# Symantec Endpoint Protection 14.3 RU10 新功能

**最新更新日期：2025 年 2 月 14 日**

## 防護功能

- 您現在可以在內部部署 Symantec Endpoint Protection Manager 中完全架構和管理自適應防護政策，而不是僅能在雲端中。調適型防護使用豐富的行為分析引擎以及全球威脅遙測和專業知識來保護您的組織免於受到鎖定攻擊。您可以使用「**進階安全性**」頁面上的熱圖來檢視感染狀況行為和相關聯的 MITRE 技術。您接著可以使用自適應防護政策來自動攔截不受信任的行為或手動允許信任的行為。

  透過自適應防護攔截 Living Off the Land (LOTL) 攻擊

- 為了更好地防止攻擊者停止或移除 Symantec Endpoint Protection 用戶端，您需要設定網站層級的預設用戶端密碼。用戶端使用者必須鍵入密碼，才能執行下列工作：

  －使用 smc - stop 命令來停止用戶端服務。

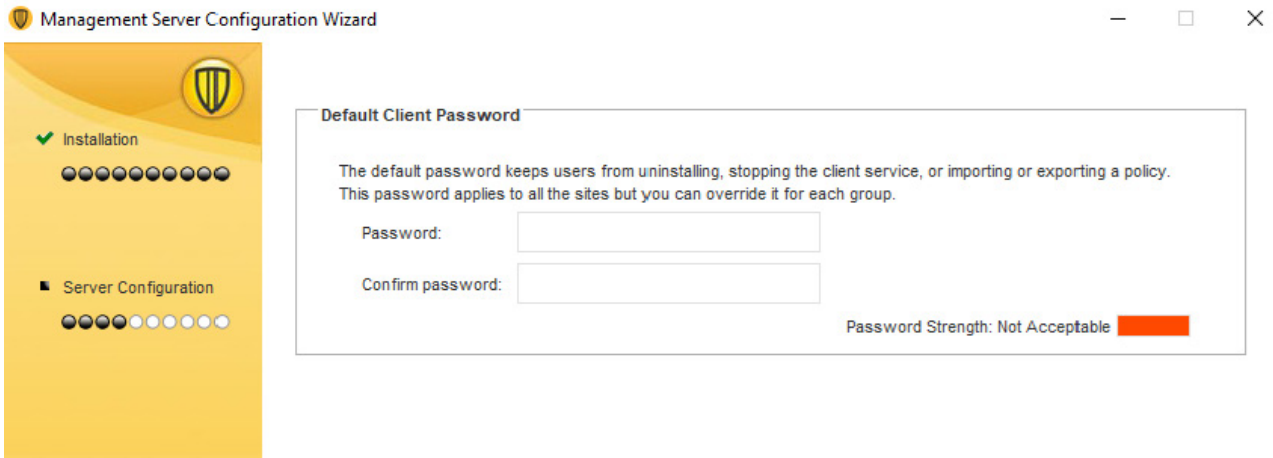
  －手動或使用 CleanWipe 工具來解除安裝用戶端。

  下載 CleanWipe 移除工具來解除安裝 Endpoint Protection

  －匯入或匯出政策。

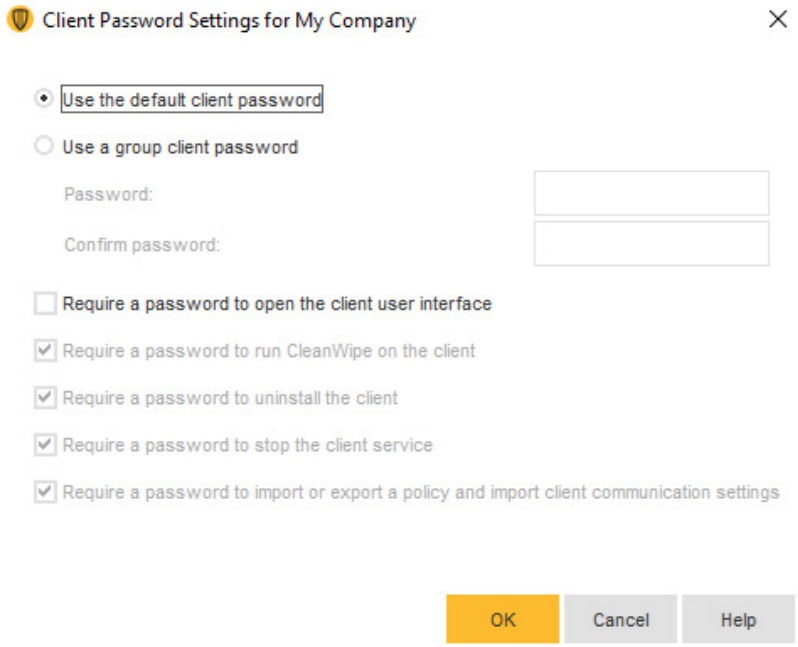
  －使用 Sylink.xml 檔案來匯入用戶端通訊設定檔案。

  您可以在管理伺服器安裝或升級期間設定預設用戶端密碼。




安裝後架構 Symantec Endpoint Protection Manager

- 安裝之後，您可以在群組層級變更密碼。在舊版本中，這些功能是「**用戶端**」>「**政策**」標籤 >「**密碼**」對話方塊中的選用核取方塊。




－為了進一步防止在沒有密碼的情況下無意中修改或解除安裝用戶端，已移除下列選項。

－用戶端部署精靈」中的「**密碼防護**」選項。

存取此選項的方式是按一下「**用戶端**」頁面 >「**安裝用戶端**」>「**通訊更新套件部署**」>「**針對在 Windows 上執行的 Symantec Endpoint Protection 用戶端建立套件**」>「**密碼防護**」選項。

如需在使用通訊檔案匯入用戶端安裝套件時使用密碼的相關資訊，請參閱使用「通訊更新套件部署」還原用戶端伺服器通訊。

－「**管理**」頁面 >「**安裝套件**」>「**用戶端安裝設定**」>「**基本設定**」標籤上的「**移除無法解除安裝的現有 Symantec Endpoint Protection 用戶端軟體**」選項。

如需解除安裝 Symantec Endpoint Protection 用戶端的其他方法的相關資訊，請參閱解除安裝 Symantec Endpoint Protection 用戶端。

• SONAR 日誌已重新命名為「SONAR：行為分析」日誌。

## Symantec Endpoint Protection Manager

• 已新增 Windows Server 2025 的支援。

• 已捨棄 Windows Server 2012 和 Windows Server 2012 R2 的支援。

## 用戶端和平臺更新

- Symantec Endpoint Protection Client for Mac
- Symantec Endpoint Protection Client for Mac 沒有規劃版本。
- Symantec Single Agent for Linux
- Symantec Single Agent for Linux 沒有規劃版本。

## Symantec Endpoint Security 雲端主控台

從雲端主控台管理的用戶端電腦獲得類似的功能和防護。

- 若要進一步瞭解 Symantec Endpoint Security 授權提供的雲端式功能，請參閱：Symantec Endpoint Security 的新功能。
- 若要移轉至雲端主控台，請參閱：移轉至雲端主控台。

最新版本的雲端主控台針對 Symantec Endpoint Protection 用戶端提供下列增強功能：

SymantecAI 聊天機器人具有全新外觀，並針對準確性進行調整。

## 說明文件

新主題包括：

- 如需您必須新增至支援案例的資訊的詳細資訊，請參閱如何提交功能要求或建立支援案例。
- 如需此版本中修正的相關資訊，請參閱 Symantec Endpoint Protection 14.3 RU10 的新修正和元件版本。

若要檢視資料庫綱要，請聯絡技術支援。

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
**(好記：幫您節省時間.的公司.在台灣)**

## 關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。( 美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員 )。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

## 關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。