

賽門鐵克端點防護 SEP 14.x Windows 相容性列表

Windows desktop versions										
Win 7 Win 8	Win 8.1	Win 10 註1	Win 10 Anniversary 註2	Win 10 Creators, Fall Creators	Win 10 (2018/ 4、10)	Win 10 19H1, 22H2	Win 11 21H2- 22H2	Win 11 23H2	Win 11 24H2 註3	Win 11 25H2
14.3 RU5 ^{註4}										
14.3 RU7										
14.3 RU8 ^{註5}										
14.3 RU9、14.3 RU10										
14.4										

Windows server versions							
Windows Server 2008 R2	Windows Small Business Server 2011	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025
14.3 RU5 ^{註4} 、14.3 RU7							
14.3 RU8 ^{註5}							
14.3 RU9 ^{註6} 、14.3 RU10							
14.4							

註3 = Windows 11 24H2 包含 Windows 11 Enterprise LTSC 2024。

註2 = Windows 10 週年更新 (版本 1607) 包含 Windows 10 Enterprise 2016 LTSC。

註1 = Windows 10 (版本 1507) 包含 Windows 10 Enterprise 2015 LTSC。

註6 = Windows Server 2025 的 14.3 RU9 支援目的在實現與 SEP 用戶端的早期功能相容性。完整支援將於 14.3 RU10 中加入。

註5 = 2023 年 8 月 31 日 - 安裝或升級用戶端前，14.3 RU8 必須已安裝 Microsoft Azure 程式碼簽署 (ACS) 支援。Windows 10 21H2 或更新版本以及 Windows 11 或更新版本會自動安裝 ACS 支援。Windows 8.1/Windows 2012 及更新版本提供 ACS 支援。將 Windows 用戶端電腦升級至 14.3 RU8 及更新版本並啟用 Microsoft Azure 程式碼簽署支援

註4 = 32 位元裝置必須使用 14.3 RU5 用戶端。這是 14.3.x 系列中最後一個支援 32 位元作業系統的版本。更多資訊：[Symantec Endpoint Protection 14.3 RU6 有哪些新功能？](#)

在裝置升級作業系統之前，請先將 Symantec Endpoint Protection 升級至支援該作業系統的版本。若在升級作業系統時保留不支援的 Symantec Endpoint Protection 版本，可能會導致意外結果。

其他資訊

- 有關特定系統需求的詳細資訊，請參閱所有版本的 [Endpoint Protection](#) 之發行說明、新修正項目及系統需求。
- 如何查詢 [Endpoint Protection](#) 的服務終止日期。
- 14.3 RU6 已終止服務。
- 14.3 RU4 及更早版本已終止服務。
- 當在 Server 2025 上安裝 SEP 14.3 RU9 時，會出現一個輕微的文字顯示問題，此問題不會影響用戶端的防護功能。14.3 RU10 已解決此問題。
- 在 SEPM - 首頁 - 檢視詳細資訊 - 端點狀態中，顯示為 Windows Server 2022 標準版，而非 Windows Server 2025 標準版。

◆ SEP14.3RU3/4特別針對加密勒索軟體最棘手的就地取材 (living-off-the land) 攻擊的強化防護技術說明下載

原廠網址：<https://knowledge.broadcom.com/external/article/163625#Win10>

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。2026/4/24



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)



Symantec
A Division of Broadcom

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。



保安資訊
KEEPSAFE
INFORMATION SECURITY

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, 以及基於比原廠更熟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、可以提供良好諮詢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。