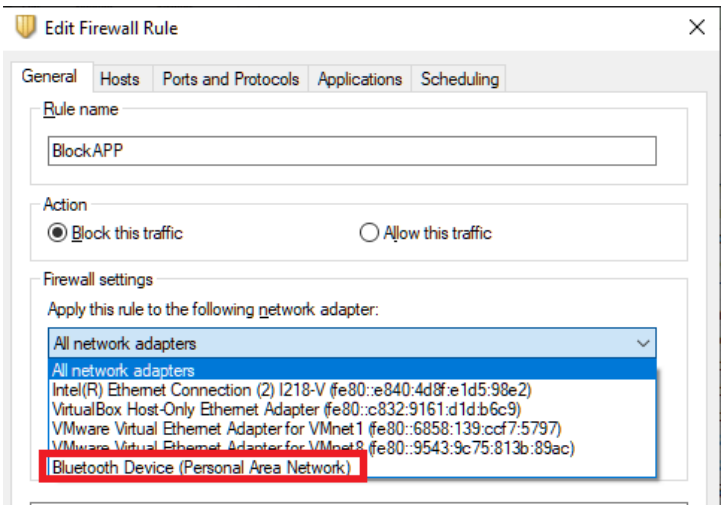
Symantec Endpoint Protection 14.3 RU4 新功能

最新更新日期：2022 年 4 月 4 日

防護功能

- 改進使用行為規則的防護，以防止損毀某些檔案類型 (如 Microsoft Word 和 .jpg) 以及大容量寫入。
  SEP 防禦「就地取材攻(living-off-the land)」技術所使用的勒索軟體防護
- Web 和雲端存取防護政策現在使用 Symantec Web Security Service (WSS) Agent 的最新版本：版本 7.x。7.x 版本提供許多增強功能。
  WSS -- 最近功能
- 您可以使用 SymDiag 來收集具有整合式 WSS 元件之 SEP 用戶端的除錯和疑難排解資訊。SymDiag 會收集封包擷取 (PCAP) 檔案，而賽門鐵克技術支援使用這些檔案來協助您分析和修正連線問題。
  SEP 用戶端健康狀態疑難排解和檢查
- 最近的鎖定勒索軟體攻擊衝擊越來越多地使用 Living Off the Land (LOTL) 技術，而這些技術利用受信任應用程式和工具來執行攻擊鏈結的各種階段。賽門鐵克已引進突破性的端點技術：調適型防護。調適型防護可協助企業防止攻擊者以惡意方式使用受信任應用程式和工具，而不影響一般使用者和公司營運。
  Symantec Endpoint Protection 使用簡化的工作流程，使您能夠快速且輕鬆地將 SEP 註冊到雲端主控台。此工作流程對 Symantec Endpoint Security Complete 中 ICDm 雲端主控台的完整益處提供不衝突的存取。若要深入瞭解此解決方案以及它在您環境中的實作方式，請參閱：在 Symantec Endpoint Protection 中啟用調適型防護。
- 在防火牆規則中選取網路配接卡，以攔截透過藍牙裝置存取的未過濾流量。
  - 在 SEPM 防火牆政策中，架構可指定「全部配接卡」或「乙太網路」的防火牆規則。在「政策」頁面 >「政策元件」標籤上，您可新增特定藍牙裝置名稱。

  - 在 SEP 用戶端上，選取「一般」標籤 >「藍牙裝置 (個人區域網路)」網路配接卡，以架構防火牆規則。



- 為了保護 SEP 用戶端免受勒索軟體攻擊，SEPM 會提醒您設定密碼，以要求用戶端使用者在執行幾項任務前使用密碼。這些任務包括開啟或解除安裝用戶端、停止用戶端服務、匯入或匯出政策，或是匯入用戶端通訊設定。需要密碼可保護用戶端免受可在攻擊執行前停止 SEP 服務的勒索軟體攻擊。若要設定密碼，請按一下「用戶端」頁面 >「政策」標籤上的「密碼」。
  每隔六個月就會接收到下列通知，提醒您至少啟用一個密碼選項：一些 Symantec Endpoint Protection 群組未獲指派密碼。如果您為所有群組都設定此密碼，則不會顯示通知。這些通知會顯示在「監視器」>「通知」標籤上。
  使用密碼保護 Symantec Endpoint Protection 用戶端

Symantec Endpoint Protection Manager (SEPM)

- 已為 Symantec Endpoint Protection Manager、Windows、Mac 和 Linux 用戶端新增回簡體中文和繁體中文的語言支援。
- 已升級下列第三方元件：Apache Commons Compress、Apache Server、log4j、Spring Framework、Spring Security、Spring Boot 和 OpenJDK。
- 指定電子郵件伺服器所連線之電子郵件通訊協定的選項標籤已變更。「使用 STARTTLS」和「使用 SMTPS」已取代「使用 TLS」和「使用 SSL」。這些選項位於「管理員」>「伺服器」>「編輯伺服器屬性」>「電子郵件伺服器」標籤。
- 14.3 RU4 是在 Windows Server 2008 R2 上安裝或升級之 SEPM 的最後一個版本。賽門鐵克建議您升級為含 TLS 1.2 支援的較新 Windows 版本，以進行更安全的通訊。

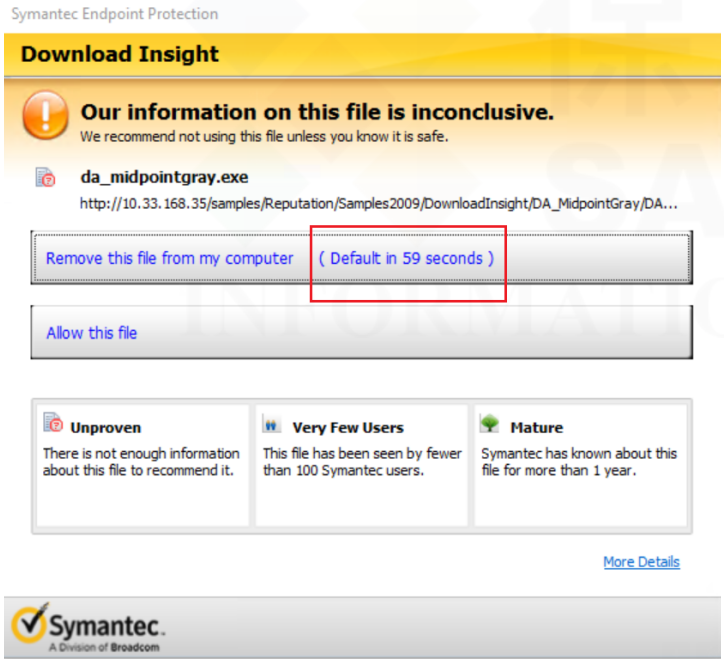
用戶端和平臺更新

Windows 用戶端

- 如果您要在 Windows、Mac 或 Linux 電腦上安裝 Symantec Endpoint Protection 用戶端 14.3 版 RU3 或更新版本，則不需要重新啟動用戶端。如果您要在 Windows、Mac 或 Linux 電腦上升級 Symantec Endpoint Protection 用戶端 14.3 版 RU3 或更新版本，則在大部分情況下不需要重新啟動用戶端。
  從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦
- 如果您在雲端中註冊 SEPM 以從 Symantec Integrated Cyber Defense Manager (ICDm) 管理政策，則系統政策會顯示在「疑難排解」>「混合管理」面板中。您只能從雲端主控台新增系統政策，而不是 SEPM。
- Windows 用戶端引進新的日誌：攻擊面減少日誌。此日誌會取代 SEP 用戶端上安裝

Data Center Security (DCS) 時顯示的強化事件檢視器。攻擊面減少日誌不包括「覆寫和例外要求」選項或「賽門鐵克信任的檔案」選項。若要存取用戶端上的日誌，請按一下「檢視日誌 > 應用程式強化」。只有在您從 ICDm 雲端主控台管理用戶端時，才能看到日誌。

- Windows 用戶端現在正確地切換到某個位置，而此位置搭配使用 OR 關係與 DNS 搜尋、DNS 尾碼、NIC 說明、使用者和無線 SSID 準則。
- 下載鑑識預設允許用戶端使用者有 3 分鐘的時間可以在移除可疑檔案之前允許該檔案。在 14.3 RU4 中，「從電腦中移除檔案」訊息後面接著用戶端使用者必須做出決策的時間量。



- 您無法再重新安裝 12.1.x 用戶端。

Mac 用戶端

> **附註**
> 14.3 RU4 沒有 Mac 用戶端版本。

Linux 用戶端

> **附註**
> Symantec Endpoint Protection Manager 14.3 RU4 隨附 14.3 RU3 版的 Symantec Endpoint Protection for Linux 用戶端。2022 年 2 月提供 Linux 用戶端 14.3 RU4 時，LiveUpdate 會將 Linux 用戶端安裝套件下載到 Symantec Endpoint Protection Manager。

- Symantec Agent for Linux 14.3 RU4 和 Symantec Data Center Security Linux Agent 6.9.2 可以共存於單一工作站或伺服器上。您可以從管理主控台同時管理 Symantec Agent for Linux 14.3 RU4 和 Symantec Data Center Security Linux Agent 6.9.2。

刪除的功能

- 已從「病毒和間諜軟體防護政策」>「其他」頁面移除「顯示 Windows 資訊安全中心內的防毒警示」選項。用戶端不再支援此設定。
  其他設置
- 已移除「用戶端」頁面 >「用戶端」標籤 >「外部通訊」中「當私用伺服器不可用時，使用賽門鐵克伺服器」選項的警告。不再支援 12.1.5 用戶端。

說明文件

- 《Symantec Endpoint Protection for Mac 用戶端指南》和《Symantec Endpoint Protection for Linux Agent 指南》PDF 檔案翻譯為法文、日文、葡萄牙文、西班牙文、簡體中文和繁體中文。
- 若要尋找目前和先前 Symantec Endpoint Protection Manager 資料庫綱要，請聯絡支援部門。
  Symantec Endpoint Protection 所有版本中的新功能

原廠網址：https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/Whats-new-for-Symantec-Endpoint-Protection-14-3-RU4.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。2022/4

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588