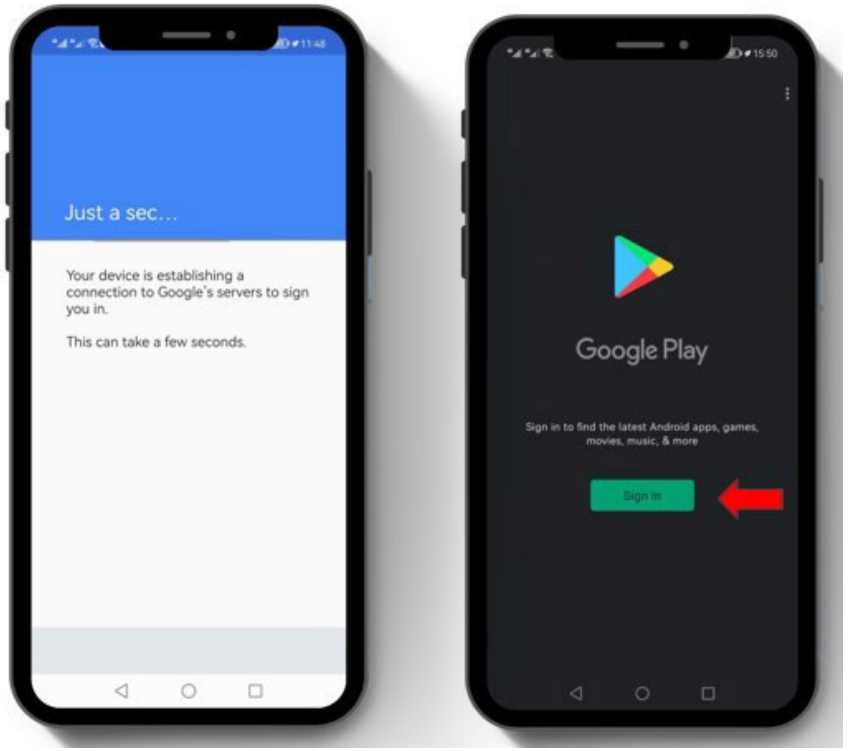
2. Select **Install** and click on **Agree**



Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

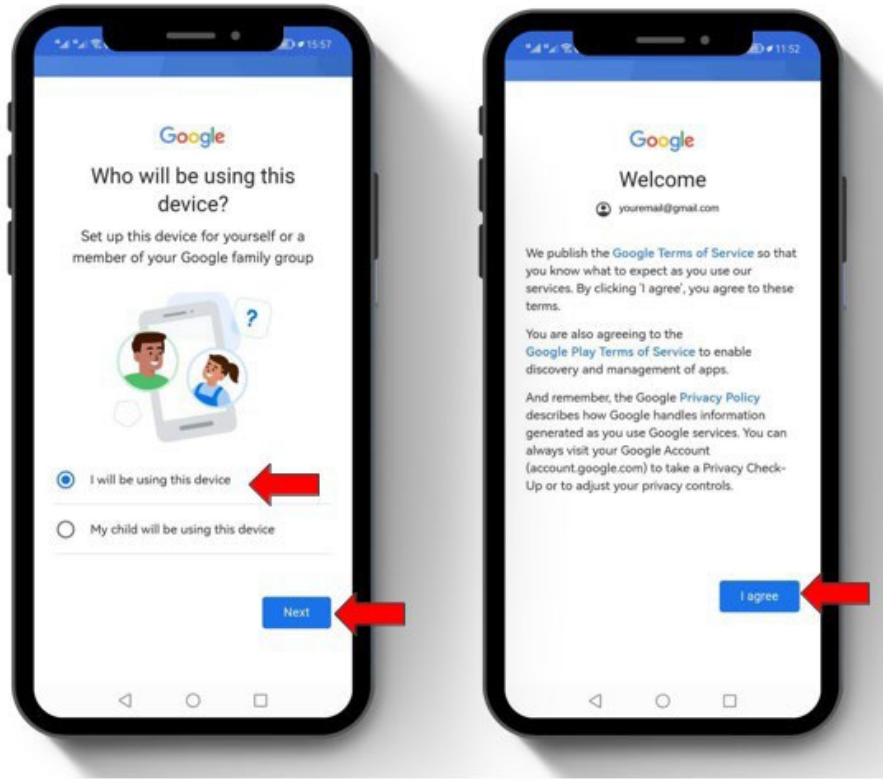
3. Go to the magnifying glass icon and search google authenticator.

4. Click on **Sign in.**

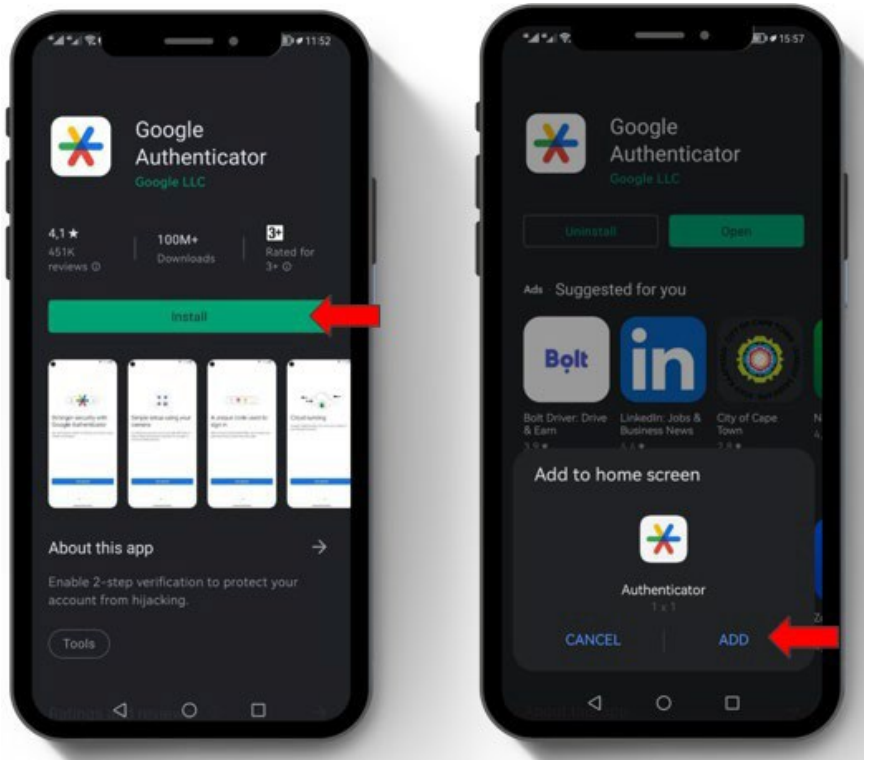


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

5. Select **I will be using this device** (if you are using your OWN device) and click **Next.** Then select **I agree.**

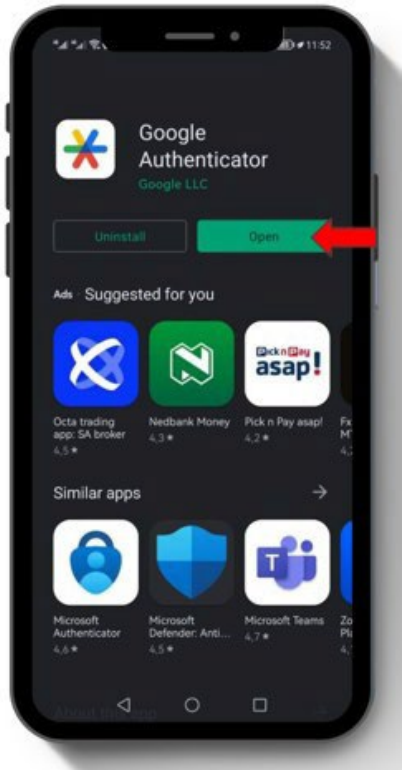


6. Click on Install and select **ADD**, to add the Authenticator app to your home screen.

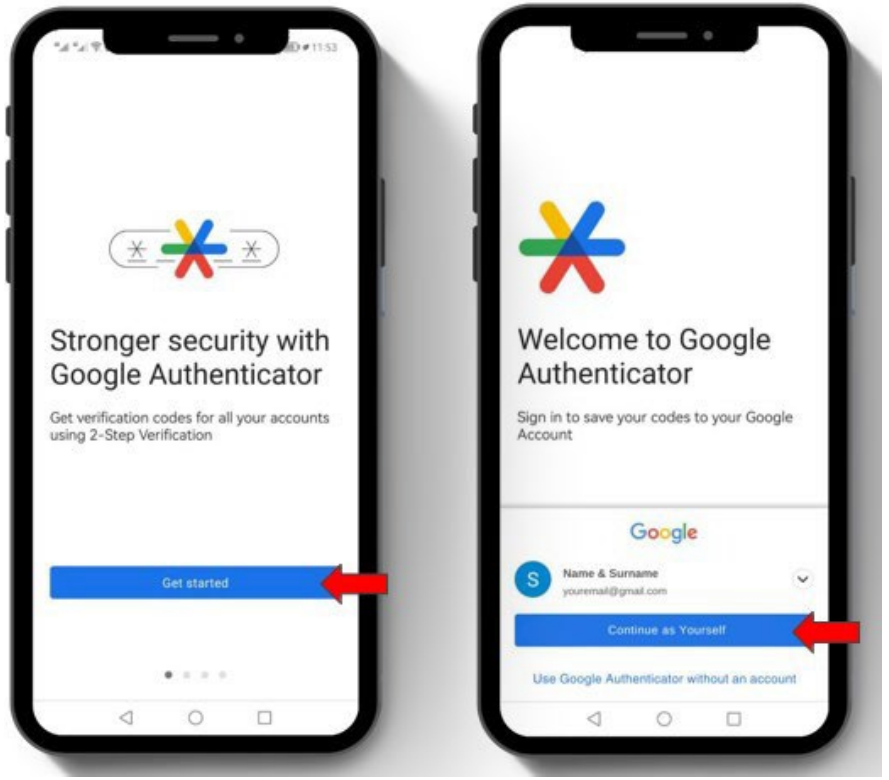


Home
How to use the guide
What is MFA?
What must I do?
Microsoft Authenticator Application
Google Authenticator Application
Hardware Token
SMS/Voice to Authenticator app
Passkeys
FAQ

7. Select **Open**.



8. Click on **Get Started** and choose **Continue as...**

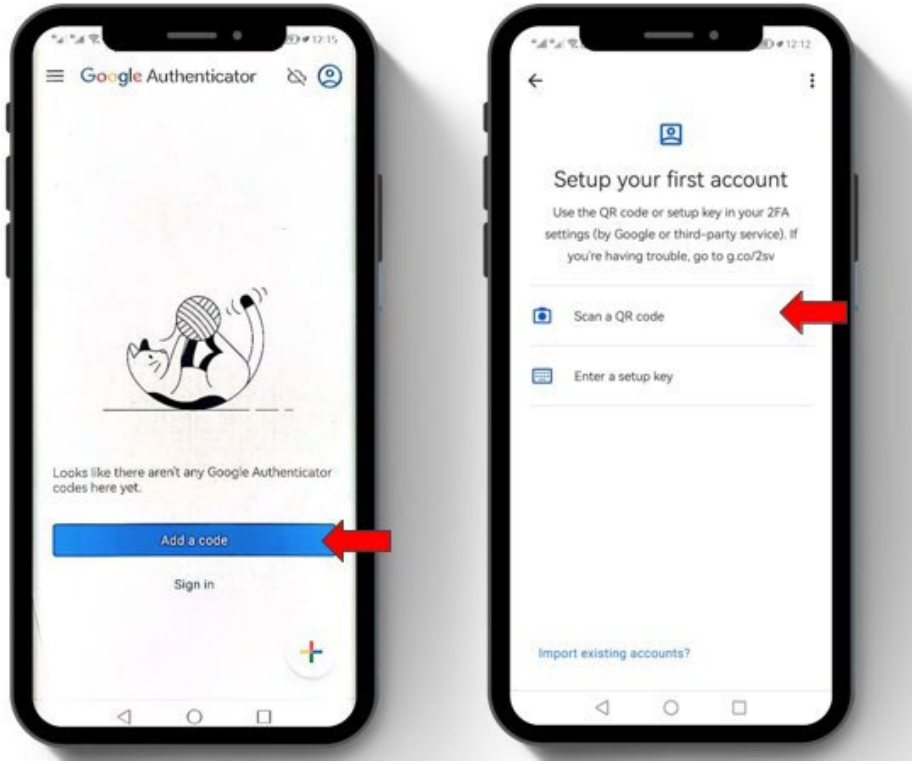


FAQ: 5/5 10 Easy steps

NB! Every time you want to authenticate you need to open GBox

9.

Click on **Add a code**, then select **Scan a QR code.**



10.

A code will now appear that you can use to authenticate with when signing onto a Microsoft product or service. This code changes every few seconds.