Symantec™ Endpoint Protection 14.3 版本說明

上次更新時間：**2020** 年 **6** 月

Table of Contents

版權聲明

Symantec Endpoint Protection 14.3 的新功能

本節描述 14.3 版本中的新功能。

防護功能

- 第三方應用程式開發人員可以保護其客戶免受動態程序檔式的惡意軟體和非傳統網路攻擊途徑的影響。第三方應用程式呼叫 Windows AMSI 介面請求掃描使用者提供的程序檔，該程序檔路由到 Symantec Endpoint Protection 用戶端。 用戶端以一個判斷來回應，以指示程序檔行為是否為惡意。 如果行為不是惡意的，則程序檔執行將繼續。 如果程序檔的行為是惡意的，則應用程式不會運行它。在用戶端上，「偵測結果」對話方塊顯示狀態為「拒絕存取」。第三方程序檔的範例包括 Windows PowerShell、JavaScript 和 VBScript。 必須啟用「自動防護」。 此功能適用于 Windows 10 和更新版本的電腦。
  反惡意軟體掃描介面 (AMSI) 如何幫助您抵禦惡意軟體
  防惡意軟體掃描介面 (AMSI)

Symantec Endpoint Protection Manager

- Symantec Endpoint Protection 遠端主控台現在支援 JAVA 11 而非 JAVA 8。若要存取遠端主控台，請開啟受支援的網頁瀏覽器，然後在位址方塊中輸入下列位址：`#HTTP://SEPMServer:9090/symantec.html`，並下載新的遠端主控台套件。 遵照提及的指示進行。 不再支援 Symantec Endpoint Protection Manager 遠端主控台的早期版本。
  登入 Symantec Endpoint Protection
- 您可以將網站上的 Symantec Endpoint Protection Manager 之一配置為主要日誌伺服器，以將日誌轉送到系統日誌伺服器。 如果主要日誌伺服器離線，則第二個管理伺服器將接管日誌並轉送到系統日誌伺服器。 當主要日誌伺服器重新連線時，將恢復轉送日誌。
  為外部日誌記錄配置容錯移轉伺服器
- 集成政策有一個 WSS 流量重新導向的新選項，啟用**LPS**自訂**PAC**檔。此選項允許您將用戶端上的 LPS 伺服器託管的預設 PAC 檔替換為自訂 PAC 檔。 自訂 PAC 檔解決了與第三方應用程式的相容性問題，這些應用程式不能用於在回送配接卡上接聽的本地代理伺服器。
  架構 WSS 流量重新導向
- 支援 Microsoft SQL Server 2019 資料庫。
- 防病毒掃描程序現在使用獨立于主要非安全性服務的服務。 這種新的掃描過程帶來了更高效的記憶體使用、持續防護，並減少對主要服務問題的依賴性。
- 資料庫架構包括新欄，作為未來版本功能的一部分。
  (AGENT_SECURITY_LOG_1、AGENT_SECURITY_LOG_2、SEM_AGENT 表)
- 其餘 API 在 /sepm/api/v1/電腦 API 回應 JSON 中具有以下欄位，用於呼叫和下載電腦狀態報告：quarantineStatus、quarantineCode、wsStatus、pskVersion。
- 將以下元件升級到較新版本：Apache Tomcat、Boost C++ Libraries、CURL、Jackson-core、Jackson-databind、Jakarta Activation、Java、logback、用於 SQL Server 的 Microsoft JDBC 驅動程式、OpenSC、OpenSSL、Spring Security、Spring-framework、sqlite。
- 若要在雲端主控台中註冊 Symantec Endpoint Protection Manager 網域，必須首先通過 Symantec Endpoint Security 主控台獲取註冊 Token。 在這之前，按一下「雲端」頁面上的「開始使用」取得註冊Token。

用戶端和平臺更新

- Windows 用戶端支援 Windows 10 20H1 (Windows 10 版本 2004)
- Linux 用戶端現在支援 Ubuntu 18.04、RHEL 8 和 CentOS 8。
- AppRemover 工具已更新為較新版本。在安裝 Windows 用戶端之前，AppRemover 工具將移除第三方應用程式。有關移除哪些應用程式的資訊，請參閱：Endpoint Protection 14.3 中的第三方安全軟體移除

已移除的功能

- 以下通知不再顯示風險嚴重性和風險類型欄位：風險爆發、單一風險事件、檢測到的新風險。

Symantec Endpoint Protection 所有版本中的新功能

已知問題與因應措施

本節中的項目適用於此版本的 Symantec Endpoint Protection。

Table 1: 升級問題

問題	說明和解決方案
啟用 FIPS 模式後，從 2017 版升級到 2019 版的 SQL Server 失敗 [14.3]	您可能會看到錯誤：發生了以下錯誤。 安裝具有錯誤訊息的擴展功能時發生錯誤：AppContainer 建立失敗，錯誤訊息為狀態為「無」。 此操作不是 Windows 平台 FIPS 驗證加密演算法的一部份。 如果您具有啟用 FIPS 的 Symantec Endpoint Protection Manager 14.3，並且從 Microsoft SQL Server 2017 升級到 2019，便會發生這種錯誤。[SEP-61473] 若要解決此問題，請停用作業系統層級的 FIPS： 1. 在 `C#\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`，按一下「本機安全政策」>「本機政策」>「安全性選項」，然後停用系統加密：使用符合 **FIPS** 的演算法進行加密、雜湊和簽署 2. 從 SQL Server 2017 版升級到 2019 版。 3. SQL Server 成功升級後，重新啟用 FIPS。 啟用 FIPS 模式後，從 2017 版升級到 2019 版的 SQL 失敗
自訂名稱可能會阻止在升級至 14.2 或更新版本期間更新防火牆政策	升級至 Symantec Endpoint Protection 14.2 或更新版本時，如果您變更了某些預設名稱，則防火牆政策無法納入 IPv6 的變更。 預設名稱包括預設政策的名稱和預設規則名稱。 如果無法在升級期間更新規則，則不會出現 IPv6 選項。 您在升級後建立的任何新政策或規則不受影響。 如有可能，請將任何變更的名稱還原回預設名稱。 否則，請確保您新增至預設政策的任何自訂規則不會以任何方式攔截 IPv6 通訊。 請確保針對您新增的任何新政策或規則相同。

Table 2: Symantec Endpoint Protection Manager 問題

問題	說明和解決方案
如果使用混合管理選項和代理伺服器，則在 Symantec Endpoint Security 中將其他 URL 加入許可清單 [14.2.2.1 或更新版本]	隨著 Broadcom 最近收購 Symantec Enterprise Security，用戶端到雲端通信的 URL 在 14.2.2.1 中發生了變化。[CDM-42467] 您必須在以下情況將用戶端升級到版本版本 14.2.5569.2100 或更新版本 • 您使用 Symantec Endpoint Security 來管理用戶端和政策，同時您的內部部署 Symantec Endpoint Protection Manager 網域在雲端主控台中註冊 • 您使用代理伺服器。 若要將完全雲端管理或混合管理的代理程式中的 URL 列入許可清單，請將它們在 Symantec Endpoint Security 中列入許可清單： 1. 在 Symantec Endpoint Security 中，移至「端點」>「政策」>「[政策名稱] 許可清單政策」。 2. 在「許可清單政策」中，在「依網域排除」旁，選擇「新增」，一次新增一個 URL，然後選擇「新增」： `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (如果您在歐洲有裝置，請新增此項)。 如果您使用更新版本管理用戶端，請保留 spoc.norton.com。 3. 選取「儲存政策」然後選取「是」以更新政策並將其套用至現有群組。 請參閱要列入 Symantec Endpoint Security 許可清單的 URL。 請參閱在 2020 年 5 月 4 日之前將雲端管理的 Symantec Agent 升級到版本 14.2 RU2 MP1 或更新版本 。
Symantec Endpoint Protection Manager 器遠端主控台不再支援 32 位元 Windows 平台 [14.3]	自 14.3 起，如果運行 32 位元版本的 Windows，則無法登入 Symantec Endpoint Protection Manager 遠端主控台。 Oracle Java SE Runtime Environment 不再支援 32 位元版本的 Microsoft Windows。[SEP-61106] 如果看到以下訊息，請本機登入 Symantec Endpoint Protection Manager： 「此版本的 C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe 與您執行的 Windows 版本不相容。 請檢查電腦的系統資訊，然後與軟體發行者聯繫。」 登入 Symantec Endpoint Protection Manager
安裝 Symantec Endpoint Protection Manager 時出現「無法安裝 Microsoft Visual C++ Runtime」錯誤 [14.3]	在 Windows 2012 R2 上安裝 Symantec Endpoint Protection Manager 時，您可能會看到以下錯誤：「安裝 Microsoft Visual C++ Runtime 時失敗」 [SEP-60396] 若要解決此問題，請啟動 Windows 並安裝 Windows 更新。 Windows 更新會安裝可再發行的 Visual C++ 2017，這是 Symantec Endpoint Protection Manager 14.3 在 Windows 2012 R2 上安裝的先決條件。
更新以啟用 TLS 1.1 和 TLS 1.2 作為 Windows 中 WinHTTP 中的預設安全通訊協定 [14.3]	升級為或安裝雲端主控台中註冊的 Symantec Endpoint Protection Manager 版本 14.3 後，管理伺服器無法再將日誌成功上載到雲端。 在 uploader.log 中，您可能會看到以下錯誤： `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` 此問題是由於缺少 Microsoft 更新所引起的，該更新為 TLS 1.1 和 1.2 提供支援。 若要解決此問題，請安裝 Microsoft 更新：KB3140245。 如需詳細資訊，請參閱： 更新以啟用 TLS 1.1 和 TLS 1.2 作為 Windows 中 WinHTTP 的預設安全通訊協定
在用戶端收到 AD 的 Endpoint Threat Defense 更新政策後，Symantec Endpoint Protection Manager 中仍顯示「部署正在進行中」[14.2 RU1 MP1 和更新版本]	這是預期狀況。 僅自版本 14.2 RU1 MP1 起的用戶端支援 AD 3.3 政策的 Endpoint Threat Defense。 將 Symantec Endpoint Threat Defense for Active Directory 3.3 的政策套用到群組。 此群組包含一些執行 Symantec Endpoint Protection 14.2 RU1 或更早版本的用戶端。 這些用戶端按預期接收並套用政策，但 Symantec Endpoint Protection Manager 中的狀態會繼續顯示「部署進行中」訊息。

Table 3: Windows、Mac 和 **Linux** 用戶端問題

問題	說明和解決方案
Symantec Endpoint Protection 14.3 Windows 用戶端安裝可能會失敗，除非您首先安裝 SHA-2 支援 [14.3]	如果執行舊版作業系統版本 (Windows 7 RTM 或 SP1、Windows Server 2008 R2 或 R2 SP1 或 R2 SP2)，則您的設備上需要安裝 SHA-2 代碼簽署支援，才能安裝 2019 年 7 月或之後發佈的 Windows 更新。 如果沒有 SHA-2 支援，Windows 用戶端安裝有時會失敗。 無論您是首次安裝用戶端還是從以前的版本自動升級，安裝都可能會失敗。[SEP-61175/61403] 若要獲得 Microsoft 強制實施 SHA-2 代碼簽署支援，請參閱： Windows 和 WSUS 的 2019 SHA-2 代碼簽署支援需求 Symantec Endpoint Protection 14.3 Windows 用戶端可能無法安裝，除非您首先安裝 SHA-2 支援
Symantec Endpoint Protection Windows 用戶端在啟用 UWF 的 Windows 10 1803 上安裝時無法執行 [14.3]	如果啟用統一寫入篩選器 (UWF) 並保護安裝 Windows 用戶端的磁碟機時，Symantec Endpoint Protection 用戶端在 Windows 10 10 RS4 1803 32 位作業系統上執行，則用戶端無法正常執行。 此 Windows 作業系統包含阻止 Windows 用戶端執行的 UWF 缺陷。 若要解決此問題，可以： • 升級至不包含該缺陷的另一個作業系統版本。 • 停用 UWF。請參閱：在啟用 UWF 的 Windows 10 1803 上安裝 Endpoint Protection 時出現故障
啟用 WSS 流量重新導向的 Mac 用戶端不支援 LiveUpdate 的自訂代理設定 [14.2 RU1 MP1 和更新版本]	您已為 Symantec Endpoint Protection 14.2 RU1 MP1 或更新版本架構受管 Mac 用戶端，可透過外部通訊設定使用 LiveUpdate 的自訂代理設定。 但是，透過 Symantec Endpoint Protection Manager 政策為 Mac 用戶端啟用 WSS 流量重新導向 (WTR) 後，您會發現 LiveUpdate 流量不再支援您的自訂代理設定。 相反，LiveUpdate 會嘗試直接連線。 若要解決此問題，請僅在停用 WSS 流量重新導向的情況下使用 LiveUpdate 的自訂代理設定。
Microsoft Edge 意外地允許在啟用強化的情況下下載 PDF [14.2 RU1 MP1 及更新版本]	在 Symantec Endpoint Protection 用戶端中啟用應用程式強化的情況下，如果您使用 Microsoft Edge 瀏覽器，則能夠意外地下載 PDF 檔案。 在其他瀏覽器中，防止下載 PDF 檔案如預期般運作。 計劃將於未來版本中修正此問題。

隨著 Broadcom 最近宣佈 Symantec Enterprise Protection 已正式加入 Broadcom，賽門鐵克將文件移轉到 Broadcom Symantec Security Tech Docs Portal。

若要查找Endpoint Protection 文件，請按一下「賽門鐵克安全軟體」標籤，然後按一下「**Endpoint Security** 和管理」>「**Endpoint Protection**」。

Table 4: 文件問題

問題	說明和解決方案
HOWTO 文章已過期。	作為 Symantec Endpoint Protection Manager 說明中重複主題的 HOWTO 文章已重新發佈在 Endpoint Protection 網站上，現在具有不同的 URL。 若要尋找文章，請使用「搜尋欄位」。
PDF 檔	賽門鐵克在 DOC 文章上發佈了所有 PDF 檔。 這些頁面已過期。 若要尋找 PDF 檔的最新版本，請移至相關文件頁面。 將來，Broadcom 將新增舊版 PDF 檔和翻譯的 PDF 檔。

如需查詢已解決的問題，請參閱：Symantec Endpoint Protection 14.3 的新修正和元件

Symantec Endpoint Protection (SEP) 的系統需求

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。

NOTE
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 14.0.1 或更早版本無法正確提供版本 14.2 用戶端及其特定版本的 Moniker。 對於早於 14 MP2 的版本，Symantec Endpoint Protection Manager 無法正確提供 14.0.1 之後的用戶端版本及其特定版本的 Moniker。

下表描述了 Symantec Endpoint Protection 的軟體和硬體需求。

Table 5: Symantec Endpoint Protection Manager (SEPM) 軟體系統需求

元件	需求
作業系統	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** 不支援桌面作業系統。 **Note:** 不支援 Windows Server Core 版本。 Windows Server Core 不包括 Symantec Endpoint Protection Manager 工作所需的 Internet Explorer。
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 注意：32 位元版本的 Windows 10 不支援在 Edge 瀏覽器上存取 Web 主控台。 • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x 至 68.x • Google Chrome 75.x
資料庫	**Symantec Endpoint Protection Manager** 包含內嵌資料庫。 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 2008 SP4 • SQL Server 2008 R2，SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014，RTM - SP3 • SQL Server 2016、RTM、SP1、SP2 • SQL Server 2017，RTM • SQL Server 2019，RTM (自 14.3 版起) **Note:** 不支援 SQL Server Express 版本資料庫。支援 Amazon RDS 上託管的 SQL Server 資料庫 (自 14.0.1 MP2 版起)。 **Note:** 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。如果沒有 SQL Server 修補程式來支援 TLS 1.2，從 Symantec Endpoint Protection 12.1 升級至 14 時可能會發生問題。 **Note:** Microsoft SQL Server 支援 TLS 1.2

元件	需求
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。

Table 6: Symantec Endpoint Protection Manager 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 **Note:** 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 **Note:** 您的 Symantec Endpoint Protection Manager 伺服器可能需求額外的 RAM，視已安裝的其他應用程式的 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。
顯示器	1024 x 768 或更大
硬碟機 (安裝到系統磁碟機時)	搭配內嵌資料庫或本機 **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 100 GB) 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)	搭配內嵌資料庫或本機 **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

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。

Table 7: 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)	• Windows 7 (32 位元、64 位元；RTM 和 SP1) • Windows Embedded 7 Standard、POSReady 和 Enterprise (32 位元和 64 位元) • Windows 8 (32 位元、64 位元) • Windows Embedded 8 Standard (32 位元和 64 位元) • Windows 8.1 (32 位元、64 位元)，包括 Windows To Go • Windows 8.1 四月更新 (2014) (32 位元、64 位元) • Windows 8.1 八月更新 (2014) (32 位元、64 位元) • Windows Embedded 8.1 Pro、Industry Pro 和 Industry Enterprise (32 位元和 64 位元) • Windows 10 (1507 版) (32 位元、64 位元)，包括 Windows 10 企業版 2015 長期維護 • Windows 10 11 月更新版 (1511 版) (32 位元、64 位元) • Windows 10 年度更新版 (1607 版) (32 位元、64 位元)，包括 Windows 10 企業版 2016 長期維護 • Windows 10 Creators Update (1703 版) (32 位元、64 位元) • Windows 10 Fall Creators Update (1709 版) (32 位元、64 位元) • Windows 10 2018 年 4 月更新版 (1803 版) (32 位元、64 位元) • Windows 10 2018 年 10 月更新版 (1809 版) (32 位元、64 位元)，包括 Windows 10 Enterprise 2019 LTSC。 • Windows 10 2019 年 5 月更新版 (1903 版) (32 位元、64 位元) • Windows 10 2019 年 11 月更新版 (1909 版) (32 位元、64 位元) (從 14.2 RU1 開始) • Windows 10 20H1 (Windows 10 2004 版) (自 14.3 版起)
作業系統 (伺服器)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 四月更新 (2014) • Windows Server 2012 R2 八月更新 (2014) • Windows Server 2016 • Windows Server 2019 • Windows Server，1803 版 (伺服器核心) (從 14.2 RU2 開始) • Windows Server，1809 版 (伺服器核心) • Windows Server，1903 版 (伺服器核心) (從 14.2 RU1 開始) • Windows Server，1909 版 (伺服器核心) (從 14.2 RU1 開始)
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) 引擎的版本為基礎。 請參閱 Endpoint Protection 中瀏覽器入侵預防支援的瀏覽器。

Table 8: 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)	• 32 位元處理器：最少 2 GHz Intel Pentium 4 或效能相當的處理器 (建議使用 Intel Pentium 4 或效能相當的處理器) • 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 **Note:** 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) **Note:** 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)

元件	需求
顯示器	800 x 600 或更大
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。 硬碟機系統需求： • 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說明 Symantec Endpoint Protection 安裝到系統磁碟機時的硬碟機系統需求。 • 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說明 Symantec Endpoint Protection 安裝到替代磁碟機時的硬碟機系統需求。 **Note:** 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。

Table 9: 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

用戶端類型	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。

Table 10: 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

用戶端類型	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。 但是在安裝期間，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。

Table 11: 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 **Note:** 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 用戶端需要下列可用硬碟空間： • 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。

元件	需求
內嵌作業系統	• Windows Embedded Standard 7 (32 位元和 64 位元) • Windows Embedded POSReady 7 (32 位元和 64 位元) • Windows Embedded Enterprise 7 (32 位元和 64 位元) • Windows Embedded 8 Standard (32 位元和 64 位元) • Windows Embedded 8.1 Industry Pro (32 位元和 64 位元) • Windows Embedded 8.1 Industry Enterprise (32 位元和 64 位元) • Windows Embedded 8.1 Pro (32 位元和 64 位元)
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)。 建議的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)。

Table 12: 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
實體 RAM	2 GB RAM
硬碟機	500 MB 可用硬碟空間用於安裝
顯示器	800 x 600
作業系統	• macOS 10.13 • macOS 10.14 • macOS 10.15 到 10.15.5 macOS 10.14.5 及更新版本支援 kext 存證收據需求。 請參閱 macOS 10.14.5 的 Endpoint Protection 14.2 RU1 和 kext 存證收據。 如需以前版本受支援的作業系統清單，請參閱：Mac 與 Endpoint Protection 用戶端的相容性

Table 13: Linux 適用的 Symantec Endpoint Protection 用戶端系統需求

元件	需求
硬體	• Intel Pentium 4 (2 GHz) 處理器或更新的處理器 • 1 GB RAM • 7 GB 可用硬碟空間
作業系統	• Amazon Linux • 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 Symantec Endpoint Protection 支援的 Linux 核心。
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

其他環境需求	• Glibc
	不支援執行 glibc 2.6 之前版本的任何作業系統。
	• 64 位元電腦上的 i686 型相依套件
	Linux 用戶端中的很多可執行檔都是 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。
	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：
	– 針對以 Red Hat 為基礎的派送：`sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– 針對以 Debian 為基礎的派送：`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`
	• 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

所有 Endpoint Protection 版本的版本說明和系統需求

支援升級到最新版本的 Symantec Endpoint Protection 14.x 的路徑

NOTE

通常，對於低於最新版本的 Symantec Endpoint Protection 版本，清單上位於它之前的每個版本都受支援。 不過，您應該參考特定版本的版本說明進行確認。

所有 Endpoint Protection 版本的版本說明、新修正和系統需求

Symantec Endpoint Protection Manager 和 Windows 用戶端

下列 Symantec Endpoint Protection Manager 版本和 Symantec Endpoint Protection Windows 用戶端版本可以直接升級到目前版本：

- 11.x 和 Small Business Edition 12.0 (僅限 Symantec Endpoint Protection 用戶端，適用於支援的作業系統)
- 12.1.x，最高是 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Mac 用戶端

下列適用於 Mac 的 Symantec Endpoint Protection 用戶端版本可以直接升級到目前版本：

- 12.1.4 - 12.1.6 MP9
  Mac 用戶端不會更新為版本 12.1.6 MP10。
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

適用於 Mac 的 Symantec Endpoint Protection 用戶端未針對 14.0.1 MP2 進行更新。

Linux 用戶端

下列適用於 Linux 的 Symantec Endpoint Protection 用戶端版本可以直接升級到目前版本：

- 12.1.x，最高是 12.1.6 MP9
  Linux 用戶端不會更新為版本 12.1.6 MP10。
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Symantec AntiVirus for Linux 1.0.14 是可直接移轉至 Symantec Endpoint Protection 的唯一版本。 您必須先解除安裝所有其他版本的 Symantec AntiVirus for Linux。 您無法將受管用戶端移轉到非受管用戶端。

不支援的升級路徑

您無法從所有賽門鐵克產品移轉到 Symantec Endpoint Protection。 您必須先移除下列產品，然後再安裝 Symantec Endpoint Protection 用戶端：

- 不受支援的賽門鐵克產品 Symantec AntiVirus 和 Symantec Client Security
- 所有賽門鐵克 Norton™ 產品
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- 早於 12.1.4 的 Mac 適用的 Symantec Endpoint Protection 版本

您無法將 Symantec Endpoint Protection Manager 11.0.x 或 Symantec Endpoint Protection Manager Small Business Edition 12.0.x 直接升級到任何版本的 Symantec Endpoint Protection Manager 14。 您必須先解除安裝這些版本或升級到 12.1.x，然後再升級到 14.x。

無法將 Symantec Endpoint Protection Manager 12.1.6 MP7 升級到版本 14，因為 12.1.6 MP7 中的資料庫架構版本高於 14。 您必須改為將 12.1.6 MP7 升級到 14 MP1 或更新版本。

不支援從 14 MP1 (14.0.2332.0100) 升級到 14 MP1 重新整理版次 (14.0.2349.0100)。

降級路徑不受支援。 例如，如果想要從 Symantec Endpoint Protection 14.2.1.1 移轉到 12.1.6 MP10，必須先解除安裝 Symantec Endpoint Protection 14.2.1.1。

如果您有版次號碼，但不確定如何轉換為發行版本，請參閱：

- Symantec Endpoint Protection 的發行版本
- 關於 Endpoint Protection 發行類型和版本

取得相關資訊的位置

Endpoint Protection 資訊顯示了您可以從中取得最佳實務、疑難排解資訊和其他資源來協助您使用本產品的網站。

Table 14: Endpoint Protection 網站資訊

資訊類型	網站連結
試用版	請與您的帳戶代表聯繫。
手冊和說明文件更新	• 最新版本的產品指南 (英文) • 最新版本的產品指南 (其他語言) • Symantec Endpoint Protection 14.x 所有版本的產品指南 (英文) 其他語言：
技術支援	Endpoint Protection 技術支援 包含知識庫文章、產品版本詳細資料、更新和修正程式以及用於支援的聯絡選項。
威脅資訊和更新	Symantec Protection Center
訓練	教育訓練服務 存取訓練課程、線上產品說明庫等。
Symantec Connect 論壇	Endpoint Protection


Symantec
A Division of Broadcom