Symantec Endpoint Protection (SEP) 14.3 RU9 的系統需求

更新日期：2024 年 7 月 16 日

Symantec Endpoint Protection 軟體和硬體需求

一般而言，以下產品的系統需求與其支援的作業系統之系統需求相同。

附註

早期版本的 Symantec Endpoint Protection Manager 可能無法使用較早版本正確管理用戶端。可能會出現內容更新和用戶端管理的問題。例如：Symantec Endpoint Protection Manager 14.3 RU4 或更早版本無法正確提供版本 14.3 RU5 用戶端及其特定版本的 Moniker。

Symantec Endpoint Protection Manager(SEPM)管理主控台軟體系統需求

元　件	需　　求
作業系統	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (自14.3 RU3開始支援) **附註** 不支援桌面作業系統。 不支援 Windows Server Core 版本。

元　件	需　　求
網頁瀏覽器	下列瀏覽器支援透過 Web 主控台存取 Symantec Endpoint Protection Manager 以及檢視 Symantec Endpoint Protection Manager 說明： • Microsoft Edge Chromium 型瀏覽器 (14.3 及更新版本) • Microsoft Edge • Mozilla Firefox 5.x through 107 • Google Chrome 113 至 115
資料庫	Symantec Endpoint Protection Manager 包括一個預設資料庫： • Microsoft SQL Server Express 2014 • Microsoft SQL Server Express 2017 更新與 Endpoint Protection Manager 一起封裝的 SQL Express 2017 以解決漏洞或缺陷 • Sybase 內嵌資料庫 (僅 SEP 14.3 MP.x 和更舊版本) 您也可以選擇使用下列其中一種 Microsoft SQL Server 版本的資料庫： • SQL Server 2012 RTM - SP4 (14.3 RU5 及更早版本) • SQL Server 2014 RTM - SP3 • SQL Server 2016 SP1、SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 及更新版本) • SQL Server 2022 (14.3 RU6 及更新版本) **附註** 支援 Amazon RDS 上託管的 SQL Server 資料庫(14.0.1 MP2 和更新版本) **附註** 如果 Symantec Endpoint Protection 使用 SQL Server 資料庫並且您的環境僅使用 TLS 1.2，請確保 SQL Server 支援 TLS 1.2。您可能需要修正 SQL Server。此建議適用於 SQL Server 2008、2012 和 2014。請參閱： Microsoft SQL Server 支援 TLS 1.2
其他環境需求	• 在純 IPv6 網路中，仍須安裝 IPv4 堆疊，但須將其停用。如果移除 IPv4 堆疊，Symantec Endpoint Protection Manager 則無法運作。 • Microsoft Visual C++ 2017 可轉散發套件 (x64／x86) **附註** 請注意，在安裝 Symantec Endpoint Protection Manager 期間會自動安裝所需的 Visual C++ 版本。

Symantec Endpoint Protection Manager(SEPM) 管理主控台硬體系統需求

元　件	需　　求
處理器	至少 Intel Pentium Dual-Core 或效能相當的處理器，建議使用 8 核心或更多核心 **附註** 不支援 Intel Itanium IA-64 處理器。
實體 RAM	至少 2 GB 可用 RAM；建議 8 GB 或更高可用 RAM **附註** 您的 Symantec Endpoint Protection Manager 伺服器可能需求額外的 RAM，視已安裝其他應用程式的 RAM 需求而定。例如：如果 Symantec Endpoint Protection Manager 伺服器上安裝有 Microsoft SQL Server，伺服器至少應該有 8 GB 可用 RAM。
顯示	1024 x 768 或更大
硬碟機 (安裝到系統磁碟機時)	搭配本機 SQL Server 資料庫： • 至少 40 GB (建議使用 200 GB) 可用於管理伺服器和資料庫 搭配遠端 SQL Server 資料庫： • 至少 40 GB (建議使用 100 GB) 可用於管理伺服器 • 遠端伺服器上可用於資料庫的額外磁碟空間
硬碟機 (安裝到替代磁碟機時)	搭配本機 SQL Server 資料庫： • 系統磁碟機需要至少 15 GB 的可用空間 (建議使用 100 GB) • 安裝磁碟機需要至少 25 GB 的可用空間 (建議使用 100 GB) 搭配遠端 SQL Server 資料庫： • 系統磁碟機需要至少 15 GB 的可用空間 (建議使用 100 GB) • 安裝磁碟機需要至少 25 GB 的可用空間 (建議使用 100 GB) • 遠端伺服器上可用於資料庫的額外磁碟空間
其他	已啟用的網路介面卡

如果使用 SQL Server 資料庫，可能需要更多可用磁碟空間。額外空間的數量和位置視 SQL Server 使用的磁碟機、資料庫維護需求和其他資料庫設定而定。

適用於 Windows 的 Symantec Endpoint Protection 用戶端軟體系統需求

元　件	需　　求
作業系統 (桌面)	如需目前版本和舊版支援的作業系統清單，請參閱： Windows 與 Endpoint Protection 用戶端的相容性 • 從 14.3 RU8 開始，您必須在用戶端上安裝 Microsoft Azure Code Signing (ACS) 支援。Microsoft ACS 支援僅適用於 Windows 8.1 和更新版本。 以 Microsoft Azure Code Signing (ACS) 支援升級 Windows 用戶端電腦 14.3 RU8 及更新版本 • 14.3 RU6 和更新版本不再支援執行 Microsoft Windows 32 位元作業系統的電腦。32 位元的電腦應執行 14.3 RU5 客戶端。
作業系統 (伺服器)	如需目前版本和舊版支援的作業系統清單，請參閱： Windows 與 Endpoint Protection 用戶端的相容性 如要在 Windows 7、Windows Server 2008 或 Windows Server 2008 R2 上接收最新的 SONAR、CIDS 或 ERASER 內容，請參閱： Windows 7、Windows Server 2008 和 2008 R2 的 SONAR 12.3.0、CIDS 17.2.6 和 ERASER 119.1.3 作業系統需求
瀏覽器入侵預防	瀏覽器入侵預防支援以用戶端入侵偵測系統 (CIDS) 引擎版本為基礎。 請參閱：Endpoint Protection 中瀏覽器入侵預防支援的瀏覽器

適用於 Windows 的 Symantec Endpoint Protection 用戶端硬體系統需求

元　件	需　　求
處理器 (適用於實體電腦)	64 位元處理器：最少包含 x86-64 支援的 2 GHz Pentium 4 或效能相當的處理器 **附註** 不支援 Itanium 處理器。
處理器 (適用於虛擬電腦)	一個虛擬通訊端和每個通訊端一個核心，至少 1 GHz (一個虛擬通訊端和每個通訊端兩個核心，建議為 2 GHz) **附註** 必須啟用 Hypervisor 資源保留。
實體 RAM	1 GB 或以上 (視作業系統需求而定，建議使用 2 GB)
顯示	800 x 600 或更大

元　件	需　　求
硬碟機	磁碟空間需求視您安裝的用戶端類型、要安裝到哪個磁碟機，以及程式資料檔案所在的位置而定。程式資料資料夾通常位於系統磁碟機的預設位置 C:\ProgramData 中。 不管您選擇哪個安裝磁碟機，系統磁碟機上都必須始終有可用磁碟空間。 **附註** 可用空間的需求依 NTFS 檔案系統而定。此外，還需要可用於內容更新和日誌的額外空間。

安裝到系統磁碟機時，適用於 Windows 的 Symantec Endpoint Protection 用戶端可用的硬碟機系統需求

元　件	需　　求
標準	當程式資料資料夾位於系統磁碟機時： • 395 MB* 當程式資料資料夾位於替代磁碟機時： • 系統磁碟機：180 MB • 替代安裝磁碟機：350 MB
Embedded/VDI	當程式資料資料夾位於系統磁碟機時： • 245 MB* 當程式資料資料夾位於替代磁碟機時： • 系統磁碟機：180 MB • 替代安裝磁碟機：200 MB
暗網	當程式資料資料夾位於系統磁碟機時： • 545 MB* 當程式資料資料夾位於替代磁碟機時： • 系統磁碟機：180 MB • 替代安裝磁碟機：500 MB

* 安裝期間需要額外的 135 MB 可用空間。

安裝到替代磁碟機時，適用於 Windows 的 Symantec Endpoint Protection 用戶端可用的硬碟機系統需求

元　件	需　　求
標準	當程式資料資料夾位於系統磁碟機時： • 系統磁碟機：380 MB • 替代安裝磁碟機：15 MB* 當程式資料資料夾位於替代磁碟機時：** • 系統磁碟機：30 MB • 程式資料磁碟機：350 MB • 替代安裝磁碟機：150 MB
Embedded／VDI	當程式資料資料夾位於系統磁碟機時： • 系統磁碟機：230 MB • 替代安裝磁碟機：15 MB* 當程式資料資料夾位於替代磁碟機時：** • 系統磁碟機：30 MB • 程式資料磁碟機：200 MB • 替代安裝磁碟機：150 MB
暗網	當程式資料資料夾位於系統磁碟機時： • 系統磁碟機：530 MB • 替代安裝磁碟機：15 MB* 當程式資料資料夾位於替代磁碟機時：** • 系統磁碟機：30 MB • 程式資料磁碟機：500 MB • 替代安裝磁碟機：150 MB

* 安裝期間需要額外的 135 MB 可用空間。

** 如果程式資料資料夾與替代安裝磁碟機相同，請向程式資料磁碟機新增總計 15 MB 可用空間以供您使用。但在安裝期間，安裝程式仍需要替代安裝磁碟機上有完整的 150 MB 可用空間。

Windows Embedded 適用的 Symantec Endpoint Protection 用戶端系統需求

元　件	需　　求
處理器	1 GHz Intel Pentium
實體 RAM	256 MB **附註** 此圖適用於安裝 Symantec Endpoint Protection 內嵌式用戶端。如果您也從整合的解決方案實作其他功能，例如：EDR 則需要額外的實體 RAM。
硬碟機	Symantec Endpoint Protection Embedded/VDI 用戶端需下列可用硬碟空間： • 安裝到系統磁碟機：245 MB • 安裝到替代磁碟機：系統磁碟機上為 230 MB，替代磁碟機上為 15 MB 安裝期間需要額外的 135 MB 可用空間。 這些圖假設程式資料資料夾位於系統磁碟機上。如需更多詳細資訊或其他用戶端類型的需求，請參閱適用於 Windows 的 Symantec Endpoint Protection 用戶端系統需求。
內嵌作業系統	14.3 RU7 及更早版本： • Windows Embedded Standard 7 (64 位元) • Windows Embedded POSReady 7 (64 位元) • Windows Embedded Enterprise 7 (64 位元) • Windows Embedded Standard 8 (64 位元) • Windows Embedded 8.1 Industry Pro (64 位元) • Windows Embedded 8.1 Industry Enterprise (64 位元) • Windows Embedded 8.1 Pro (64 位元) 從 14.3 RU8 開始，您必須在用戶端上安裝 Microsoft Azure Code Signing (ACS) 支援，其不可用於 Windows Embedded。
所需的最少元件	• Filter Manager (FltMgr.sys) • 效能資料協助程式 (pdh.dll) • Windows Installer 服務
範本	• 應用程式相容性 (預設值) • 數位告示板 • 工業自動化 • IE、媒體播放器、RDP • 機上盒 • 精簡型用戶端 不支援最低架構範本。 不支援加強型寫入過濾器 (EWF) 和統一寫入過濾器 (UWF)。建議寫入過濾器是隨登錄過濾器一起安裝的檔案型寫入過濾器 (FBWF)。

Mac 適用的 Symantec Endpoint Protection 用戶端系統需求

元　件	需　　求
處理器	• 64 位元 Intel Core 2 Duo 或更新版本 • Apple M1晶片(自 SEP 14.3 RU2 起) • Apple M2 晶片 (自 14.3 RU5 起)
實體 RAM	2 GB RAM
硬碟機	1 GB 可用硬碟空間以供安裝 不支援在區分大小寫的檔案系統上執行 Symantec Endpoint Protection 安裝程式。
顯示	800 x 600
作業系統	如需目前版本和舊版支援的作業系統清單，請參閱：Endpoint Protection 的 MacOS 和 OSX 相容性。
網際網路連線	需要存取網際網路主機。請參閱： 在企業網路上使用 Apple 產品

Linux 的 Symantec Endpoint Protection 用戶端系統需求

元　件	需　　求
硬體	• 實體：Intel Pentium 4 (2 GHz) 或至少等同於 2 核心 (建議為 4 核心) • 虛擬：一個至少具有 2 核心的虛擬通訊端 (建議為 4 核心) • RAM：至少 512MB 的可用 RAM (建議為 4GB) • 如果 /var、/opt 和 /tmp 共用相同的檔案系統/磁碟區，則有 2 GB 可用磁碟空間 • 如果是不同的磁碟區，則每個 /var、/opt 和 /tmp 中有 1 GB 可用磁碟空間 **附註** 若啟用任何 Symantec Endpoint Detection and Response 功能，建議在 /opt 中額外增加 5 GB 磁碟空間。
作業系統	支援的作業系統： • Amazon Linux 2023 • Amazon Linux 2 • CentOS 6、7、8* 自 SEP 14.3 RU7 起不再支援 CentOS 串流 • Debian 9、10 (14.3 RU2 和更新版本) • Oracle Enterprise Linux 6、7、8* • Rocky Linux 8、9 • Red Hat Enterprise Linux 6、7、8*、9 雙受管單一代理程式 (例如：DCS 和 SEP Linux) 不支援 Linux 6.x。在 RHEL 6.x 上，支援獨立式 SEP Linux 代理程式 (SEPM 受管或 Cloud 受管)

元　件	需　　求
	• SuSE Linux Enterprise Server 12.x、15.x • Ubuntu 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS(14.3 RU6 和更新版本) * 如果您正在使用 DCS 代理程式執行以雙受管模式啟用 FIPS 模式的 RHEL/OEL/CentOS 8.x，則代理程式無法與 DCS 伺服器通訊。當您停用 FIPS 並重新啟動系統時，會還原通訊。 如需詳細資訊以及所支援次要 Linux OS 版本的清單，請參閱： 支援的 Symantec Linux Agent 核心
作業系統	14.3 MP1 版及更舊版本支援的作業系統： • Amazon Linux 和 Linux 2 • CentOS 6U3 - 6U9、7 - 7U7、8；32 位元和 64 位元 • Debian 6.0.5 Squeeze、Debian 8 Jessie；32 位元和 64 位元 • Fedora 16、17；32 位元和 64 位元 • Oracle Linux (OEL) 6U2、6U4、6U5、6U8、7、7U1、7U2、7U3、7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9、7 - 7U8、8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4，32 位元和 64 位元；12、12 SP1、12 SP3，64 位元 • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4，32 位元和 64 位元；12 SP3，64 位元 • Ubuntu 12.04、14.04、16.04、18.04 (自 14.3 版起)；32 位元和 64 位元 如需受支援的先前版本作業系統核心清單，請參閱 Linux 派送及核心的清單，以及適用於 Symantec Endpoint Protection for Linux 14.x 之預先編譯的自動防護驅動程式／模組
相依性	您必須在建立安裝套件的電腦上安裝下列相依套件清單。這些套件和程式庫會由安裝程序特別檢查。 核心系統套件： • ccheckpolicy：SELinux 政策編譯器。 • policycoreutils-python：SELinux 政策核心 Python 公用程式。 • upstart：事件驅動的初始化系統。 • bash：GNU Bourne Again Shell (bash)。 • dmidecode：擷取 SMBIOS/DMI 表格資訊。 • sed：GNU 串流文字編輯器。 • gzip：GNU 資料壓縮程式。 • tar：GNU 檔案封存程式。 • gawk：GNU 版本的 awk 文字處理公用程式。 • grep：GNU 版本的 grep 型樣比對公用程式。 • findutils：GNU 版本的 find 公用程式 (find 和 xargs)。 • coreutils：GNU 核心公用程式 - 一組常用公用程式應用程式。 • module-init-tools：核心模組管理公用程式。 • util-linux-ng：基本系統公用程式集合。

元　件	需　　求
相依性	• filesystem：Linux 系統的基本目錄配置。 • shadow-utils：管理帳戶和陰影密碼檔案的公用程式。 • zip：與 PKZIP 相容的檔案壓縮和封裝公用程式。 相依程式庫： • aauditd：稽核精靈會產生日誌項目來記錄資訊。 • openssl：OpenSSL 工具組 (x86_64)。(從 14.3 RU4 開始不再需要) • glibc：GNU libc 程式庫 (x86_64)。 • libstdc++：GNU 標準 C++ 程式庫第 4 版 (x86_64)。 • libgcc：GCC 版本 4.0 共用支援程式庫 (x86_64)。 • pam：PAM 驗證程式庫 (64 位元 libpam.so)。 • zlib：Massively Spiffy Yet Delicately Unobtrusive Compression Library (x86_64)。 • libacl：管理存取控制清單的公用程式 (x86_64)。 • at：工作多工緩衝處理工具。 • libelf：用於建立自訂工具的程式庫，以操作 ELF 程式庫和共用程式庫。 • libdw1：提供對於儲存在 ELF 檔案內 DWARF 除錯資訊之存取權的程式庫。
圖形桌面環境	您可使用下列圖形桌面環境檢視 Symantec Endpoint Protection for Linux 用戶端： • KDE • Gnome • Unity **附註** Symantec Agent for Linux 14.3 RU1 沒有圖形化使用者介面。
舊版環境需求	14.3 RU1 到 14.3 RU3： • OpenSSL 1.0.2k-fips 或更新版本 14.3 MP1 和更舊版本： • Glibc 不支援執行 glibc 2.6 之前版本的任何作業系統。 • net-tools 或 iproute2 Symantec Endpoint Protection 會使用這兩個工具之一，視電腦上安裝了哪個工具而定。 • 開發人員工具 自動防護核心模組的自動編譯和手動編譯程序需要您安裝某些開發人員工具。這些開發人員工具包含 gcc 以及核心來源和標頭檔案。如需有關需安裝項目以及如何針對特定 Linux 版本安裝這些項目的詳細資訊，請參閱： 手動編譯 Endpoint Protection for Linux 的自動防護核心模組 • 64 位元電腦上的 i686 型相依套件 Linux 用戶端中的很多執行檔都是 32 位元程式。對於 64 位元電腦，您必須先安裝 i686 型相依套件，再安裝 Linux 用戶端。

元　件	需　　求
舊版環境需求	如果您尚未安裝 i686 型相依套件，則可透過指令行安裝這些套件。此安裝需要進階使用者權限，即以下指令示範中帶有 sudo 的指令： －針對 Red Hat 型散佈： sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686 －針對 Debian 型散佈：sudo apt-get install ia32-libs －針對以 Ubuntu 為基礎的派送： sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386

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好用資源。

保安資訊連絡電話：**0800-381-500**。

賽門鐵克端點防護(SEP14x)-各版本說明-新增功能-修復疑問-核心版次對照表

原廠網址：https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/system-requirements-for-v53308029-d69e1453.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。2024/07