ISTITUTO ITALIANO DI TECNOLOGIA

Multi Factor Authentication - User Guide

Contents

ICT User Guide

rev. 02 - 10/2021

Multi Factor Authentication

How does it work?

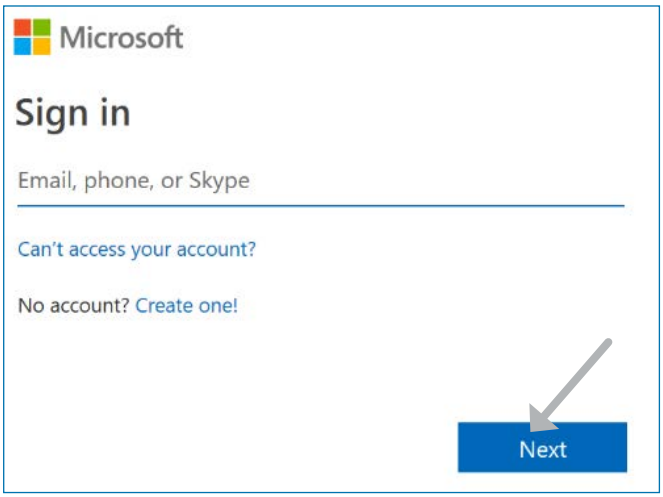
Multi Factor Authentication (MFA) is security method that ensures that only you can log into your account.
It does this by requiring at least 2 methods of authentication – your password and another piece of information.
Under certain conditions and on specific systems, a further verification step (of your choice) will be required which consist of one of the following operations:

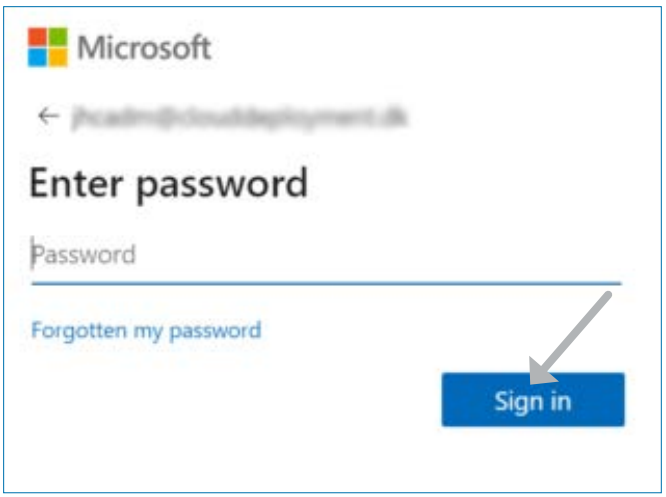
- Approval of a notification generated on your smartphone by the Microsoft Authenticator app (recommended).
- Entering a temporary verification code received on your smartphone through the Microsoft Authenticator app. (available for Apple and Android).
- Entering a temporary verification code received on your smartphone via SMS.
- Inserting a temporary code that can be viewed on a personal authentication token (for this option you need to contact ICT_Servicedesk@iit.it)

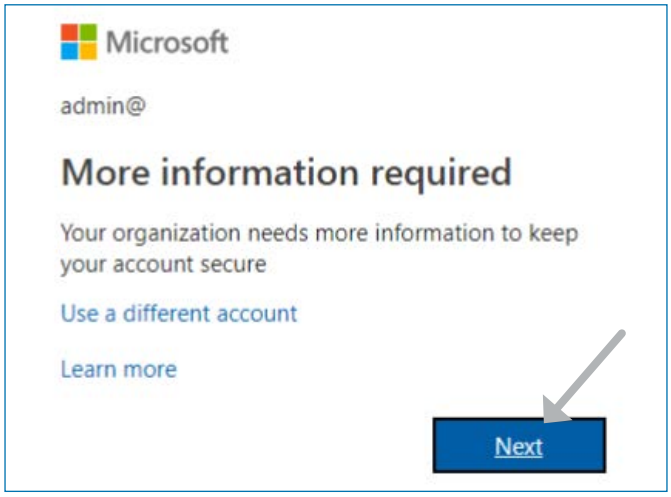
This guide will help you set up and register for MFA.

1. Register to MFA

1. To register for **MFA** visit: **https://aka.ms/MFASetup**
2. Login using your account **name.surname@iit.it**;
3. Enter your password;
4. You'll be prompted to set-up a method for secondary factor authentication on your account: Click **Next**;

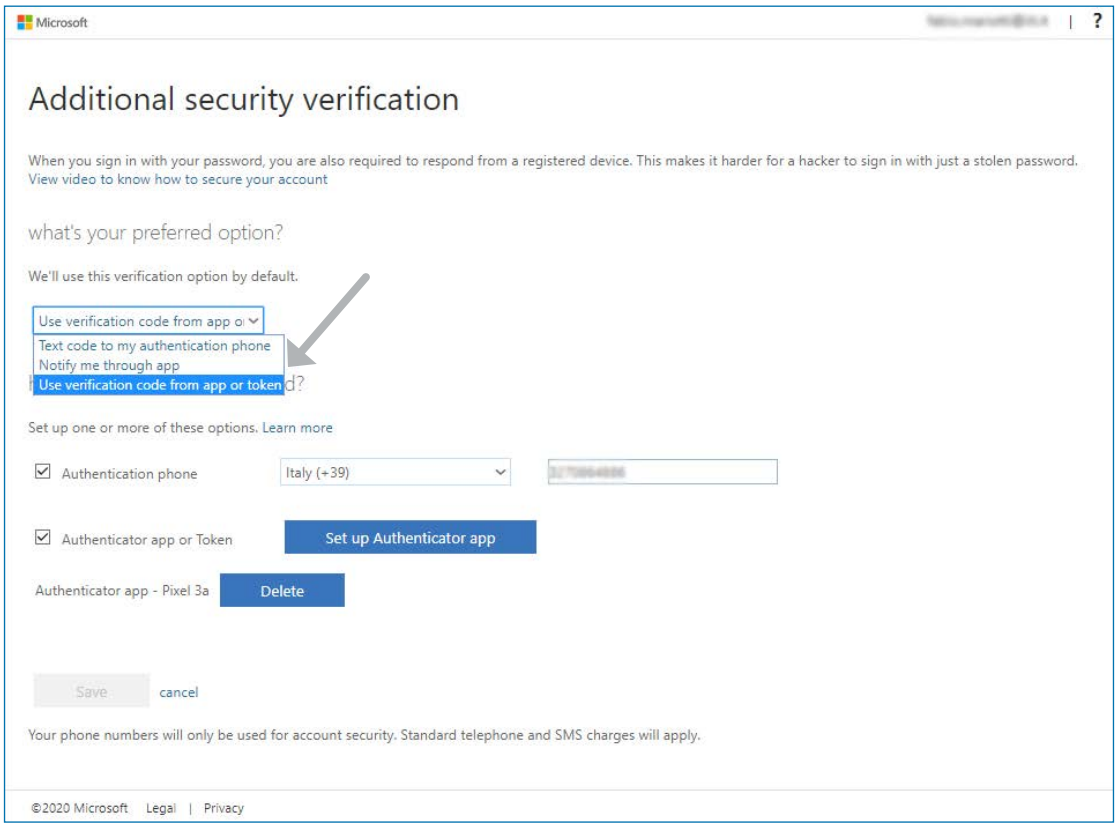




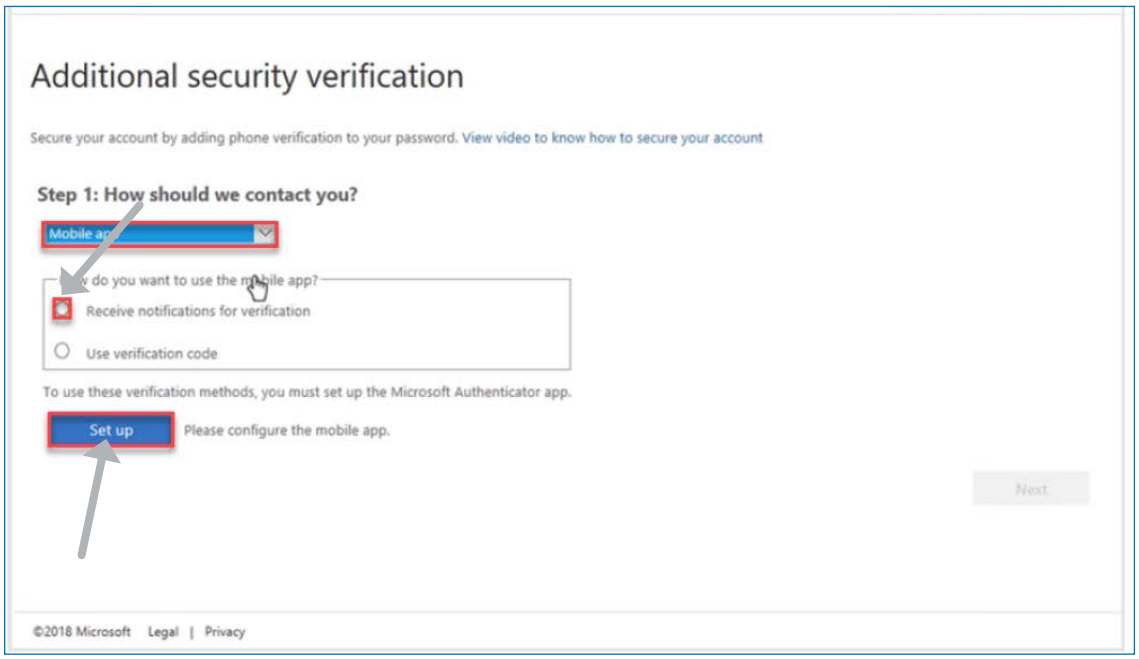


2. Set-up Microsoft Authenticator App

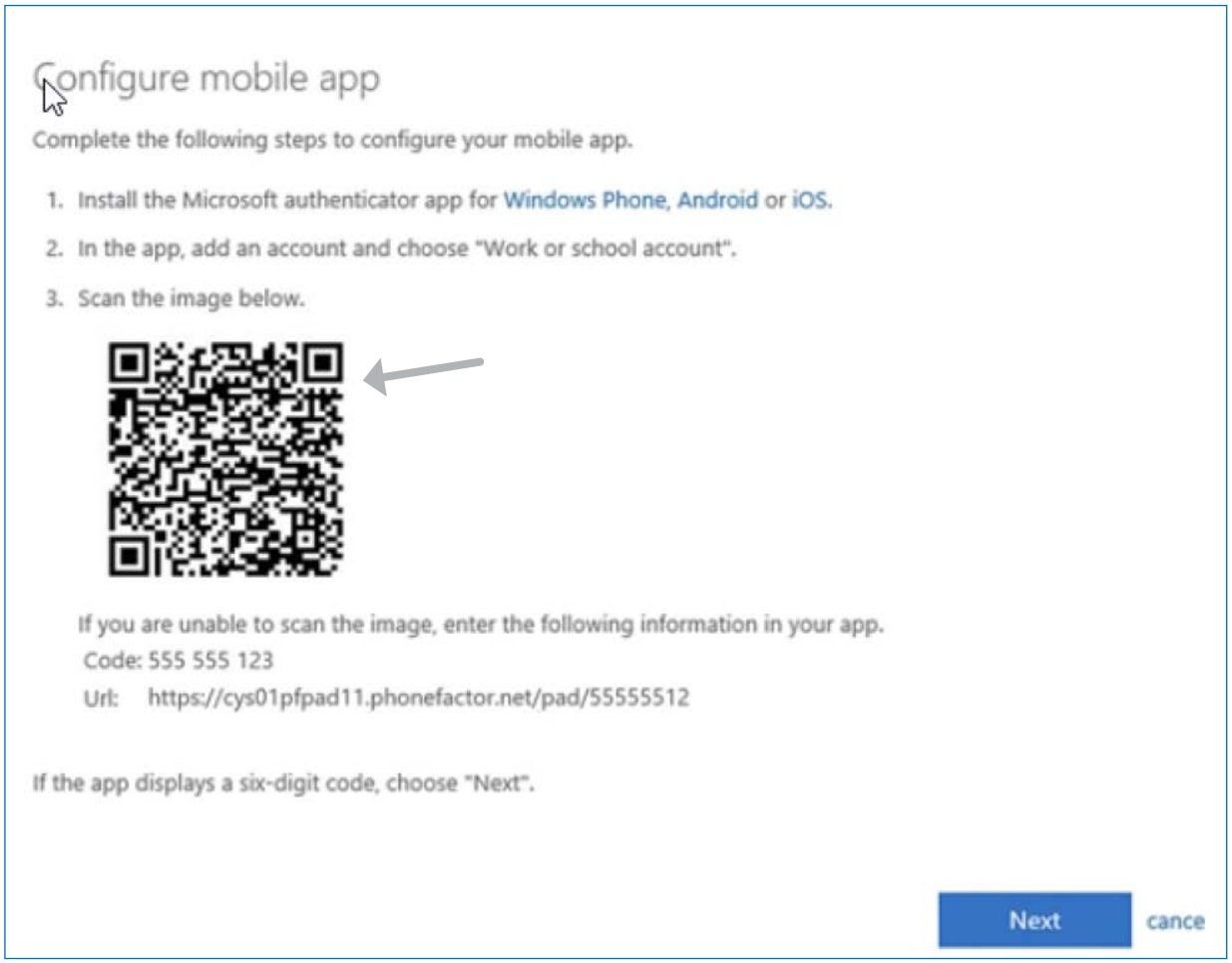
1. Choose **Use Verification Code** from app or token from the drop-down list;



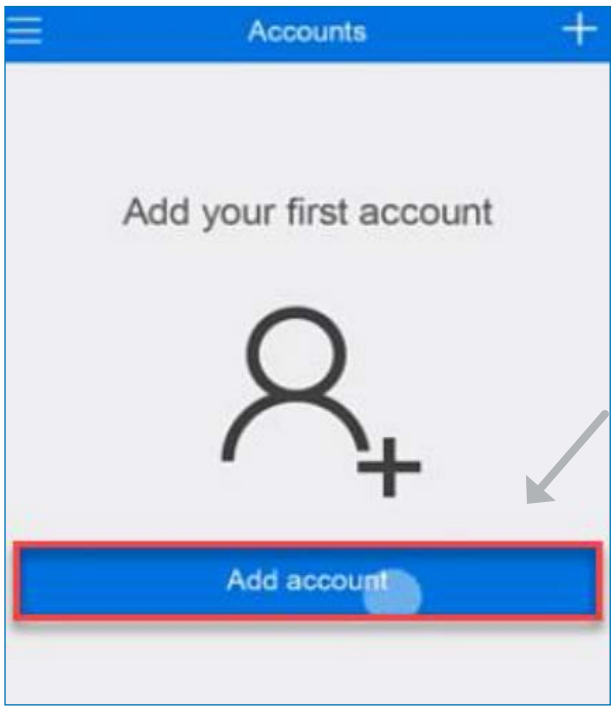
2. Click on **Receive notifications** for verification. Click **Setup**;

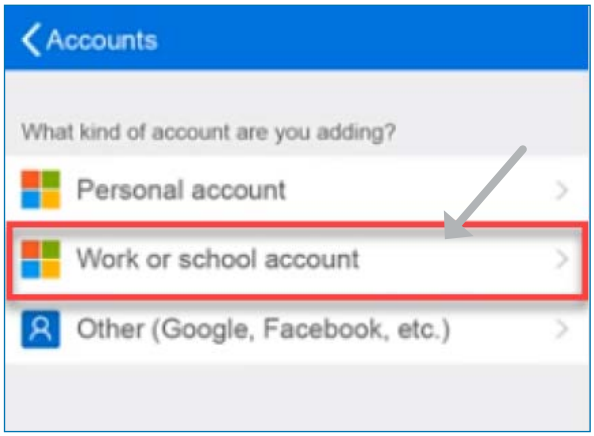


3. A **QR code** and instructions for your smart device will appear on the screen. Follow the instructions to set up the **Microsoft Authenticator App** on your device;

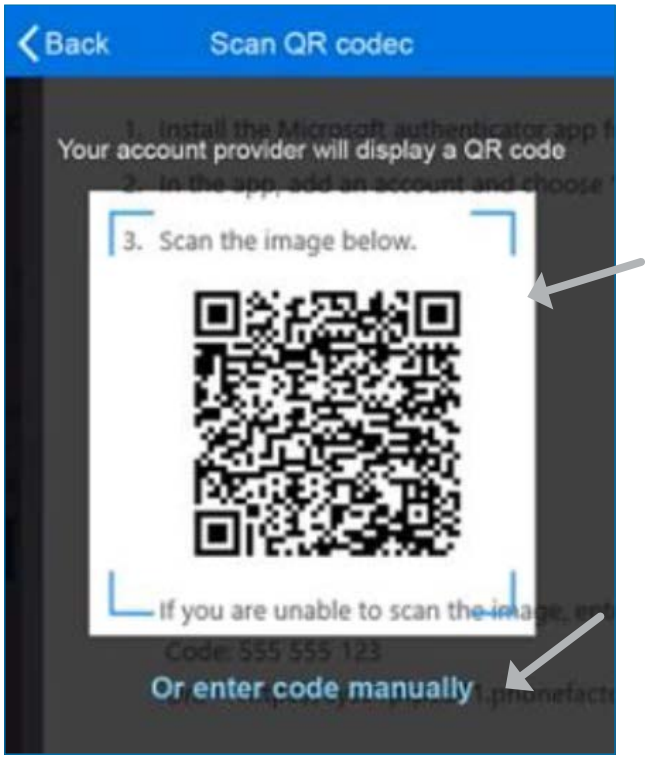


4. From **your mobile or tablet** device install the **Microsoft Authenticator App** (Android, iOS, Windows Phone).
   Open the app and choose **Add account** followed by **Work or school account account**.
   This will o**pen the camera** on your device;

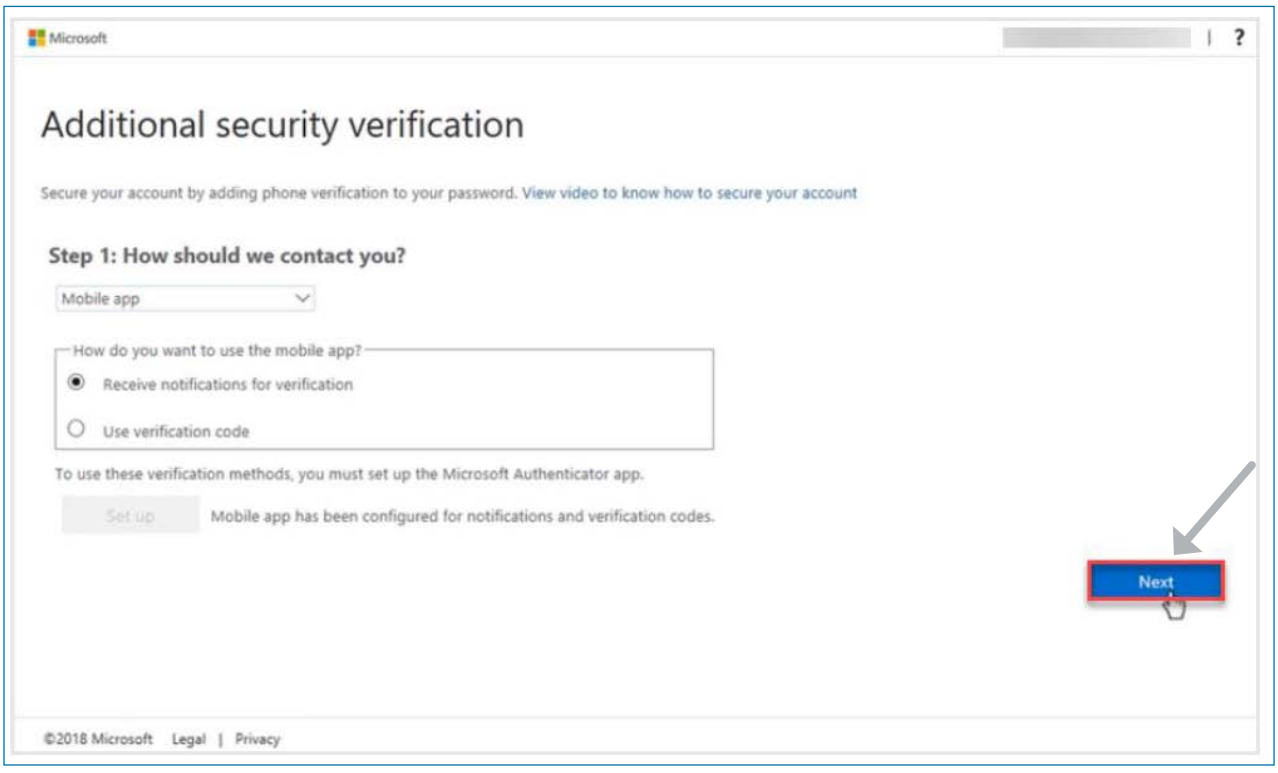




Scan the **QR code** on your computer or laptop using your smart device. Click **Next**.
If you are unable to scan the image a code is also available on screen:
To enter the manual code, you will need to click on **Or enter code manually**;

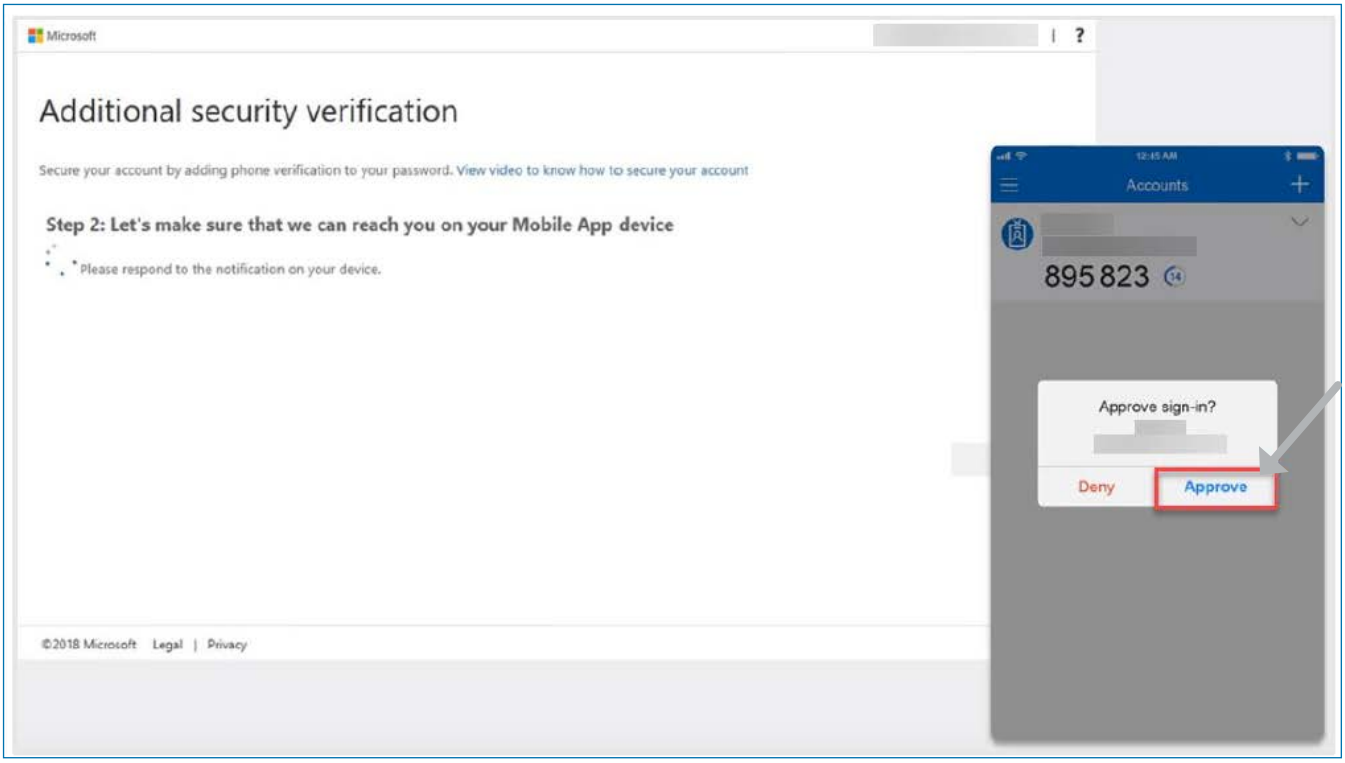


5. The account is now added. Click **Next**;



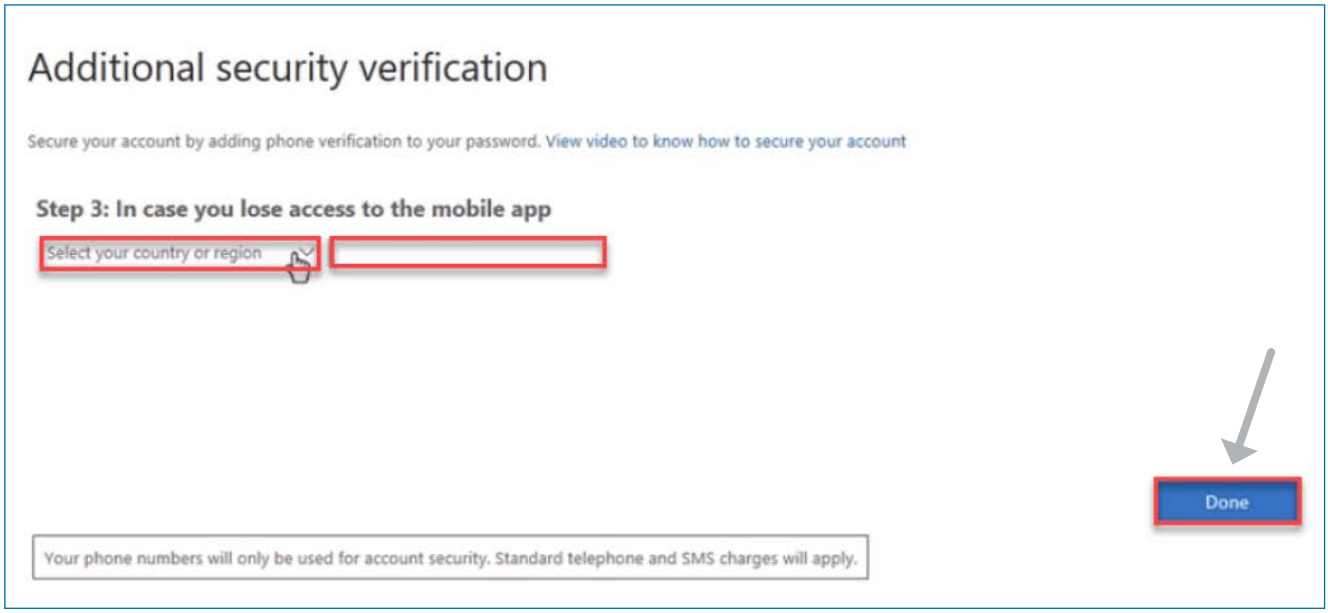
6. Next you will need to verify that the app works. It will send a notification to your phone to approve. Click **Approve**.

Remember to approve only notifications you know you have initiated:
If you have not initiated it, **ignore the request** or click on **Deny**.



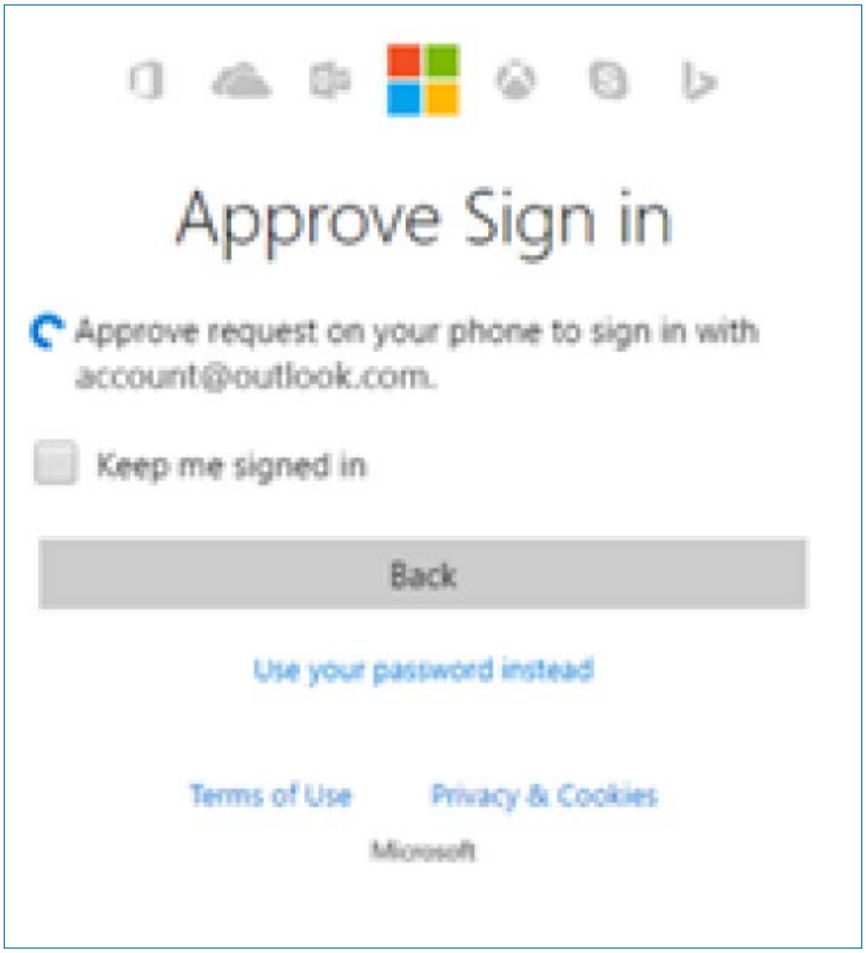
3. Add a mobile phone number

1. Finally, **enter a phone number** in case you lose access to your mobile app.
You will need to **choose your country code and enter your telephone number**.
Click **Done** to **complete MFA setup**.



4. Approve sign in using the Microsoft Authenticator App

Once you have set up MFA on your device you will be able to use your smart device to authenticate your login if prompted. If you are asked to approve a sign in a screen similar to the one below will appear on your screen.

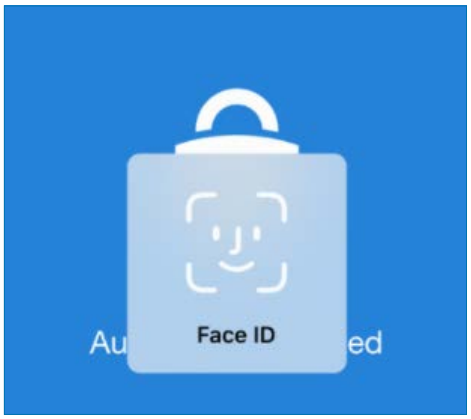


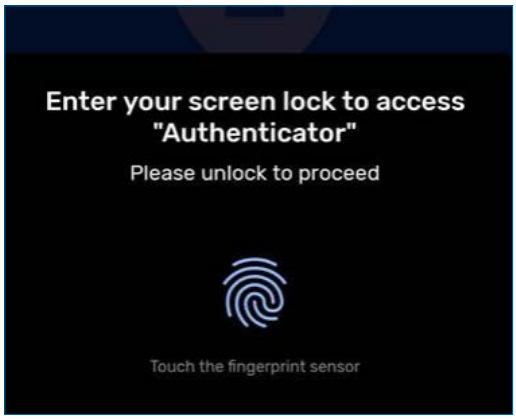
If this happens you will need to open the **Microsoft Authenticator App from your device** and click on **Approve** or enter a code generated from the app. to gain access to your account.

Remember to approve only notifications you know you have initiated:
If you have not initiated it, **ignore the request** or click on **Deny**.

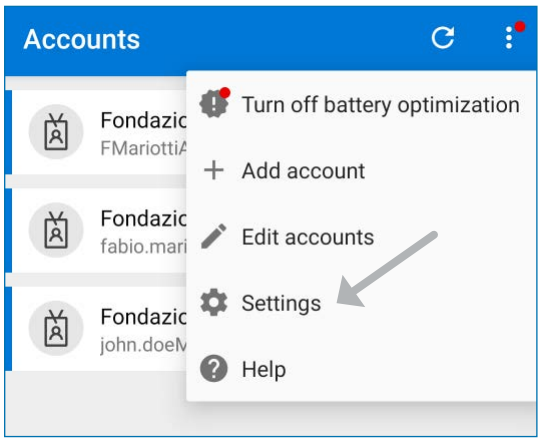
5. MFA notifications App Lock

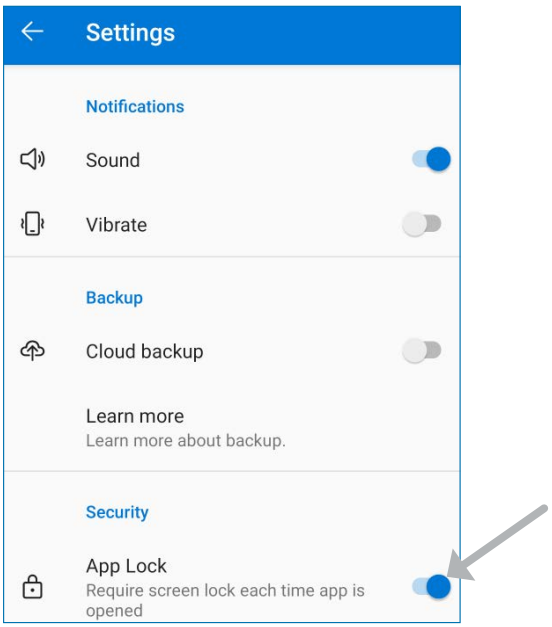
Currently, when the notification arrives on the phone, you can click approve/deny from the lock screen. However, when app lock is enabled, you will have to launch the app (on iOS) or launch a dialog (on Android) before you can click approve/deny, and you'll also need to provide an additional PIN/bio gesture to successfully authenticate. Thus, even if you leave your phone unlocked on your desk and walk away, a passerby cannot approve the notification for you.





You can disable this feature in the app, tap **Settings** > then tap **App Lock** switch to turn off:





If you **change your mobile device** please associate it on the **MFA Portal**: using this portal you can also check at any time which mobile devices you have registered.