

LumineOne

雙重驗證 (2FA)

操作使用手冊

本手冊以實際使用情境為主軸，帶您一步步完成帳號安全設定
適用對象：所有系統使用者（一般員工 / 管理員）

目錄

情境一 管理員啟用全公司強制 2FA	3
✎ 情境說明	3
📄 操作步驟	4
📊 啟用後：追蹤員工設定進度	5
情境二 收到通知信後，設定 TOTP 驗證器	6
✎ 情境說明	6
📱 事前準備	6
📄 操作步驟	7
🔒 之後如何登入？	11
情境三 設定指紋 / 臉部辨識登入 (WebAuthn)	13
✎ 情境說明	13
📱 支援的裝置與方式	13
📄 操作步驟	13
🔒 之後如何登入？	18
情境四 寬限期到期，系統強制設定 2FA	20
✎ 情境說明	20
📄 操作步驟	20
💡 寬限期內的提示	22
情境五 手機遺失，使用備援碼登入	23
✎ 情境說明	23
📄 操作步驟	23
情境六 管理員：有員工 Email 錯誤，無法收到通知	25
✎ 情境說明	25
📄 操作步驟	25
情境七 管理員：關閉強制 2FA	27
✎ 情境說明	27
📄 操作步驟	27
✎ 關閉後的影響	28
常見問題 Q&A	29

情境一 管理員啟用全公司強制 2FA

適用對象：公司管理員

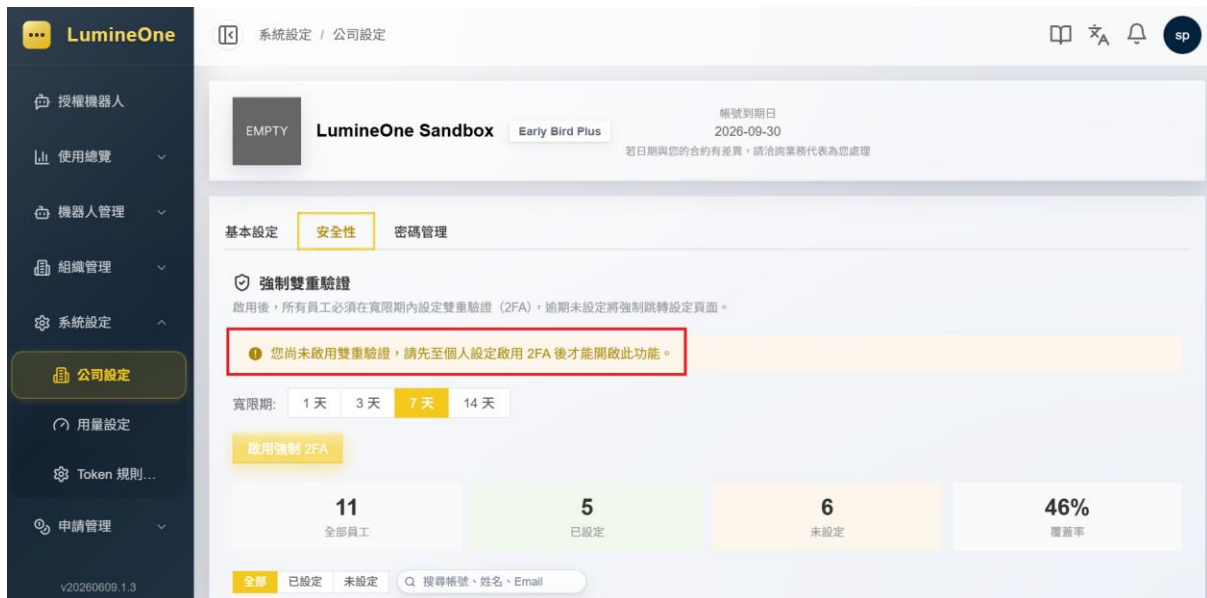
情境說明

您是公司管理員，希望要求所有員工在指定期限內完成雙重驗證設定，以提升整體帳號安全性。

重要

管理員本人必須先完成 2FA 設定，才能開啟此功能。若尚未設定，請先參閱「情境二」完成個人 2FA 設定。

完成「個人設定 > 多因素驗證 (MFA)」設定後，請重新整理頁面，以更新雙重驗證狀態。



系統設定 / 公司設定

EMPTY LumineOne Sandbox Early Bird Plus 帳號到期日 2026-09-30 若日期與您的合約有差異，請洽詢業務代表為您處理

基本設定 安全性 密碼管理

強制雙重驗證
啟用後，所有員工必須在寬限期內設定雙重驗證 (2FA)，逾期未設定將強制跳轉設定頁面。

❗ 您尚未啟用雙重驗證，請先至個人設定啟用 2FA 後才能開啟此功能。

寬限期: 1天 3天 7天 14天

啟用強制 2FA

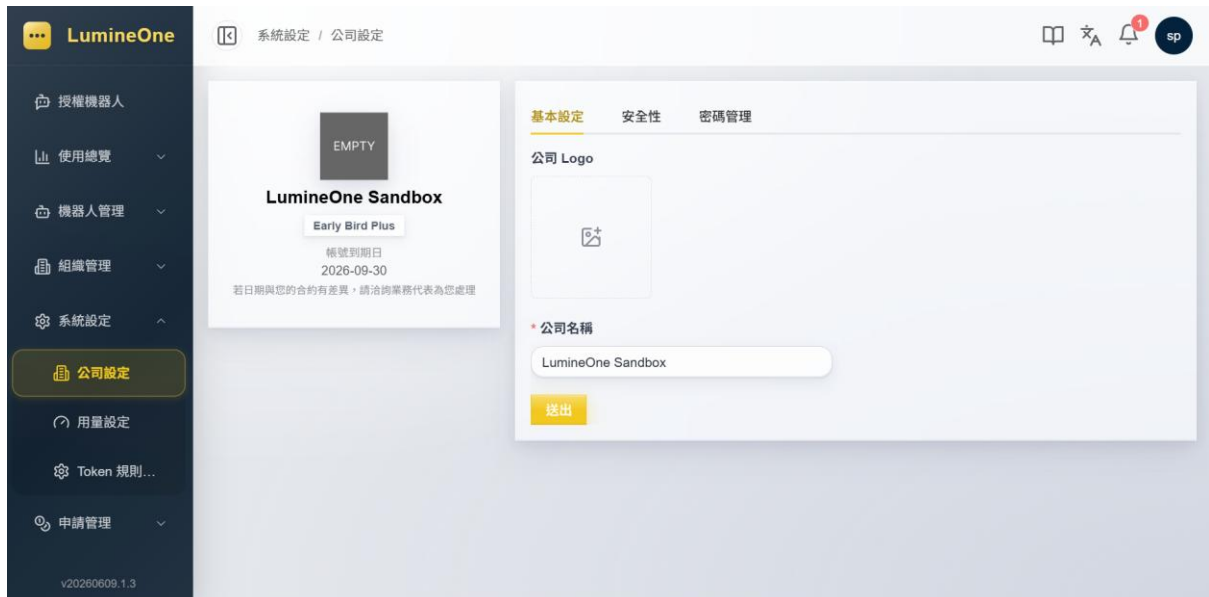
11	5	6	46%
全部員工	已設定	未設定	覆蓋率

全部 已設定 未設定 Q 搜尋帳號、姓名、Email

📄 操作步驟

路徑：系統管理 > 公司設定 > 安全性

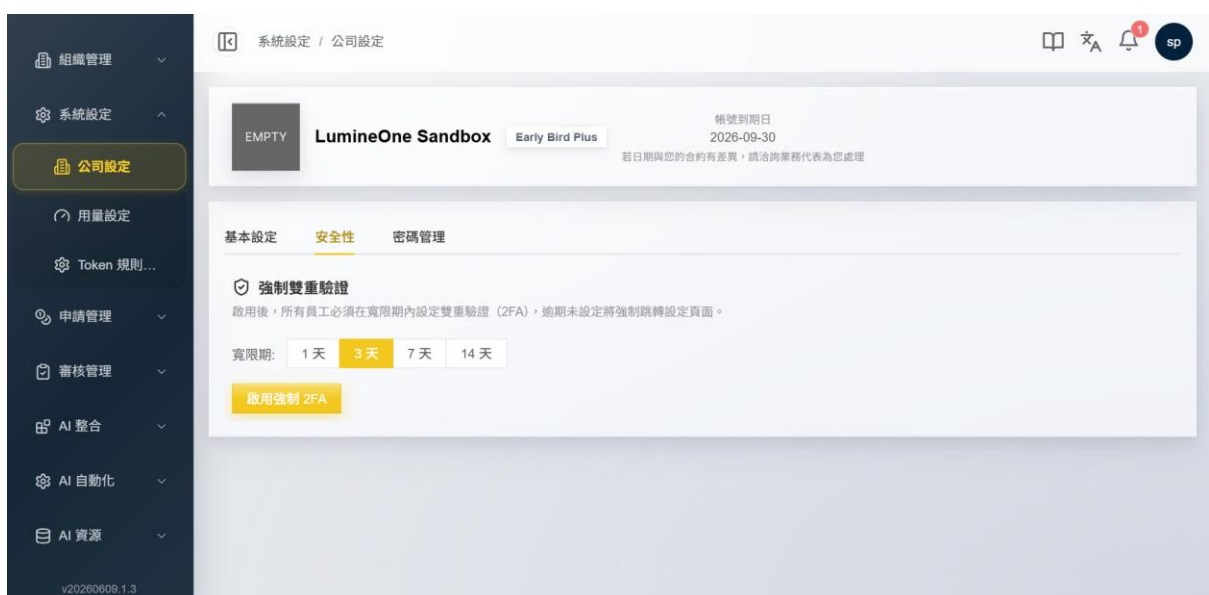
- 1 登入系統後，點擊上方導覽列「系統管理」，選擇「公司設定」



💡 提示

如找不到公司設定頁面，記得至角色管理 > 選單權限 勾選「公司設定」頁面，並重新進行登入

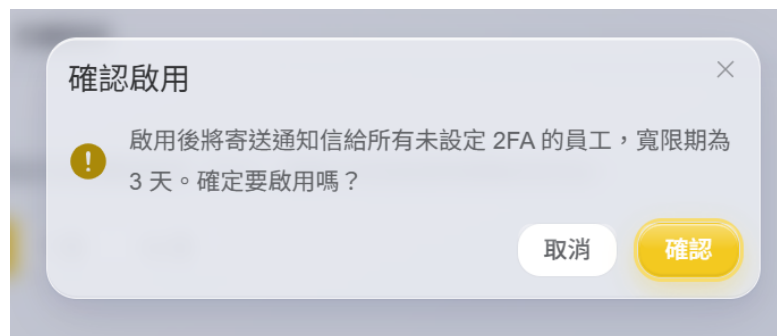
- 2 切換到「安全性」頁籤，選擇寬限期（預設為 7 天），並點擊「啟用強制 2FA」按鈕
可選：1 天 / 3 天 / 7 天 / 14 天



寬限期適用場景說明：

寬限期	適用場景
1 天	緊急安全需求，需立即全員啟用
3 天	短期推動，給員工基本準備時間
7 天（建議）	一般推動，多數情況建議使用
14 天	大型組織，需較長導入期

- 5 確認彈出視窗內容，點擊「確認」
系統將立即寄出通知信給所有尚未設定 2FA 的員工



啟用後：追蹤員工設定進度

啟用後，安全性頁面會顯示即時統計資訊：

- 全部員工：公司員工總數
- 已設定：已完成任一種 2FA 設定的員工數
- 未設定：尚未設定 2FA 的員工數
- 覆蓋率：已設定 / 全部員工的百分比

系統設定 / 公司設定

EMPTY LumineOne Sandbox Early Bird Plus 帳號到期日 2026-09-30 若日期與您的合約有差異，請洽詢業務代表為您處理

基本設定 安全性 密碼管理

🛡️ 強制雙重驗證
啟用後，所有員工必須在寬限期內設定雙重驗證 (2FA)。逾期未設定將強制跳轉設定頁面。

已啟用 截止時間: 2026-09-04 19:56

關閉強制 2FA

11 全部員工 6 已設定 5 未設定 55% 覆蓋率

全部 已設定 未設定 Q 搜尋帳號、姓名、Email 重置全部

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
hi.hi.hi	hi.hi.hi	hi.hi.hi@hi.com	未綁定	2026-09-03 19:56	重寄
spadmin	spadmin	yayalin1515+0826@pic.net.tw	已綁定	-	
spadmin02	spadmin02	yayalin1515+spadmin02@pic.net.tw	已綁定	-	

情境二 收到通知信後，設定 TOTP 驗證器

適用對象：一般員工（使用手機驗證器 App）

情境說明

您收到公司寄出的「雙因素驗證 (2FA) 設定通知」Email，需要在寬限期內完成設定。本章節將引導您使用手機驗證器 App (TOTP) 完成設定。

[外部]【LumineOne Sandbox】雙因素驗證 (2FA) 設定通知



Lumine AI Sandbox System Mail <ai-system-sandbox-no-reply@pic.net.tw>

收件者 yayalin1515+user03@pic.net.tw

回覆 全部回覆 轉寄 ...

2026/8/28 (週五) 下午 06:28

按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

提醒：此郵件來自外部寄件者，請小心處理附件和網址連結。

Notice: This email is from an external sender.

雙因素驗證設定通知

員工3-前台 您好，

您所屬的公司 **LumineOne Sandbox** 已啟用強制雙因素驗證 (2FA) 政策。

請儘速登入系統完成 2FA 設定，以確保您的帳號安全。

如何設定：

1. 登入 CMS 系統
2. 系統將自動引導您進行 2FA 設定
3. 使用 Google Authenticator 或其他驗證器 App 掃描 QR Code
4. 輸入驗證碼完成綁定

注意：寬限期結束後，未完成設定將無法正常使用系統。

如有任何問題，請聯繫您的系統管理員。

事前準備

請先在手機上安裝以下任一驗證器 App（免費）：

- Google Authenticator (iOS / Android)
- Microsoft Authenticator
- Authy
- 1Password (若已使用)



Google Authenticator



Microsoft Authenticator



Authy



1Password

提示

任何支援 TOTP 標準的驗證器 App 皆可使用，選擇您最熟悉的即可。
後續測試情境將以 Microsoft Authenticator 進行操作展示。

📋 操作步驟

路徑：右上角頭像 > 個人設定 > 多因素驗證 (MFA)

- 1 登入系統後，點擊右上角頭像，選擇「編輯個人資料」



- 2 切換到「多因素驗證 (MFA)」頁籤



3 在「驗證器 App (TOTP)」區塊，點擊「啟用多因素驗證」

個人資料

修改密碼

多因素驗證 (MFA)

申請代理人

通知設定

驗證器 App (TOTP)

啟用多因素驗證後，登入時除了密碼，還需通過第二重驗證（驗證器 App 驗證碼、生物辨識或安全金鑰），以提升帳號安全。

啟用多因素驗證

生物辨識 / 安全金鑰

使用裝置的指紋、臉部辨識或實體安全金鑰 (FIDO2) 登入，免輸入驗證碼。

尚未註冊任何生物辨識或安全金鑰。

為此裝置命名 (如：MacBook 指紋、YubiKey) 0 / 255

新增生物辨識 / 安全金鑰

4 畫面顯示 QR Code，打開手機驗證器 App，掃描 QR Code
若無法掃描，可點擊「或手動輸入此金鑰」，將文字金鑰手動輸入到 App

個人資料

修改密碼

多因素驗證 (MFA)

申請代理人

通知設定

驗證器 App (TOTP)

請使用驗證器 App (如 Google Authenticator、Authy) 掃描下方 QR Code。

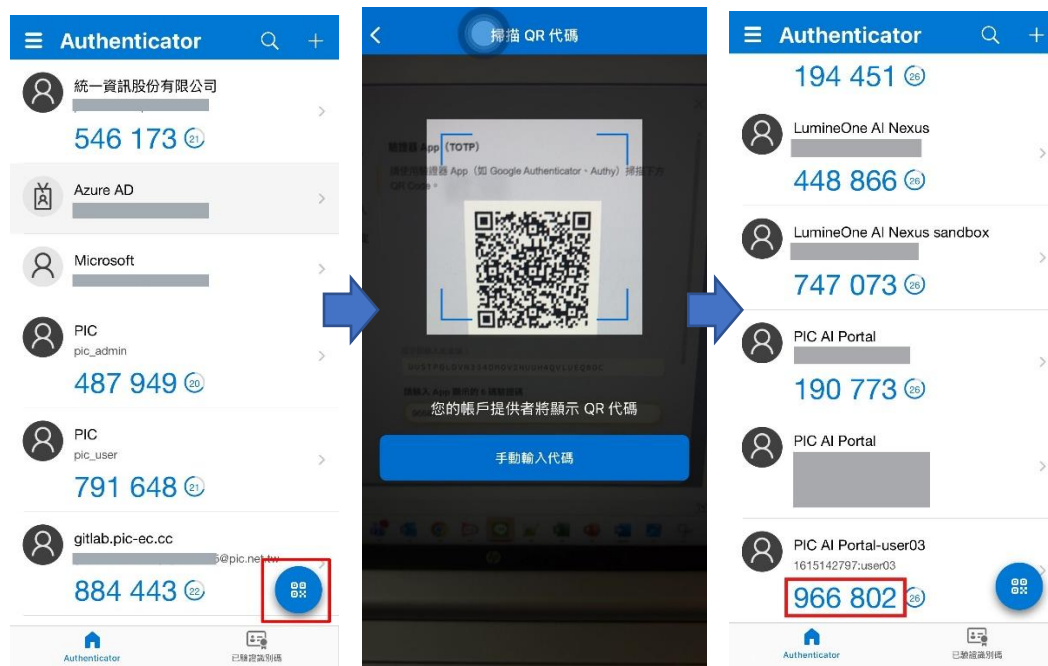
或手動輸入此金鑰：

UUSTPGLDVN334DMOV2HUUH4QVLUEQBDC

請輸入 App 顯示的 6 碼驗證碼

請輸入驗證碼

取消 確認並啟用



5 在驗證碼欄位輸入 App 顯示的 6 位數驗證碼，並點擊「確認並啟用」



7 系統顯示 8 組備援碼，請立即複製或抄寫保存

個人資料

修改密碼

多因素驗證 (MFA)

申請代理人

通知設定

驗證器 App (TOTP)

請妥善保存備援碼

每組備援碼僅能使用一次。當無法使用驗證器 App 時，可用備援碼登入。此畫面關閉後將無法再次查看。

DT76-JJLF	2UFA-4KVP
P48L-VJ7S	68F8-9VA3
XL77-W3HK	L7AF-88K6
V57E-YVMP	AQR8-SR69

複製備援碼

確認

生物辨識 / 安全金鑰

使用裝置的指紋、臉部辨識或實體安全金鑰 (FIDO2) 登入，免輸入驗證碼。

尚未註冊任何生物辨識或安全金鑰。

為此裝置命名 (如：MacBook 指紋、YubiKey) 0 / 255

● 重要

備援碼僅在此步驟顯示一次，關閉此畫面後將無法再次查看。請務必妥善保存（建議使用密碼管理器或紙本存放於安全處）。

8 點擊確認後系統顯示 已啟用多因素驗證，代表已完成多因素驗證設定

個人資料

修改密碼

多因素驗證 (MFA)

申請代理人

通知設定

驗證器 App (TOTP)

已啟用多因素驗證

輸入驗證碼或備援碼以停用

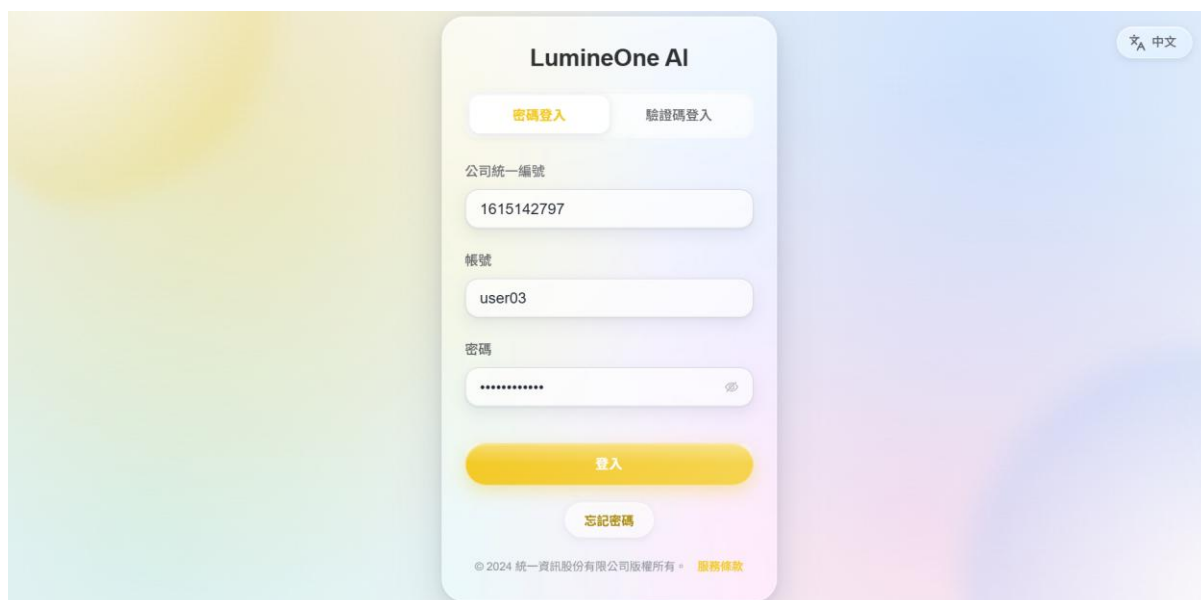
請輸入驗證碼

停用多因素驗證

之後如何登入？

完成設定後，每次登入流程如下：

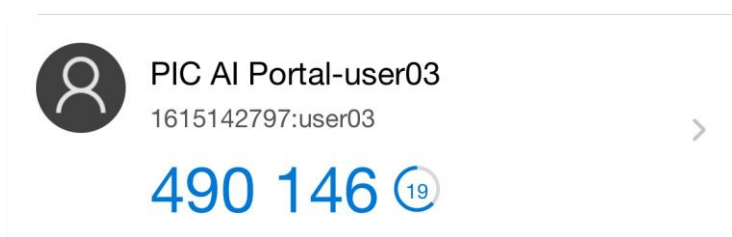
- 1 輸入帳號 (User ID) 和密碼，點擊「登入」



- 2 系統彈出「多因素驗證 (MFA)」對話框



- 3 打開手機驗證器 App，查看 6 位數驗證碼



4 輸入驗證碼，點擊「確認」，完成登入



多因素驗證 (MFA)

請輸入驗證器 App 顯示的 6 碼驗證碼。

490146

無法使用驗證器 App？可改輸入備援碼。

取消 確認

💡 提示

驗證碼每 30 秒更新一次。若輸入後提示不正確，請確認手機時間是否準確（建議開啟手機「自動設定時間」功能）。

情境三 設定指紋 / 臉部辨識登入 (WebAuthn)

適用對象：想使用生物辨識或安全金鑰的使用者

情境說明

您希望使用電腦指紋、臉部辨識或實體安全金鑰（如 YubiKey）登入，不需每次輸入驗證碼，更快速也更安全。

支援的裝置與方式

- MacBook / iPad 的 Touch ID 或 Face ID
- Windows Hello（指紋 / 臉部辨識 / PIN）
- Android 手機指紋
- 實體安全金鑰（YubiKey 等 FIDO2 相容裝置）

注意

部分舊版瀏覽器可能不支援 WebAuthn。建議使用最新版 Chrome、Safari、Edge 或 Firefox。

操作步驟

路徑：右上角頭像 > 個人設定 > 多因素驗證 (MFA)

1 登入系統後，進入「個人設定」>「多因素驗證 (MFA)」頁籤



個人資料

修改密碼

多因素驗證 (MFA)

申請代理人

通知設定

✓ 已啟用多因素驗證

輸入驗證碼或備援碼以停用

請輸入驗證碼

停用多因素驗證

生物辨識 / 安全金鑰

使用裝置的指紋、臉部辨識或實體安全金鑰 (FIDO2) 登入，免輸入驗證碼。

尚未註冊任何生物辨識或安全金鑰。

為此裝置命名 (如：MacBook 指紋、YubiKey) 0 / 255

新增生物辨識 / 安全金鑰

- 2 在「生物辨識 / 安全金鑰」區塊，輸入裝置名稱
例如：MacBook 指紋、辦公室桌機、YubiKey

生物辨識 / 安全金鑰

 使用裝置的指紋、臉部辨識或實體安全金鑰 (FIDO2) 登入，免輸入驗證碼。

尚未註冊任何生物辨識或安全金鑰。

user03_01 9 / 255

新增生物辨識 / 安全金鑰

- 3 點擊「新增生物辨識 / 安全金鑰」，瀏覽器彈出系統驗證提示（指紋掃描 / 臉部辨識 / 插入安全金鑰）



選擇「aiportal-sandbox.pic.net.tw」密碼金鑰的儲存位置

 Google 密碼管理工具 >

 使用手機、平板電腦或安全金鑰 >

取消

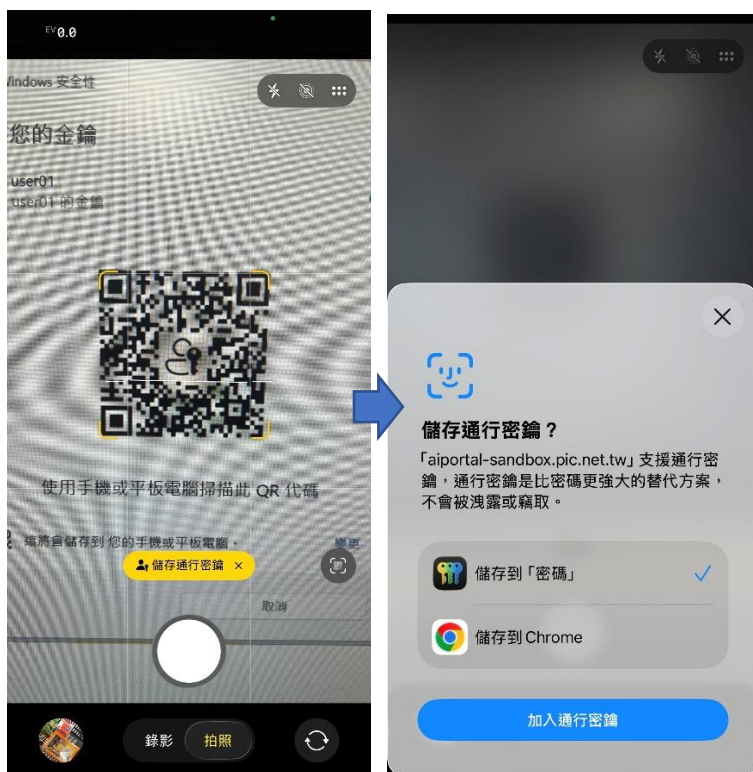
4-1 方法一：選擇使用 Google 密碼工具，並點擊建立，即可儲存密碼金鑰**4-2** 完成儲存密碼金鑰

5-1 方法二：選擇使用手機、平板電腦或安全金鑰，並點擊 iPhone、iPad 或 Android 裝置



5-2 手機開啟相機並掃描 QRCode，依提示進行驗證





5-3 完成生物辨識驗證

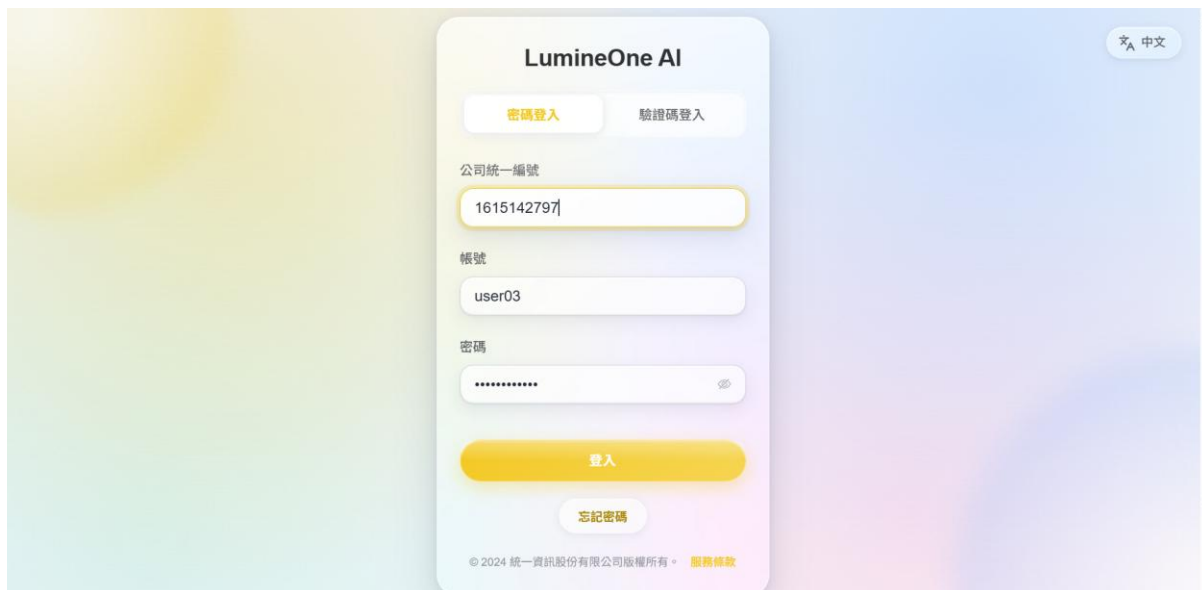


💡 提示

您可以為多台裝置分別註冊（如辦公室電腦指紋 + 個人 YubiKey），方便在不同場景使用。每個裝置會顯示名稱和上次使用時間，可隨時點擊「移除」刪除不再使用的裝置。

之後如何登入？

- 1 輸入帳號和密碼，點擊「登入」



The image shows the LumineOne AI login page. It features a central white card with a light blue header containing the text "LumineOne AI". Below the header, there are two tabs: "密碼登入" (Password Login) and "驗證碼登入" (Verification Code Login). The "密碼登入" tab is active. The form includes three input fields: "公司統一編號" (Company Unified Number) with the value "1615142797", "帳號" (Account) with the value "user03", and "密碼" (Password) with masked characters "*****". Below the password field is a yellow "登入" (Login) button and a smaller "忘記密碼" (Forgot Password) button. At the bottom of the card, there is a copyright notice: "© 2024 統一資訊股份有限公司版權所有。" and a "服務條款" (Terms of Service) link. In the top right corner of the page, there is a language selector button labeled "中文".

- 2 系統彈出 MFA 對話框，選擇「使用生物辨識 / 金鑰」



The image shows a "多因素驗證 (MFA)" (Multi-Factor Authentication) dialog box. It has a title bar with a close button (X). The dialog contains two buttons: "使用生物辨識 / 金鑰" (Use Biometric / Key) and "使用驗證碼" (Use Verification Code). Below these buttons, there is a text prompt: "請依瀏覽器提示完成指紋、臉部辨識或安全金鑰驗證。" (Please complete fingerprint, facial recognition, or security key verification according to the browser prompt). At the bottom, there are two buttons: "取消" (Cancel) and "使用生物辨識 / 安全金鑰" (Use Biometric / Security Key).

- 3 瀏覽器彈出驗證提示，點擊「使用其他密碼金鑰」，可依需求完成指紋 / 臉部辨識 / 安全金鑰驗證



- 4 擇一方式驗證完成後即可進入系統

情境 四 寬限期到期，系統強制設定 2FA

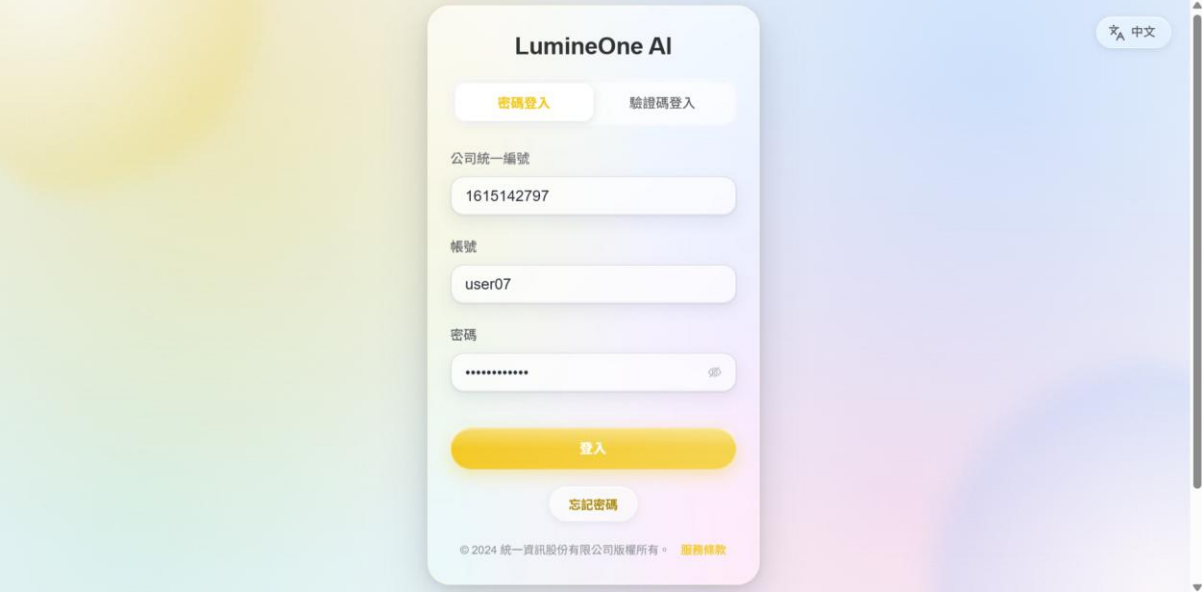
適用對象：尚未設定 2FA、寬限期已到期的員工

情境說明

公司啟用強制 2FA 後，若您在寬限期內未完成設定，登入後系統將自動跳轉到「設定雙重驗證」頁面，無法跳過，必須完成設定才能繼續使用系統。

操作步驟

1 登入系統（輸入帳號和密碼）



The login screen for LumineOne AI features a central white card on a light blue background. At the top of the card is the title 'LumineOne AI'. Below it are two buttons: '密碼登入' (Password Login) in yellow and '驗證碼登入' (Code Login) in white. The form includes three input fields: '公司統一編號' (Company Unified Number) with the value '1615142797', '帳號' (Account) with the value 'user07', and '密碼' (Password) with masked characters. A yellow '登入' (Login) button is positioned below the password field, with a '忘記密碼' (Forgot Password) link underneath. At the bottom of the card, a copyright notice reads '© 2024 統一資訊股份有限公司版權所有。' followed by a '服務條款' (Terms of Service) link. In the top right corner of the page, there is a language selector showing '中文'.

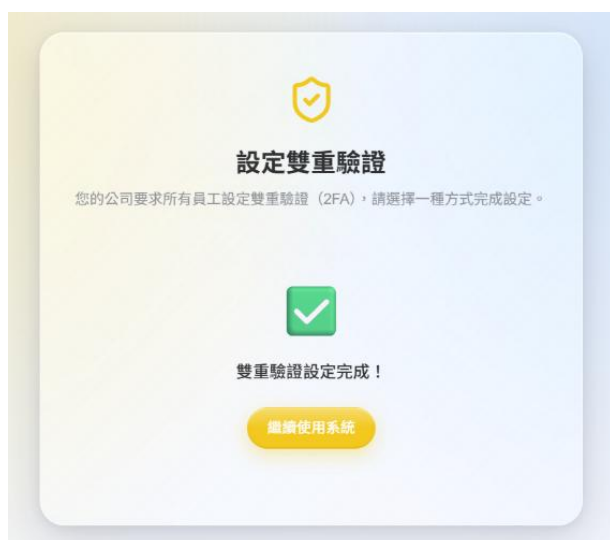
2 系統自動跳轉到「設定雙重驗證」頁面，頁面顯示：「您的公司要求所有員工設定雙重驗證（2FA），請選擇一種方式完成設定。」



The '設定雙重驗證' (Set up 2FA) screen has a light blue background with a white central card. At the top of the card is a yellow shield icon with a checkmark and the title '設定雙重驗證'. Below the title is a message: '您的公司要求所有員工設定雙重驗證（2FA），請選擇一種方式完成設定。' The card contains two main options, each with an icon and a button. The first option is '驗證器 App (TOTP)' with a key icon and a button labeled '設定驗證器'. The second option is '生物辨識 / 安全金鑰' with a hand icon and a button labeled '設定生物辨識'. Below each option is a brief description: '使用驗證器 App 產生一次性驗證碼' for TOTP and '使用指紋、臉部辨識或安全金鑰' for biometrics.

- 3 依所選方式，「設定驗證器」(TOTP，需手機 App) 或「設定生物辨識」(WebAuthn，使用指紋 / 臉部辨識) 完成設定
詳細步驟請參閱「情境二」(TOTP) 或「情境三」(WebAuthn)

- 4 設定完成後，頁面顯示「雙重驗證設定完成！」，點擊「繼續使用系統」即可正常使用



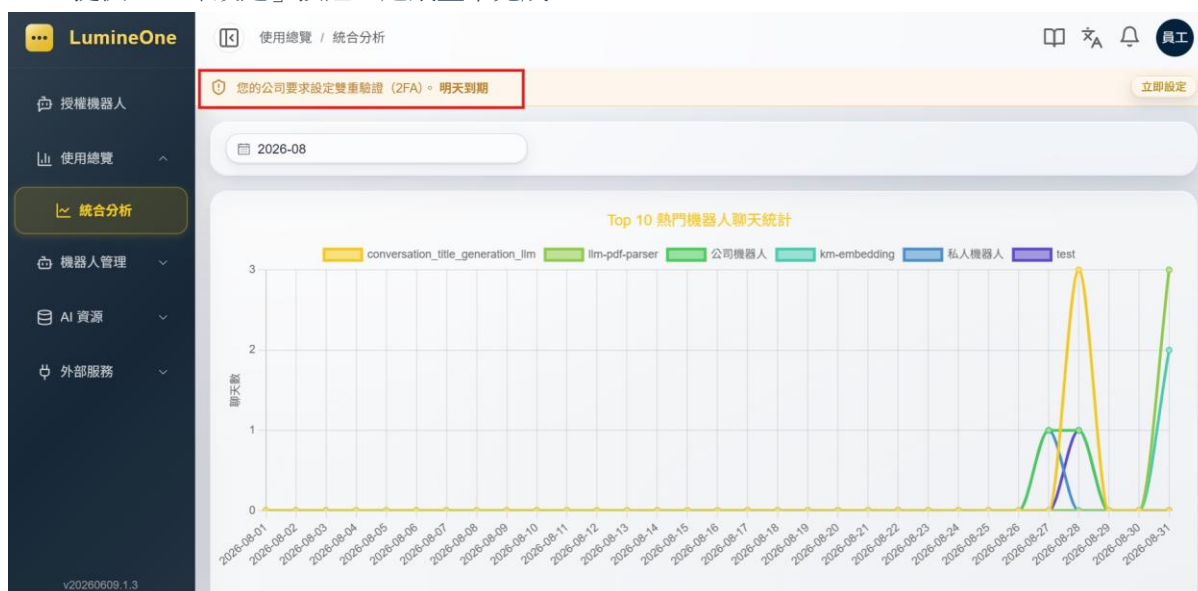
⚠ 注意

寬限期到期後，此頁面無法跳過或關閉，請選擇任一方式完成設定。

💡 寬限期內的提示

若您在寬限期內登入，頁面頂部會出現黃色提示條：

- 提示條顯示「您的公司要求設定雙重驗證 (2FA)。」
- 顯示倒數天數 (剩餘 X 天 / 明天到期)
- 提供「立即設定」按鈕，建議盡早完成



💡 提示

建議在寬限期內盡早完成設定，避免到期後被強制跳轉影響工作。

情境五 手機遺失，使用備援碼登入

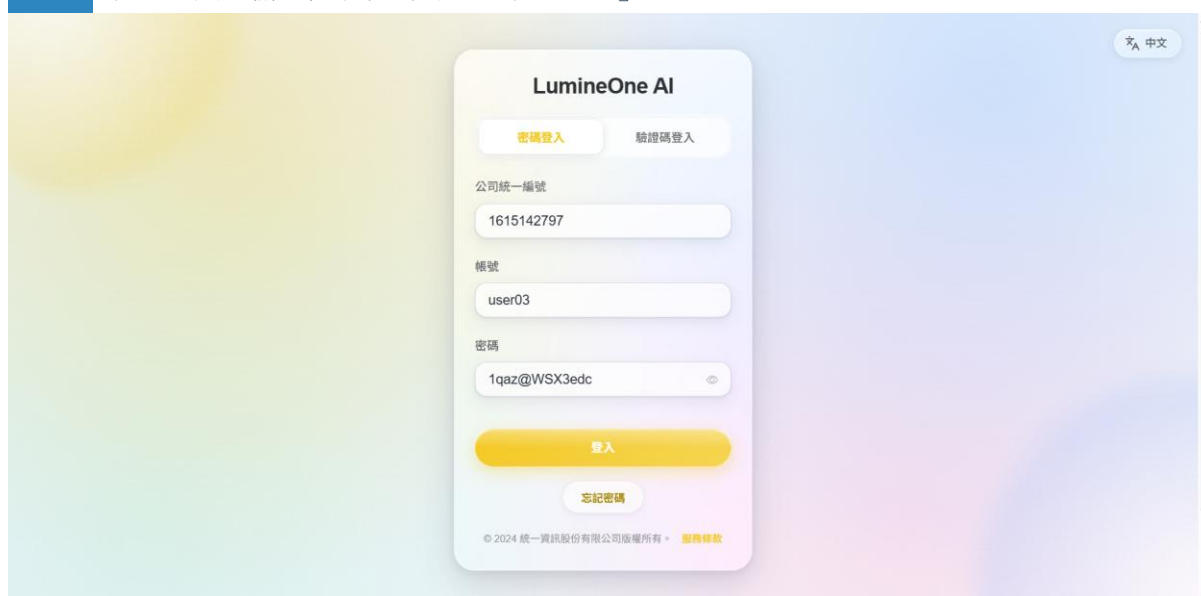
適用對象：手機遺失或驗證器 App 無法使用的使用者

情境說明

您的手機遺失或驗證器 App 無法正常運作，導致無法取得 6 位數驗證碼。此時可使用啟用 TOTP 時保存的備援碼登入。

操作步驟

- 1 在登入頁面輸入帳號和密碼，點擊「登入」



- 2 系統彈出「多因素驗證 (MFA)」對話框，切換至使用驗證碼，可找到提示：「無法使用驗證器 App？可改輸入備援碼。」

適用於使用驗證器 APP 的情境



- 3 輸入一組尚未使用的備援碼（格式如 XXXX-XXXX），點擊「確認」，完成登入



● 重要

每組備援碼僅能使用一次，使用後即失效。您共有 8 組備援碼，請妥善保管剩餘備援碼。

💡 提示

若您同時已設定 生物辨識/金鑰（如電腦指紋），也可使用該方式登入，不需備援碼。

情境六 管理員：有員工 Email 錯誤，無法收到通知

適用對象：公司管理員

情境說明

啟用強制 2FA 後，您發現部分員工 Email 設定錯誤，導致員工收不到通知信。本章節說明如何在修改 Email 後重新發送通知。

操作步驟

路徑：系統管理 > 公司設定 > 安全性

1 進入「公司設定」>「安全性」頁籤，查看員工 2FA 狀態列表

系統設定 / 公司設定

基本設定 **安全性** 密碼管理

強制雙重驗證
啟用後，所有員工必須在寬限期內設定雙重驗證 (2FA)，逾期未設定將強制跳轉設定頁面。

已啟用 截止時間: 2026-09-04 19:56

關閉強制 2FA

11 全部員工 6 已設定 5 未設定 55% 覆蓋率

全部 已設定 未設定 Q 搜尋帳號、姓名、Email 重寄全部

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
hi.hi.hi	hi.hi.hi	hi.hi.hi@hi.com	未綁定	2026-09-03 19:56	重寄
spadmin	spadmin	yayalin1515+0826@pic.net.tw	已綁定	-	
spadmin02	spadmin02	yayalin1515+spadmin02@pic.net.tw	已綁定	-	
spadmin03	spadmin03	yayalin1515+spadmin03@pic.net.tw	未綁定	2026-09-03 19:56	重寄
user01	員工1-前台	yayalin1515+user01@pic.net.tw	已綁定	2026-08-31 11:32	

2 點擊該員工旁的「重寄」按鈕，發送 2FA 設定通知信

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
user05	員工5-後台	yunwork200727+user05@gmail.com	未綁定	2026-08-28 18:28	重寄

3 員工收到通知信後，即可依照信中指引完成 2FA 設定

[外部]【LumineOne Sandbox】雙因素驗證 (2FA) 設定通知



Lumine AI Sandbox System Mail <ai-system-sandbox-no-reply@pic.net.tw>
收件者: yayalin1515+user03@pic.net.tw

回覆 全部回覆 轉寄 ...
2026/8/28 (週五) 下午 06:28

按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

提醒：此郵件來自外部寄件者，請小心處理附件和網址連結。
Notice: This email is from an external sender.

雙因素驗證設定通知

員工3-前台 您好，

您所屬的公司 **LumineOne Sandbox** 已啟用強制雙因素驗證 (2FA) 政策。

請儘速登入系統完成 2FA 設定，以確保您的帳號安全。

如何設定：

1. 登入 CMS 系統
2. 系統將自動引導您進行 2FA 設定
3. 使用 Google Authenticator 或其他驗證器 App 掃描 QR Code
4. 輸入驗證碼完成綁定

注意：寬限期結束後，未完成設定將無法正常使用系統。

如有任何問題，請聯繫您的系統管理員。

💡 提示

若需要批次重寄通知給所有未設定的員工，可點擊「重寄全部」按鈕，一次發送給所有尚未設定 2FA 的員工。

全部

已設定

未設定

Q 搜尋帳號、姓名、Email

重寄全部

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
hi.hi.hi.	hi.hi.hi.	hi.hi.hi.hi@hi.com	未綁定	2026-09-03 19:56	重寄
spadmin	spadmin	yayalin1515+0826@pic.net.tw	已綁定	-	
spadmin02	spadmin02	yayalin1515+spadmin02@pic.net.tw	已綁定	-	

情境七 管理員：關閉強制 2FA

適用對象：公司管理員

情境說明

您需要暫時關閉強制 2FA 功能（例如：需要調整寬限期、或業務需求暫緩推動）。

操作步驟

路徑：系統管理 > 公司設定 > 安全性

1 進入「公司設定」>「安全性」頁籤

系統設定 / 公司設定

基本設定 安全性 密碼管理

強制雙重驗證
啟用後，所有員工必須在寬限期內設定雙重驗證（2FA），逾期未設定將強制跳轉設定頁面。

已啟用 截止時間: 2026-09-04 19:56

關閉強制 2FA

11 全部員工 6 已設定 5 未設定 55% 覆蓋率

全部 已設定 未設定 搜尋帳號、姓名、Email 重置全部

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
hi.hi.hi	hi.hi.hi	hi.hi.hi@hi.com	未綁定	2026-09-03 19:56	重寄
spadmin	spadmin	yayain1515+0826@pic.net.tw	已綁定	-	
spadmin02	spadmin02	yayain1515+spadmin02@pic.net.tw	已綁定	-	
spadmin03	spadmin03	yayain1515+spadmin03@pic.net.tw	未綁定	2026-09-03 19:56	重寄
user01	員工1-前台	yayain1515+user01@pic.net.tw	已綁定	2026-08-31 11:32	
user02	員工2-前台	yayain1515+user02@pic.net.tw	未綁定	2026-09-03 19:56	重寄
user03	員工3-前台	yayain1515+user03@pic.net.tw	未綁定	2026-08-28 18:28	重寄

2 在已啟用狀態下，點擊「關閉強制 2FA」按鈕

系統設定 / 公司設定

基本設定 安全性 密碼管理

強制雙重驗證
啟用後，所有員工必須在寬限期內設定雙重驗證（2FA），逾期未設定將強制跳轉設定頁面。

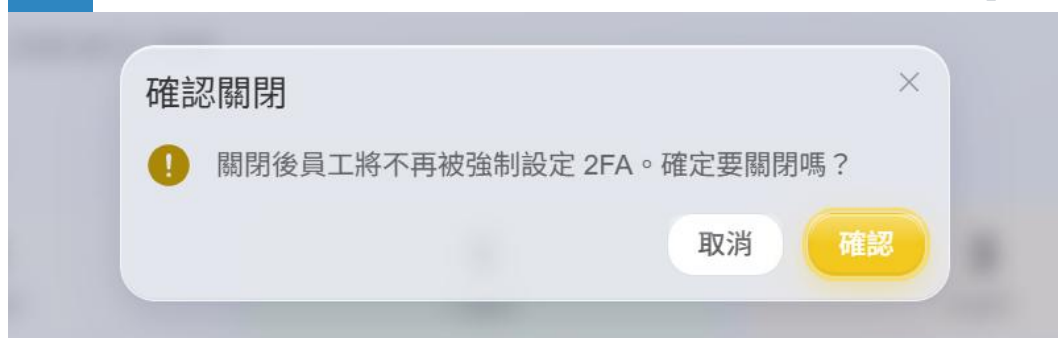
已啟用 截止時間: 2026-09-04 19:56

關閉強制 2FA

11 全部員工 6 已設定 5 未設定 55% 覆蓋率

全部 已設定 未設定 搜尋帳號、姓名、Email 重置全部

帳號	姓名	電子郵件	2FA 狀態	通知時間	重寄
hi.hi.hi	hi.hi.hi	hi.hi.hi@hi.com	未綁定	2026-09-03 19:56	重寄
spadmin	spadmin	yayain1515+0826@pic.net.tw	已綁定	-	
spadmin02	spadmin02	yayain1515+spadmin02@pic.net.tw	已綁定	-	
spadmin03	spadmin03	yayain1515+spadmin03@pic.net.tw	未綁定	2026-09-03 19:56	重寄
user01	員工1-前台	yayain1515+user01@pic.net.tw	已綁定	2026-08-31 11:32	
user02	員工2-前台	yayain1515+user02@pic.net.tw	未綁定	2026-09-03 19:56	重寄
user03	員工3-前台	yayain1515+user03@pic.net.tw	未綁定	2026-08-28 18:28	重寄

3 確認彈出視窗：「關閉後員工將不再被強制設定 2FA。確定要關閉嗎？」**4** 點擊「確認」，強制設定解除 關閉後的影響

對象	影響
已設定 2FA 的員工	不受影響，2FA 仍正常運作，登入時仍需驗證
未設定 2FA 的員工	不再被強制跳轉設定頁面，可照常使用系統
員工自行設定	員工仍可在個人設定中自行啟用 2FA

 提示

若需要重新啟用強制 2FA（例如調整寬限期），可再次點擊「啟用強制 2FA」，以新的寬限期重新開始，會自動寄出通知信給未綁定的員工。

常見問題 Q&A

Q 驗證器 App(TOTP) 和 生物辨識 / 安全金鑰(WebAuthn) 需要同時設定嗎？

A 不需要。兩種方式獨立運作，啟用任一種即可。同時啟用可在登入時選擇偏好的方式。

Q 手機遺失又沒有備援碼怎麼辦？

A 若有已註冊的生物辨識 / 安全金鑰(WebAuthn) 裝置（如電腦指紋），可使用該方式登入。若完全無法驗證，請聯絡系統管理員協助重置。

Q 驗證碼輸入正確但系統提示不正確？

A 請確認手機時間是否準確。TOTP 依賴裝置時間，偏差超過 30 秒可能導致失敗。建議開啟手機的「自動設定時間」功能。

Q 「強制 2FA」啟用後，已設定的員工會受影響嗎？

A 不會。已設定 2FA 的員工不會收到通知信，也不會看到強制設定頁面。此功能僅針對尚未設定的員工。

Q 寬限期可以修改嗎？

A 啟用後無法直接修改寬限期。若需調整，可先關閉強制 2FA，再以新的寬限期重新啟用。

Q 管理員本人不想設定 2FA 可以嗎？

A 若要開啟「強制 2FA」功能，管理員必須先自行設定 2FA。設定後仍可在個人設定中停用；但若「強制 2FA」仍在有效期內，停用後會再次被要求設定。若未啟用「強制 2FA」功能，管理員的個人 2FA 則為選填。

Q 員工可以自行停用 2FA 嗎？

A 可以在個人設定中停用。但若公司已啟用「強制 2FA」且仍在有效期內，停用後會再次被要求設定。

Q 備援碼可以重新產生嗎？

A 停用再重新啟用 TOTP 時，系統會產生一組全新的備援碼。舊的備援碼全部失效。

Q 生物辨識 / 安全金鑰(WebAuthn) 可以在多台電腦上使用嗎？

A 可以。每台電腦分別註冊（如「辦公室桌機指紋」、「筆電 Hello」），登入時使用當前裝置的生物辨識即可。

Q 通知信沒有收到怎麼辦？

A 請先確認 Email 是否設定正確。管理員可在儀表板查看員工的通知時間，並使用「重寄」按鈕重新發送。也請檢查垃圾郵件匣。

Q 5 分鐘內未完成 MFA 驗證會怎樣？

A MFA 驗證挑戰會逾時自動失效，需重新輸入帳號密碼登入。這是系統安全機制，防止未完成的驗證被盜用。