

Microsoft Azure Active Directory Premium

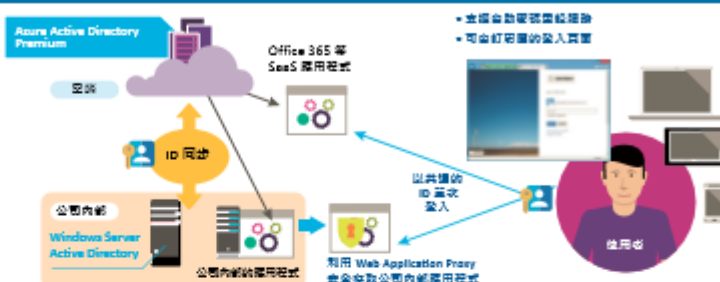


透過混合 IP 管理，提高使用者的便利性與管理性

通過 Azure Active Directory Premium，您將使用以單點登入方式連接公司內部網絡上的應用程序，以確保應用程序的兼容性，同時將全公司內部網絡的 ID 以透明方式編譯。

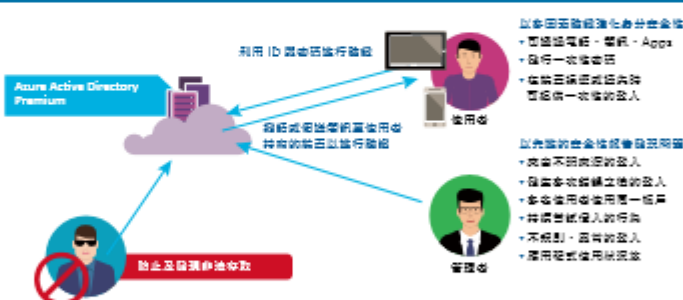
可輕易且安全公開公司內部的各種 Web 應用程式

Azure Active Directory Premium 與公司內部的 Active Directory 之整合可進行 ID 同步、藉由 ID 整合，只需單一登入即可使用 Office 365 或其他 SaaS 在應用程式以及公司內部在應用程式、提升使用者生產力、另外，這種整合的雲端服務，還能更有效地加強、減少更新這些雲端服務的複雜與手續。此外，利用可輕鬆且在全公司公司內部在應用程式的 Web Application Proxy，也能夠有效配置管理 DMZ 上，即可強化使用 on-premises 的安全性。



以強大的認證功能與先進的安全性報告防止非法存取

利用 Azure Active Directory Premium 的密鑑式驗證。除了基本的 ID 與密碼驗證之外，可追加驗證或智慧卡認證。使用者持智慧卡認證方式，藉由磁化存取設備與資料與儲存在雲端式的驗證，可防止非法存取而造成的資訊外洩。另外，亦可藉由安全報告，可供從遠端來不來來回的登入或不相關的登入，是異常人等情形，可在發現並發覺該使用者應立即停用其帳號。



利用機器學習發現 ID 風險

利用 Azure Active Directory Premium 的權限管理系統保護您的應用，包括防止其被惡意使用。您可以將權限分配給您的應用，為其提供安全策略。此外，還可防止惡意使用 ID 憑證，以確保您的應用能安全地在您的環境中運行。Azure Active Directory Premium 可導致其他 Microsoft 產品，如 Office 365 及 Microsoft Intune 等，資源。



Azure Active Directory Premium 的主要功能

Azure Active Directory Premium 包含先進的 ID 管理功能，例如，您可以選擇 Plan 2 (P2) 或 Plan 1 (P1) 其中之一。P2 除了可應用 P1 的所有功能之外，還可應用尋找 ID 與金鑰的時候，以及保護密碼、強制密碼以數位式驗證 ID 與除應用密碼金鑰的認證。

功能描述	狀態
雲端網路存取	已啟用
應用程式存取權	○
針對 SaaS 應用程式存取權的 SSO	僅可登入雲端存取
雲端可移工具	○
多因素認證	○
Web Application Proxy	○
雲端存取	雲端存取、雲端存取、雲端存取
雲端登入憑證管理	○
安全保護	雲端/網路的保護
雲端格式應用程序保護	○
雲端管理設備 (GDM)	○
Microsoft Identity Manager 應用程式 C&L	○
本地 ID、向雲端管理設備	○ (選擇 P2)
向雲端管理設備 ID 管理	○ (選擇 P2)
Cloud App Discovery	○
Microsoft 365 雲端管理工具、雲端管理工具	○