

Multi-Factor Authentication

Multi-Factor Authentication for All

Multi-factor Authentication (MFA) is a way of verifying that people logging into our systems are indeed the people we think they are. In these times when malicious and phishing email attacks are a daily occurrence, MFA provides a way to limit the impact of these attacks and help ensure that only authorized people are accessing our systems. Through our existing licensing, we have access to the Microsoft MFA solution. This helps us to protect not only our email, but all of our data and applications connected to Office 365.

What is MFA?

Simply put, MFA is a method of authentication that requires more than one verification method. This adds a critical second layer of security when users sign-in to their UAPB Office 365 account. It does this by requiring more than one method of verifying that it is really *you* logging into the account.

How it works: MFA works by requiring both of the following verification methods to access your account:

- Something you know (your UAPB username & password)
- Something you have (a trusted device - your mobile phone).



Getting Started

Pre-Requisites

In order to use multi-factor authentication with your UAPB account, you will need to ensure the following pre-requisites are met:

- You have a phone that can receive SMS texts and/or download the Microsoft Authenticator app
- Office 2016 is installed on your computer (if you use the full Outlook App on your computer)

Setup Multi-Factor Authentication

First, verify that you meet the pre-requisites above. Then, you will need your mobile phone, a computer, and Internet access to complete the setup.

1. Select Your Multi-Factor Verification Option

When you sign into your O365 account, an additional verification request is sent to you. The following are a list of methods that can be used for this second type of verification.

ITS recommends the *Mobile App notification* method - while it takes a bit longer to set up, it is the fast verification option allowing you to just tap approve on your phone. The mobile app is also available even when you don't have cellular coverage by using the code generated within the app every 30 seconds.

Verification method	Description
Phone call	A call is placed to a your mobile phone asking you to verify that it is you signing in. Press the # key on your phone to complete the verification process.
Text message	A text message is sent to a your mobile phone with a 6-digit code. Enter this code to complete the verification process.
Mobile app notification (requires download of Microsoft Authenticator App on your phone)	A verification request is sent to your mobile phone asking your complete the verification by selecting Verify/Approve from the mobile app. This occurs if app notification is the primary verification method. If you receive this notification when you are not signing in, you can report it as fraud.
Verification code with mobile app (requires download of Microsoft Authenticator App on your phone)	The mobile app on your device generates a verification code. This occurs if you selected a verification code as your primary verification method.

2. Download the Microsoft Authenticator App on your Mobile Phone

IPHONE

1. **Go to App Store**
2. Search for **Microsoft Authenticator**
3. *Tap* on the Microsoft Authenticator app to download
4. Click "Get" to begin installation
5. Once the app is installed, click on **Open**.
6. Tap **Allow** on the "Authenticator would like to send you notifications screen"
7. On the Accounts screen, tap **ADD ACCOUNT**
8. Under "*What kind of account are you adding?*" Select **Work or school account**.
9. A pop-up box will appear asking, "*Authenticator Would Like to Access the Camera?*"
10. Tap **OK** (You will need to take a picture of the QR code found in the next step of setup instructions).
11. Your camera will turn on and is ready to record the QR code. Set your phone down temporarily and go to your computer.

ANDROID

1. Go to *Apps*, select *Play Store*
2. Search for **Microsoft Authenticator**
3. Click **Install**
4. Once the app is installed, click on **Open**.
5. On the Accounts screen, click on **ADD ACCOUNT**
6. Under "*What kind of account are you adding?*" Select **Work or school account**.
7. A pop-up box will appear asking, "*Allow Authenticator to take pictures and record video?*"
8. Tap **ALLOW** (You will need to take a picture of the QR code found in the next step of setup instructions).
9. Your camera will turn on and is ready to record the QR code. Set your phone down temporarily and go to your computer.

3. MFA Setup in Office 365 using the Mobile App (Note: if you previously set up MFA and have a new phone/lost your phone see the FAQs for instructions)

Complete the remainder of the setup process in Office 365 at a computer. You will also need your mobile phone near you for the following steps.

Setup Multi-Factor Authentication in Office 365

Note: These instructions are for the first time/initial setup of MFA. Make sure you have already downloaded the Microsoft Authenticator App on your phone.

1. Go to portal.office.com
2. Sign into Office 365 on your computer with your UAPB account & password. Click on the blue box under your name that says "Set it up now"
3. In the drop-down box next to Step 1: How should we contact you? choose Mobile App
4. Next to How do you want to use the mobile app? Choose "Receive notifications for verification".
5. Click on Set up.

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

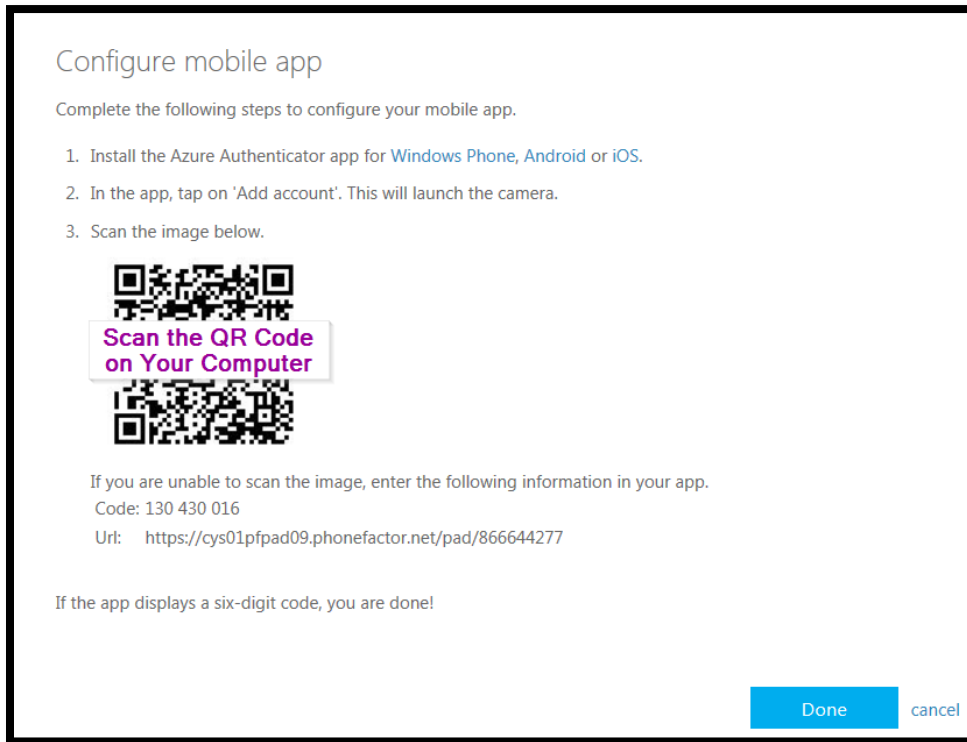
Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Azure Authentication app.

Mobile app has been configured for notifications and verification codes.

6. You will see the Configure mobile app dialog box on your computer. (You should already have the app installed on your smartphone). On your mobile phone open the Authenticator app
7. Scan the QR image displayed in your browser.
8. Once you have successfully scanned the image, your account will be added automatically to the Authenticator app on your phone, and it will display a six-digit code.



9. On your computer, Choose Contact Me in your browser on the Office 365 page.
10. Next you will verify that Office 365 can reach your mobile phone.
11. You should receive a push notification on your mobile phone. Tap Approve/ Verify (Android/iPhone)
12. On your computer you will next see the follow screen. O365 sets up an initial app password for you to use with other applications so these other apps can connect to your Office 365 account. If you're using other apps like the default email on an android mobile phone, you'll need to create an app password so these other apps can connect to your Office 365 account.
13. Go to your mobile phone and open up your default email account (Note: iPhone users - if you are using iOS 11 on your phone you will not need to use the app password for the default mail app). You will need to change your password to the app password provided by Office 365 (like the one shown on the screenshot above).
14. Your mobile phone should now be able to access Office 365. Go to your computer, click Done in your browser.

You are now set up to use Multi-Factor Authentication on Office 365 and on your mobile phone default email application.