

# Onboarding Guest Accounts to UNHCR

DIVISION OF INFORMATION SYSTEMS & TELECOMMUNICATIONS (DIST)

## End-User Guide on how to set up the Microsoft Authenticator Application

**June 2025**

**PREPARED BY: CISO office.**

## Contents

1. Objective.....	3
Prerequisites .....	3
2. Setting up a multi-factor authentication for Guest accounts .....	4
2.1 Setting up Microsoft Authenticator app.....	5
2.2 Setting up MFA with an alternative method.....	10

# 1. Objective

The Objective of this document is to define the steps involved in configuring the Microsoft Authenticator Application for guest accounts and allowing them to access UNHCR resources.

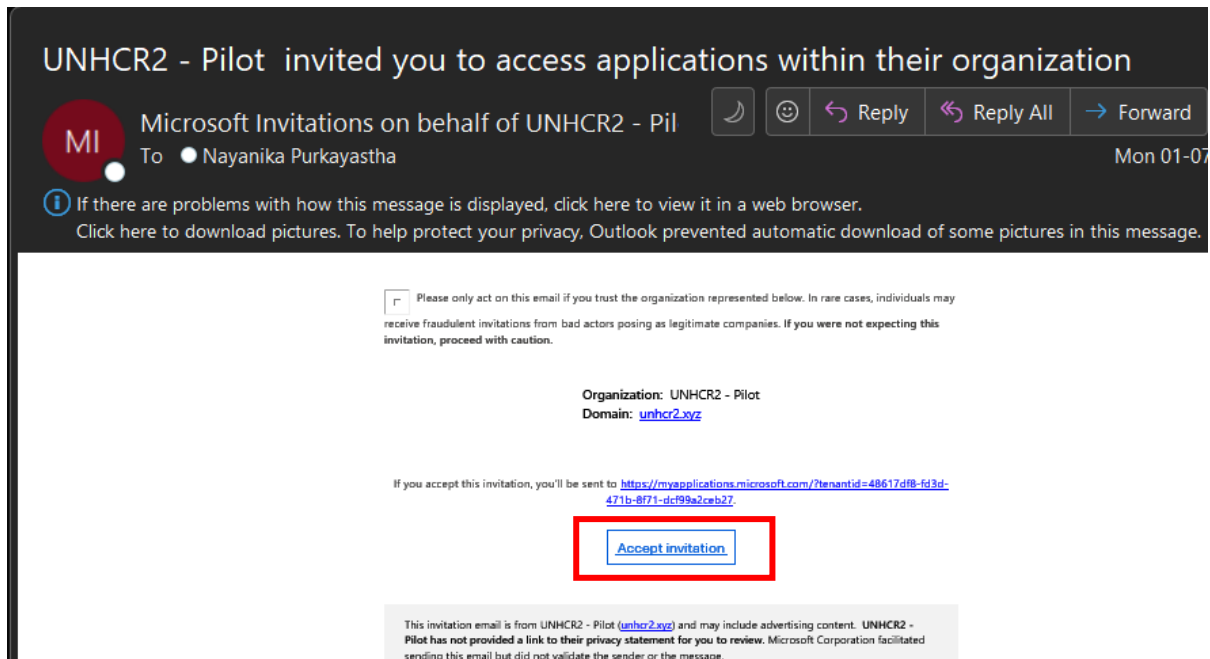
Guest users are accounts belonging to any external domain (partners) that are allowed to access UNHCR resources. Either UN organization domains (e.g., @unicef.org, @wfp.org, etc) or external domains, public or private (e.g., gmail.com, savethechildren.org, etc.) may be assigned a UNHCR guest account, upon invitation from an internal UNHCR member.

## Prerequisites

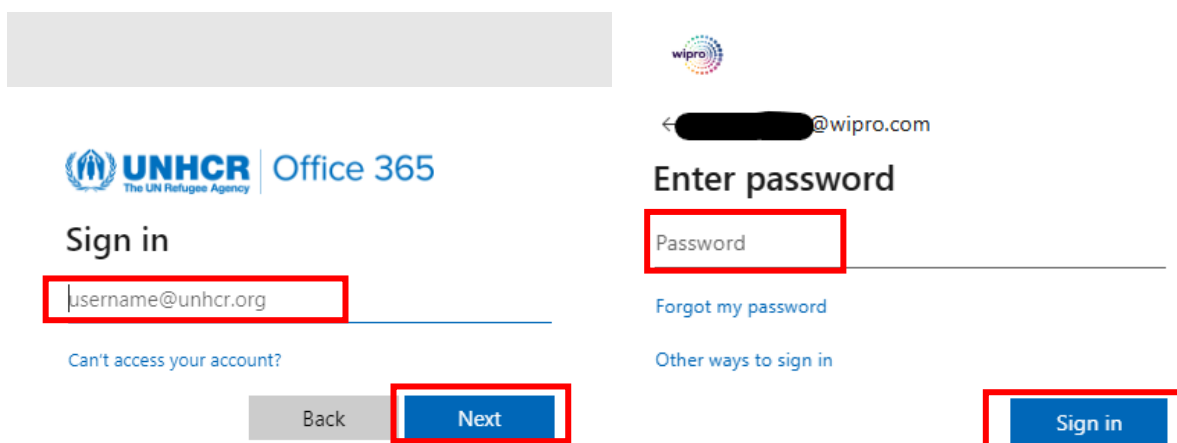
- You will need your UNHCR guest user account username (the email address\* to which the guest access rights were granted, e.g., [username@unicef.org](mailto:username@unicef.org) or [username@gmail.com](mailto:username@gmail.com)).
- To have a phone or tablet or desktop or laptop to be configured as a second factor of authentication (using any of the available methods described in Appendix A).
- Your devices (computer or laptop and phone or tablet) should have Internet access.

## 2. Setting up a multi-factor authentication for Guest accounts

- If you are an existing user, you will be prompted to set-up MFA when you login to any UNHCR resource for the first time post MFA enforcement.
- If you have just joined UNHCR as a guest user, you should have received an invitation email in your mailbox containing a link to accept such an invitation. Click on “**Accept invitation**”, you will be taken to the My Applications Portal. Log in to UNHCR on the My Applications portal



- Once connecting to the UNHCR environment as a guest user, enter your UNHCR guest username (guest email address) in the pop-up window and click “**Next**.” In the subsequent window, enter the guest account password and click “**Sign in**”.



- At this step, the system will request additional information to set up your MFA. “**Accept**” the requested permissions and click “**Next**” to start setting up MFA:



██████████@gmail.com

## More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

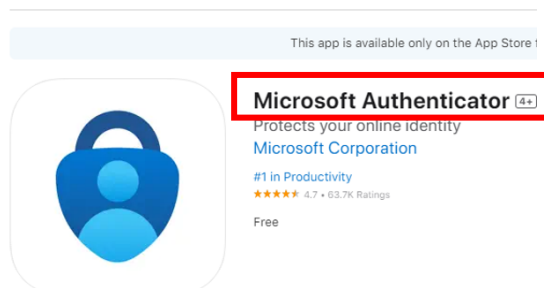
**Next**

## 2.1 Setting up Microsoft Authenticator app

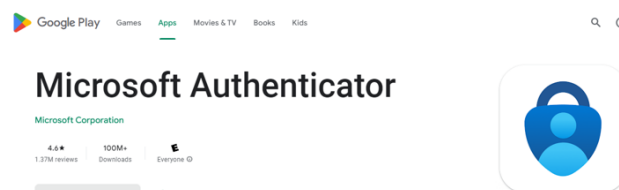
- Ensure you have installed the “Microsoft Authenticator app” on your smartphone or tablet. This application is available for free for “Android” and “iOS”. Please visit the pertinent application store depending on your device and install it:

### iOS

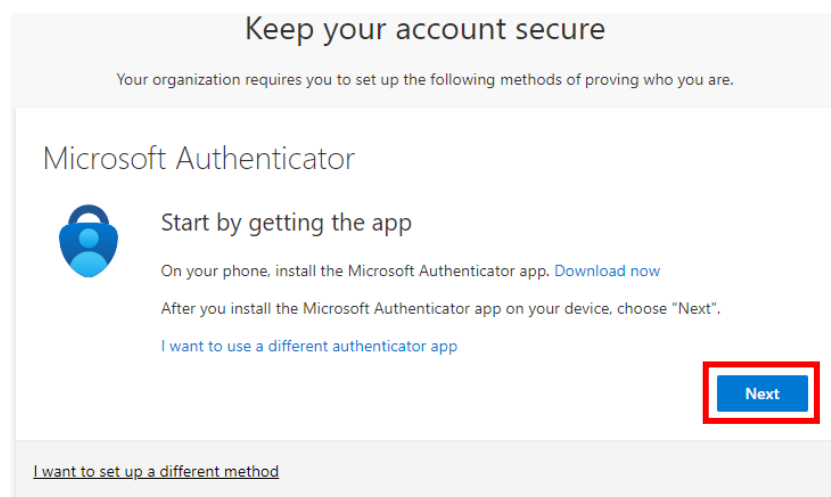
#### App Store Preview



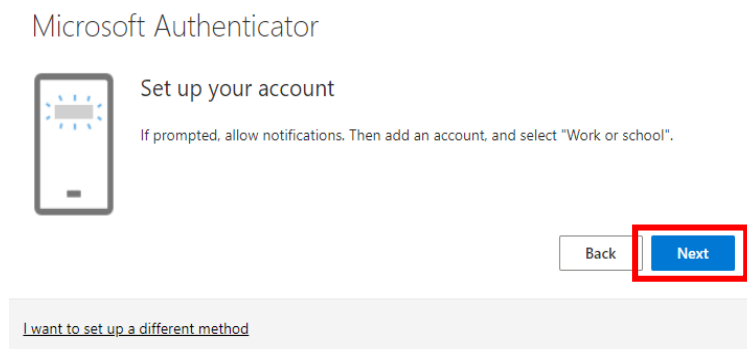
### Android



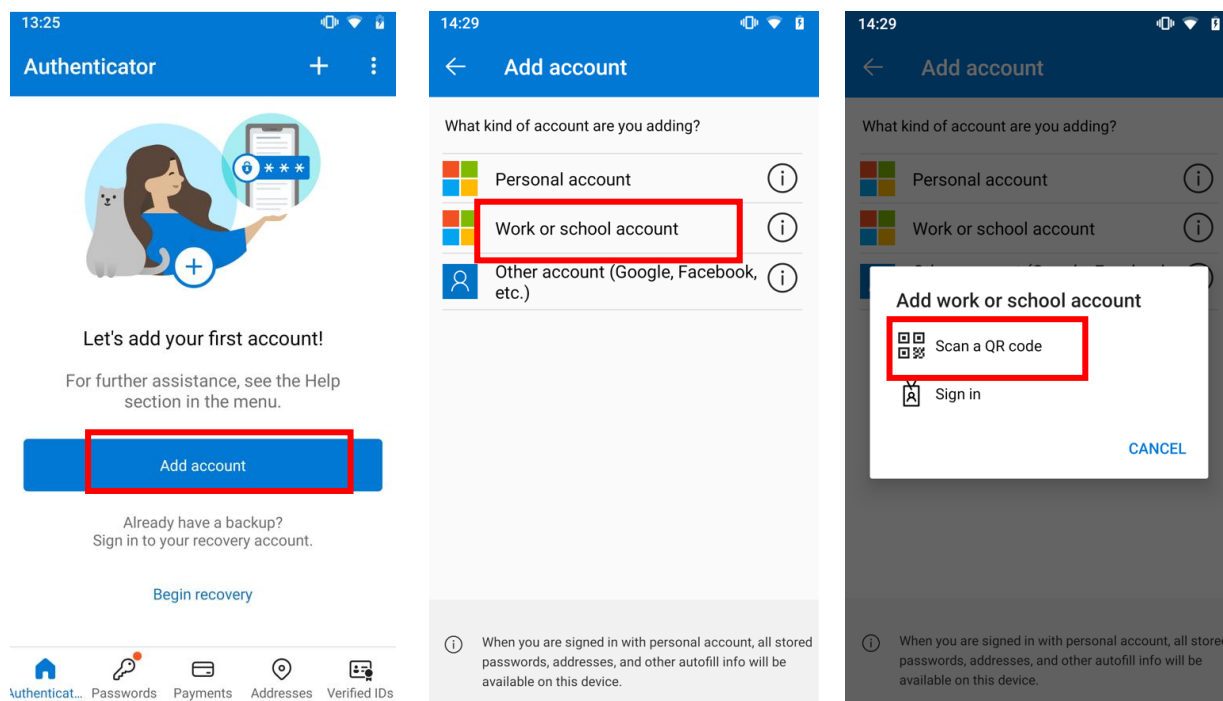
- On your computer or laptop, in the “Start by getting the app” screen, click “**Next**”



- In the “Set up your account” screen, click “Next” to proceed to setup:



- On your mobile phone/tablet, open the Microsoft Authenticator app. If prompted, allow notifications. Then, click on “**Add account**” button, select “**Work or school account**”, and choose **Scan QR code**.



- On your computer, in the “Scan the QR code” screen, **scan the QR code** shown using the Microsoft Authenticator app in your phone/tablet. You are now pairing your device and the account. Please note that the pairing process requires having an Internet connection active on both devices.

### Microsoft Authenticator

#### Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose “Next”.

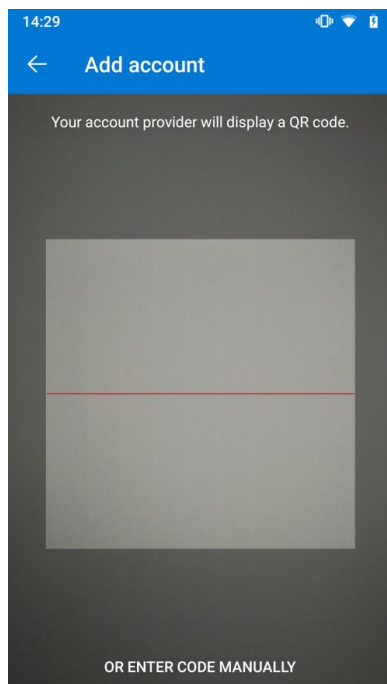


Can't scan image?

Back

Next

[I want to set up a different method](#)



**NOTE:** If the mobile camera is damaged or not working, you can manually enter the numeric code displayed on the desktop system when clicking on the “**Can’t scan image?**” button. Note that this process also requires an Internet connection.

## Microsoft Authenticator

### Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose “Next”.



Can't scan image?

Enter the following into your app:

Code: 489018485



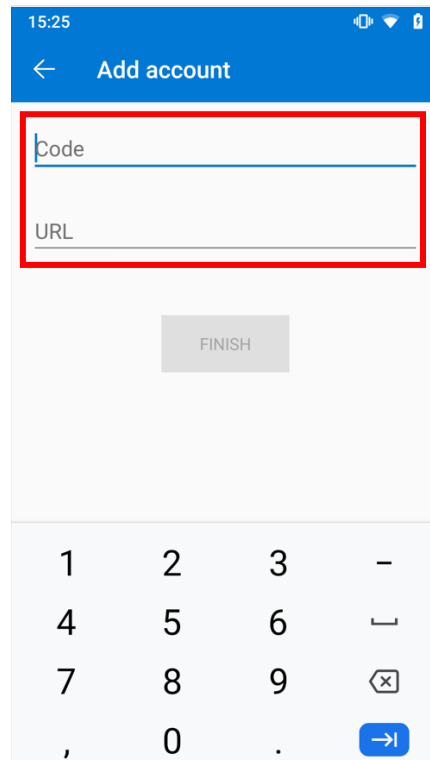
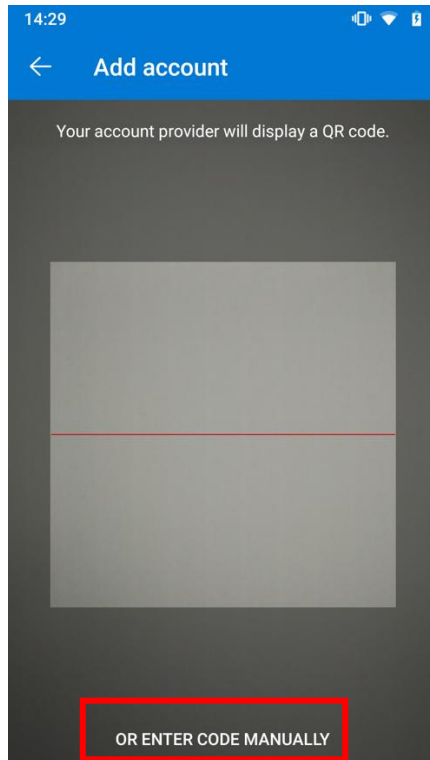
URL: <https://mobileappcommunicator.auth.microsoft.com/activate/369039924/WEU>



Back

Next

Use both, the “Code” and the “URL” shown on the desktop screen to fill in manually the data requested in the Microsoft Authenticator app when clicking on the option “**OR ENTER CODE MANUALLY**” at the bottom, as shown below. Then press the “Finish” button:





- After you scan (or enter manually) the QR code in the Microsoft Authenticator app, go back to the desktop screen and click “Next”. Then you should see a new screen with a two-digit code as shown below:

### Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

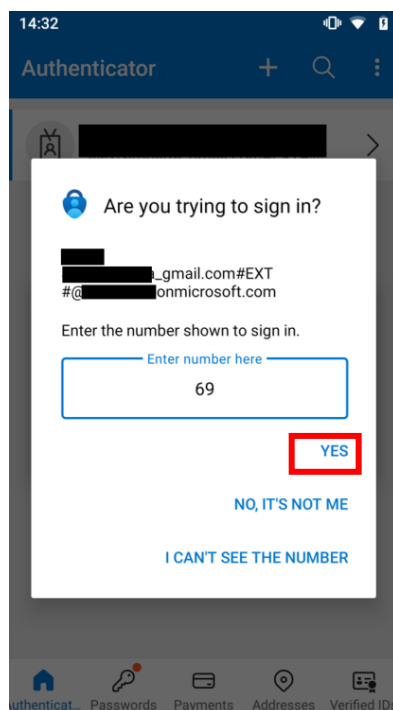
69

Back

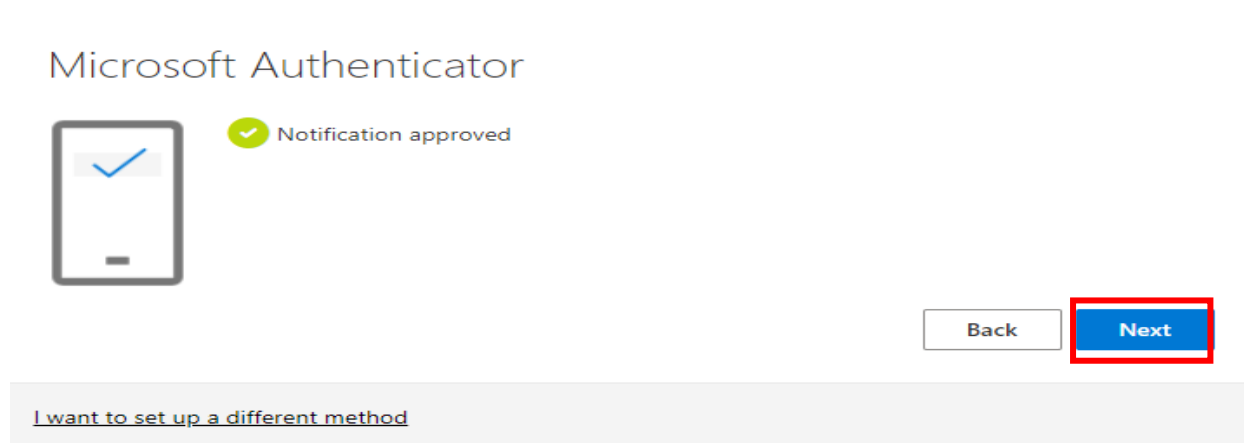
Next

[I want to set up a different method](#)

- Upon a successful configuration of the Microsoft Authenticator app, the application in your phone/tablet should display a pop-up message as shown below. Type the two-digit code shown in your computer (step above) in the Mobile Authenticator app and press “Yes”:



- Click “Next” in the “Notification approved” screen on your computer:



- Configuration of your primary MFA method has been completed successfully. Click **“Done”** to complete the setup assistant:

## Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

### Default sign-in method:

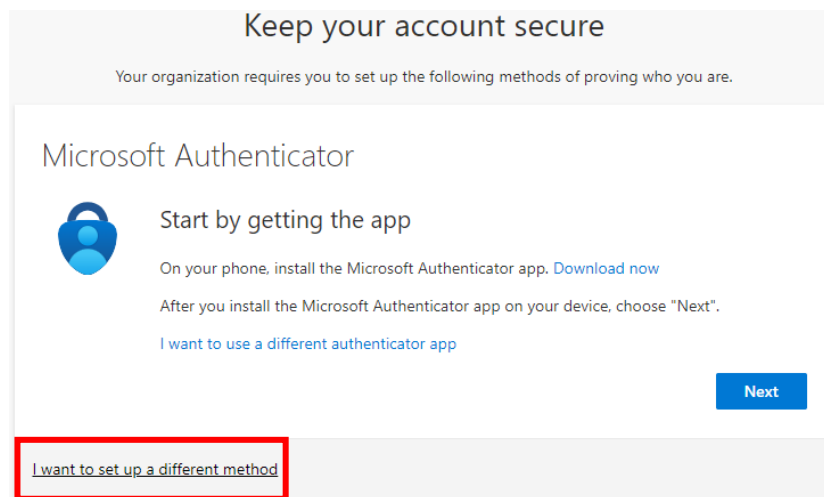


Microsoft Authenticator

Done

## 2.2 Setting up MFA with an alternative method

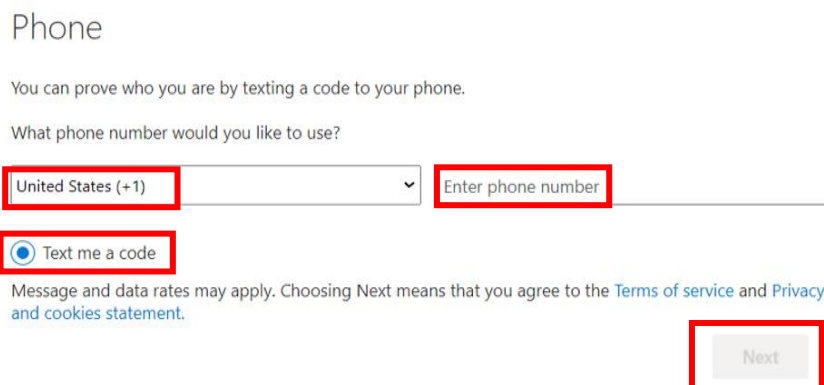
- If you can't use Microsoft Authenticator as the primary MFA method (e.g., don't have access to a smartphone or tablet) and need to configure a different method as the primary MFA alternative, click on **“I want to set up a different method”** (at the lower left corner):



- On the pop-up screen, choose one of the methods available to configure as alternative. One of the most commonly used alternative methods is “Phone” which allows to either send an SMS or receive a phone call on the specified phone number as a MFA method. Select “Phone”:



- Select one of the available options (in our example, “Text me a code” to get an SMS as an MFA method), choose your country from the drop-down list (this is essential to define the right country code) and enter the phone number on which you would like to receive the SMS. Then click “Next”:



- You should receive an SMS with a 6 digits code which you need to enter in the next screen to continue with the alternative MFA method configuration. Once specified, click on “Next”:

Phone

×

We just sent a 6 digit code to [REDACTED] Enter the code below.

Enter code

[Resend code](#)

Back

Next

- The MFA has been configured using an SMS as a primary verification method. Click “Done” to finish:

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose “Done” to continue signing in.

Default sign-in method: Phone [REDACTED]

Phone [REDACTED]

Done

**NOTE:** For security purposes and to help UNHCR keeping guest accounts secure in external devices, you will be requested to use the Multi-Factor Authentication (MFA) on each login, to confirm your identity during the authentication process.