جـامعــة الشــارقــة
UNIVERSITY OF SHARJAH

Multi-Factor Authentication – FAQ

What is Multi-Factor Authentication (MFA)?

MFA is an authentication method that requires more than one verification method to sign into the Office 365 Portal.

The University of Sharjah has enabled Azure MFA on your Office 365 account for this purpose. Azure MFA is Microsoft's ***two-step verification*** solution. When you log into your Office Portal (Office 365 account) from outside the County network you will be required to enter your username and password as well as a verification code.

More details on Azure MFA are available here.

Why do we need MFA?

Passwords alone are easy to hack. There are many techniques used by bad actors to harvest or guess your password. We see evidence of this daily. As we adopt cloud-based solutions and applications we gain many benefits. Global access to applications and data does come with a cost. Our applications and data are available from anywhere, by anyone with a username and password. Statistically, MFA can reduce the likelihood that your account will be compromised by 99.9%.

How is MFA being used at UoS?

Not all applications and services will require MFA. Initially, only Microsoft 365 will require MFA. This includes:

- Email
- Teams
- OneDrive
- SharePoint
- Office web apps (Word, Excel, etc.)
- Other M365 applications (accessed via the Microsoft 365 Portal)
- UoS apps related to your UoS account.

What application do I use for MFA?

Technology Services recommends using the Microsoft Authenticator app. The app is available for **free** in both Google's Play Store and Apple's App stores. It can be used with your university account.

How often do I have to re-authenticate for MFA?

If you connect using a new computer or device, or a new browser, you will be asked to authenticate. But you will not continually be asked to authenticate through MFA once you've logged in. And as other systems come become a part of it, your access will become even smoother.

Here are some general tips to help reduce how often you're prompted:

- When logging in through a web browser on personal devices, select "Stay signed in". NOTE: Do not do this when using shared or public computers.
- Use an UoS-owned device (for faculty and staff) whenever possible.
- Use desktop/mobile apps instead of a web browser – you'll be prompted to log in less often if you download apps like Teams, Outlook (for checking email/calendar), and Office Apps (Word, Excel, etc.) directly onto your computer or mobile device instead of using the web versions.

Can I add additional/backup authentication methods?

Yes, you can add additional/backup authentication methods to your account at any time. In fact, we recommend that you have more than one authentication method especially if you have multiple work locations and devices. Go to https://myaccount.microsoft.com

1. Login with your UoS email and password if prompted (*if you're already logged in to M365, you won't need to log in*)
2. In the Security info section, click **Update Info >**
3. Click **+ Add method**.

We suggest that users use the Authenticator app with a phone method as a backup. For traveling, the 6-digit code method works best. All other methods: Auth app Approve/Deny, Phone call, and SMS require cellular or Wi-Fi, the 6-digit code method via the Auth app does not require any connection for the phone at all.

There are several notification methods, which one should I use?

Technology Services recommends using the Microsoft Authenticator app push notification. We suggest that you also provide at least one other method of contact (i.e., mobile phone, landline) to help prevent being locked out of your account if your phone is lost or not with you.

How do I change my default authentication method?

1. Go to https://myaccount.microsoft.com
2. Login with your UoS Email and Password if prompted (*if you're already logged in to M365, you won't need to log in*)
3. In the Security info section, click **Update Info >**
4. Next to the *Default sign-in method:* click **Change**
5. Select the method you would like from the drop-down then click **Confirm**

What if I forget my phone?

If possible, retrieve your device. Or click "sign in another way" and use your backup method(s).

If you don't have a backup option, and cannot easily retrieve your device, please contact the IT Service Desk.

Update your security info to include other methods to ensure you have backup methods: MFA Guide.

How do I switch my MFA on a new phone?

If you get a new phone, you can switch the MFA to the new device. Follow the instructions in MFA Guide.

Do I need data or Wi-Fi to use the authenticator app on my phone?

No. The Authenticator app provides a verification code option that will work even if you aren't connected to Wi-Fi or using cellular data. See Microsoft's Authenticator app FAQ for more information.

To use a verification code instead of an approval notification to sign in:

1. When prompted for MFA, click the 'sign in another way' link
2. Select the 'Use a verification code from my mobile app' option
3. Open the authenticator app on your mobile device and click on your Acadia account (displayed as 'Azure AD' followed by your Acadia email address). A one-time password code will be displayed
4. Enter the one-time password code from the app on the log-in screen to finish logging in

If desired, you can also change your default authentication method to always use verification codes.

The 6-digit code method via the Authenticator app does not require any Wi-Fi or cellular connection for the phone.

What if I use a different SIM card when traveling? Will authentications still work?

This depends on the method used for MFA - The app-based method with Microsoft Authenticator uses data (mobile and/or Wi-Fi) so it will remain active, however, the Authenticator app will continue to produce one-time use codes regardless of data, cell signal, or Internet use abilities.
If your phone number changes for any reason, phone calls and SMS (text) push will not function until updated numbers are entered into your account as authentication methods.

We are also strongly suggesting that anyone traveling abroad or to locations with poor cell service use the Authenticator app via the 6-digit code method. The 6-digit code method via the Auth app does not require any connection for the phone at all.

How is my Personal Information protected?

Personal Information: You do need personal information, such as **phone number** to use two-step verification authentication to set up.

This information is used by Technology Services to support you in terms of identity verification in case of lost/forgotten devices or passwords or during a cybersecurity breach (i.e., compromised account).

Microsoft will never call or text or share your **number or other Personal Information**.

Authenticator App: The Microsoft Authenticator app itself only has permission to send you push notifications and access the camera when taking a picture of the QR code. It does not give UoS access to any of the data on your device or the traffic that passes through it. The Authenticator app is not set to track the location of its users.

The Microsoft Authenticator app is an industry-standard form of protection. It attaches your account to a device you own, providing a second factor of authentication to your password. It only exists to confirm your identity with something that is owned and accessed **by you only** and to ensure that it is you signing into your account.

My mobile device was lost or stolen. What should I do?

If your mobile device with the Microsoft Authenticator App is lost or stolen, please contact ITC Service Desk to let them know about the loss or theft of the device. Our team will work with you to determine how best to proceed with both the MFA options and the loss of the device.

You should also visit https://myaccount.microsoft.com using one of your alternate MFA methods to deactivate your phone to prevent it from being used to access your account. This is in the "Security Info" section.

On the initial setup, you can also create a backup which would give you access to your information in case of a lost or stolen device.

I just got a new mobile device. What should I do?

If you get a new phone, or if you've re-installed the Microsoft Authenticator app, you'll need to re-add the app as an authentication method to your account.

To do this, you'll need to log in using a backup MFA method you already have set up.
If you don't have a backup method set up or can't use your backup method, contact the IT Service Desk. for help.

Can I set up MFA and trust my device for a period of time?

Registering your device with Microsoft Authenticator will enable it to receive push notifications when your account is accessed. However, at the current time, it's not possible to automatically accept the notifications on a trusted device.

I set up MFA according to the guide, but it does not appear to be prompting me?

After you register and enroll for MFA, there is a process that runs to enable the account. Once this has run MFA will prompt you to authenticate. You will receive a confirmation email that MFA is enabled on your account. If you do not receive an email within 24 hours, please contact the Service Desk. Please note that you will not be enabled over the weekend to ensure a smooth transition and that support is available.

I received a notification to approve a sign-in when I wasn't trying to log in to a service. What should I do?

Do not approve the sign-in and contact the **IT Service Desk.** Someone might be trying to log in to your account as you.

Note: If a service stop working for you after you deny the login, it was likely you.

You can review your M365 sign-ins at any time in your M365 account portal (https://myaccount.microsoft.com) - click 'My sign-in's in the menu. These details can help you figure out if the device attempting to log in is yours.

If you have any questions or concerns related to a sign-in attempt, please contact the IT Service Desk.