OneLogin Single Sign-On (SSO)

一鍵式安全地存取您的所有應用程式

企業組織希望能快速且安全地提供使用者存取權限，以存取他們被公司批准使用的應用程式，並確保由正確的人員 (如：全職員工、兼職員工、承包商等) 存取其被授權的公司資訊。實際上，企業組織和終端使用者都希望能減少或取消密碼的使用，當以員工生產力和使用者體驗為優先考量時，對公司應用程式的單一登入 (SSO) 就尤為關鍵。

OneLogin's Single Sign-On (SSO)

有了 OneLogin Single Sign-On (SSO) 的單一登入平台，使用者只需輸入一組憑證，即可透過桌上型電腦、智慧型手機和平板電腦，安全地存取雲端和防火牆後的 Web 應用程式。此種作法大大提高了工作效率，同時確保了資料安全。

ONELOGIN'S SINGLE SIGN-ON 主要優勢

安全地存取

OneLogin 由政策驅動的密碼安全性和多重身分驗證 (MFA) 原則，可確保只有被授權的使用者才能存取敏感資料。您還可以實施更嚴格的密碼策略，例如：密碼長度、複雜性和重複使用的限制，以及逾時和密碼重設自助服務策略，在不影響使用者的體驗下強化保護力。

重複登入

使用 OneLogin Single Sign-On，在一個應用程式登入多個帳號。假設您擁有五個 WordPress 網站或兩個 G-Suite 帳號，OneLogin 可透過一個密碼一次性完成登入，並存取應用程式。如果您有不同的測試或生產環境，重複登入功能可幫助節省時間。

減少 IT 成本

OneLogin Single Sign-On 可以節省密碼重置時間，有助於減少 IT 成本。當每位員工都被要求在每個應用程式使用不同的使用者名稱和密碼時，員工忘記密碼的可能性就會很高，這也意味著 IT 人員收到密碼重設的需求會堆積如山。透過 OneLogin Single Sign-On，使用者只需要記住一組憑證，如此可大幅減少要求密碼重置的需求，並提供使用者自行重設密碼的功能，減少 IT 人員的負擔。

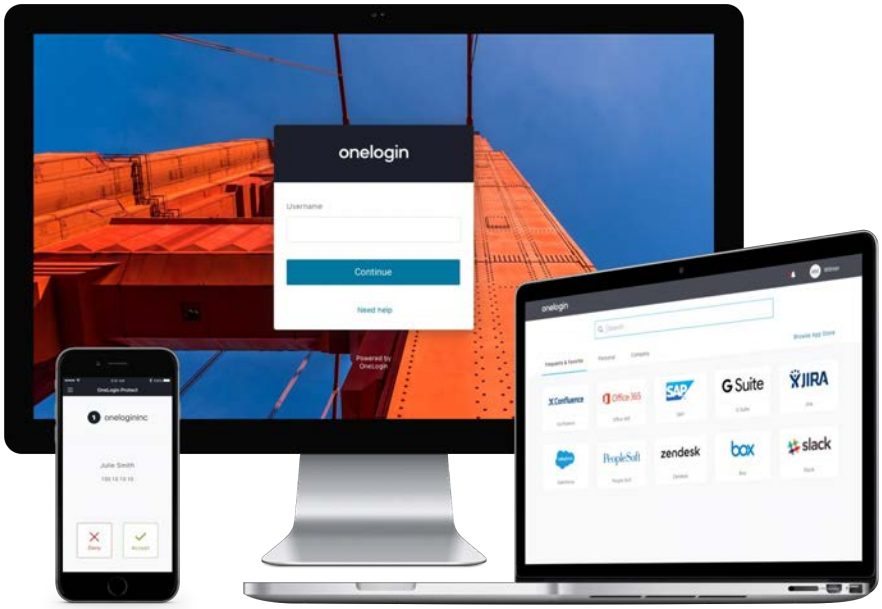
無縫使用者體驗

終端使用者可以一鍵快速地存取被核准的企業應用程式，消除了最終用戶管理、紀錄和重設多個密碼的不便。借助 OneLogin 單一登入，不論使用者是透過桌上型電腦或是行動裝置，都能以相同的方式存取應用程式。

"事實證明，OneLogin 提供的單一登入服務對於向整個組織實施新應用程式至關重要。
不僅幫助我們簡化了快速發展的應用程式，借助 OneLogin，未來我們可以很有信心的擴展並整合更多軟體。"

MIKE LYNCH | Berwin Leighton Paisner IT 總監

Secure Single Sign-On



ONELOGIN'S SINGLE SIGN-ON 主要功能如下:

基於標準的聯合協議	OneLogin 使用 SAML、WS-Federation、OpenID Connect 和 Web 服務與雲端和本機應用程式整合，提供任何裝置簡單、快速的單一登入。
Windows 網域驗證	OneLogin 的 Windows 網域驗證使用整合式 Windows 驗證 (IWA)，在使用者登入他們的 Active Directory 網域時，可自動登入 OneLogin。您可以指定一個特定的 IP 位址範圍，使用者從此範圍透過 OneLogin 自動化進行身分驗證。
高可用性的安全基礎設施	所有 OneLogin 的構件以高可用性被安全地儲存，並在每一層 (DNS、資料中心、應用程式伺服器和資料庫伺服器) 使用內建冗餘。同時於北美和歐洲建立資料冗餘，即時同步首要資料中心和次要資料中心，以實現完整的故障轉移。
密碼金庫	OneLogin 為不支援與密碼庫聯合的 Web 應用程式安全的解決方案，如此一來，組織就能夠為最終用戶提供所有 Web 應用程式的單一登入。 密碼金庫使用先進的加密標準，透過強大的對稱加密演算法安全地儲存密碼。
社群登入	社群身分驗證提供最終用戶使用來自社群身分供應商的憑證登入 OneLogin，包括 Facebook、Linkedin 和 Twitter 等。使用者不需要建立 OneLogin 密碼也可以存取 OneLogin 單一登入網站中的所有應用程式，讓 OneLogin 管理員可以輕鬆實現社群登入。
應用程式目錄	OneLogin 已整合了數千個網路應用程式，並且每天都會持續更新加入新的應用程式。這讓組織可以更輕鬆地快速搜尋、新增並向最終用戶配置其公司核准的應用程式。

更多詳細資訊請參考 OneLogin Single Sign-On https://www.onelogin.com/product/sso.