# Symantec Endpoint Protection 14.3 RU7 新功能

**最新更新日期：2023 年 4 月 15 日**

## 防護功能

- 「**與 Windows Defender 共存**」選項已加回至病毒和間諜軟體防護政策。此選項可確保即使停用 Microsoft Defender，也會執行自動保護。您可以在「**政策**」>「**病毒和間諜軟體防護**」>「**Windows 設定**」>「**其他**」頁面上找到此選項。 Symantec 建議您將已啟用此選項的病毒和間諜軟體防護政策套用至僅執行 14.3 RU7 和更新版本的用戶端電腦。
  如需此選項的詳細資訊，請參閱：其他

## Symantec Endpoint Protection Manager

- 已加強聯邦客戶和某些商業客戶遵從 FIPS 140-2 等級 1。FIPS 140-2 遵從會使用已驗證的程式庫進行用戶端和伺服器端加密。在安裝 Symantec Endpoint Protection Manager 並架構 Microsoft SQL Server 資料庫之後，您可以啟用 FIPS 140-2 模式。
  如需 FIPS 140-2 遵從的相關資訊，請參閱：將 Symantec Endpoint Protection 架構為遵從 FIPS 140-2
- 已加強聯邦組織的智慧卡支援，包括改善了 Thales SafeNet IDPrime 卡的支援。
  請參閱：使用智慧卡架構驗證
- 「**伺服器活動**」日誌現在會顯示通知，以提供 SEPM 和雲端主控台同步狀態。這些通知包括：
  - Symantec Endpoint Protection Manager 無法與雲端同步。
  - Symantec Endpoint Protection Manager 與雲端的同步狀態不明。
  - Symantec Endpoint Protection Manager 未與雲端同步。

  您可以在「**監視器**」頁面 >「**日誌**」標籤 >「**系統**」日誌類型上找到這些通知。
  請參閱：針對混合 Symantec Endpoint Protection Manager、用戶端與雲端主控台之間的通訊問題進行疑難排解
- 「**管理**」日誌現在會顯示您在「**說明**」欄位中重新命名的群組名稱。前往「**監視器**」>「**日誌**」>「**系統**」日誌類型 >「**管理**」。
  請參閱：系統日誌和快速報告
- 升級或新增了以下第三方元件：
  - Apache httpd
  - Apache Tomcat
  - apr
  - apr-util
  - curl
  - JDK (Eclipse Temurin)
  - jQuery UI
  - openssl

- PHP
- protobuf
- zlib

## 用戶端和平臺更新

*適用於 Windows 的 Symantec Endpoint Protection 用戶端*

- 在中文語言的舊版 SEP 用戶端中，風險日誌中的自訂資料夾已出現在具有三個問號的用戶端路徑中，例如 C:\Windows\???。在此版本中，正確的中文字元會出現，例如 C:\Windows\訓練
  請參閱：關於 Symantec Endpoint Protection Manager 日誌的類型
- 內部部署 Windows 用戶端說明在下列位置是線上說明：
  Windows 適用的 Symantec Endpoint Protection 用戶端指南

**附註**

Symantec 會在稍後日期發行 Symantec Endpoint Protection for Mac 用戶端和 Symantec Agent for Linux。

## Symantec Endpoint Security 雲端主控台

從雲端主控台管理的用戶端電腦獲得額外的功能和防護。

- 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。
- 若要移轉到雲端主控台，請參閱：移轉至雲端主控台。

最新版本的雲端主控台為 14.3 RU7 用戶端提供了下列增強功能：

- 支援 Windows ARM 裝置 (完全受雲端管理或不受雲端管理)。
- 調適型防護以及端點偵測和回應 (EDR) 的增強功能。

## 說明文件

Symantec Endpoint Protection Client for Mac 文件現在是 線上 文件，可在 下列位置取得：
Symantec Endpoint Protection Client for Mac 指南

新主題包括：

- 針對混合 SEPM、SEP 用戶端與 ICDm 雲端主控台之間的通訊問題進行疑難排解
- 將 Symantec Endpoint Protection 架構為遵從 FIPS
- 如何提出功能要求。

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)

原廠網址：https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/Whats-new-for-Symantec-Endpoint-Protection-14-3-RU7.html
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/4

## 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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。