

Multi-Factor Authentication (MFA) Set-Up Guide v2.0

In order to use the MFA, two things need to happen:

1. Set up the MFA
2. The MFA must be activated for your account by the administrator

If you have not received the email announcing the activation of the MFA for your account you can request it (see [Multi-Factor Authentication \(MFA\) Manual](#) (section 12)).

This guide provides details on how to set up the MFA (step 1). You can do this at any time before the activation (step 2).

There are five ways of using the MFA with the UN Office 365 accounts:

1. approving a request in the Authenticator app,
2. using a verification code from the Authenticator app,
3. receiving a text message to a mobile phone,
4. receiving a phone call, and
5. receiving a phone call to an alternative mobile phone.

You should set up all the authentication methods provided by the system, as explained in this guide. If one authentication method is not available, e.g. you forget your phone at home, you can still use another method, e.g. receive a phone call to your office phone.

How to set up MFA?

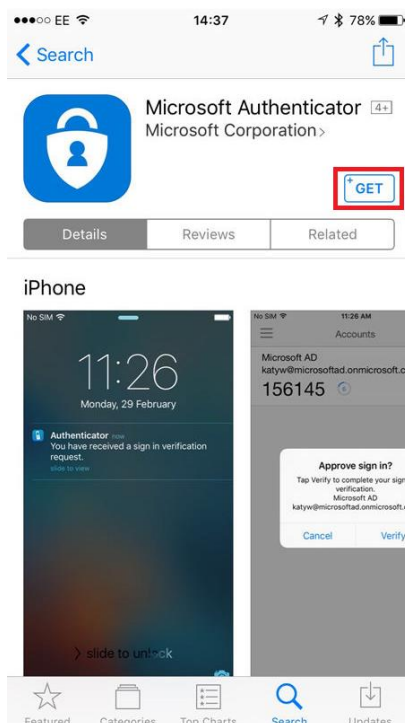


STEPS TO BE EXECUTED ON YOUR PHONE

Download Microsoft Authenticator for mobile devices

1. Open the application store
2. Search for **Microsoft Authenticator**
3. Install it

The Microsoft Authenticator is available for iOS, Android and Windows Phone.





STEPS TO BE EXECUTED ON YOUR DESKTOP

Configure MFA

4. Go to: <https://aka.ms/MFASetup>
5. Provide your email address and click **Next**

Microsoft

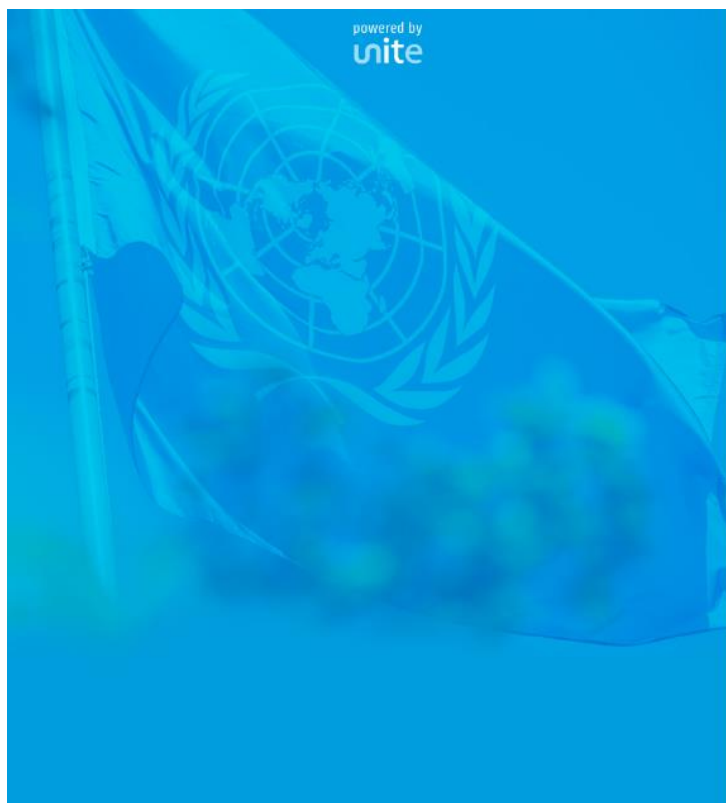
Sign in

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

[No account? Create one!](#)

Next

6. Provide your email address again and put in your Unite Identity password
7. Click **Sign in**



Sign in with your organizational account

Sign in

Sign in with your **@un.org** email address and **Unite Identity password**

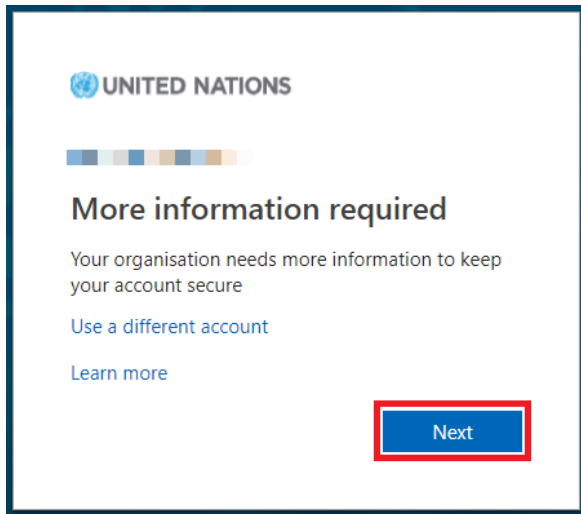
Forgot your password?

[Reset your Unite Identity password online](#)

An increasing number of fake websites designed to steal personal information, including usernames and passwords have been identified.

Please verify that this website is authentic before entering your username and password.

8. Click **Next**



UNITED NATIONS

More information required

Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

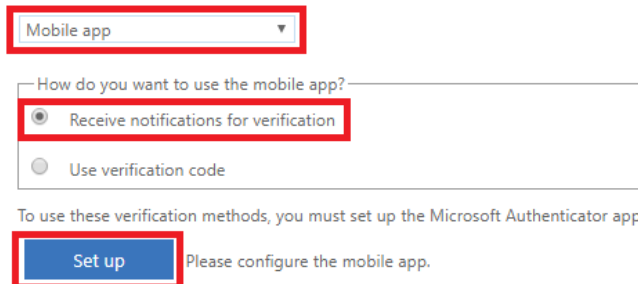
Next

9. Select **Mobile app** (recommended)
10. Select **Receive notifications for verification** (recommended)
11. 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 Please configure the mobile app.

Next

12. You should see a window, like the one below, open

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Azure 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: 555 555 555

Url: <https://urlheretocopy.phonefactor.net/555555555555>

If the app displays a six-digit code, you are done!

iPhone

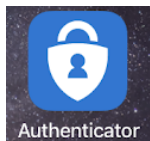


Windows Phone

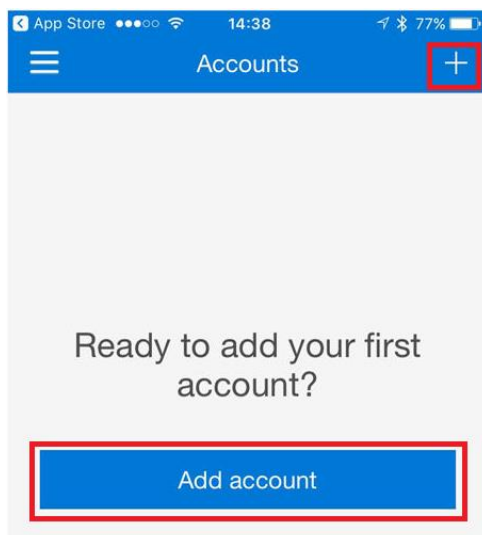
STEPS TO BE EXECUTED ON YOUR PHONE

Link Microsoft Authenticator to your UN Office 365 account

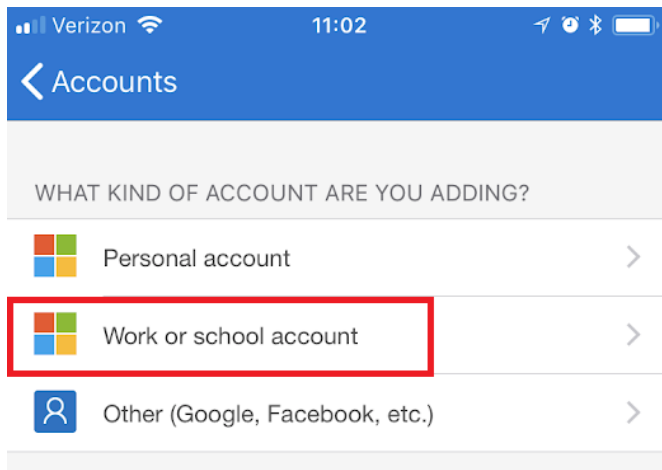
13. Open the Authenticator app



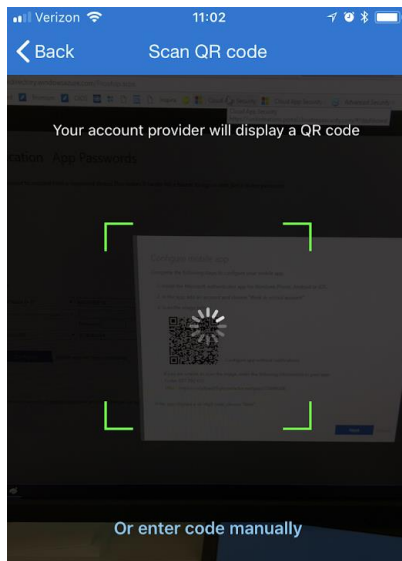
14. Click **Add account** or click the '+' button



15. Click **Work or school account**



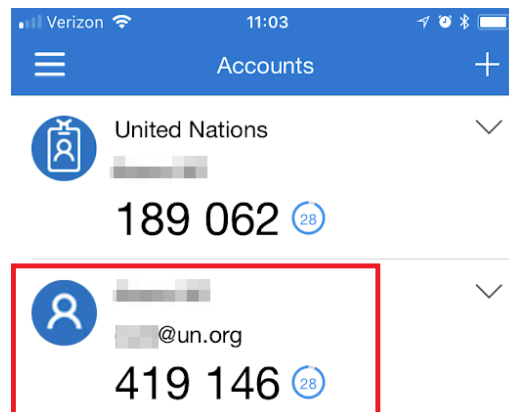
16. Direct the camera towards the barcode on your PC



If you cannot use your phone camera, you will have to manually enter the 9-digit code and the URL.

If the phone is not able to scan the QR code try to increase the brightness of the screen.

17. Your account will be added to the Authenticator app automatically





STEPS TO BE EXECUTED ON YOUR DESKTOP

Set up verification via Microsoft Authenticator

18. Click **Next**
19. After a few seconds you should see a message confirming the set-up of the Authenticator app
20. Click **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.

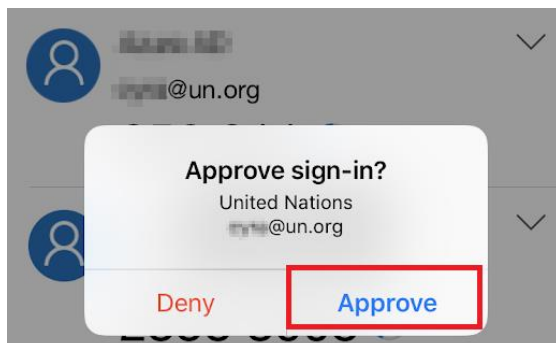
Next



STEPS TO BE EXECUTED ON YOUR PHONE

Approve request in Microsoft Authenticator

21. You will receive a notification; click **Approve**





STEPS TO BE EXECUTED ON YOUR DESKTOP

Set up alternative verification method

22. Wait for a few seconds till the phone entry form is shown
23. Provide the country of your phone number and put in the phone number
24. Click **Finished**

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

This phone number will be your alternative means of authentication. If you provide a mobile phone number you will be able to use both: calls and text messages to authenticate.

Finished

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

25. Click **Done** (skip this step if you have been redirected immediately to the **Additional security verification** form)
26. If the office phone number is populated, check the **Office phone** box
27. Check the **Alternative authentication phone** box, select the country of your phone number and provide a phone number, which is different from the phone number provided in step 23
28. Click **Save**

If the **Office phone** number is not populated by the system, you need to have your Global Contact Directory details updated. See <https://iseek.un.org/content/update-information-global-contact-directory>. The phone number has to be updated to the standard format (a space between the country code and the rest of the number is required, e.g. +1 212 963-3564).

Meanwhile provide your office phone number as the alternative authentication phone, as explained in step 27.

The alternative phone number can be used for receiving calls only. Only the primary authentication phone can be used for receiving text messages.

Additional security verification App Passwords

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 States (+1) ▼

☒ Office phone

United States (+1) ▼

Extension

Contact your admin if you need to update your office phone number. Do not use a Lync phone.

☒ Alternative authentication phone

Poland (+48) ▼

☒ Authenticator app

Set up Authenticator app

Authenticator app - iPhone

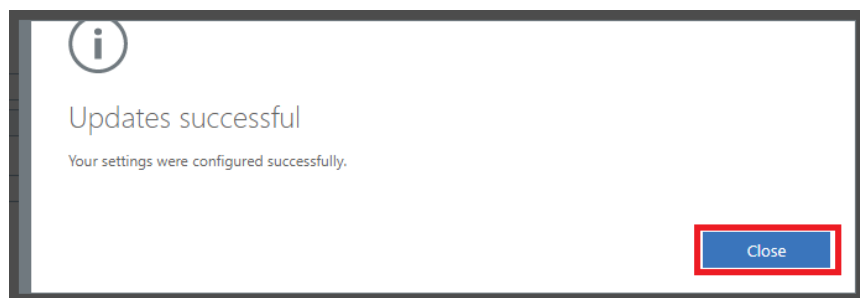
Delete

Save

Cancel

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

29. Click **Close**



MFA set up is complete. Remember that the MFA may not be active yet. It will be enabled on the day communicated to you in the email with which you received this guide. If you requested the MFA functionality on your own or if your account has been compromised, it will be activated when your service request gets resolved.