


樹林廠新人Office 無法登入

2025-12-04 14:32 - 正達 駱


狀態:	Closed-關閉	開始日期:	2025-12-04
優先權:	High	完成日期:	2025-12-04
被分派者:	正達 駱	完成百分比:	100%
分類:		預估工時:	0:00 小時
版本:		耗用工時:	3:00 小時
需求人員:	謝尚谷	聯絡人e-mail:	
需求部門單位:	廠端	希望完成日期:	
聯絡人分機/手機:		完成日期:	

概述



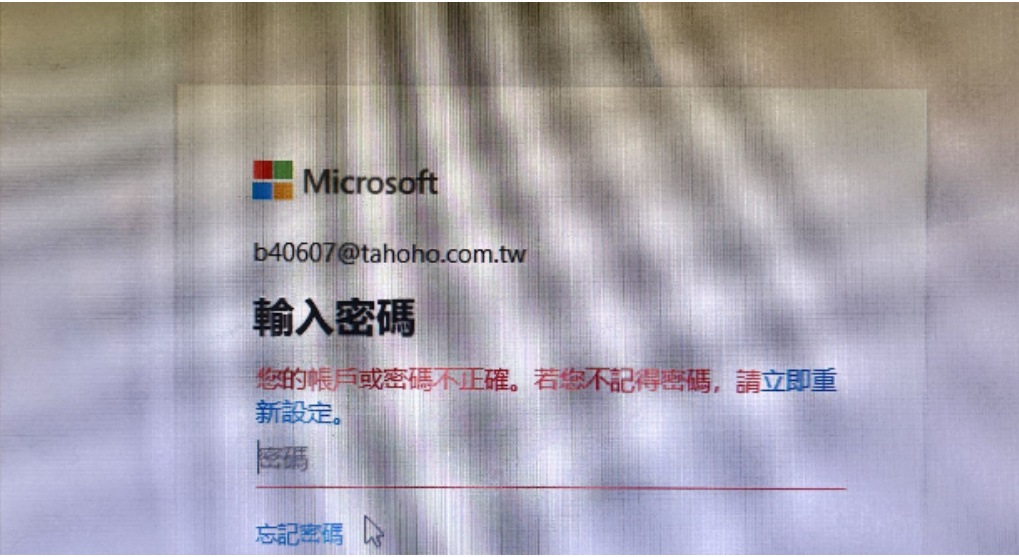
「樹林廠」謝尚谷

jashwa/阿璋



駱sir 我們新人 b40607梁郭晏璇 office 及mail無法登入。。網域(開機)可以

上午 9:43



歷史

#1 - 2025-12-04 15:18 - 正達 駱

- 完成日期 設定為 2025-12-04
- 狀態 從 New-新增 變更為 Resolved-解決
- 完成百分比 從 0 變更為 100

12/3新增樹林廠新進同仁帳號及給予office授權。
本次錯誤是Azure entraID sync的密碼同步失敗，所以無法登入
處理方式如下
1.檢查連結器及服務是否啟用
Get-ADSyncConnector 輸出：

您有兩個連接器：tahotw.onmicrosoft.com - AAD (類型為 AAD) 和 tahoho.com.tw (類型為 AD)。這是正確的。
Get-ADSyncAADPasswordSyncConfiguration 輸出：

您已成功使用正確的 AD 連接器名稱 (tahoho.com.tw) 執行此命令。
結果顯示 Enabled: True。
這是一個重要的發現！這表示從 PowerShell 的角度來看，密碼雜湊同步 (Password Hash Synchronization, PHS) 功能在您的 Azure AD Connect 上是已啟用的。

問題點與下一步
既然 PHS 顯示為已啟用，但 Microsoft 365 管理中心卻顯示「上次密碼同步處理時間：50 天前」，這表示：

PHS 雖然已啟用，但實際的密碼雜湊同步過程可能因為某些原因未能成功執行。
管理中心的顯示可能存在延遲或錯誤。(但 50 天的延遲不太尋常)
最可能的原因是 Azure AD Connect 服務帳戶在本地 Active Directory 中缺乏必要的權限，導致它無法讀取使用者的密碼雜湊進行同步。

建議的解決方案步驟：
步驟 1：確認 ADSync 服務帳戶的權限 (最常見原因)
Azure AD Connect 服務帳戶 (通常是 MSOL_ 開頭的帳戶) 需要在您的本地 Active Directory 網域中具有特定的權限，才能讀取密碼雜湊。

找出 ADSync 服務帳戶名稱：MSOL_c81edcf6ffef

在 Azure AD Connect 伺服器上，開啟 Synchronization Service Manager (同步處理服務管理員)。
點擊「Connectors」(連接器)。
找到您的 AD 連接器 (tahoho.com.tw)，右鍵點擊「Properties」(屬性)。
在「Connect to Active Directory Forest」(連接到 Active Directory 樹系) 頁面，您會看到「User name」(使用者名稱)，這就是 ADSync 服務帳戶。
檢查該帳戶在本地 AD 的權限：

在您的 網域控制器 (Domain Controller) 上，開啟 Active Directory 使用者和電腦 (Active Directory Users and Computers)。
右鍵點擊您的網域 (tahoho.com.tw)，選擇「委派控制」(Delegate Control)。
點擊「下一步」，然後點擊「新增」，找到您的 ADSync 服務帳戶並新增。
點擊「下一步」，選擇「建立自訂工作以委派」(Create a custom task to delegate)。
點擊「下一步」，選擇「此資料夾、現有物件中的物件，以及此資料夾中的新物件」(This folder, existing objects in this folder, and creation of new objects in this folder)。
點擊「下一步」，在「權限」列表中，確保以下權限已勾選：
Replicating Directory Changes (複寫目錄變更)
Replicating Directory Changes All (複寫所有目錄變更)
完成委派精靈。

手動強制執行一次完整的密碼同步
即使 PHS 顯示為啟用，強制執行一次完整的同步週期可以確保所有必要的組件都被觸發。

Import-Module ADSync

```
1. 停止同步排程器，以確保我們能手動控制
Set-ADSyncScheduler -SyncCycleEnabled $false
```

1. 執行一次完整的同步週期，這會包含密碼雜湊同步

```
Start-ADSyncSyncCycle -PolicyType Initial
```

1. 等待同步完成 (可能需要一些時間，視您的 AD 大小而定)
2. 您可以執行 Get-ADSyncScheduler 查看 SyncCycleInProgress 是否變為 False

```
1. 重新啟用同步排程器
Set-ADSyncScheduler SyncCycleEnabled $true
```

執行上述密碼同步後，M365監控密碼同步恢復正常，也可以正常登入了。

#2 - 2026-01-12 13:08 - Joy Liao
- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案			
clipboard-202512041431-205y2.png	21.6 KB	2025-12-04	正達 駱
clipboard-202512041432-qca8d.png	347 KB	2025-12-04	正達 駱