技能解封初始篇章-資源環境風險漏洞(Conditional Access)

前言

<https://ithelp.ithome.com.tw/articles/10213976>

成本評估

**Conditional Access 依下列定價面向計費：**

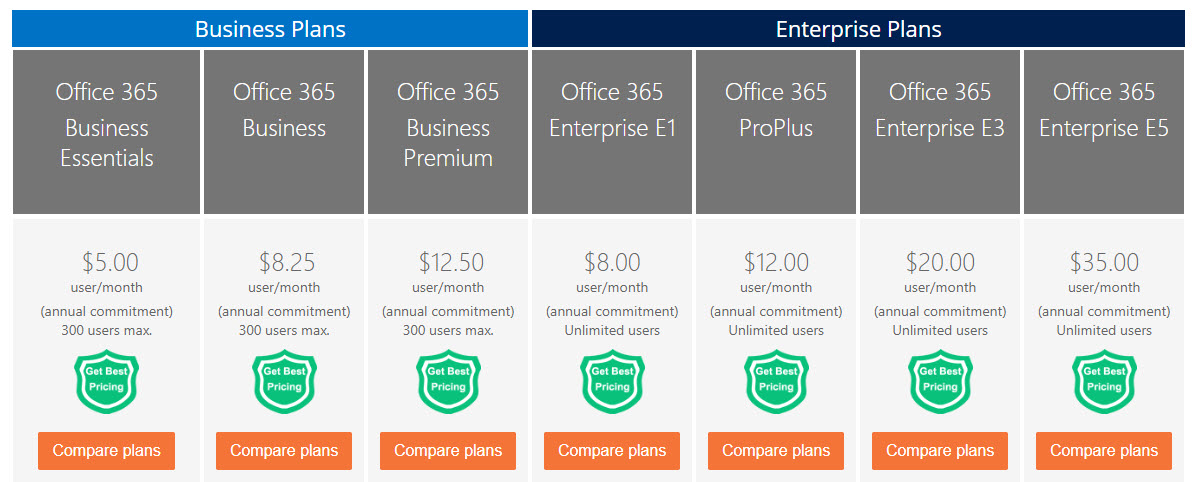
Azure Active Directory 共有四種版本：Free、Office 365 應用程式版本、Premium P1 及 Premium P2。Azure 訂用帳戶即包含免費版。您可以透過 [Microsoft Enterprise 合約](https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise.aspx)、[開放大量授權計劃](https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx)與[雲端方案提供者](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** 與 **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 AAD Premium P1 含以上而Office 需要至 E5 可用此功能。**

前置作業

執行帳戶本身需有全域管理員權限才能執行 AD 使用者與群組功能

Conditional Access Q&A

**明明已經設置原則但均未生效套用至使用者時該如何解決？**

下列其他資訊是選擇性的, 但有助於縮小特定案例的範圍。

* 雲端應用程式或動作
* IP 位址
* Country
* 裝置平台
* 用戶端應用程式 (預覽)
* 裝置狀態 (預覽)
* 登入風險

一張含有 桌 的圖片

自動產生的描述

將套用原則

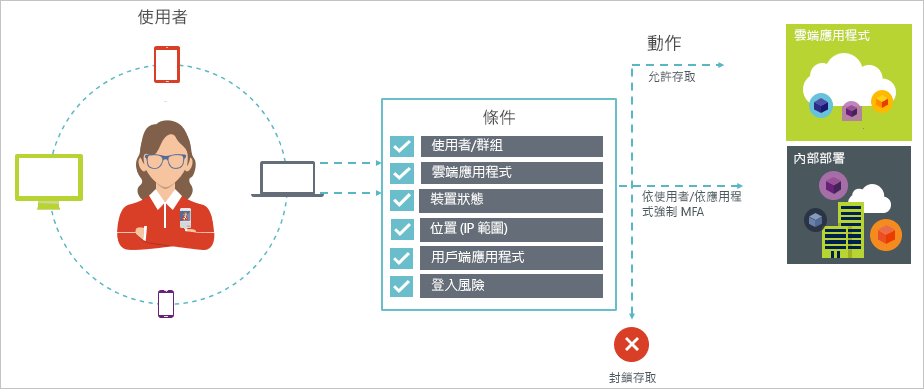
上述清單會顯示條件下的存取原則。同時含蓋適用的授權和Session控制。如：需要多重要素驗證才能存取特定應用程式。

不適用的原則

上述清單會顯示條件下的存取原則。當套用條件會涵蓋任何原則其不適用的原因。如：可從原則中排除使用者與群組。

服務架構

雲端安全性關鍵在於人員，故身分識別和存取在現代化使用資訊行為都透過各種裝置和應用程式、從任何位置環境下都能存取企業組織的重要資源。所以只將重點放在誰能存取或誰不能存，已經無法在足夠掌握其安全。 為了掌控安全與商務生產力間的平衡，在進行存取控制決策時，也須考量資源存取因素。



簡易實測環境

圖1. 在Azure AD 找到條件式存取



圖2. 預設的原則如下包含有對管理者或使用者帳戶個別做MFA強制保護等.一張含有 文字 的圖片

自動產生的描述

圖3. 以下是針對管理者有哪些權限類型都會被一次強制套用的範圍清單



圖4. 本次是透過自訂原則來示範，先從要對何人(用戶或群組均可)我選擇指定的群組

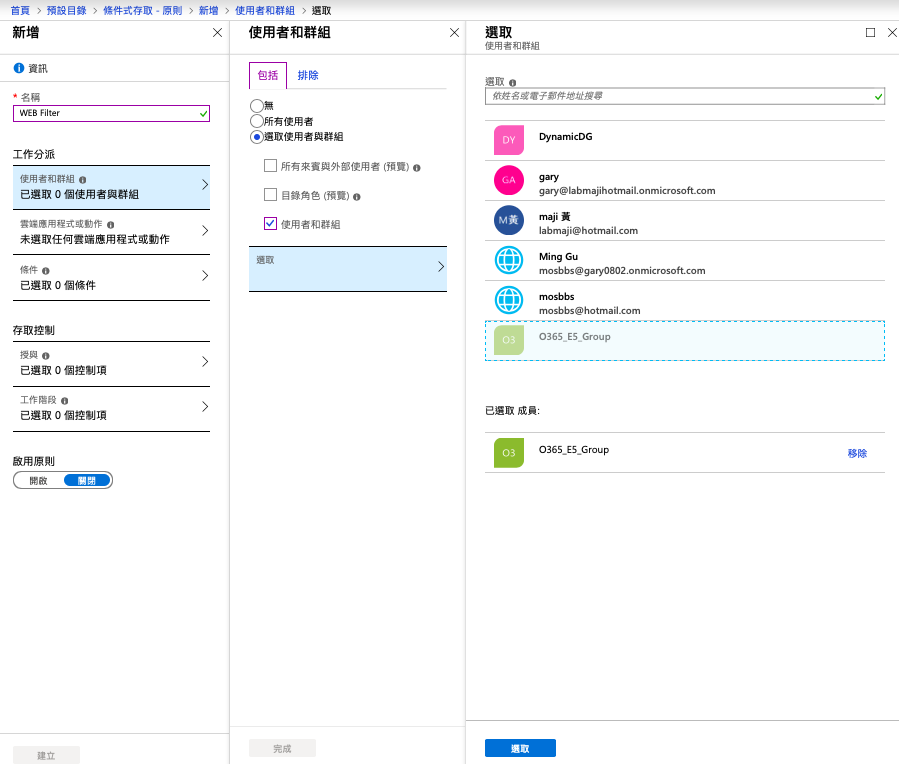


圖5. 裡面排除掉某帳戶不在此限制

一張含有 文字 的圖片

自動產生的描述

圖6. 接下來就是對什麼雲端應用程式，我指定透過Application Proxy來發佈的網站



圖7. 選擇風險性類型

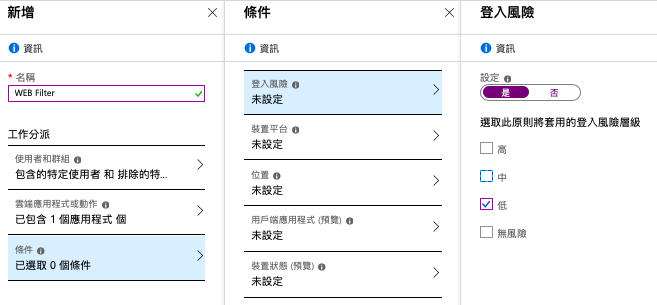


圖8. 指定的平台才允許登入存取應用程式

一張含有 文字 的圖片

自動產生的描述

圖9. 強制授權下的執行原則



圖10. 都完成後就啟用原則

一張含有 桌 的圖片

自動產生的描述

圖11. 補充一下地區的部份會需要事先設置信任的IP或是可指定哪些國家地區

一張含有 文字 的圖片

自動產生的描述

圖12. 舉例信任台灣地區才允許連線

一張含有 文字 的圖片

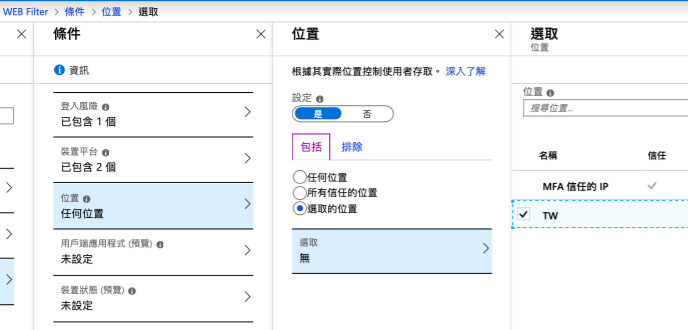
自動產生的描述

圖13. 信任地區設置完成

一張含有 文字 的圖片

自動產生的描述

圖14. 再回到剛剛的條件存取原則在位置地方指定僅允許台灣



上述就是標準的條件存取設置的步驟示範(大家可以再自行測試練習)