技能解封初始篇章-暴力黃袍加身(Privileged Identity)

前言

<https://ithelp.ithome.com.tw/articles/10213979>

成本評估

**Privileged Identity 依下列定價面向計費：**

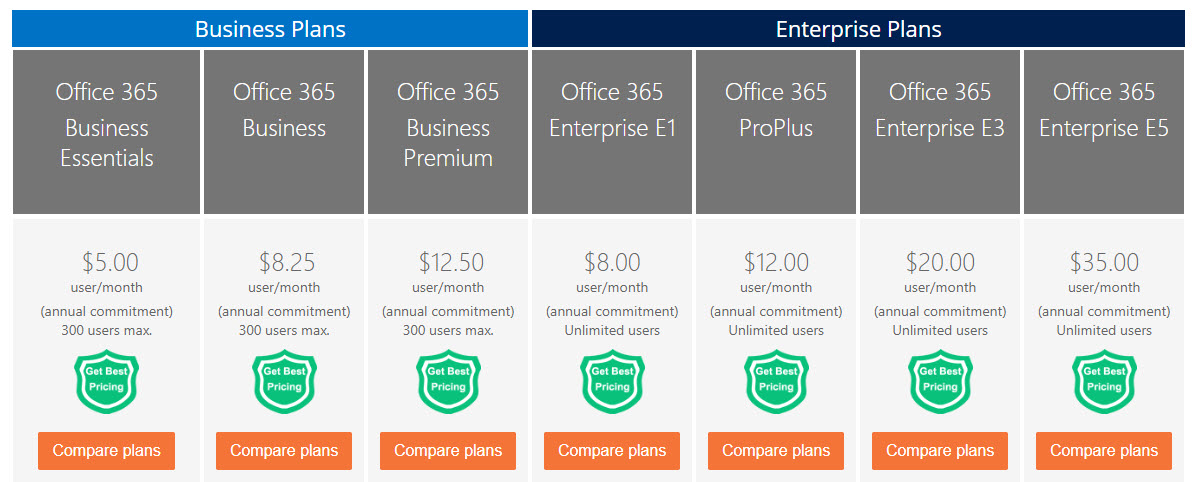
Azure Active Directory 共有四種版本：Free、Office 365 應用程式版本、Premium P1 及 Premium P2。Azure 訂用帳戶即包含免費版。您可以透過 [Microsoft Enterprise 合約](https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise.aspx)、[開放大量授權計劃](https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx)與[雲端方案提供者](https://go.microsoft.com/fwlink/?LinkId=614968&clcid=0x404)計劃取得 Premium 版本。

Azure 及 Office 365 訂閱者也可以線上購買 Azure Active Directory Premium P1 or P2。於此處[登入](https://portal.office.com/Commerce/Catalog.aspx)購買。

一張含有 文字 的圖片

自動產生的描述

**企業版本類型一次滿足**



常見E1 / E3 / E5 功能比較(本次驗證為 E5 約NT$1,135.00 每個用戶/月)

一張含有 文字 的圖片

自動產生的描述

總結上述功能需求需要以下任意授權才能開始使用

* Azure AD Premium P2
* Enterprise Mobility + Security (EMS) E5
* Microsoft 365 M5

前置作業

1. Azure 管理員需要有全域管理權限外並有上述之一的授權
2. 建立幾組帳戶可以測試比對之用

簡易實測環境

圖1. 從Azure Portal上搜尋"Privileged Identity"

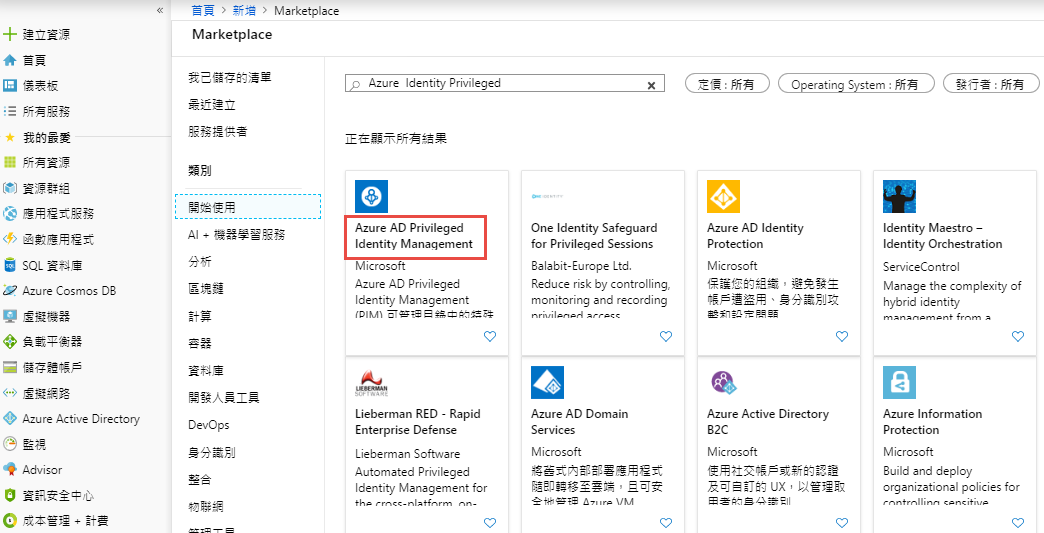


圖2. 選擇此後按下建立

一張含有 文字 的圖片

自動產生的描述

圖3. 建立完成可以釘選至左列表中方便操作

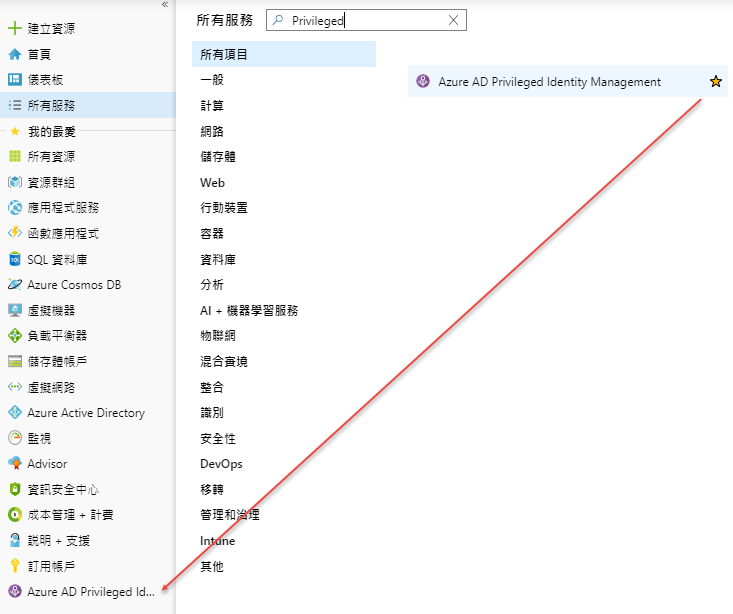


圖4. 預設的登入畫面中間的簡介說明了以下的新功能服務文件列表(可以拿掉勾勾關閉它)

一張含有 文字 的圖片

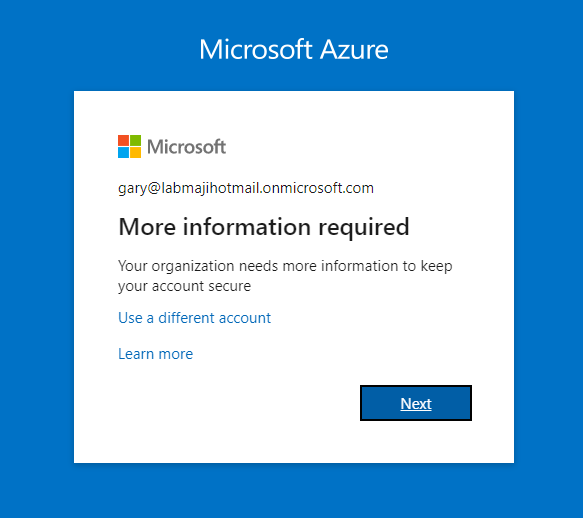
自動產生的描述

圖5. 一開始需要對目前的帳戶目錄做身份驗證

一張含有 文字 的圖片

自動產生的描述

圖6. 需要對此帳戶做驗證動作



**圖7. 指定你能收到簡訊的手機,下一步繼續**

一張含有 文字 的圖片

自動產生的描述

圖8. 驗證進行中

一張含有 文字 的圖片

自動產生的描述圖9. 驗證完成

一張含有 文字 的圖片

自動產生的描述

圖10. 驗證登入(按No不記憶密碼)

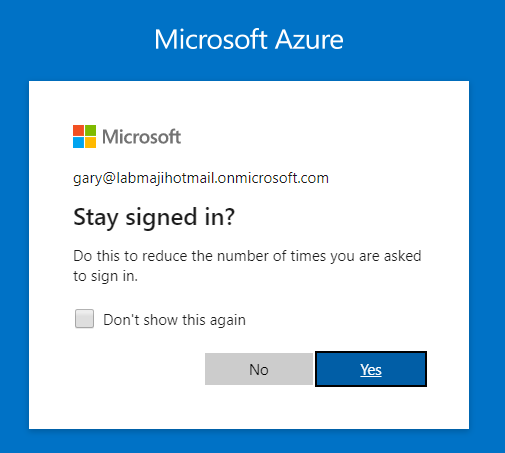


圖11. 驗證完成

一張含有 文字 的圖片

自動產生的描述

圖12. 需要執行同意動作

一張含有 文字 的圖片

自動產生的描述

圖13. 同意註冊完成後就可以開始正常使用PIM

一張含有 文字 的圖片

自動產生的描述

圖14. 查看成員地方可以看到原來已經在上面的帳戶及所賦予的權限(均為永久啟用)

一張含有 文字 的圖片

自動產生的描述

圖15. 警示地方也發現到過多的全域管理員帳戶過多的問題,可能需要視需求調整改善

一張含有 文字 的圖片

自動產生的描述

圖16. 個別帳戶可以看到其每個角色的歷程紀錄以及透過長條統計各角色的數量

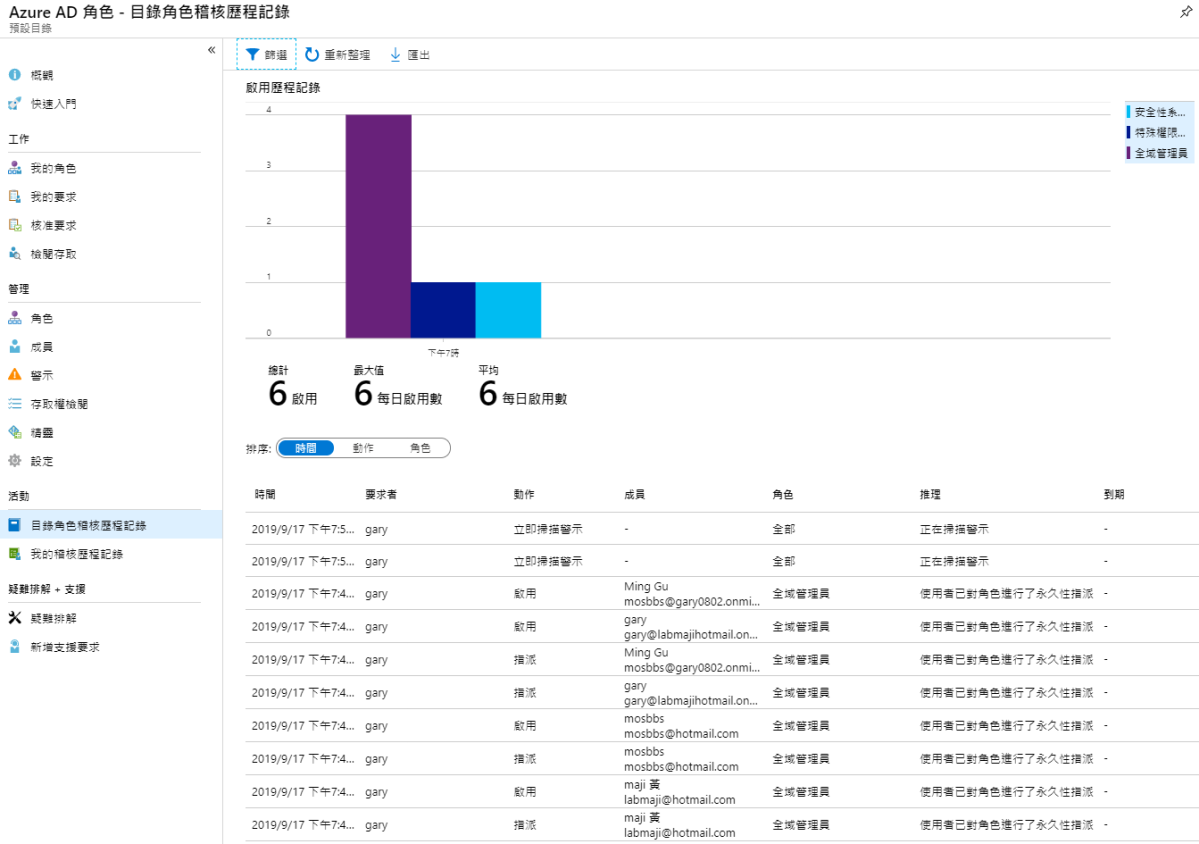


圖17. 我們可以從快速入門開始進行指派權限的作業

一張含有 文字 的圖片

自動產生的描述

圖18. 加入成員前先選擇指定的角色權力(我選擇安全性讀取)

一張含有 文字 的圖片

自動產生的描述

圖19. 選擇指定的成員

一張含有 文字 的圖片

自動產生的描述

圖20. 選擇完成會顯示類型為"合格"

一張含有 文字 的圖片

自動產生的描述

| 詞彙或概念 | 角色指派類別 | 說明 |
| --- | --- | --- |
| 合格 | 類型 | 需要使用者執行一或多個動作才能使用角色的角色指派。 如果使用者已有資格使用角色，即表示他們可以在需要執行特殊權限工作時啟用該角色。 使用者不論是具有永久角色指派還是合格角色指派，獲得的存取權並無差異。 唯一的差異在於有些使用者並不一直需要該存取權。 |
| 作用中 | 類型 | 不要求使用者執行任何動作即可使用角色的角色指派。 指派為有效的使用者具有指派給角色的權限。 |
| 啟用 |  | 此程序會執行一或多個動作，讓使用者使用有資格使用的角色。 動作可能包含執行多重要素驗證 (MFA) 檢查、提供業務理由，或是向指定的核准者要求核准。 |
| 已指派 | State | 具有作用中角色指派的使用者。 |
| 已啟用 | State | 具有合格角色指派、已執行動作來啟用角色，且目前為作用中的使用者。 啟動後，使用者便可在必須加以重新啟動之前，先為預先設定的期限使用該角色。 |
| 永久合格 | Duration | 使用者一律有資格啟用角色的角色指派。 |
| 永久有效 | Duration | 使用者一律可以使用角色而不需執行任何動作的角色指派。 |
| 合格過期 | Duration | 使用者有資格在指定的開始和結束日期內啟用角色的角色指派。 |
| 有效過期 | Duration | 使用者可以在指定的開始和結束日期內使用角色而不需執行任何動作的角色指派。 |
| just-in-time (JIT) 存取 |  | 一種模型，使用者會在其中獲得臨時權限以執行特殊權限的工作，這可防止惡意或未經授權的使用者在權限過期後取得存取權。 只有當使用者需要時才會獲得存取權。 |
| 最低權限存取的原則 |  | 建議的安全性做法，每位使用者只會獲得所需的最低權限，以便完成他們獲得授權而可執行的工作。 這種做法只需要最少量的全域管理員，並會改為針對特定案例使用特定的管理員角色。 |

圖21. 我們可以針對帳戶做權限檢閱

一張含有 文字 的圖片

自動產生的描述

圖22. 重新在檢視成員會看到啟用的地方有原本合格(有時效性)與永久

一張含有 桌 的圖片

自動產生的描述

圖23. 透過精靈示範把原來既有的成員帳戶轉至合格類型

一張含有 文字 的圖片

自動產生的描述

圖24. 任選一帳戶

一張含有 桌 的圖片

自動產生的描述

圖25. 將此帳戶從永久轉成合格

一張含有 桌 的圖片

自動產生的描述

圖26. 此帳戶已經指派為合格類型

一張含有 文字 的圖片

自動產生的描述

圖27. 合格轉換流程已完成

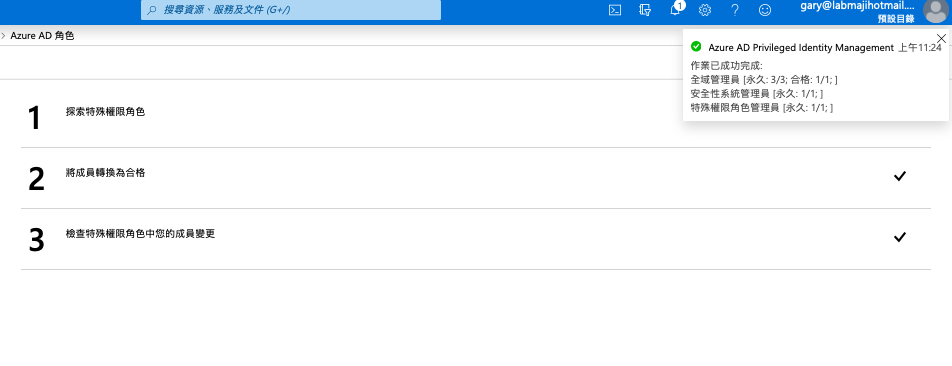


圖28.當然你也是可以把原來的合格時效性轉為永久

一張含有 文字 的圖片

自動產生的描述

圖29. 設置完成

一張含有 文字 的圖片

自動產生的描述

圖30. 也會同時收到調整的PIM警示通知

一張含有 文字 的圖片

自動產生的描述

圖31. 而如果你嫌警示通知煩人也是可以解除掉的

一張含有 文字 的圖片

自動產生的描述