Symantec™ Endpoint Protection 14.3 RU9 版本說明

Updated: June 2024

Table of Contents

Symantec Endpoint Protection 14.3 RU9 的新功能？ 3
Symantec Endpoint Protection (SEP) 14.3 RU9 的系統需求 8
Symantec Endpoint Protection (SEP) 的已知問題和因應措施 17
最新版本 Symantec Endpoint Protection 支援和不支援的升級路徑 28
取得相關資訊的位置 30

Symantec Endpoint Protection 14.3 RU9 的新功能？

這些章節描述此版本中的新功能。

Symantec Endpoint Protection Manager

- 入侵防護政策中的「啟用適用於 **Windows** 的瀏覽器入侵防護」選項會自動為 Symantec Endpoint Protection 載入 Google Chrome 和 Microsoft Edge 瀏覽器延伸。但是，此選項會覆寫組織在使用其他管理工具時安裝的第三方延伸。14.3 RU9 提供了一個選項，允許您使用所選工具 (如 Chrome 瀏覽器雲端管理或 Microsoft InTune) 安裝和管理延伸。
  若要存取此選項，請前往入侵防禦政策，並確認勾選「啟用 **Windows** 的瀏覽器入侵防禦」選項，並清除「啟用延伸的第三方管理」選項。
  請參閱：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站
- 修正了 Symantec Endpoint Protection Manager 於在 14.3 RU8 中新增傳輸層安全性 (TLS) 主機名稱驗證而使用公共 CA 簽署憑證時的 問題：
  - Symantec Endpoint Protection Manager 安裝和升級會要求管理伺服器名稱也必須符合伺服器憑證中列出的其中一個或多個主旨備用名稱 (SAN)。此外，伺服器名稱必須使用有效的主機名稱、完全合格網域名稱 (FQDN) 或 IP 位址。如果伺服器名稱和 SAN 不相符，繼續之前必須重新命名伺服器。
    請參閱：疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本)
  - 如果 Symantec Endpoint Protection Manager 偵測到複寫合作夥伴主機名稱或 IP 位址不相符 Symantec Endpoint Protection Manager 的一個或多個 SAN，Symantec Endpoint Protection Manager 將允許升級。升級之後，您可以重新啟用驗證以提高安全性。
    如果要存取此選項，請右鍵按下複寫合作夥伴網站，按「編輯複寫合作夥伴屬性」，清除「停用合作夥伴伺服器主機名稱驗證」選項。
    如果要修正此問題，請參閱：Symantec Endpoint Protection Manager 偵測到配置的複寫夥伴需要停用憑證驗證 (14.3 RU9 或更新版本)
  - 登入到 Symantec Endpoint Protection Manager 時，您可能會看到以下伺服器憑證相關訊息。
    `##########`
    此訊息存在於早期版本中，但提供了有關此錯誤原因的其他資訊，包括： `########## IP ##########`
    `########## IP ###### Symantec Endpoint Protection Manager#`
    如果要修正此問題，請參閱：錯誤：您的伺服器憑證無效，因為電腦主機名稱或 IP 位址已變更 (14.3 RU8 或更新版本)
- 在早期版本中，要封鎖 Symantec Endpoint Protection Manager 上傳檔案提交，您必須將防火牆設定為封鎖檔案提交 URL。14.3 RU9 讓您可以允許或封鎖向 **Symantec** 匿名提交可疑檔案，以增強威脅防護情報選項，該選項根據預設開啟。
  若要存取此選項，請前往「用戶端」>「政策」標籤 >「外部通訊」>「傳送」標籤 >「更多選項」，來存取這些選項。
- 已改善下列混合管理問題：
  - 在 Symantec Endpoint Protection Manager 和雲端伺服器之間進行多網站複寫的大型組織中，同步可能無法正確執行。雲端有時會少報群組或用戶端的數量。在 14.3 RU9 中，在使用「將群組切換到雲端託管」指令將群組從 Symantec Endpoint Protection Manager 遷移之前，您可以執行
    `ASSET_SYNC_RESET`
    指令以同步群組階層。您可以使用此指令來重新同步多達 5,000 個用戶端。
    如果要在執行指令後查看事件，請前往「監控」>「日誌」標籤 >「系統」日誌類型 >「伺服器活動」內容類型。此訊息在以下情況會出現：

Symantec Endpoint Protection Bridge ##################################

– Symantec Endpoint Protection Manager 現在會在雲端取消註冊成功但對雲端伺服器的 API 呼叫失敗時顯示以下事件：

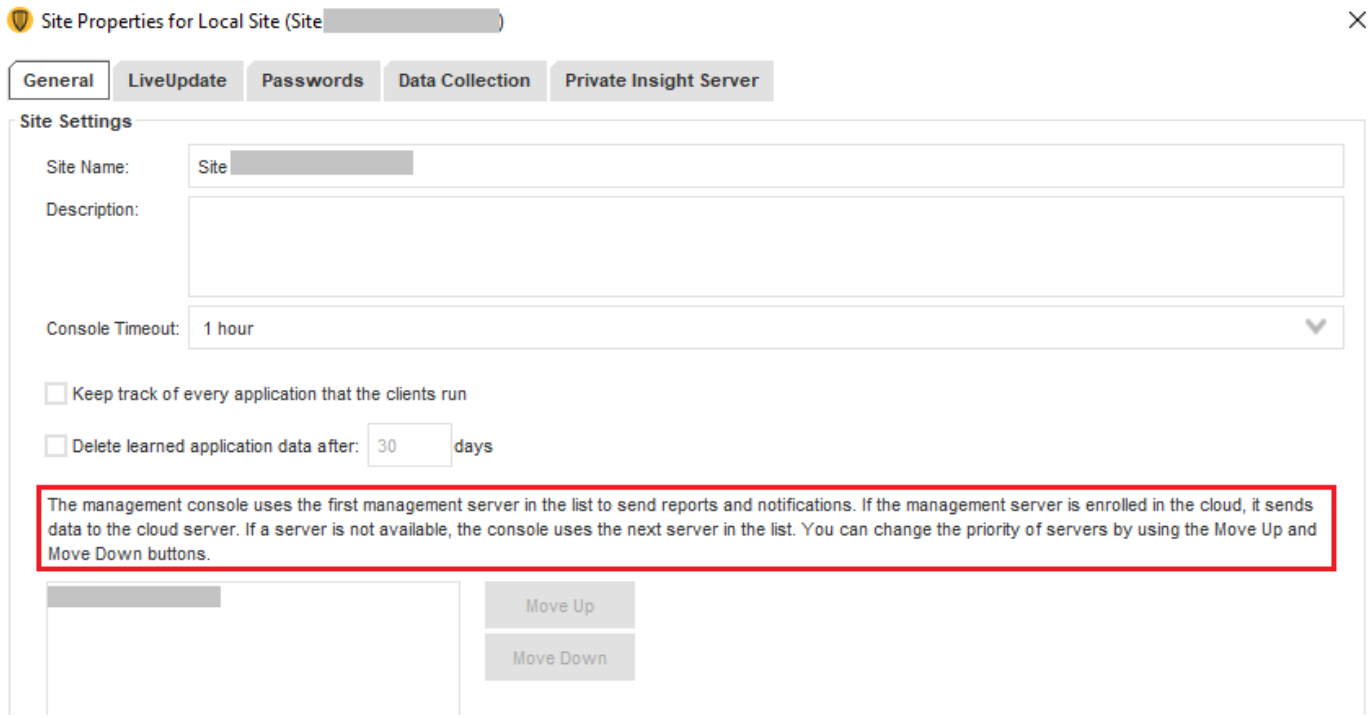
Symantec Endpoint Protection Manager ##################################**##**#######
Symantec Endpoint Protection Manager**##########**

如果要存取這些日誌事件，請前往「監控」>「日誌」標籤 >「系統」日誌類型 >「伺服器活動」內容類型。

如果要從雲端主控台取消註冊管理伺服器，請參閱：從雲端伺服器註冊和取消註冊 Symantec Endpoint Protection Manager 網域

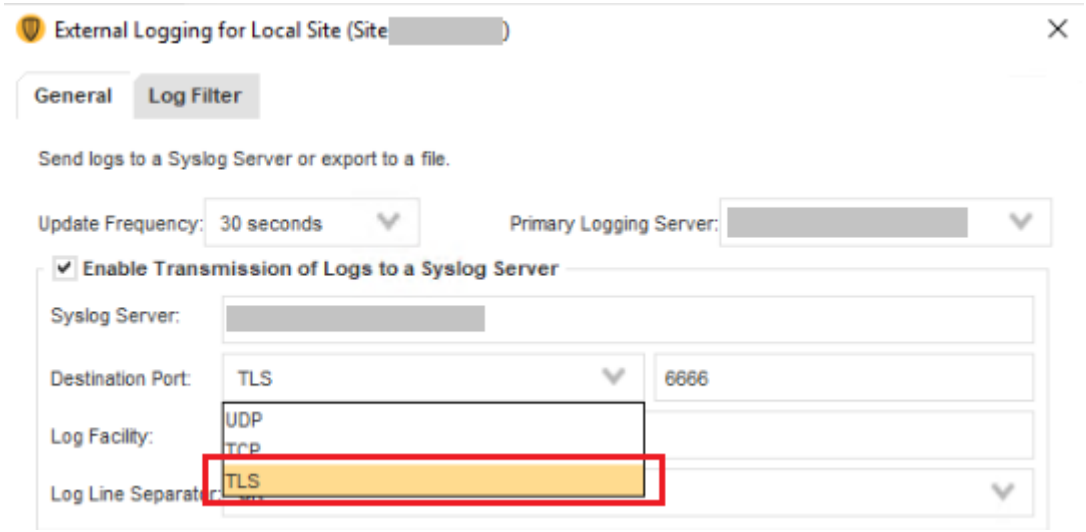
– 在變更代理設定之後，雲端連接器會成功上傳資料。
– 減少了在用戶端執行狀態下到雲端伺服器的不必要流量。
– 改善具有多網站複寫環境的資料收集。
– 改善 Symantec Endpoint Protection Manager 和雲端主控台之間的資料一致性。
– 闡明管理伺服器在雲端主控台註冊時如何傳送資料的說明。

前往「管理」頁面 >「伺服器」>「網站屬性」頁面 >「一般」標籤。下圖顯示您在「上移」和「下移」按鈕上方看到的說明。



請參閱：站台屬性：一般

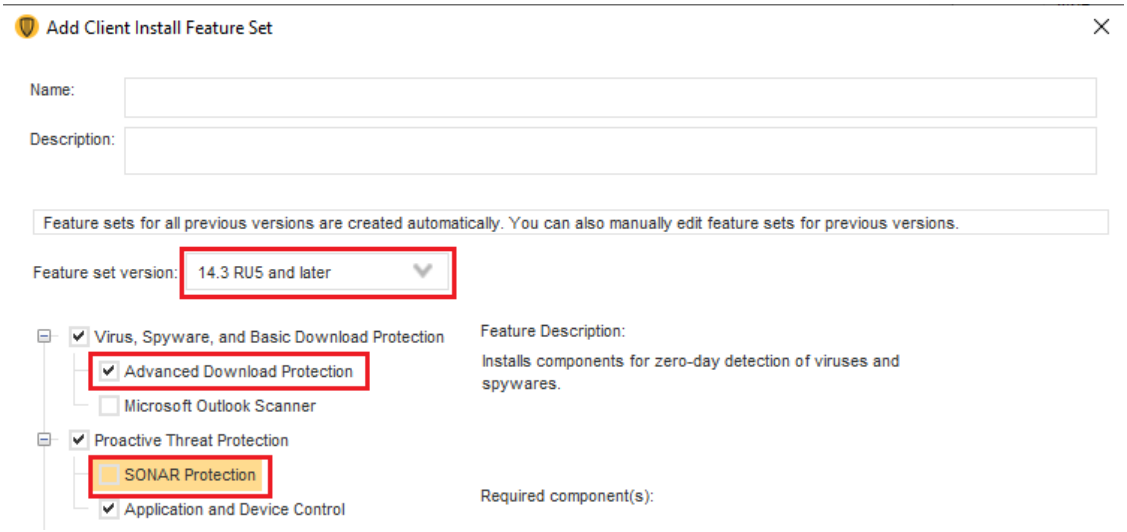
- 報告包括以下增強功能：
  – 您可以設定與 Syslog 伺服器的安全通訊 (TLS)。
  您可以在「外部日誌」對話框的「一般」標籤上存取此選項。在「目的通訊埠」下拉式選單中，選擇「**TLS**」。



請參閱：將資料匯出至 Syslog 伺服器

– Syslog 報告包括 TAA 資安事端 ID 的關聯 **ID** 欄位。

- 安裝進階下載防護時，新增的 **14.3 RU5** 及更新版本的用戶端安裝功能集不再需要安裝 SONAR 防護 (行為分析)。
  若要查看此選項，請前往「管理」頁面 >「安裝套件」>「新增用戶端安裝功能集」，然後按「功能集版本」下拉式選單。



請參閱：選擇要在用戶端上安裝哪些安全性功能

- REST API 支援以下指令：
  – 如果要快速將大量 IP 位址和 MAC 位址新增到防火牆規則中，您可以將現有位址的清單匯入主機群組，然後使用一組支援主機組的 GET、POST 和 PUT 方法的 REST API。
  請參閱：Symantec Endpoint Protection API 指令
  – 針對遵從報告，您可以使用以下 REST API 指令找到 IPS 和行為分析的更新詳細資訊：`GET /api/v1/computers returns ipsDefsetVersion` 和 `GET /api/v1/computers returns behavioralAnalysisDefsetVersion`。
- 升級或新增了以下第三方元件：

- Apache Commons Codec
- Apache Commons 壓縮
- Apache Commons IO
- Apache Commons Lang
- Apache HTTP 伺服器
- Apache Tomcat
- Apache Tomcat Native
- curl
- google guava
- Jackson
- JSON-java
- libexpat
- libssh2
- libxml2
- Nimbus JOSE+JWT
- OpenJDK
- OpenSC
- OpenSSL
- Spring Security
- Spring Framework
- zlib

用戶端和平臺更新

適用於 *Windows* 的 *Symantec Endpoint Protection* 用戶端

- 已減少必須在代理或周邊防火牆中列出，以與用戶端通訊的 URL 數量，您只需要允許以下 URL。

用戶端管理類型	要允許的 **URL**
所有用戶端	• https://liveupdate.symantec.com • https://ent-shasta-rrs.symantec.com • https://sp.cwfservice.net
雲端管理用戶端	• https://us.spoc.securitycloud.symantec.com (北美) • https://eu.spoc.securitycloud.symantec.com (歐洲) • https://in.spoc.securitycloud.symantec.com (印度)

  如果您從 14.3 RU8 和更早版本的用戶端升級，則無需新增或刪除任何 URL。反之，用戶端會在 LiveUpdate 下次下載內容後自動升級。
  若要詳細瞭解您需要允許的所有 URL，請參閱：Symantec Endpoint Protection (SEP) 和 Symantec Endpoint Protection (SES) 所需的外部 URL
- Windows 11 24H2 支援 Windows 用戶端。

Symantec Endpoint Protection Client for Mac

Symantec Endpoint Protection Client for Mac 於 2024 年 7 月發行。

Symantec Single Agent for Linux

Symantec Single Agent for Linux 於 2024 年 7 月發行。

Symantec Endpoint Security 雲端主控台

最新版本的雲端主控台為 14.3 RU9 用戶端提供了下列增強功能：

- 手動隔離裝置後， Symantec Endpoint Security 雲端主控台可以向用戶端使用者傳送自訂通知。
- 您可以使用「停用通知區域圖示」選項來封鎖在終端伺服器上執行的用戶端上出現多個使用者工作階段程序。
- Threat Defense for Active Directory (TDAD) 包括一些更新，例如取消用戶端上正在執行的拓撲的功能。

更多資訊

- 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 SES 雲端主控台

說明文件

文件包括以下新主題：

- 疑難排解伺服器名稱不符伺服器憑證時，Symantec Endpoint Protection Manager 會封鎖您登入或升級 (14.3 RU9 或更新版本)Symantec Endpoint Protection Manager
- 請參閱：Symantec Endpoint Protection Manager 偵測到配置的複寫夥伴需要停用憑證驗證 (14.3 RU9 或更新版本)
- 如何使用 Endpoint Protection (SEP) 封鎖網站？
- 使用「裝置控制」和「應用程式控制」封鎖或允許裝置
- 「應用程式控制」如何封鎖設備
- 刪除用戶端

若要檢視資料庫綱要，請聯絡技術支援。

若要查找原始碼屬性檔案，請登入到 Broadcom 入口網站並前往：Symantec Endpoint Protection 開放原始碼屬性

Symantec Endpoint Protection (SEP) 14.3 RU9 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	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (14.3 RU3 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 • 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。您可能需要修正 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:** 請注意，在安裝 Symantec Endpoint Protection Manager 期間會自動安裝所需的 Visual C++ 版本

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	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

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)	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。
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 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。 **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 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。
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)。

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	• 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 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 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* • 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) * 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 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。這些套件和程式庫會由安裝程序特別檢查。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 Symantec Agent for Linux 14.3 RU1 沒有圖形化使用者介面。

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`

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

Symantec Endpoint Protection (SEP) 的已知問題和因應措施

本節中的項目適用於這版 Symantec Endpoint Protection。

NOTE

「問題」欄顯示出現問題的版本號碼。例如，[14.3 RU1] 表示問題適用於 14.3 版 RU1 和更新版本。 這些問題在修正後會出現在 fix-it 附註中。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

14.3 RU9 中的已知問題

Table 10: 版本 **14.3 RU9**

問題 ID	說明	因應措施
INFODEVSEP-70	Symantec Endpoint Protection 用戶端 14.3 RU9 與內部部署 Symantec EDR 4.9 及更舊版本不相容。此問題是由於 14.3 RU9 用戶端必須允許的 URL 數量較少而導致。[14.3 RU9] Symantec Endpoint Protection (SEP) 和 Symantec Endpoint Protection (SES) 所需的外部 URL	此問題已在 Symantec EDR 版本 4.10 中修正，該版本計劃於 2024 年 6 月發佈。 如果您的環境包括 Symantec EDR，請執行以下任一動作： • 等到 Symantec EDR 4.10 發佈再升級到 SEP 14.3 RU9，然後同時升級兩者。 • 隨時升級到 SEP 14.3 RU9 並安裝 Symantec EDR 4.9 修正程式。
INFODEVSEP-54	以下錯誤資訊每隔 24 小時就會出現在「管理 > 伺服器」頁面：`#### Symantec Endpoint Protection Manager ######### ##########[{_}sitename{_}]` 當 Symantec Endpoint Protection Manager 已在雲端控制台註冊，且至少兩個週期未與其複寫夥伴進行複寫時，就會出現此問題。當主要網站離線時，複寫夥伴通常不會進行複寫。[14.3 RU9]	您必須在網站之間進行複寫。

Symantec Endpoint Protection 14.3 RU9 的新修正和元件版本

14.3 RU8 中的已知問題

Table 11: 版本 **14.3 RU8**

問題 ID	說明	因應措施
SEP-85508	在用戶端或雲端主控台中使用 Live Shell 時，某些文字可能無法正確顯示。字元可能會替換為 Unicode 替換字元 (帶問號的菱形) 或其他非預期的字元。[14.3 RU8 和更舊版本] 請參閱：ICDm 中的 Live Shell 顯示 Unicode 替換字元或其他難以理解的字元	升級至 14.3 RU9
ESMAC-7043	檔案活動 [8003] 事件不再由連線到 Symantec Endpoint Detection and Response (EDR) 的 Mac 代理程式傳送。[14.3 RU8] 針對在 Symantec Endpoint Security (SES) 中向雲端主控台報告的 Mac 代理程式，觸發「完全傾印」以檢視 8003 事件。	架構以將事件傳送到 EDR 4.8 及更早版本的內部部署 Mac 代理程式，會在未來的 EDR 版本中增強。

Symantec Endpoint Protection 14.3 RU8 的新修正和元件版本

14.3 RU7 中的已知問題

Table 12: 14.3 版 RU7

問題 ID	說明	因應措施
SEP-82895	在還原 SEP 用戶端所隔離的檔案，接著對還原的檔案執行「自動防護」掃描後，SEP 用戶端並未偵測到病毒。[14.3 RU7] 在啟用「與 **Windows Defender** 共存」選項並從隔離區還原檔案時，會出現此問題。Windows Defender 會攔截「自動防護」偵測還原檔案中的病毒，但可以進行其自己的偵測。	1. 停用「與 **Windows Defender** 共存」選項。 2. 還原任何已在隔離區和已清除的檔案。 3. 重新啟用「與 **Windows Defender** 共存」。
SEP-82580	在「病毒和間諜軟體防護」政策中停用「與 **Windows Defender** 共存」選項後，Windows Defender 並未依預期停用。[14.3 RU7] 停用共存模式時，若啟用了「Windows Defender 竄改防護」，則「端點防護/安全代理程式」無法停用 Windows Defender，因為「Windows Defender 竄改防護」會攔截該動作。	如要允許「端點防護/安全代理程式」在停用共存模式時停用 Windows Defender，則必須停用「Windows Defender 竄改防護」。 或者，可以手動方式停用 Windows Defender。 請參閱：於「端點防護」中關閉共存模式時不會停用 Windows Defender
SEP-83786	「Windows 用戶端疑難排解 > **Web** 和雲端存取防護」頁面會顯示下列狀態訊息：`##### CTCv1 (#### Token)` [14.3 RU7]	請參閱：警告：在 SEP 用戶端 14.3 RU7 或更新版本上「Web 和雲端存取防護」中的「使用 CTCv1 (缺少註冊 Token)」警告

Symantec Endpoint Protection 14.3 RU7 中的新修正和元件版本

14.3 RU6 中的已知問題

Table 13: 版本 14.3 RU6

問題 ID	說明	因應措施
SEPLINUX-1468	EDR 功能尚不支援監視 NFS 檔案系統上的檔案系統活動。	在 14.3 RU6 及更新版本中，僅擷取檔案重新命名和刪除事件。
SEP-81247	如果您從 Windows 用戶端中移除進階下載防護功能，SEPM 仍會顯示進階下載防護功能已啟用。[14.3-RU6] 下載防護使用 IPS 來擷取有關正在存取檔案的資訊。如果移除「進階下載防護」，則不會移除 IPS。因此，「用戶端」頁面 >「用戶端」標籤仍會將「下載防護狀態」欄顯示為「已啟用 - 進階防護」。	您可以安裝「基本下載防護」和「入侵預防」功能，其功能與「進階下載防護」相同。

Symantec Endpoint Protection 14.3 RU6 的新修正和元件版本

14.3 RU5 中的已知問題

Table 14: 版本 **14.3 RU5**

問題 ID	說明	因應措施
SEP-79993	從 14.3 RU4 用戶端升級到 14.3 RU5 用戶端並匯入使用 SHA-256 指紋的檔案指紋清單時，系統鎖定清單不會正確攔截應用程式。這是因為 14.3 RU5 和更新版本用戶端使用 14.3 RU4 版本的 `sysfer` 和 `sysplant` 服務。	從 14.3 RU4 升級之後，重新啟動 14.3 RU5 和更新版本用戶端。
SEP-80222	在 Symantec Endpoint Protection Manager 14.3 RU5 所管理 14.3 RU4 Windows 用戶端上的「狀態」頁面會顯示下列錯誤：「`############`。」[14.3 RU5]	該問題是因為在 14.3 RU4 和更早版本中，SONAR 依賴於啟用的自動防護。 在 14.3 RU5 中，停用自動防護時，不再停用 SONAR。因此，當 14.3 RU4 用戶端從 Symantec Endpoint Protection Manager 14.3 RU5 接收到病毒和間諜程式防護政策時，將會啟用 SONAR，但用戶端仍會顯示錯誤。 在自動防護因政策被禁用和鎖定時，14.3 RU5 之前的安全代理程式警告主動型威脅防護將會失效
SEPLINUX-1502	在 SEP 14.3 RU4 和更舊版本中，當您對 Linux 代理程式執行蒐證命令時，該命令可能保留在「進行中」狀態延長一段時間。[14.3 RU5]	以下是此問題的變通方法： 1. 從 Symantec Endpoint Security (SES) 主控台取消該命令，並重新發佈該命令。 2. 允許命令在伺服器上逾時。 3. 登入代理系統，然後重新啟動 CAFDaemon。
SEPLINUX-1472	在 RHEL9 上執行智慧型更新小幫手 (Intelligent Updater) 指令碼時，主控台上會顯示一條訊息，指出系統上不存在 "ncompress" 可執行檔。[14.3 RU5]	自 RHEL9 起，`ncompress` 已被取代。如果正在執行 RHEL9，則必須獲得 `ncompress rpm`，並將其安裝在您的系統上以便智慧型更新小幫手執行。 RHEL9 不支援智慧型更新程式

14.3 RU4 中的已知問題

Table 15: 14.3 版 RU4

問題 ID	說明	因應措施
SEP-77602	攻擊面減少日誌 - 強化日誌大小會忽略政策設定，而且一律等於或大於 5MB。[14.3 RU4] 在 Symantec Endpoint Protection (SEP) 代理程式 14.3 版 RU4 中，攻擊面減少日誌大小上限為 5MB (5,120 KB)，即使用戶端日誌設定中的安全與風險日誌大小上限架構成小於 5,120 KB 也是一樣。如果值大於 5,120 KB，則會遵守該值。 發生這種情況的原因是，攻擊面減少日誌 (ASRman.log) 包含的事件數目多於其他安全與風險日誌 (avman.log、tdadman.log 等)。因此，若要保留足夠的事件，則需要較大的預設值。	除非將可架構的攻擊面減少值新增至用戶端日誌設定，否則 5 MB 最小值是臨時方式。之後，日誌將會是 5MB 或符合安全與風險日誌中所架構的值 (使用較大者)。 攻擊面減少日誌 - 強化日誌大小會忽略政策設定，而且一律等於或大於 5MB
	若停用自動防護，Symantec Endpoint Protection (SEP) 14.3 RU4 和更舊版本的用戶端會在其 SONAR 狀態顯示訊息「#######」。 顯示此訊息的用戶端由 Symantec Endpoint Protection Manager 14.3 RU5 或更新版本管理。 對於 14.3 RU4 及更新版本用戶端，停用自動防護時部分 SONAR 仍能正常運作，但 SONAR 元件效能會受影響。	請確認自動防護保持啟用狀態。
SEPLINUX-1488	智慧型更新小幫手無法重新啟動 RHEL6 上的 AMD 服務。[14.3 RU4]	如果正在執行 RHEL6，則必須在執行智慧型更新小幫手指令碼之後重新開機 sisamdagent 服務 (service sisamdagent restart)。
SEPLINUX-483	Linux 代理程式未與 DCS 伺服器進行通訊。[14.3 RU4] 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。不支援雙受管 DCS 和 SEP Linux。

適用於 Symantec Endpoint Protection 14.3 RU4 的新修正和元件

14.3 RU3 中的已知問題

Table 16: 14.3 版 RU3

問題 ID	說明	因應措施
SEP-72814	Endpoint Protection (SEP) 14.2 RU1 MP1 和更舊版本的用戶端不會採用用戶端升級政策中的「升級排程」設定。[14.3 RU3]	如需詳細資訊，請參閱： Endpoint Protection 14.3 RU1 MP1 和舊版用戶端未遵循用戶端升級政策
SEPM-433	當您按一下「進階安全性」頁面時，可能會出現含下列錯誤訊息的空白頁面：######## - ############ [含 Symantec Endpoint Security Complete 授權的 14.3 RU3] 如果 Symantec Endpoint Protection Manager 與 Data Center Security 用戶端安裝在相同電腦上，則 LiveUpdate 無法顯示「進階安全性」頁面內容，而且您無法在雲端主控台中註冊 SEPM。	架構 **DCS** 防護政策： 1. 在 Symantec Data Center Security (DCS) 伺服器管理員主控台中，開啟套用至 DCS 用戶端的防護政策。 2. 按一下「應用程式規則」。 3. 在「應用程式規則」面板中，選取「**Symantec Endpoint Protection**」項目。 4. 按下「編輯」。 5. 新增下列規則： – 程式路徑：%%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaEXE%% – 程式路徑：%%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaW%% 6. 輸入規則名稱和敘述作為 **SEPM** 主控台。 7. 將規則的其餘欄位空白。 8. 儲存政策，並將其套用至 DCS 用戶端。 9. 在「## 」指令中，停止並重新啟動 Symantec Endpoint Protection Manager 服務，如下所示： – net stop semsrv – net stop semapisrv – net stop semwebsrv – net stop semlaunchsrv – net start semsrv – net start semapisrv – net start semwebsrv – net start semlaunchsrv
	Endpoint Protection 14.3 RU3 Web 和雲端存取防護日誌會把 Windows 10 作業系統報告為 Windows 11。[14.3 RU3] 在 SEP 用戶端 Web 和雲端存取防護日誌時，如果在 Windows 11 裝置上安裝用戶端，則日誌會將作業系統顯示為 Windows 10。 在用戶端主控台上，按一下「**Web** 和雲端存取防護」>「選項」>「檢視日誌」。	

問題 ID	說明	因應措施
SEP-75086	將驗證影像相依性完整性緩和技術套用至 Windows 10 或 11 作業系統之後，無法啟動 Microsoft Edge 瀏覽器和 Google Chrome 瀏覽器。[14.3 RU3] Microsoft Edge 用來保護 Windows 作業系統的其中一種緩和技術是驗證影像相依性完整性技術。 對於執行 Symantec Endpoint Protection 用戶端 14.2 版 RU2 MP1 或更新版本的 Windows 10 或 11 電腦，如果啟用此選項，則不會啟動 Microsoft Edge 和 Google Chrome Web 瀏覽器。	若要確保 Microsoft Edge 啟動，請停用驗證影像相依性完整性技術。如需 Microsoft Edge 緩和技術的詳細資訊，請參閱：自訂攻擊防護 另請參閱：如果套用「驗證影像相依性完整性」緩和技術並安裝 SEP 14.2 RU2 MP1 或更新版本，則不會開啟 Microsoft Edge 和 Google Chrome
SEP-73327	您必須重新啟動無重新開機 Windows 用戶端來取得最新 EDR 事件。[14.3 RU3] 若要讓其他 ETW 事件可在 14.3 RU3 中使用，您必須重新啟動 Symantec Endpoint Protection 用戶端。在下列情況下，您必須重新啟動用戶端： • 如果已啟用 EDR，而且您將用戶端更新為 RU3。 • 已安裝 14.3 RU3，而且您啟用或停用 EDR。您必須重新啟動用戶端來啟用或停用剛新增的事件。	請參閱：可能需要重新開機才能開始查看 EDR 和 SEP 14.3 RU3 的一些 ETW 事件
SEP-74510	登入 Endpoint Protection Manager 而且用戶端在系統時間變更之後不再通訊時發生非預期伺服器錯誤。[14.3 RU3] 如果您將系統時鐘設定回前一個日期和/或時間，則可能會發生下列錯誤： • 在您登入 Symantec Endpoint Protection Manager 之後，出現非預期的伺服器錯誤。 • 用戶端未與 SEPM 通訊，這會報告 503 錯誤。	• 手動重新啟動 SEPM 服務。 • 請等到系統上的日期/時間經過系統上的原始時間，然後再重新予以設回。
ESMAC-3339	在 Mac 用戶端上，如果停用或啟用漏洞防護，則會遺失 VNC/螢幕共用連線。[14.3 RU3] 在 MacOS 12 和 MacOS 11.4 (ARM) 上觀察到問題。	

適用於 Symantec Endpoint Protection 14.3 RU3 的新修正和元件

14.3 RU2 中的已知問題

Table 17: 14.3 版 RU2

問題 ID	說明	因應措施
SEP-72531	下列錯誤訊息隨即顯示：`Symantec Endpoint Protection 14.3 # RU2 for Win64bit ##############` [14.3 RU2]	Symantec Endpoint Protection Manager 中出現來自多個版本的套件時，您無法刪除用戶端安裝套件。自 14.3 RU2 起，LiveUpdate 可以下載多個具有不同版次號碼的用戶端安裝套件，這些套件會顯示在「管理」頁面 >「安裝套件」>「用戶端安裝套件」表格。
SEP-72490	如果您使用「如果目前安裝的語言不受支援，則升級為英文」選項將語言不受支援的用戶端升級為英文，則 AutoUpgrade 會失敗。[14.3 RU2] 導致此問題的原因是用戶端語言使用所支援作業系統的語言 (在此情況下為日文)。AutoUpgrade 預期使用支援的語言，而不是英文。	請再次嘗試 AutoUpgrade，並關閉「如果目前安裝的語言不受支援，則升級為英文」選項。

問題 ID	說明	因應措施
	從 14.3 RU2 Symantec Endpoint Protection Manager (SEPM) 匯出用戶端安裝套件時，會出現下列警告訊息：「########## 」[14.3 RU2]	如果 Symantec Endpoint Protection Manager 與要用來匯出套件之主控台間的通訊中斷，則會發生此問題。請參閱： 從 Endpoint Protection Manager 匯出安裝套件時出現「用戶端安裝套件沒有內容。」警告
SEP-72292	將最新的用戶端安裝套件匯入至舊版 Symantec Endpoint Protection Manager 時出現錯誤。[14.3 RU2]	14.3 RU1 MP1 或更舊版本的 Symantec Endpoint Protection Manager 無法管理 Symantec Endpoint Protection 14.3 RU2 用戶端。
SEP-70385	將 Symantec Endpoint Protection Manager 升級到 14.3 RU2 之後，php-cgi.exe 會當機，並在事件檢視器中出現錯誤。[14.3 RU2] 14.3 RU2 用戶端中 17.4.1.1 版的 Microsoft ODBC Driver for SQL Server 會發生此問題。	請在 Windows 下載並安裝 17.7.2 版的 Microsoft ODBC Driver for SQL Server。 Microsoft ODBC Driver for SQL Server on Windows 的版本說明 升級到 14.3 RU2 之後，Endpoint Protection Manager 上發生 php-cgi.exe 當機
	如果您從 14.3 RU1 Symantec Endpoint Protection Manager 升級到更新版本之後，可能會出現「########## 」通知。[14.3 RU2] 從 14.3 RU1 Symantec Endpoint Protection Manager 或更舊版本升級到 14.3 RU2 或更新版本之後，管理員可能會開始接收到「########### 」通知。此問題僅適用於 Mac 用戶端。	升級到 Symantec Endpoint Protection Manager 14.3 RU2 之後，可能會出現「已重新命名用戶端電腦」通知
	自訂名稱可能會防止在升級到 14.2 或更新版本期間更新防火牆政策。[14.3 RU2] 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。
	Rosetta 可能會攔截 Apple Silicon (M1) 裝置上的 Mac 代理程式安裝，並出現下列錯誤：「Apple M1 晶片上不支援這版 Symantec Agent for Mac。」[14.3 RU2]	如需詳細資訊，請參閱： Rosetta 可能會攔截在Apple Silicon (M1) 裝置上安裝 Mac 用戶端

14.3 RU1 中的已知問題

Table 18: 14.3 版 RU1

問題 ID	說明	因應措施
SEP-67175	有些 EDR 事件不會出現在用戶端上。[14.3 RU1]	Symantec Endpoint Protection 用戶端必須執行 Windows 10 組建 14393 或更新版本，才能收集 Symantec EDR Event Tracing for Windows (ETW) 事件。
SEP-68700	Web 和雲端存取防護功能有一些限制。[14.3 RU1] • Symantec Cloud Secure Web Gateway (Cloud SWG) 交付於 IPv4 而非 IPv6。 • 通道重新導向方法： – 在 Windows 10 x64 版本 1703 及更新版本 (每半年服務通道)、Windows 11、SEP Mobile 和 Mac 上執行。 [SEP-67927] – 不支援啟用 HVCI 的 Windows 10 64 位元裝置。[SEP-67648] – 將 Symantec Endpoint Protection 用戶端的出埠流量在用戶端的防火牆或 URL 信譽規則對其進行評估之前重新導向到 Cloud SWG。反之，會根據 WSS 防火牆和 URL 規則評估該流量。例如，如果 SEP 用戶端防火牆規則攔截了 google.com，而 WSS 規則允許 google.com，則該用戶端允許使用者存取 google.com。仍然由 Symantec Endpoint Protection 防火牆處理至用戶端的入埠本地流量。[SEP-67488] – SAML 驗證取代網頁驗證入口網站，驗證 Symantec Endpoint Protection 用戶端的使用者和群組。 – 如果用戶端電腦使用通道方法連線至 WSS 並裝載虛擬機器，則每個訪客使用者都必須安裝 Cloud SWG 入口網站中提供的 SSL 憑證。 – 本機網路 (如主目錄或 Active Directory 驗證) 的流量不會重新導向。 – 與 Microsoft DirectAccess VPN 不相容。	
SEP-68965	從 14.2.x 升級到 14.3 MP1 和更新版本之後，用戶端註冊項目重複。[14.3 RU1] 將 Symantec Endpoint Protection 用戶端從 14.2.x 升級到 14.3 MP1，然後接著在 Symantec Endpoint Protection Manager 的「用戶端」頁面上為這些用戶端建立重複的代理程式註冊項目。	沒有任何功能性影響，您可以繼續為 14.3 RU1 用戶端使用新項目。Symantec Endpoint Protection 會移除較舊的代理程式項目。
SEP-75205	當您從預設 SEPM 內嵌資料庫升級到 Microsoft SQL Server Express 資料庫時，可能會出現下列錯誤：############### [14.3 RU1] 因為 SQL Server Express 密碼需求使用 Windows 密碼需求，所以發生此錯誤。如果預設資料庫密碼需求比預設 SEPM 安裝程序檔所使用的密碼需求還要嚴格，則會發生此錯誤。	請參閱：將 SEPM 內嵌資料庫升級到 14.3 RU1 時，請參閱錯誤「指定的密碼不符合強式密碼需求」
SEP-69125	暗網中的 Symantec Endpoint Protection Manager 會將舊的用戶端入侵偵測系統 (CIDS) 內容下載到新用戶端，因為 LiveUpdate 在升級期間未執行。[14.3 RU1] 當 14.3 RU1 Symantec Endpoint Protection Manager 或更新版本無法訪問 Internet 或 LiveUpdate Administrator (LUA) 伺服器時，其會將舊的不相容的內容保留在其快取中。此舊內容通常會傳送至新用戶端。若要更新管理伺服器快取中的內容，請手動下載經過驗證的病毒定義檔和 CIDS.jdb 檔。	若要確保新用戶端不會取得舊內容，請先在 SEPM 上手動安裝 CIDS.jdb 檔，然後再安裝新用戶端或升級舊用戶端。請參閱： 下載 .jdb 檔案以更新 Endpoint Protection Manager 的定義檔

問題 ID	說明	因應措施
	停用網路介面卡時，您無法登入 Symantec Endpoint Protection Manager (SEPM)。[14.3 RU1] 如果在安裝 Symantec Endpoint Protection Manager 之後無法登入主控台，則會出現以下錯誤訊息： `#########` 如果在安裝 SEPM 時將電腦的網路介面卡停用，則可能會出現此問題，因為 SEPM 可防止產生伺服器憑證。 若憑證驗證於安裝期間失敗，則會出現此問題。因為若停用所有網路卡，SEPM 安裝程式便無法取得主機名稱。`...\apache\conf\server.crt`檔案中，「發出目標」和「核發者」欄位皆為空白。	啟用至少一個網路配接卡，移除 SEPM，然後重新安裝 SEPM。 請參閱：如果在未啟用 NIC 的伺服器上安裝 SEPM 登入，則會發生非預期的伺服器錯誤
SEP-68670	當您解除安裝 SEPM 以及使用選項來移除預設資料庫並離開 SQL Server Express 實例時，會發生下列錯誤：「`################`」。[14.3 RU1] 如果解除安裝 Symantec Endpoint Protection Manager 並選取「僅移除資料庫，並保留與 **SEPM** 一起安裝的 **SQL Server Express** 執行個體」選項，您可能會看到以下錯誤：「`################`」。新增預設使用者 DBA 的憑證之後，且該憑證可能與使用者權限相關時，將發生此問題。	透過執行 SEPM setup.exe 並在解除安裝期間按一下「僅移除資料庫，並保留與 **SEPM** 一起安裝的 **SQL Server Express** 執行個體」選項。
SEP-70996	用於全新安裝的升級安裝套件將安裝預設功能集。[14.3 RU1 MP1 及更早版本] 如果您勾選「更新時保留現有用戶端功能」選項來建立升級安裝套件，並使用此套件進行全新安裝，則預設功能集將安裝在您的用戶端裝置上。	如果要安裝自訂功能集，則必須為全新安裝建立一個單獨的安裝套件。
SEP-72481	如果您自動將語言不受支援的用戶端升級為英文，則用戶端會繼續使用英文顯示定義的日期設定。[14.3 RU1 和更新版本]	解除安裝舊版用戶端，並手動安裝新的英文用戶端安裝套件。此外，應該修正自動升級的用戶端。

適用於 Symantec Endpoint Protection 14.3 RU1 MP1 的新修正和元件

適用於 Symantec Endpoint Protection 14.3 RU1 的新修正和元件

14.3 及較舊版本中的已知問題

Table 19: 版本 **14.3.x** 和更舊版本

問題 ID	說明	因應措施
SEP-61473	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。	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。 如需詳細資訊，請參閱： 啟用 FIPS 模式後，從 2017 版升級到 2019 版的 SQL 失敗
SEP-61106	Symantec Endpoint Protection Manager 遠端主控台不再支援 32 位元 Windows 平台。[14.3] 自 14.3 及更新版本中，如果執行 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。	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。」
SEP-60396	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」	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 內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
	如果您在與 WSS Agent 相同的電腦上安裝 SEP，則獨立式 Symantec WSS Agent 會攔截 Symantec Endpoint Protection 用戶端安裝。 Web 和雲端存取防護元件使用與獨立式 Symantec WSS Agent (WSSA) 相同的檔案。Web 和雲端存取防護預設會安裝在 Symantec Endpoint Protection 和 Symantec Endpoint Security 雲端主控台中。如果在端點上安裝 Web 和雲端存取防護，則無法安裝 WSSA。同理，如果安裝 WSSA，則不會安裝 Web 和雲端存取防護。	您可以使用下列其中一種方法，從現有端點移除 Web 和雲端存取防護功能，而不需要解除安裝整個用戶端： • 在 Symantec Endpoint Protection Manager 中，建立未包括「Web 和雲端存取防護」的「用戶端安裝功能集」，然後將它套用至端點。請參閱： 新增或移除現有 Endpoint Protection 用戶端的功能 • 下列指令行選項使用用戶端安裝檔案來移除「Web 和雲端存取防護」：`setup.exe /s /v" REMOVE=NTR /qn"`

問題 ID	說明	因應措施
SEP-61175/61403	Symantec Endpoint Protection 14.3 Windows 用戶端安裝可能會失敗，除非您先安裝 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，才能更新 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。無論是首次安裝用戶端或從較舊版本自動升級，安裝都有可能失敗。若要在此類電腦上執行 Windows Update，則必須預先安裝相關修正程式。	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
CDM-42467	如果您使用混合管理選項、代理伺服器或周邊防火牆，則允許 Symantec Endpoint Security 中的 URL。[14.3] 隨著 Broadcom 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。 已在 Symantec Endpoint Security 雲端主控台註冊 Symantec Endpoint Protection Manager 時，會發生此問題。	您必須在下列情況將用戶端升級至版本組建 14.3 MP1 (14.3.1169.0010) 或更新版本。 • 在雲端主控台中註冊了您的內部部署 Symantec Endpoint Protection Manager 網域時，您可以使用 Symantec Endpoint Security 來管理用戶端和政策。 • 您使用代理伺服器。 您允許完全雲端管理或混合管理代理程式中的 URL，也允許代理伺服器和/或周邊防火牆中的 URL。請參閱： • Endpoint Protection (SEP) 和 Endpoint Protection (SES) 所需的外部 URL • 將 Symantec Endpoint Protection 用戶端從受管的內部部署轉換為雲端管理
	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。
	Microsoft Edge 意外地允許在啟用強化的情況下下載 PDF。[14.2 RU1 MP1 和更新版本] 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。

適用於 Symantec Endpoint Protection 14.3 MP1 的新修正和元件

適用於 Symantec Endpoint Protection 14.3 的新修正和元件

說明文件

您可以在 Broadcom Symantec Security Tech Docs Portal 上找到文件。

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**」。

若要尋找 PDF 檔案，請前往「相關文件」頁面。

若要尋找 Symantec Endpoint Protection Manager 資料庫綱要，請聯絡支援部門。

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

如果是混合選項：

- *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

取得相關資訊的位置

下表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 20: 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	相關文件頁面 對於其他語言，請按一下「語言」下拉式功能表。
技術支援	Broadcom 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連絡選項。
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	端點防護 - Symantec Enterprise (broadcom.com)


Symantec
by Broadcom Software