

Outlook 登入全面啟用手機驗證 (Microsoft 365 電子郵件服務)

(安裝與首次使用操作說明)

適用對象：首次啟用 Microsoft MFA

(Microsoft Authenticator) 之個人使用者

一、準備事項

- 一支可連網的智慧型手機 (Android 或 iPhone)
- 已可正常登入的 Microsoft 帳號
- 可接收網路連線 (Wi-Fi 或行動網路)

二、下載、安裝 Microsoft Authenticator App



Android 使用者	iPhone 使用者
<u>請開啟 Google Play 商店，搜尋</u>	<u>請開啟 App Store，搜尋</u>
<u>「Microsoft Authenticator」後</u>	<u>「Microsoft Authenticator」後</u>
<u>進行安裝。</u>	<u>進行安裝。</u>

	
<u>Google Play Store 下載 QR Code</u>	<u>iOS App Store 下載 QR Code</u>

三、電腦與手機綁定設定步驟

在開始前，請先在手機上下載並安裝 [Microsoft Authenticator APP](#)。

步驟 1：在電腦上觸發 MFA 設定

1. 開啟瀏覽器，瀏覽學校首頁，點選 Mail 登入 Microsoft 365(Outlook)。
2. 在「保護您帳戶安全」頁面，點選「下一步」，在「安裝 Authenticator 應用程式」頁面，點選「下一步」。
3. 螢幕頁面上顯示出 QR Code 條碼。

步驟 2：在手機 App 上掃描綁定

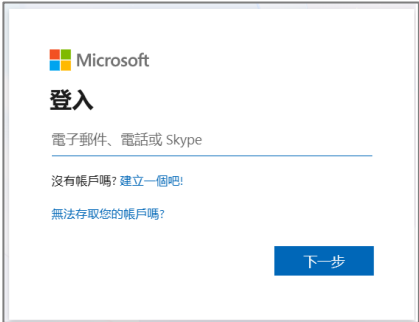
1. 打開手機上的 Microsoft Authenticator App。

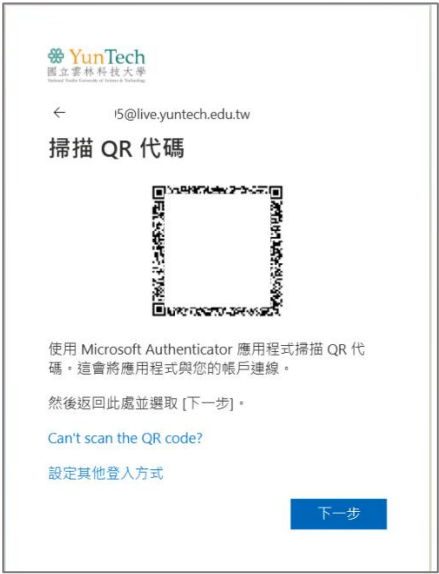
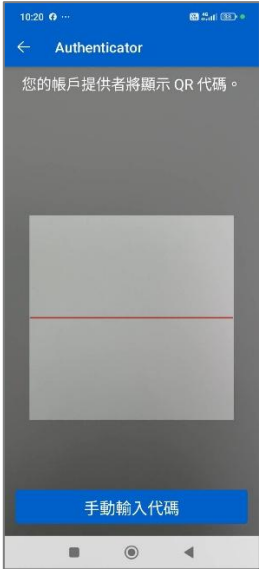
2. 點選右上角的「+」號或「新增帳戶」。
3. 選擇「公司或學校帳戶」，並點選「掃描 QR 代碼」。
4. 將手機鏡頭對準電腦螢幕上的 QR Code 進行掃描。掃描成功後，App 內就會出現您的 M365 帳號。

步驟 3：完成雙向驗證測試

1. 在電腦畫面上點選「下一步」。
2. 此時電腦螢幕會顯示一組 **2 位數數字**（例如：45）。
3. 您的手機會跳出推播通知，請在手機上輸入該數字並按下「是」（或進行人臉/指紋解鎖）。
4. 電腦畫面顯示「註冊成功」，即完成綁定。

以下將**電腦端**與**手機端**的設定步驟，以雙欄對照方式呈現。
請依序由上往下同步操作：

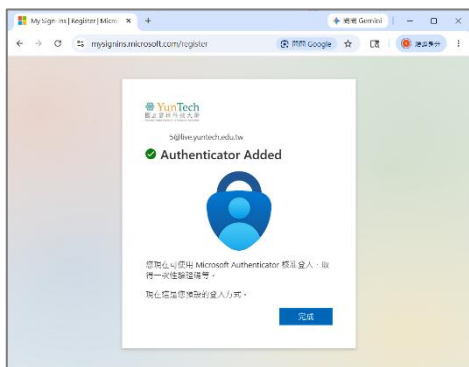
步驟	電腦端操作 (網頁瀏覽器)	手機端操作 (Authenticator App)
1. 準備 工作	開啟瀏覽器，瀏覽學校首頁，點選 Mail 登入 Microsoft 365(Outlook)。 	手機先下載並安裝好 Microsoft Authenticator。 
2. 觸 發 設 定	在「保護您帳戶安全」頁面，點選「下一步」，在「安裝 Authenticator 應用程式」頁面，點選「下一步」。 	開啟 App，點選右上角的「+」號，或點選「新增帳戶」。 

3. 帳 戶 類 型	螢幕頁面上顯示出 QR Code 條碼。 	在選單中點選「公司或學校帳戶」→ 接著點選「掃描 QR 代碼」。 
4. 掃 描 綁 定	將 QR Code 保持顯示在電腦螢幕上。	將手機鏡頭對準電腦螢幕上的 QR Code 進行掃描。(成功後 App 內會出現您的帳號) 

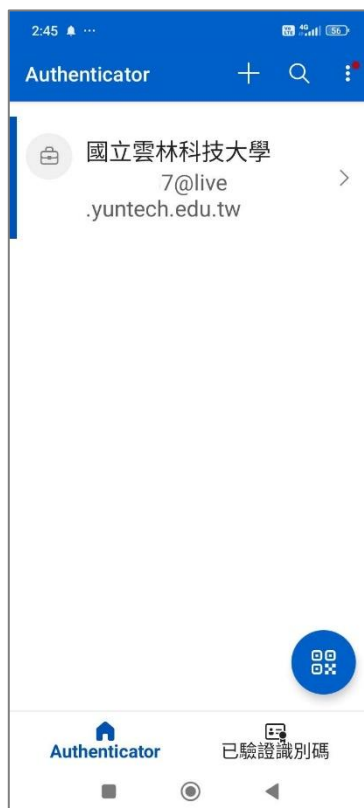
5. 觸 發 測 試	在電腦畫面上點選「下一步」。 此時電腦螢幕上會跳出一組 2 位數數字 (例如：38)。 	手機畫面上會彈出推播通知，要求您進行身分驗證。
6. 輸 入 核 准	等待手機端回應，畫面上會顯示正在驗證中。	在手機上輸入電腦顯示的那組 2 位數數字，並點選「是」(隨後進行人臉/指紋解鎖)。 

7.
完
成
設
定

電腦網頁顯示「通知已核准」與「註冊成功」，點選完成。



帳戶列表中的 M365 帳號已啟用成功，正式進入防護狀態。



如果您因為收不到驗證而完全無法登入安全性資訊頁面，請聯繫本校的 M365 資訊管理員 (IT Administrator)。

在 Microsoft 365 (M365) 中啟用多因子驗證 (MFA) 並綁定手機 Authenticator App，是保護帳號安全最重要的防護手段。

四、運作原理：它是如何保護帳號的？

1. 什麼是 Microsoft 多因子驗證(MFA)？

Microsoft 多因子驗證 (Multi-Factor Authentication , MFA) 是一種提升帳號安全性的機制。除了輸入帳號與密碼外，還需要透過智慧型手機 App 進行驗證，可有效降低帳號遭盜用風險。

2.M365 的 MFA 綁定主要基於時間型隨機密碼 (TOTP)與非對稱加密型推播通知技術：

- **共享金鑰基礎**：綁定時，伺服器與手機 App 會透過 QR Code 共享一串「秘密金鑰 (Secret Key)」。
- **時間同步計算 (TOTP)**：雙方利用該金鑰與「當前時間」，透過特定演算法 (如 HMAC-SHA1) 同步計算出一組 **6 位數動態驗證碼**。因為時間持續推進，該驗證碼**每 30 秒自動變更一次**，且過期即失效。
- **雙向安全推播 (以 Microsoft Authenticator 為例)**：當您在電腦登入時，M365 伺服器會透過加密管道對您的手機發送推播。電腦螢幕會顯示一組兩位數號碼，您必須在手機 App 上輸入相同號碼並點選「核准」，才能成功登入。這確保了即使密碼外洩，駭客沒有您的實體手機也絕對無法登入。

五、常見問題

Q1：手機遺失怎麼辦？

A：請立即通知資訊單位協助重設 MFA。

Q2：沒有收到驗證通知？

A：請確認手機網路正常，並檢查是否允許 App 通知。

Q3：更換新手機如何處理？

A：需重新安裝 Microsoft Authenticator 並重新綁定 MFA。

六、安全建議

1. 不要將 MFA 驗證通知隨意核准。
2. 發現異常登入通知時，請立即修改密碼。
3. 定期更新手機作業系統與 App 版本。