Microsoft Account Two Factor authentication (2FA)

Microsoft allows you to protect your Office 365 (O365) account with Two-Factor authentication (2FA) using a mobile-generated pass-code which can be sent to you using one of three methods: a text message, a phone call, or via a third-party 2FA app like Duo Mobile, which you may already use for UICs VPN service.

To configure this additional protection, update the Security Info section of the Microsoft Sign-Ins website located at https://mysignins.microsoft.com/security-info.

If you have not configured these settings before, your Security Info page will show No items to display, as seen in the image below.

![](image1.png)

If you have configured a 2FA method, the current, default sign-in method will be listed as the Default sign-in method, as underlined in the sample image below. In this example, it lists Authenticator app or hardware token-code, which simply means that an app like Duo Mobile is configured.

![](image2.png)
Microsoft Account Two Factor authentication (2FA)

Any of the methods listed in the image below, can be used as an authentication method regardless of what your current default is set to.

To use your phone as a sign-in method (either Text or Phone call), or to add a third-party 2FA app, click on the plus sign next to Add Method.
Microsoft Account Two Factor authentication (2FA)

After clicking Add method, you will see the pop out box below, on the left. Then click on the drop down to view the methods available, as shown on the right.

To receive a code via a text message, select Alternate Phone and provide a phone number where you can receive text messages.

**Note:** the methods Alternate Phone and Office Phone, will give you the option of receiving a phone call or a text message depending on your current default.
Microsoft Account Two Factor authentication (2FA)

To use Duo Mobile to generate codes for your Microsoft account, select Authenticator app.

The default app for Microsoft 2FA is Microsoft Authenticator, freely available for iOS and Android devices, but if you want to use Duo Mobile, select the I want to use a different authenticator app link when prompted.

Once clicked, you will be instructed to set up your Microsoft account in your other app (e.g., Duo Mobile).

Click on the Next button to obtain a QR code on-screen, which you will scan in the next step.
Microsoft Account Two Factor authentication (2FA)

The displayed QR code (see example image below) will need to be scanned with your **Duo Mobile** app, as outlined in the next steps. Do not click next until you have scanned the QR code.

Open Duo Mobile on your mobile device and add your other account. In your **Duo Mobile** app, click on the plus sign to add your Microsoft account, outlined in red in the sample image below.
Microsoft Account Two Factor authentication (2FA)
This will open up the camera lens and ask you to scan a bar code.

At this point, return to your web browser Security Info page and proceed to click Next at the Authenticator app prompt (see image below).
Microsoft Account Two Factor authentication (2FA)

Once scanned, the Microsoft 2FA code will be displayed in the Duo Mobile app. It will generate a new code every 30 seconds while the account is selected in the Duo Mobile app. You are now ready to use 2FA with Microsoft sign-ins when needed using Duo Mobile.