

# Mobile Device Setup Instructions

## Setting up MS Authenticator, Email and O365 Office apps

Version 3.0

\* \* \* If you have problems with these instructions, please contact your local IT Help Desk \* \* \*

Here is a video version of these instructions! <https://web.microsoftstream.com/video/38424335-5908-43fe-9dd7-f5a0ca793d77>

### PART A - Setting up the MS Authenticator App

Setting up your GFE (Government Furnished Equipment) iOS mobile device for Office 365 (O365) email will require access to a FWS computer on the FWS network.

Please read these instructions **thoroughly** before you begin the configuration process. The instructions contain two separate columns because your computer (left column) **AND** mobile device (right column) are both required to set up MS Authenticator.

Note in Step 6 of the instructions that the MS Authenticator app may have already been pushed down to your mobile device by the FWS mobile device managers; take a look at your device home or secondary screens to look for the MS Authenticator icon:

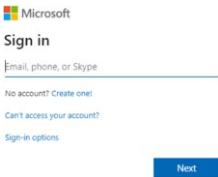
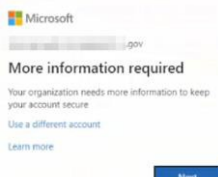

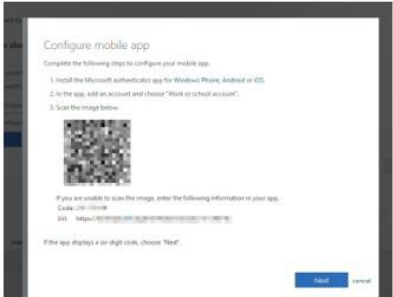

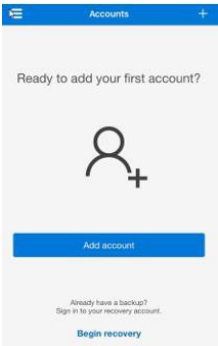




If you see the MS Authenticator app already on your device, you can skip Step 6 in the instructions, and you won't need your Apple ID as listed in Requirement 6 below.

### Requirements

Prior to starting the setup process, you must have the following information or items at hand:

1. Your Active Directory user name (your email address)
2. Your Active Directory Password
3. Your PIV card
4. A GFE laptop or desktop connected to the FWS network (on location at your office or using Pulse SecureVPN)
5. Your GFE Mobile device connected to the internet via wireless or cellular connection
6. Your Apple-ID/Password (used to setup your GFE iOS device) to access Apple App Store and download necessary Apps

On your GFE Workstation	On your GFE Smartphone/Tablet
<p>1. Open <a href="https://aka.ms/mfasetup">https://aka.ms/mfasetup</a></p> <p>2. At the Microsoft “Sign in” page, enter your FWS email address, click “Next”</p>  <p>a. If prompted for type of account, select the “Work or School” account option</p> <p>3. On the “More information required” screen, click “Next”</p>  <p>4. On the “Additional Security Verification” screen, select the following:</p> <p>a. Select “Mobile App”</p> <p>b. Select “Receive notifications for verification”</p>  <p><b>Note:</b> The rest of the instructions assume user selected the “Receive notifications for verification” option in 4.b above.</p> <p>5. Click Setup - <b>DO NOT CLOSE</b> the “configure mobile app” WINDOW THAT OPENS</p>  <p>Go to your Smartphone or Tablet and perform steps 6-13 as shown on the right-hand side column of this table.</p>	<p>6. Go to the App Catalog and download and install the Microsoft Authenticator app </p> <p>7. Open the Authenticator app. When prompted, select “Allow” notifications. <b>Note:</b> The app will NOT work properly if you do not click allow.</p> <p>8. Click “OK” if prompted</p> <p>9. Please select “Skip” until you reach this screen</p>  <p>10. Select “Add Account”</p> <p>a. Disregard backup popup, click “Continue”</p> <p>11. Select “Work or School” account</p> <p>a. Allow app to access Camera: click “OK”</p> <p>12. Using your device, hover camera over QR code that is displayed on your computer’s screen</p>  <p>13. MS Authenticator app will now show an account.</p>  <p><b>Note:</b> You will see a 30-sec countdown clock. You are okay, please continue with the remaining steps.</p> <p>Go back to your computer and perform steps 14-16 as shown on the left-hand side column of this table.</p>

14. After you are done with step 13, click **“Next”** on the **“Configure mobile App”** screen.

a) If you don't see the blue Next button, press Ctrl and –

That will zoom out your screen

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.



If you are unable to scan the image, enter the following information in your app:

Code: 216-108088  
URI: https://login.microsoftonline.com/0365-00000000-0000-0000-0000-000000000000

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



Next

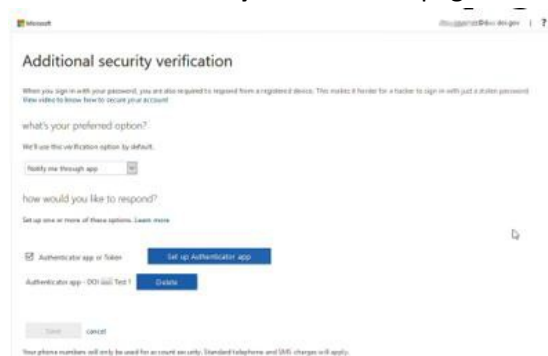
15. **“Checking activation status”** will appear

16. Click **“Next”**

Go back to your Smartphone or Tablet and perform step 17 as shown on the right-hand side column of this table.

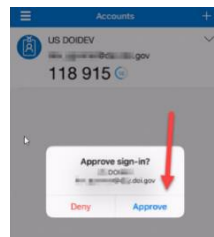
18. System is ensuring communication to your Authenticator App is successful

19. Verification Successful; close the **“Additional Security Verification”** page



**You are done setting up the MS Authenticator!**

17. When prompted, click **“Approve”**




Go back to your computer and perform steps 18-19 as shown on the left-hand side column of this table.

## Move on to Part B to set up your email.

If you have additional GFE iOS devices that you want email or the O365 Office apps on, you'll need to set up Authenticator on those devices, but you won't have to go through the full setup described above. Please go to the Appendix at the end of this document to set up Authenticator on additional devices.

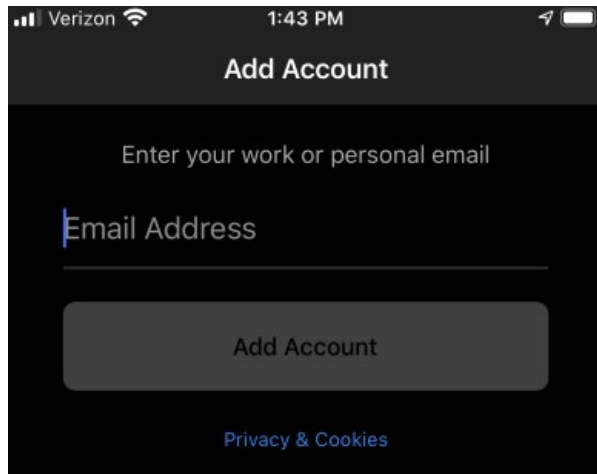
## PART B - Install the Outlook mobile app (and other O365 Apps)

### Configure the Outlook Mobile app

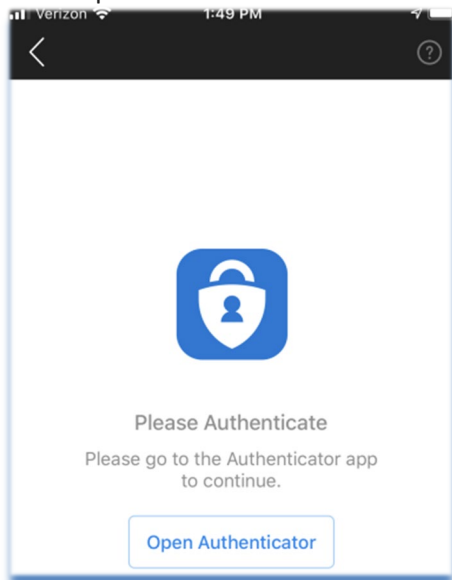
1. On your mobile device, look for the Outlook mobile app icon . If you don't see it, open the

MaaS app catalog  and select and install the Outlook mobile app.

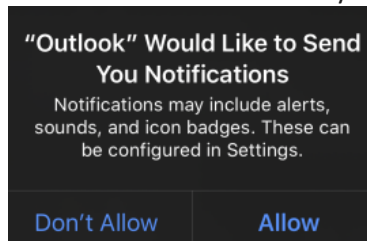
2. Open the Outlook mobile app.
3. You will be taken to the Add Account page. Enter your government email address and then click the “Add Account” button



4. Press “Open Authenticator”:



5. Enter your Active Directory password.
6. You will get to a screen for Additional Security Verification – choose Azure MultiFactor Authentication at the bottom of the screen.
7. You will get another popup for the sign in – click Approve/Allow.
8. Outlook will close at this point. Click on the Outlook app to reopen and you should now be able to see your email.
9. Enable Notifications, Click "Turn On"
10. Outlook would like to send you Notifications. Click "Allow"



11. To ensure your Contacts sync down to the phone:
  - a. Open the Outlook app on your iPhone
  - b. Press the circle icon at the top left (to the left of Inbox)
  - c. On the bottom left, press the gear icon to access **Settings**
  - d. Press your Office 365 account under Mail Accounts
  - e. Toggle on the **Save Contacts** switch
  - f. Press **Save to My iPhone**
  - g. Press **OK** to allow Outlook to access your Contacts

**This completes the Outlook mobile app configuration.**

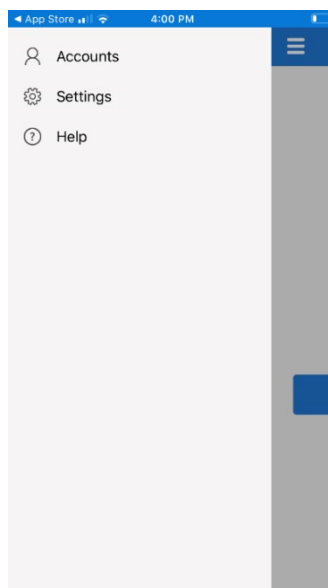
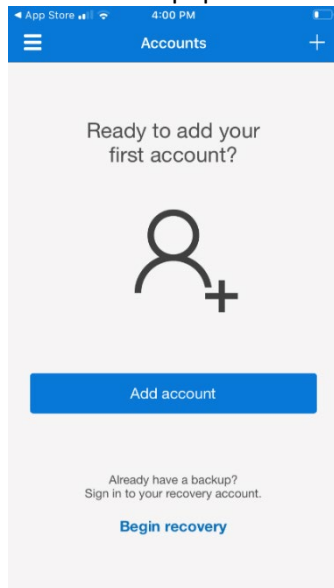
## **Install and configure additional Office mobile apps**

To install additional Office mobile apps, find the desired apps in the MaaS App Catalog and install them. When you open the app for the first time, you may be asked to sign in with your Active Directory username; the exact process seems to vary depending on the app and your iOS device model. Some apps will then have an additional step of taking you to the DOI Sign In screen, where you'll need to enter your Active Directory password, then select the **Azure Multifactor Authentication** link at the bottom of the screen, then **Allow** the sign in.

## Appendix A – Setting up MS Authenticator on additional devices

If you have additional GFE iOS devices that you want email or the O365 Office apps on, on each additional device perform the following steps:

1. The MS Authenticator app may already have been pushed to your secondary mobile device. Check your device's home or secondary screens to see if the Authenticator app already shows up. If so, open the app. If you don't see it, go the App Catalog, download and install the Microsoft Authenticator app.
2. Open the MS Authenticator app.
3. At the Add Account screen, click on the “hamburger” icon (three stacked horizontal lines) in the upper left corner, and from the pop-out menu select Settings.



4. From the Settings screen, select Device Registration:



5. Enter your email address (if it's not already entered) then select **Register Device**.

6. At the DOI Sign in page, enter your Active Directory password then select **Sign in**.
7. The DOI Sign in page will reload; scroll to bottom and select **Azure Multi-Factor Authentication**.
8. On your primary device, open the Authenticator app and approve the sign-in of your secondary device.