

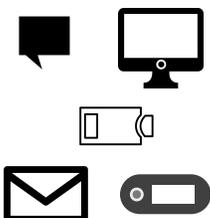


## SafeNet Authentication Manager

### SafeNet 認證管理系統

#### 優勢

- **安全登入延伸至雲端**  
安全登入、單點登入和自動設定使用者的Office 365和SaaS應用程序。
- **安全登入延伸至行動裝置**  
提供iOS設備使用憑證設定和認證管理的功能,可以確保只有受信任設備的員工可以使用企業資源。
- **使用context-based的身份驗證精確控制授權狀況**  
可設定策略規則提供細微的控制級別的身份驗證,用於使用者每次登錄的時候。
- **多樣認證方式**  
架構上可以使用多種認證方式,包括OTP和CBA的解決方案,以及先進的安全應用。
- **降低技術人員成本**  
自動化流程、網路啟動、軟體權杖安裝和直覺化自助服務工具,以方便為終端使用者,企業可以用較低的技術支援成本來維護。



#### 提供您不斷變化的身份認證需求

SafeNet Authentication Manager (簡稱SAM)是企業用全面性認證服務器系統,可以提供企業多樣化身份驗證策略,確保使用者可以安全地使用本地端和遠端登入眾多的企業資源。

提供OTP和USB 解決方案,提供context-based和Step-up認證方式,SAM使企業能夠解決他們當前安全登入。

#### 可整合於廣泛應用的雲端服務

隨著企業開始轉移到至雲端計算環境和SaaS應用,面臨著確保核心應用和高度保密的資源不再存留在企業網絡內部的挑戰,需要重新思考安全和便利的問題。

SAM解決了這方面的難題,提供使用者無縫操作體驗。一致性的強化認證,使用者可以安全登入雲端服務,如Office 365、GoogleApps和[SalesForce.com](https://www.salesforce.com)。

#### 行動裝置專用強化認證和憑證管理

員工越來越多地使用自有設備來登入企業敏感資料和客戶資料。IT部門正在努力實施安全策略在員工自有的設備上,而沒有加強防護的企業在資料洩露和未授權訪問的狀況上,有著嚴重的安全漏洞。

通過提供憑證管理工具和OTA無線憑證傳遞技術來管理行動裝置,SAM可以提供身份驗證使用者,讓他們通過信任的行動裝置可以登入企業資源和應用程式。

#### 一個人 多樣認證方式

您可以同時使用簡訊發送、手機Apps產生二次驗證,或是使用實體裝置和PC軟體來產生二次驗證,且只收您一次的費用<sup>註1</sup>。

註1:簡訊會產生電信和其他服務費用



THE  
DATA  
PROTECTION  
COMPANY

**PRONEW**  
TECHNOLOGIES  
正新電腦有限公司

台灣區代理商  
04-24738309

[www.pronew.com.tw](http://www.pronew.com.tw)

## 相容USB 和 OTP

eToken 3000



eToken 3500



eToken 7000



eToken 5100/5105



eToken 5200



## 多樣化的應用

可以整合在您的VPN系統,或是員工使用的client端應用軟體和內部Web mail。同時支援多樣知名的Web端SaaS的服務。

Logon

VPN

E-Mail

Web

Apps

RDP

## 功能

- 支援 Context-based 認證
- 支援 Step-up 認證
- 支援 Certificate-based, OTP, 軟體和OOB認證
- 支援下列遠端安全登入：
  1. 支援SAML協定的SaaS應用服務
  2. iOS裝置登入網路資源
  3. OWA 和其他 Web-Based 網站
  4. Office 365
  5. VPNs
  6. 虛擬桌面環境
- 區域網路登入
  - 支援離線和連線狀態，用OTP和certificate-based區網登入本地網絡
- 全面管理功能：
  - 分離職責和role-based驗證
  - 跨Domain 管理加上multi-forest AD 支援
  - 支援跨平台自助服務和遠端遙控
  - iOS設備配置和管理憑證
  - 自動化使用者設定的SaaS應用
  - 自助服務窗口，允許使用者自行註冊和Token管理
  - 多樣化報告和偵查追蹤
  - 驗證人轉讓、登記、更新、吊銷、暫時使用和更換
  - 憑證週期管理
  - 臨時Token資源調配
  - 密碼重置或更改



**PRONEX**  
TECHNOLOGIES  
正新電腦有限公司

台灣區代理商  
04-24738309

www.pronex.com.tw