



Symantec™ Endpoint Protection 14.4 版本說明

Updated: January 2026

Table of Contents

Symantec Endpoint Protection 14.4 的新功能.....	3
所有 Symantec Endpoint Protection (SEP) 14.x 版本的系統需求.....	5
最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑.....	14
Documentation Legal Notice.....	16

Symantec Endpoint Protection 14.4 的新功能

這些章節描述此版本中的新功能。

Symantec Endpoint Protection Manager 14.4

- 新的 Web 主控台

在 Symantec Endpoint Protection Manager (SEPM) 14.4 中，新的 Web 主控台取代 Java 型主控台作為預設主控台。新的 Web 主控台也會取代舊版 Web 主控台。

對於需要遠端管理主控台的客戶來說，Java 型主控台面臨操作挑戰。以前，在未直接登入 SEPM 伺服器時，這些客戶需要部署遠端桌面產品才能管理主控台。

新的 Web 主控台 UI 保持與 Java 主控台幾乎完全相同的外觀，因此不需要克服學習曲線。UI 包括一些細微的視覺變更，但不會變更使用者體驗。

您也應該預期主控台效能會略有改善。

NOTE

如果您使用的網路沒有 Web 存取或 Web 存取受限，則可以繼續使用經典 Java 主控台進行本機登入。不過，不再支援遠端 Java 主控台。

如需更多詳細資訊，請參閱 [登入 Symantec Endpoint Protection Manager \(版本 14.4\)](#)。

- 對等內容派送

您現在可以架構端點，以在代理程式之間共用內容更新。內容更新包含病毒定義和行為規則這類資訊。允許網路中的裝置以將 LiveUpdate 內容分發給其對等裝置，代理程式即可節省頻寬，而且可以節省資源。

NOTE

啟用「對等內容派送」時，無法啟用群組更新提供者 (GUP)。

您在 LiveUpdate 政策中啟用「對等內容派送」選項時，代理程式會採取下列動作：

- 嘗試從對等代理程式取得更新安裝套件
- 快取更新套件以供其他代理程式使用
- 廣告套件可用性

如需更多詳細資訊，請參閱 [使用對等內容派送更新用戶端上的內容](#)。

- 自適應防護增強

在「自適應防護」政策中，您現在可以按一下針對特定應用程式行為所顯示的事件計數。事件頁面的出現可協助您快速調查這些應用程式行為，並協助您判斷是否可以安全地變更或套用政策。

如需更多詳細資訊，請參閱 [自適應防護政策 - 事件](#)。

- Linux KMOD 功能增強

SEP Linux 代理程式需要使用部署至 Linux 作業系統的核心模組來支援防護功能。在此版本中，SEPM 現在會在用戶端詳細資料頁面內報告部署至裝置的核心模組版本。這項增強功能可讓您更輕鬆地判斷環境內所部署的 SEP KMOD 版本。

您現在也可以使用 LiveUpdate 來升級 SEP Linux 核心模組。

14.4 版的用戶端和平台更新

- SEP 14.4 Windows 代理程式不再支援 Windows 桌面版本 8 和 8.1。
- 不再支援 Windows Server 2012 和 2012 R2。
- SEP 14.4 for Linux 支援 RHEL 10。

已移除的功能

Java 型主控台不再是預設主控台。14.4 Web 型主控台現在是預設值。14.4 Web 主控台也會取代先前的 Web 主控台。

如果您需要 Java 主控台用於沒有 Web 存取或 Web 存取受限的網路，則可以從「開始」功能表中存取經典 Java 主控台。遠端 Java 主控台已停用，且無法再使用。

其他資源

- 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](#)。
- 如需使用技術文件、知識庫文章或訓練來取得協助的詳細資訊，請參閱[開始使用 Symantec Endpoint Protection 說明](#)。
- 若要檢視資料庫綱要 (僅限內部；KB 224279)，請聯絡技術支援。

所有 Symantec Endpoint Protection (SEP) 14.x 版本的系統需求

目前 Symantec Endpoint Protection (SEP) 版本需要下列系統需求。

NOTE

若要找較早版本的系統要求，請前往[相關文件](#)並下載合適的版本說明 PDF 檔。

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 14.3 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。

下列各表描述 Symantec Endpoint Protection 的軟體和硬體需求：

- [Symantec Endpoint Protection Manager \(SEPM\) 系統需求](#)
- [Windows 適用的 Symantec Endpoint Protection 用戶端系統需求](#)
- [Mac 適用的 Symantec Endpoint Protection 用戶端系統需求](#)
- [Linux 適用的 Symantec Endpoint Protection 用戶端系統需求](#)

Symantec Endpoint Protection Manager (SEPM) 系統需求

Table 1: Symantec Endpoint Protection Manager 軟體系統需求

元件	需求
作業系統	<ul style="list-style-type: none"> • Windows Server 2012 (14.3 RU9 和更早版本) • Windows Server 2012 R2 (14.3 RU9 和更早版本) • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (14.3 RU3 和更新版本) <p>Note: 不支援桌面作業系統。</p> <p>Note: 不支援 Windows Server Core 版本。</p>
網頁瀏覽器	<p>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：</p> <ul style="list-style-type: none"> • Microsoft Edge Chromium 型瀏覽器 (14.3 及更新版本) • Microsoft Edge • Microsoft Internet Explorer 11 (14.2.x 及更舊版本) • Mozilla Firefox 5.x through 107 • Google Chrome 87 及更新版本

元件	需求
資料庫	<p>Symantec Endpoint Protection Manager 包括一個預設資料庫：</p> <ul style="list-style-type: none"> 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 14.3 MP.x 和更舊版本) <p>您也可以選擇使用下列其中一種 Microsoft SQL Server 版本的資料庫：</p> <ul style="list-style-type: none"> 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) <p>Note: 支援 Amazon RDS 上託管的 SQL Server 資料庫。(14.0.1 MP2 和更新版本)。</p> <p>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。請參閱：</p> <p>Note: Microsoft SQL Server 支援 TLS 1.2</p>
其他環境需求	<ul style="list-style-type: none"> 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) <p>Note: 請注意，在安裝 Symantec Endpoint Protection Manager 期間會自動安裝所需的 Visual C++ 版本</p>

Table 2: Symantec Endpoint Protection Manager 硬體系統需求

元件	需求
處理器	<p>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</p> <p>Note: 不支援 Intel Itanium IA-64 處理器。</p>
實體 RAM	<p>至少 2 GB 可用 RAM；建議 8 GB 或更高可用 RAM</p> <p>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。</p>
顯示	1024 x 768 或更大
硬碟機 (安裝到系統磁碟機時)	<p>搭配本機 SQL Server 資料庫：</p> <ul style="list-style-type: none"> 至少 40 GB (建議使用 200 GB) 可用於管理伺服器和資料庫 <p>搭配遠端 SQL Server 資料庫：</p> <ul style="list-style-type: none"> 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)	<p>搭配本機 SQL Server 資料庫：</p> <ul style="list-style-type: none"> 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) <p>搭配遠端 SQL Server 資料庫：</p> <ul style="list-style-type: none"> 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

元件	需求
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。

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

Table 3: 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)	<p>如需目前版本和舊版本所支援的作業系統清單，請參閱： Windows 與 Endpoint Protection 用戶端的相容性</p> <ul style="list-style-type: none"> 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)	<p>如需目前版本和舊版本所支援的作業系統清單，請參閱： Windows 與 Endpoint Protection 用戶端的相容性</p> <p>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</p>
瀏覽器入侵預防	<p>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</p>

Table 4: 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)	<p>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</p> <p>Note: 不支援 Itanium 處理器。</p>
處理器 (適用於虛擬電腦)	<p>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)</p> <p>Note: 必須啟用 Hypervisor 資源保留。</p>
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
硬碟機	<p>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。程式資料夾通常位於系統磁碟機的預設位置 C:\ProgramData 中。</p> <p>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。</p> <p>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。</p>

Table 5: 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： <ul style="list-style-type: none"> • 395 MB* 當程式資料資料夾位於替代磁碟機時： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 245 MB* 當程式資料資料夾位於替代磁碟機時： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 545 MB* 當程式資料資料夾位於替代磁碟機時： <ul style="list-style-type: none"> • 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 6: 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： <ul style="list-style-type: none"> • 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：** <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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：** <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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：** <ul style="list-style-type: none"> • 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 7: 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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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)
所需的最少元件	<ul style="list-style-type: none"> Filter Manager (FltMgr.sys) 效能資料協助程式 (pdh.dll) Windows Installer 服務
範本	<ul style="list-style-type: none"> 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)。

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

Table 8: Mac 適用的 Symantec Endpoint Protection 用戶端系統需求

元件	需求
處理器/晶片	64 位元 Intel Core 2 Duo 和更新版本 Apple M1 晶片 (自 14.3 RU2 起) Apple M2 晶片 (自 14.3 RU5 起)
實體 RAM	2 GB RAM

元件	需求
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本所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

Symantec Single Agent for Linux 系統需求**Table 9: Symantec Single Agent for Linux 系統需求**

元件	需求
硬體	<ul style="list-style-type: none"> • 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 <p>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。</p>
作業系統	<p>支援的作業系統：</p> <ul style="list-style-type: none"> • Amazon Linux 2 • CentOS Linux 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*、9 • 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)。 • SuSE Linux Enterprise Server 12.x、15.x • Ubuntu 16.04 LTS、18.04 LTS、20.04 LTS、22.04 LTS (14.3 RU6 和更新版本) <p>* 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</p> <p>14.3 MP1 版及更舊版本支援的作業系統：</p> <ul style="list-style-type: none"> • 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 <p>如需受支援的舊版作業系統核心清單，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</p>

元件	需求
相依性	<p>您必須在建立安裝套件的電腦上安裝下列相依套件和程式庫清單。這些套件和程式庫會由安裝程序特別檢查。此清單僅適用於最新版本，而且此清單是舊版需求的累積。</p> <p>核心系統套件：</p> <ul style="list-style-type: none"> • checkpolicy：SELinux 政策編譯器。 • polycoreutils-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。 • 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。 <p>相依程式庫：</p> <ul style="list-style-type: none"> • auditd：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	<p>您可使用下列圖形桌面環境檢視 Symantec Endpoint Protection for Linux 用戶端：</p> <ul style="list-style-type: none"> • KDE • Gnome • Unity <p>Symantec Agent for Linux 14.3 RU1 沒有圖形化使用者介面。</p>

元件	需求
舊版環境需求	<p>14.3 RU1 到 14.3 RU3 :</p> <ul style="list-style-type: none"> • OpenSSL 1.0.2k-fips 或更新版本 <p>14.3 MP1 和更舊版本 :</p> <ul style="list-style-type: none"> • 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。 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： <ul style="list-style-type: none"> – 針對 Red Hat 型散佈：<code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code> – 針對 Debian 型散佈：<code>sudo apt-get install ia32-libs</code> – 針對以 Ubuntu 為基礎的派送： <pre>sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386</pre>

更多資訊

[Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正](#)

最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑

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。請參閱：

發佈 [Endpoint Security](#) 及所有 [Endpoint Protection](#) 版本的版本、附註、新修正及系統需求

另請參閱：[Endpoint Protection 14.x 的升級最佳實務準則](#)

Symantec Endpoint Protection Windows 用戶端

下列版本的 Symantec Endpoint Protection Windows 用戶端版本可以直接升級至目前版本：

- 14.x、14.2.x 和 14.3.x 的所有版本

Symantec Endpoint Protection Mac 用戶端

下列版本的 Symantec Endpoint Protection Windows 用戶端版本可以直接升級至目前版本：

- 14.x、14.2.x 和 14.3.x 的所有版本 (尚未發行 14.3 RU7)。
適用於 Mac 的 Symantec Endpoint Protection 用戶端未針對 14.0.1 MP2 進行更新。

Symantec Single Agent for Linux

NOTE

自 14.3 版 RU1 起，Linux 用戶端安裝程式會偵測並解除安裝舊版 Linux 用戶端，然後執行新用戶端的全新安裝。不會保留舊組態。

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

- 14.x、14.2.x 和 14.3.x 的所有版本 (尚未發行 14.3.7)。

在 14.3 RU1 中，適用於 Linux 的 Symantec Endpoint Protection 用戶端已改名為 Symantec Single Agent for Linux。

如果您有版次號碼，但不確定如何轉換為發行版本，請參閱：

[關於 Endpoint Protection 發行類型和版本](#)

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。

- 降級路徑不受支援。例如，若要從 Symantec Endpoint Protection 14.3 RU8 移轉至 14.3 RU7，則必須首先解除安裝 Symantec Endpoint Protection 14.3 RU8。
- 14.3 RU6 及更新版本不支援 32 位元作業系統。將電腦升級到 64 位元作業系統或安裝 32 位元作業系統的 14.3 RU5。
- 14.0.x 已捨棄對 Windows XP、Server 2003，以及基於 Windows XP 的任何 Windows Embedded 作業系統的支援。Symantec Endpoint Protection Manager 14.2 RU1 可以管理這些電腦作為舊版 12.1.x 用戶端，儘管 12.1.x 用戶端是 EOL。對於這些用戶端，您可能想要使用仍然支援這些舊版作業系統的賽門鐵克產品，如 Data Center Security (DCS)。
- 所有賽門鐵克諾頓產品
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Symantec Endpoint Security 雲端主控台的支援路徑

針對混合管理：

- *Symantec Endpoint Protection Manager*：Symantec 建議使用最新版本，但最低 14.3 MP1 (14.3.1169.0010)。
- *Symantec Endpoint Protection* 用戶端：14.3 MP1 (14.3.1169.0010) 或更新版本。用戶端執行於 Windows Server 2008 R2 或更新版本，而非執行於 Windows Server 2008 RTM/SP1/SP2。

請參閱：[移轉至 SES 雲端主控台](#)

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

