

MFA via Microsoft Authenticator App

This guide will advise you set up Microsoft Multi-factor Authentication.

Step-by-step guide

1. On your computer, visit portal.office.com You will be prompted to Sign in with your Stellenbosch University credentials. Type in your email address and click on **Next**.



Sign in

example@sun.ac.za

[Can't access your account?](#)

[Sign-in options](#)

Next

To Sign-in at Stellenbosch University requires
@sun.ac.za username. Passwords can be changed at
www.sun.ac.za/useradm.

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



← @sun.ac.za

Enter password

.....

[Forgot my password](#)

Sign in

To Sign-in at Stellenbosch University requires
@sun.ac.za username. Passwords can be changed at
www.sun.ac.za/password

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

4. When requested on how you should be contacted you select **Mobile App** and click on **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

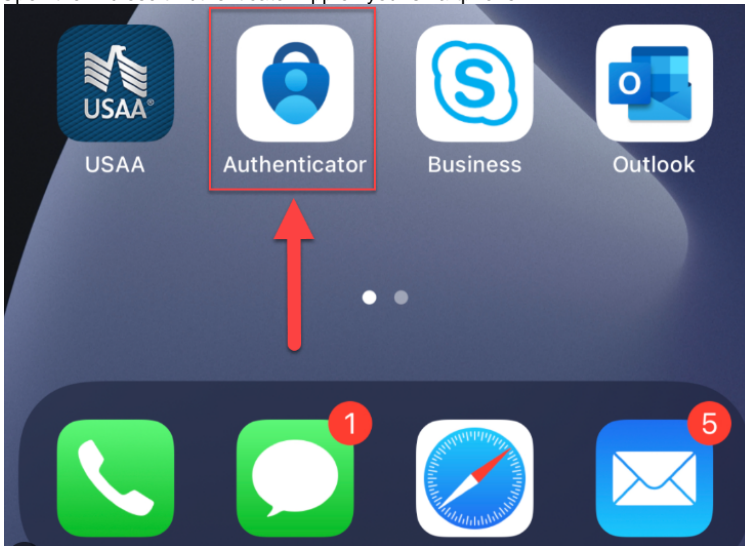
Mobile app has been configured.

Next

5. You will now have to install the Microsoft Authentication application from the application store on your mobile device.
For the Google Playstore link click [here](#)
For the AppStore link click [here](#)



6. Open the Microsoft Authenticator App on your smartphone



7. Select **OK** on Data Privacy.

Data Privacy

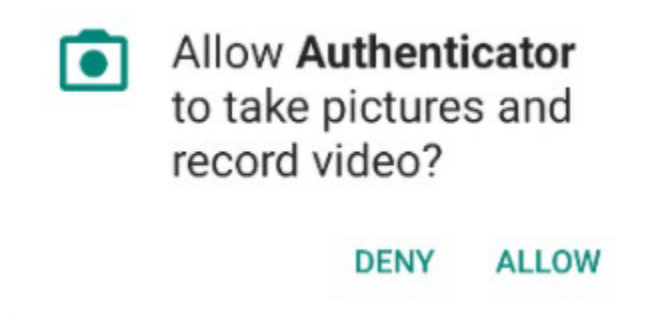
We gather non-personally identifiable usage data to help us improve the app. You can turn this off in settings. Learn more in the FAQs available under the Help menu.

OK

8. Select SCAN QR CODE.



9. Select **Allow** authenticator application to take pictures and record video.



10. Position the camera of your mobile device over the QR code displaying on your desktop. The mobile device will scan the QR code and your account will then show on the authentication application on your mobile device.



11. Return to your desktop and click **Next** on configure mobile App on your desktop.

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: 606 503 790

Url: <https://co1eupad04.eu.phonefactor.net/pad/452837391>

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

Next

[cancel](#)

12. The **Set-up** option will now be greyed out. Click on **Next**

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 for notifications and verification codes.


Next

13. The system will now try to reach your Mobile application.

Additional security verification

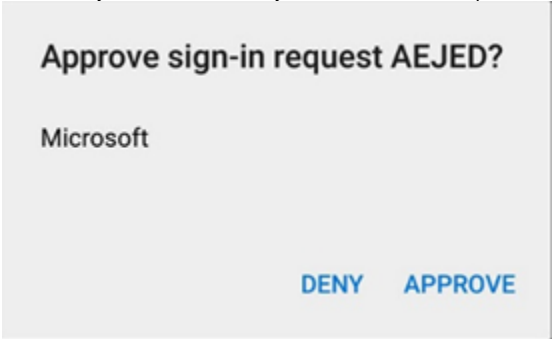
Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

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

 Please respond to the notification on your device.

Next

14. It will send you a notification to your mobile device. Tap **APPROVE** on the notification.



15. As soon as you click on **APPROVE** you will be asked to add your mobile device phone number. **We strongly suggest adding your mobile device phone number to act as a backup if you are unable to access or use the mobile App for any reason and click on Done.**

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

South Africa (+27)

Done

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

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

16. Click on **No** when asked to Stay signed in.



mfatest@sun.ac.za

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No

Yes

To Sign-in at Stellenbosch University requires
@sun.ac.za username. Passwords can be changed at
www.sun.ac.za/useradm.

17. When you see the screen below you can just close your browser. **You are now enrolled for Multi Factor Authentication via the authenticator application**

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

South Africa (+27)

0722267377

☐ Office phone

Select your country or region

☐ Alternate authentication phone

Select your country or region

Extension

☒ Authenticator app or Token

Set up Authenticator app

Authenticator app - SM-A605FN

Delete

restore multi-factor authentication on previously trusted devices

Restore

Save

cancel

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

Related articles

- Page:

[MFA via Microsoft Authenticator App](#)

- Page:

[MFA via SMS](#)

- Page:

[Cashless Payments](#)

- Page:

[Removing private\ random device mac](#)

- Page:

[RegisterMe! Windows device](#)