Symantec™ Endpoint Protection 14.3 RU10 版本說明

Updated: February 3, 2025

Table of Contents

Symantec Endpoint Protection 14.3 RU10 的新功能？ 3
Symantec Endpoint Protection (SEP) 14.3 RU10 的系統需求 6
Symantec Endpoint Protection 14.3 RU10 的已知問題 14
最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑 16
Symantec Endpoint Protection 支援和培訓資源 18

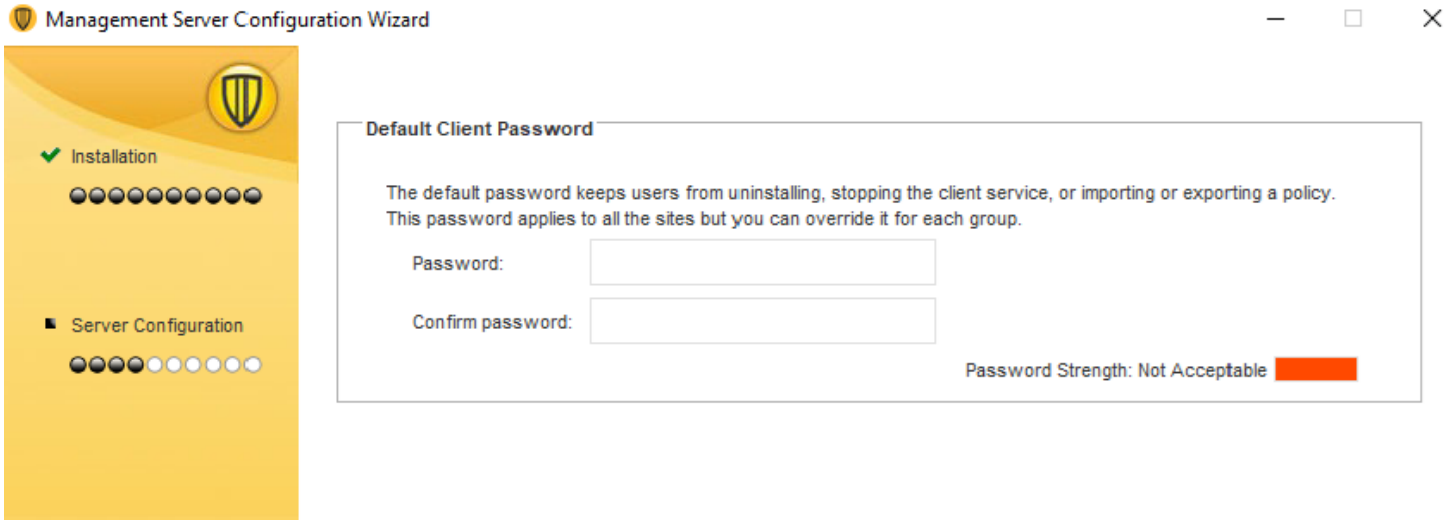
Symantec Endpoint Protection 14.3 RU10 的新功能？

本節描述此版本中的新功能。

防護功能

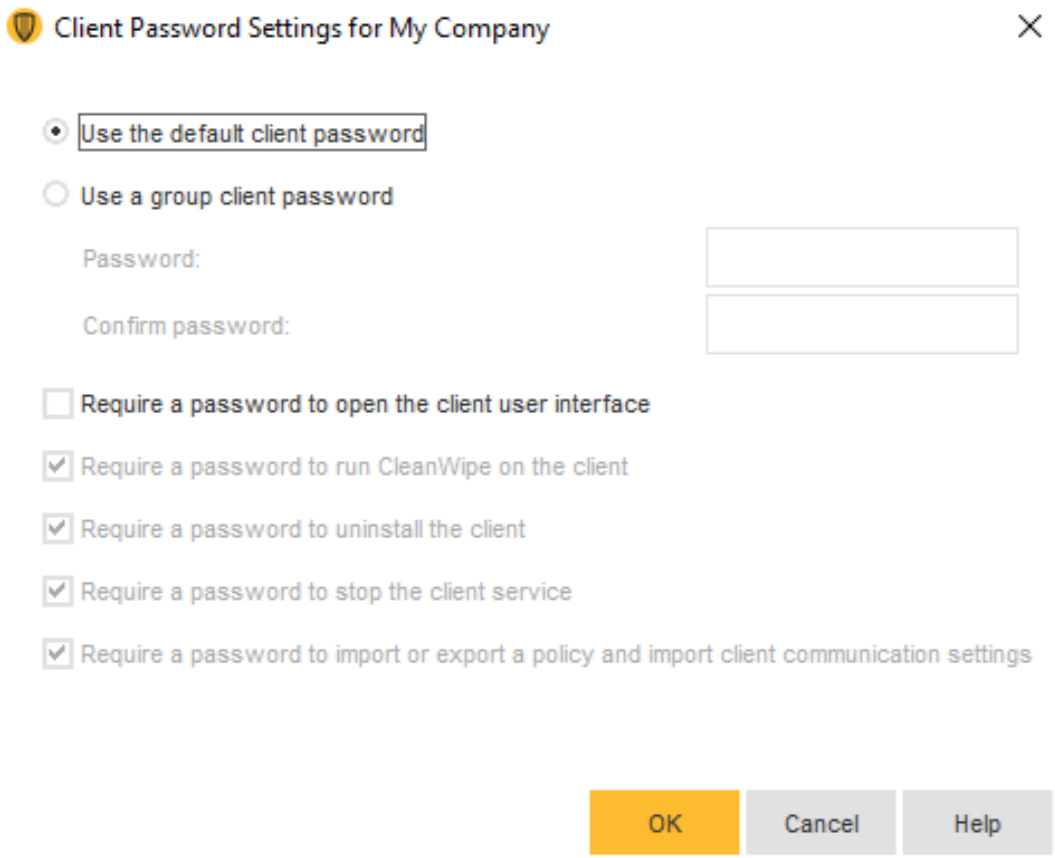
- 您現在可以在內部部署 Symantec Endpoint Protection Manager 中完全架構和管理自適應防護政策，而不是僅能在雲端中。調適型防護使用豐富的行為分析引擎以及全球威脅遙測和專業知識來保護您的組織免於受到鎖定攻擊。您可以使用「進階安全性」頁面上的熱圖來檢視感染狀況行為和相關聯的 MITRE 技術。您接著可以使用自適應防護政策來自動攔截不受信任的行為或手動允許信任的行為。
  透過自適應防護攔截 Living Off the Land (LOTL) 攻擊
- 為了更好地防止攻擊者停止或移除 Symantec Endpoint Protection 用戶端，您需要設定網站層級的預設用戶端密碼。用戶端使用者必須鍵入密碼，才能執行下列工作：
  - 使用 `smc -stop` 命令來停止用戶端服務。
  - 手動或使用 CleanWipe 工具來解除安裝用戶端。
    下載 CleanWipe 移除工具來解除安裝 Endpoint Protection
  - 匯入或匯出政策。
  - 使用 Sylink.xml 檔案來匯入用戶端通訊設定檔案。

  您可以在管理伺服器安裝或升級期間設定預設用戶端密碼。



安裝後架構 Symantec Endpoint Protection Manager

- 安裝之後，您可以在群組層級變更密碼。在舊版本中，這些功能是「用戶端」>「政策」標籤 >「密碼」對話方塊中的選用核取方塊。



  - 為了進一步防止在沒有密碼的情況下無意中修改或解除安裝用戶端，已移除下列選項。
    - 「用戶端部署精靈」中的「密碼防護」選項。
      存取此選項的方式是按一下「用戶端」頁面 >「安裝用戶端」>「通訊更新套件部署」>「針對在 **Windows** 上執行的 **Symantec Endpoint Protection** 用戶端建立套件」>「密碼防護」選項。
      如需在使用通訊檔案匯入用戶端安裝套件時使用密碼的相關資訊，請參閱使用「通訊更新套件部署」還原用戶端伺服器通訊。
    - 「管理」頁面 >「安裝套件」>「用戶端安裝設定」>「基本設定」標籤上的「移除無法解除安裝的現有 **Symantec Endpoint Protection** 用戶端軟體」選項。
      如需解除安裝 Symantec Endpoint Protection 用戶端的其他方法的相關資訊，請參閱解除安裝 Symantec Endpoint Protection 用戶端。
- SONAR 日誌已重新命名為「SONAR：行為分析」日誌。

Symantec Endpoint Protection Manager

- 已新增 Windows Server 2025 的支援。
- 已捨棄 Windows Server 2012 和 Windows Server 2012 R2 的支援。

用戶端和平臺更新

Symantec Endpoint Protection Client for Mac

Symantec Endpoint Protection Client for Mac 沒有規劃版本。

Symantec Single Agent for Linux

Symantec Single Agent for Linux 沒有規劃版本。

Symantec Endpoint Security 雲端主控台

從雲端主控台管理的用戶端電腦獲得類似的功能和防護。

- 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
- 若要移轉至雲端主控台，請參閱：移轉至雲端主控台

最新版本的雲端主控台針對 Symantec Endpoint Protection 用戶端提供下列增強功能：

SymantecAI 聊天機器人具有全新外觀，並針對準確性進行調整。

說明文件

新主題包括：

- 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。
- 如需此版本中修正的相關資訊，請參閱 Symantec Endpoint Protection 14.3 RU10 的新修正和元件版本。

若要檢視資料庫綱要，請聯絡技術支援。

Symantec Endpoint Protection (SEP) 14.3 RU10 的系統需求

目前 Symantec Endpoint Protection (SEP) 版本必須符合下列系統需求。

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。

Symantec Endpoint Protection 的系統要求還必須包括其安裝所在作業系統所設定的任何需求。

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
- Linux 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

另請參閱 Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正。

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	• 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) • Windows Server 2025 (14.3 RU10 和更新版本) **Note:** 不支援桌面作業系統。 **Note:** 不支援 Windows Server Core 版本。
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

元件	需求
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 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、SP3 • 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) **Note:** 支援 Amazon RDS 上託管的 SQL Server 資料庫。(14.0.1 MP2 和更新版本)。 **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。您應該視需要更新 SQL Server。此建議適用於 SQL Server 2008、2012 和 2014。請參閱： **Note:** 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) **Note:** Visual C++ 會在 Symantec Endpoint Protection Manager 安裝期間自動安裝

Table 2: 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 伺服器可能需要更多的 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	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，您必須提供更多可用的磁碟空間。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)	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 • 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。您不能在 64 位元電腦上執行 32 位元用戶端。
作業系統 (伺服器)	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 若要在 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 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)	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)
顯示	800 x 600 或更大
硬碟機	磁碟空間需求取決於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。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。 **Note:** 可用空間的需求依 NTFS 檔案系統而定。內容更新和記錄也需要額外的空間。

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： • 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 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： • 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 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。如果您也從整合式解決方案 (例如 EDR) 實作額外功能，則需要更多的實體 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。
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)。

Symantec Single Agent for Linux 系統需求

Table 8: Symantec Single Agent for Linux 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 512 MB 的可用 RAM (建議為 4 GB) • 如果 /var、/opt 和 /tmp 共用檔案系統或磁碟區，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 啟用任何 Symantec Endpoint Detection and Response 功能時，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： 如果您嘗試將 SEP 14.3 Linux 代理安裝至低於這些所列版本的散發版本，這將導致改為安裝與所支援清單相符的較早發行更新版本。 • Amazon Linux 2023 • Amazon Linux 2 • CentOS Linux 7、8* 自 SEP 14.3 RU9 起不再支援 CentOS 串流 • Debian 10 (14.3 RU2 和更新版本) • Oracle Enterprise Linux 6、7、8*、9 • Rocky Linux 8、9 • Red Hat Enterprise Linux 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 (Symantec Endpoint Protection Manager 受管或 Cloud 受管)。 • SuSE Linux Enterprise Server 15.x • Ubuntu 16.04 LTS、18.04 LTS、20.04 LTS、22.04 LTS (自 14.3 RU6 起)、24.04 LTS (自 14.3 RU9 MP1 起) 14.3 RU9 MP1 專門用於支援 Ubuntu 24.04 LTS。因此，針對 Ubuntu 24.04 LTS，您只能看到正在安裝 RU9 MP1 (14.3.9557.9100 版)。針對所有其他平台，安裝程式仍然使用較早的 14.3 RU9 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，然後重新啟動系統時，系統會還原通訊。 使用 SEP 14.3 RU9 時，不再支援下列平台：RHEL6、CentOS6、Ubuntu14、Debian9、SLES12。 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 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

元件	需求
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和程式庫清單。這些套件和程式庫是由安裝程序檢查。此清單是按版本累積的。 核心系統套件： • checkpolicy：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。 • 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： • 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	對於 Symantec Endpoint Protection 14.3 RU1 和更新版本，Linux 代理沒有圖形使用者介面。舊版支援的 KDE、Gnome 和 Unity。

元件	需求

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。
	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`

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

Table 9: 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) Apple M3、M3 Max 和 M3 Pro (自 14.3 RU8 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 Endpoint Protection 14.3 RU10 的已知問題

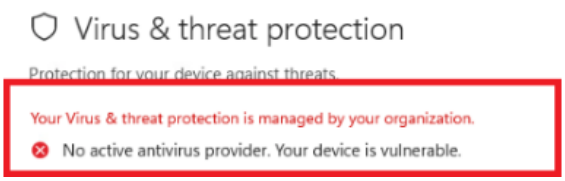
本主題列出 Symantec Endpoint Protection 最新版的已知問題和因應措施。

如需所有 Symantec Endpoint Protection 版本的相關資訊，請參閱：

- Symantec Endpoint Protection 和 Endpoint Security 的版本、系統需求、發行日期、附註和修正
- 所有 Symantec Endpoint Protection (SEP) 14.x 版本的已知問題和因應措施
- 所有 Symantec Endpoint Protection (SEP) 14.x 版本的新功能

下表列出目前版本的已知問題。

Table 10: 14.3 版 RU10

說明	因應措施
Symantec Endpoint Security (SES) 雲端和混合管理的 Symantec Endpoint Protection Manager (SEPM) 調適型防護熱圖顯示下列差異： • 在 SES 雲端熱圖上，如果在前 90 天內觸發行為，則非零感染狀況期限將從「學習」變更為 90 天。零感染行為保持為「學習」。 • 在 SEPM 熱圖上，如果觸發感染狀況行為，則除非過了 90 天之後，否則零感染狀況和非零感染狀況期限都會保持為「學習」。此外，感染狀況期限顯示如下： – 從 >= 90 且 < 180 天，感染狀況期限會顯示 90 天的事件。 – 從 >= 180 且 < 365 天，感染狀況期限會顯示 180 天的事件。 – 從 >= 365 天，感染狀況期限會顯示 365 天的事件。 而雲端熱圖顯示觸發行為時的非零感染狀況期限。 混合 Symantec Endpoint Protection Manager 熱圖檢視比 SES 雲端熱圖檢視更為保守。 [CDM-138308]	未來的修正規劃讓 SES 雲端與混合管理的 SEPM 之間的遙測收集相符。
Microsoft Windows Server 2025 中的 Windows 資訊安全中心無法將已安裝的 Symantec Endpoint Protection 用戶端辨識為防毒提供者，並且會顯示下列訊息： ####################  [SEP-87042]	Microsoft 目前沒有修正。Broadcom 正在調查是否有解決問題的因應措施。不過，Symantec Endpoint Protection 用戶端仍然會保護用戶端電腦。
目前產品語言版本 (PVL) 通常會包括 LiveUpdate Administrator (LUA) 所需的所有內容。不過，在 14.3 RU10 中： • 某些內容使用現有的 14.3 RU9 PVL 來取得內容。 • 某些內容使用新的 14.3 RU10 PVL 來取得內容。 如果您將 LUA 架構成僅下載 14.3 RU10 內容，則用戶端無法取得所需的所有內容。 [CRE-20350]	您必須架構 LiveUpdate Administrator 來下載 14.3 RU9 和 14.3 RU10 內容，以充分更新 14.3 RU10 用戶端。 將 Symantec 產品新增至產品清單

說明	因應措施
在「系統 > 伺服器活動」日誌中，您會看到下列錯誤訊息：`##############: TLS #######` 此問題的發生原因是託管 SEPM 資料庫的 SQL Server 已安裝 Symantec Endpoint Protection 14.3 RU6 到 14.3 RU9，而且 IPS 政策中已套用「頻外掃描」。 下列情況會發生此問題： • IPS 政策中已啟用頻外掃描，而且 IPS 正在處理大量流量。 • 您已在雲端伺服器中註冊 SEPM 網域，並升級至 14.3 RU10 SEPM，然後將 SEP 用戶端升級至 14.3 RU9。 • 您已從 14.3 RU6 到 14.3 RU9 SEPM 升級至 14.3 RU10。 [INFODEVSEP-203]	停用 IPS 政策中的頻外掃描。 請參閱架構入侵預防
如果您已在 14.0 MP1 和更舊版本的 Symantec Endpoint Protection Manager (SEPM) 中設定用戶端密碼防護，然後升級至 14.3 RU5 或更新版本的 SEPM，則該密碼沒有作用。如果您升級至 14.3 RU10 SEPM，則預設用戶端密碼會覆寫 14.0 MP1 和更舊版本的密碼。用戶端使用者會看到下列訊息：`############ ####` 此問題是 14.3 RU5 中進行的安全性增強所造成。 [INFODEVSEP-198]	用戶端使用者必須使用您在 Symantec Endpoint Protection Manager 14.3 RU10 中所設定的預設用戶端密碼。
14.3 RU4 和更舊版本中發生下列用戶端密碼問題： 1. 您在「用戶端密碼設定」對話方塊中設定密碼，然後按一下「確定」來儲存密碼。 2. 您在未變更密碼的情況下重新開啟密碼對話方塊，然後按一下「確定」來儲存密碼。 密碼變更為未知值。  [INFODEVSEP-198]	此問題已在 14.3 RU10 中修正。
您無法使用 PowerShell 來解除安裝您使用 Symantec Endpoint Protection Manager 14.3 RU10 所管理的任何用戶端版本。 請參閱使用指令提示解除安裝 Endpoint Protection 用戶端。 [INFODEVSEP-229]	如果您使用預設用戶端密碼或群組層級密碼，則可以解除安裝用戶端。
在 Symantec Endpoint Protection Windows 用戶端「狀態」頁面上，您可能會看到下列訊息：`Web ##########################################` 按一下「說明 > 疑難排解 > **Web** 和雲端存取防護」頁面。如果您看到下列錯誤訊息：`###80010907` ，升級至此版本時，Web 和雲端存取防護政策已經損壞。 INFODEVSEP-196	1. 撤銷該用戶端使用者的 Web 和雲端存取防護政策。 2. 刪除 `C:\ProgramData\Symantec WSS Agent` 資料夾。 3. 將 Web 和雲端存取防護政策重新指派給用戶端使用者。 SEP Web 和雲端存取防護的運作不正常 錯誤：80010907

Symantec Endpoint Protection 14.3 RU10 的新修正和元件版本

Symantec Endpoint Protection 支援和培訓資源

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

Symantec Endpoint Protection 支援和培訓資源

了解各種可供使用的 Symantec Endpoint Protection 資源，例如支援服務、講師指導培訓和社群論壇。

資源	連結
Broadcom 支援	Broadcom 支援 建立案例並查詢知識庫文章、下載和試用軟體、權利和授權資訊、Security Advisory 以及公告和法律聲明。 Broadcom 試用軟體和概念證明示範。
訓練	• 教育訓練服務 存取訓練課程、線上產品說明庫等。 • 講師指導培訓 歡迎參閱目錄，了解最新的 Broadcom Enterprise Security 群組課程。
Symantec Connect 社群論壇	Endpoint Protection 論壇 加入最新的產品討論，閱讀問答清單等。
更多文件	相關文件 • 從 Broadcom Symantec Security Tech Docs Portal 下載線上 Endpoint Protection 文件。 • 若要尋找 Symantec Endpoint Protection Manager 資料庫綱要，請聯絡支援部門。 對於其他語言，請按一下「語言」下拉式功能表。
威脅資訊和更新	Symantec Protection Center 參閱最新的 Symantec 防護公告、報告產品安全性漏洞、檢查病毒定義檔、安全更新和更多內容。


Symantec
by Broadcom Software