Symantec™ Endpoint Protection 14.2.1 安裝與管理指南

Symantec

Symantec Endpoint Protection 安裝與管理指南

產品版本 14.2.1 (14.2 RU1)

說明文件版本：1

此文件上次更新的日期： 三月 21, 2019

法律聲明

Copyright © 2019 Symantec Corporation. 版權 © 2019 賽門鐵克公司。All rights reserved. 版權所有。

Symantec、Symantec 標誌、勾選記號標誌及 TruScan 均為賽門鐵克或其附屬公司在美國及其他國家/地區的商標或註冊商標。其他名稱可能為其個別所有者的商標。

本賽門鐵克產品可能包含第三方軟體 (以下稱為「第三方程式」)，賽門鐵克在此聲明其所有權歸第三方所有。部分第三方程式係採開放原始碼或免費軟體授權方式取得。本軟體隨附之授權許可協議並未改變依開放原始碼或免費軟體授權所規定之任何權利或義務。請參閱本說明文件之「第三方版權聲明附錄」或本賽門鐵克產品隨附之讀我檔，以取得第三方程式相關資訊。

本文件中所述產品的散佈受到授權許可協議的規範，限制其使用、複製、散佈及解譯/逆向工程。未事先獲得賽門鐵克公司及其授權者 (如果有) 的書面授權，本產品的任何部分均不得以任何方式、任何形式複製。

本文件完全依「現狀」提供，不做任何所有明示或暗示的條件、聲明及保證，其中包含在任何特定用途之適售性與適用性的暗示保證、任何特定用途或不侵害他人權益，除了此棄權聲明認定的不合法部分以外。賽門鐵克公司對與提供之效能相關的意外或必然損害，或這份說明文件的使用，不負任何責任。本說明文件所包含的資訊若有變更，恕不另行通知。

根據 FAR 12.212 定義，本授權軟體和文件係「商業電腦軟體」，並受 FAR 第 52.227-19 節「商業電腦軟體限制權利」和 DFARS 第 227.7202 節 「商業電腦軟體和商業電腦軟體文件」中的適用法規，以及所有後續法規中定義的限制權利的管轄，而不論賽門鐵克是以內部部署還是託管服務形式提供。美國政府僅可根據此協議條款對授權許可的軟體和文件進行任何使用、變更、複製發行、履行、顯示或披露。

賽門鐵克公司
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com/region/tw

Symantec 支援

知識庫文章和 Symantec Connect

聯絡技術支援之前，您可以在我們的線上知識庫中找到免費內容，包括疑難排解文章、解決方案文章、警示和產品手冊。在下列 URL 的搜尋方塊中，輸入您的產品名稱：

https://support.symantec.com/

透過以下 URL，存取我們的部落格和線上論壇，以與其他客戶、合作夥伴和賽門鐵克員工密切討論廣泛的主題：

https://www.symantec.com/connect/

技術支援和企業客戶支援

Symantec 支援全年無休維護全球支援中心。「技術支援」的主要角色是回應有關產品特性與功能的特定查詢。企業客戶支援可協助解決非技術性問題，例如授權啟用、軟體版本升級、產品存取和續購。

聯絡 Symantec 支援部門之前，請參閱：

https://entced.symantec.com/default/ent/supportref

若要聯絡 Symantec 支援，請參閱：

https://support.symantec.com/en_US/contact-support.html

目錄

1

Symantec Endpoint Protection 簡介

本章包含以下主題：

什麼是 Symantec Endpoint Protection？

Symantec Endpoint Protection 是用戶端伺服器解決方案，可保護網路中的筆記型電腦、桌上型電腦和伺服器免於惡意軟體、風險和漏洞的危害。Symantec Endpoint Protection 結合了病毒防護和進階威脅防護，能主動保護用戶端電腦的安全，使其不受病毒、病蟲、特洛伊木馬程式和廣告軟體等已知和未知威脅的攻擊。Symantec Endpoint Protection 甚至能防止可躲避傳統安全措施的最複雜攻擊，如 Rootkit、零時差攻擊和變種的間諜軟體。

Symantec Endpoint Protection 具備低維護和高效能的優點，能透過網路通訊自動保護實體系統與虛擬系統使其免遭攻擊。Symantec Endpoint Protection 提供有效率且易於部署和使用的管理解決方案。

請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。

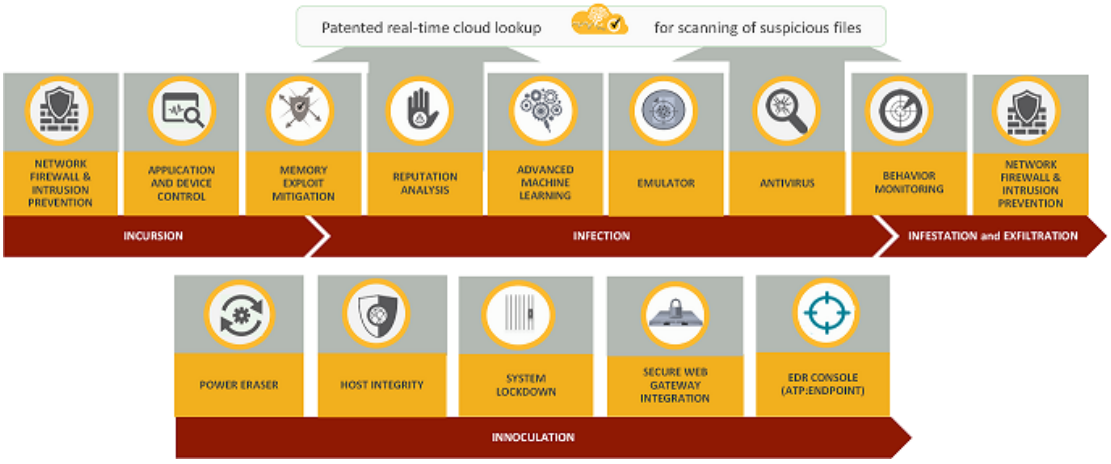
請參閱第 26 頁的「Symantec Endpoint Protection 架構元件」。

Symantec Endpoint Protection 技術如何保護您的電腦

Symantec Endpoint Protection 的已知和未知威脅核心防護功能採用分層方式進行防範。全面方式可在攻擊之前、期間和之後保護網路。Symantec Endpoint Protection 藉由提供工具，在任何攻擊入侵之前增加您的安全態勢，降低您的風險暴露程度。

若要針對網路中的電腦取得完整防護，請始終啟用所有防護。

圖 1-1 Symantec Endpoint Protection 如何透過分層防護阻止目標式攻擊和零時差威脅



Symantec Endpoint Protection 技術可防範哪些類型的攻擊？

Symantec Endpoint Protection 使用以下整體安全方式，透過下列階段跨越整個攻擊鏈保護您的環境：入侵、感染、侵擾和外滲，以及矯正和感染。

第 1 階段：入侵

在入侵階段期間，駭客通常會使用目標攻擊 (例如社交詐騙、零時差弱點、SQL 插入、鎖定惡意軟體或其他方式) 中斷組織網路。

Symantec Endpoint Protection 會在攻擊進入系統之前使用以下技術防範攻擊：

- **入侵預防/防火牆 (網路威脅防護)**：分析所有內送流量和外寄流量並提供瀏覽器防護，以便此類威脅在電腦上執行之前予以攔截。以規則為基礎的防火牆和瀏覽器防護可防範網頁式攻擊。
  請參閱第 325 頁的「管理入侵預防」。
  請參閱第 288 頁的「管理防火牆防護」。
- **應用程式控制**：控制檔案存取和登錄存取，以及允許程序如何執行。

請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。
請參閱第 433 頁的「設定應用程式控制」。

- **裝置控制**：限制存取以選取硬體，並控制哪些類型的裝置可上傳或下載資訊。
  請參閱第 463 頁的「管理裝置控制」。
- **記憶體攻擊緩和**：處理廠商未修正之常用軟體中的零時差攻擊行為，例如 Heap Spray、SEHOP 覆寫和 Java 攻擊。
  請參閱第 339 頁的「使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊」。

第 2 階段：感染

在目標式攻擊中，駭客通常會使用社交詐騙、零時差弱點、SQL 插入、鎖定惡意軟體或其他方式中斷組織網路。

Symantec Endpoint Protection 會使用下列技術，在攻擊感染您的系統之前偵測和防禦這些攻擊：

- **記憶體攻擊緩和**：偵測惡意軟體。
- **檔案信譽分析 (Insight)**：以使用 Symantec Global Intelligence Network 的人工智慧為基礎。此進階分析可從使用者、網站和檔案檢查數以億計的相關聯連結，以識別和抵禦快速變化的新惡意軟體。透過分析金鑰屬性 (例如檔案下載的原始點)，賽門鐵克可在某個檔案抵達用戶端電腦之前，準確地識別該檔案是良好還是無效檔案，並指派信譽分數。
  請參閱第 380 頁的「管理「下載鑑識」偵測」。
- **進階機器學習**：分析 Global Intelligence Network 中所包含的上萬億良好檔案和無效檔案的範例。進階機器學習是一項無需簽名的技術，可在執行前攔截新惡意軟體變體。
  請參閱第 384 頁的「Symantec Endpoint Protection 如何使用進階機器學習？」。
- **高速模擬**：使用變種自訂封包程式偵測隱藏的惡意軟體。掃描程式在導致威脅出現的輕量型虛擬機器中執行每個檔案 (以毫秒為單位)，從而改進偵測率和效能。
  請參閱第 386 頁的「Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？」。
- **防毒檔案防護 (病毒和間諜軟體防護)**：使用以特徵為基礎的防毒和檔案啟發式技術來尋找和根除系統上的惡意軟體，以防範病毒、病蟲、特洛伊木馬程式、間諜程式、Bot 傀儡程式、廣告軟體和 Rootkit。
  請參閱第 357 頁的「在用戶端電腦上管理掃描」。
  請參閱第 359 頁的「關於掃描和即時防護的類型」。
- **行為監控 (SONAR)**：利用機器學習提供零時差防護，透過在執行時即時監控將近 1,400 個檔案行為來判斷檔案風險，以阻止新威脅和未知威脅。
  請參閱第 425 頁的「管理 SONAR」。

第 3 階段：侵擾和外滲

資料外滲是對電腦中的資料進行未經授權的傳輸。一旦入侵者控制這些目標系統，便可能會竊取智慧財產或其他機密資料。攻擊者會使用擷取的資訊進行分析，然後進一步侵入或詐騙。

- **入侵預防/防火牆**：攔截透過網路傳遞的威脅。
- **行為監控**：協助阻止感染散佈。

第 4 階段：矯正和感染

Symantec Endpoint Protection 包含單一主控台和代理程式，可針對作業系統、平台和任意規模的企業提供防護。

- **Power Eraser**：可遠端觸發的主動工具，用於解決進階持續性威脅和矯正頑固的惡意軟體。
  請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。
- **主機完整性**：透過強制執行政策、偵測未經授權的變更以及執行損毀評估，確保端點受到保護且符合標準。然後，主機完整性會隔離不符合需求的受管系統。
  請參閱第 522 頁的「主機完整性的運作方式」。
- **系統鎖定**：允許許可清單中的應用程式 (已知良好) 執行，或攔截黑名單中的應用程式 (已知無效) 使其無法執行。不論哪種模式，系統鎖定都會使用總和檢查碼和檔案位置參數，以驗證應用程式通過核准或未經核准。系統鎖定對於只需執行單一應用程式的資訊站很有用。
  請參閱第 445 頁的「架構系統鎖定」。
- **Secure Web Gateway 整合**：使用可程式化 REST API 以便可與 Secure Web Gateway 進行整合，來協助快速阻止用戶端電腦中的感染散佈。
- **EDR 主控台整合**。Symantec Endpoint Protection 與 Symantec Endpoint Detection and Response 整合，旨在透過排列攻擊的優先順序來更快地偵測、回應和攔截目標式攻擊和進階持續性威脅。EDR (Endpoint Detection and Response) 功能會內建到 Symantec Endpoint Protection，可使其無須部署其他代理程式。
  請參閱第 445 頁的「架構系統鎖定」。

Symantec Endpoint Protection 技術可防範哪些類型的攻擊？

表 1-1 顯示哪些類型的 Symantec Endpoint Protection 技術可防範哪些類型的攻擊。

表 1-1 每種 Symantec Endpoint Protection 技術可防範哪些類型的攻擊？

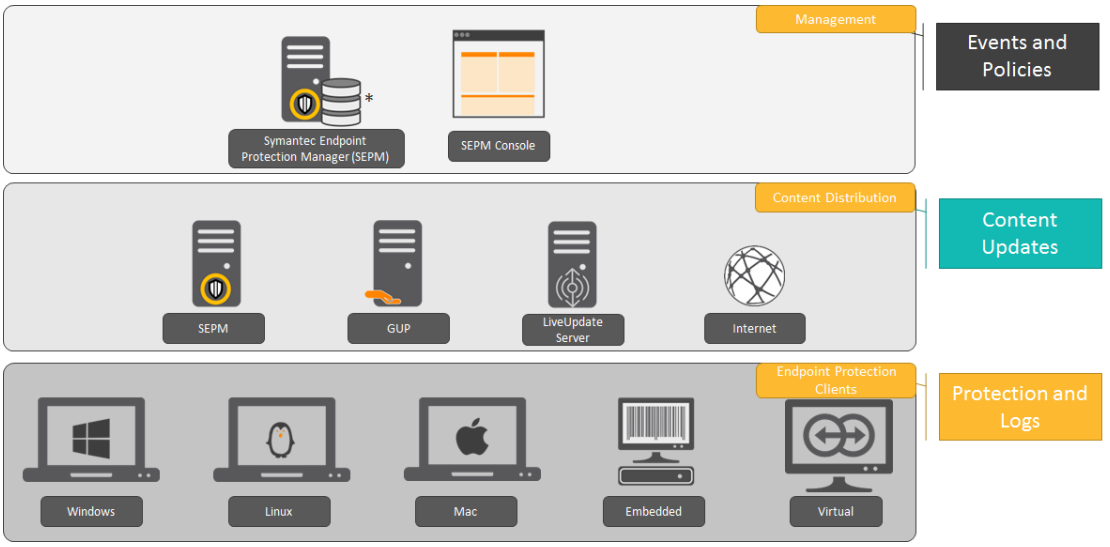
攻擊	進階機器學習	啟發式	入侵預防	網路保護	政策鎖定
零時差	√	√	√		√
社交詐騙	√	√	√	√	√
勒索軟體	√	√		√	√
目標式攻擊	√	√	√		√
進階持續性威脅	√	√	√		

攻擊	進階機器學習	啟發式	入侵預防	網路保護	政策鎖定
偷渡式下載		√	√		

Symantec Endpoint Protection 架構元件

Symantec Endpoint Protection 架構使用三個功能群組的元件。部分元件屬於多個群組，因為這些元件是多功能的。

圖 1-2 Symantec Endpoint Protection 元件



* Symantec Endpoint Protection Manager 可以使用內嵌資料庫或 Microsoft SQL Server。

主要產品元件

表 1-2 主要元件

元件	敘述
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager 是管理伺服器，用於為連線至貴公司網路的用戶端電腦管理事件、政策和用戶端註冊。 Symantec Endpoint Protection Manager 包含下列子元件： ■ 管理伺服器軟體用於提供連入及連出用戶端電腦和主控台的安全通訊。 ■ 主控台是管理伺服器的介面。 主控台軟體會協調並管理安全性政策、用戶端電腦、報告、日誌、角色和存取、管理功能以及安全性。 您也可以安裝遠端主控台，並從具有網路連線的任何電腦，使用它來登入管理伺服器。 ■ 內嵌資料庫隨 Symantec Endpoint Protection Manager 一起安裝，用於儲存安全性政策和事件。您也可以安裝 SQL Server 資料庫來取代內嵌資料庫。對於具有 1000 部以上電腦的較大型組織，建議使用 SQL Server。 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
Symantec Endpoint Protection 用戶端	Symantec Endpoint Protection 用戶端會提供解決方案的安全防護部分。用戶端會從 Symantec Endpoint Protection Manager 下載政策，有時為內容，並且在 Windows、Mac 和 Linux 上執行。

請參閱第 22 頁的「什麼是 Symantec Endpoint Protection？」。

選用產品元件

Symantec Endpoint Protection 可讓用戶端從管理伺服器、群組更新提供者、內部 LiveUpdate 伺服器或 Internet 下載內容。

表 1-3 選用元件及其功能

元件	敘述
LiveUpdate Administrator	LiveUpdate Administrator 可從內部 LiveUpdate 伺服器下載定義檔、特徵和其他內容，並將更新派送至用戶端電腦。您可以在大型網路中使用內部 LiveUpdate 伺服器，以減輕 Symantec Endpoint Protection Manager 負載。如果您的組織執行多個賽門鐵克產品且這些產品也使用 LiveUpdate 更新用戶端電腦，則您也應使用內部 LiveUpdate 伺服器。 您可以從下載 LiveUpdate Administrator (LUA) 取得 LiveUpdate Administrator。 請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。 請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

元件	敘述
群組更新提供者 (GUP)	群組更新提供者有助於在組織內部派送內容，對於位於頻寬最低的遠端位置的群組特別有用。有許多用戶端的組織可能希望對 Windows 用戶端使用「群組更新提供者」(GUP)。 GUP 會減輕管理伺服器的負載，而且比內部 LiveUpdate 伺服器容易設定。 請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。
Symantec Endpoint Protection 雲端主控台	雲端主控台提供雲端式管理，可延伸 Symantec Endpoint Protection 功能，以偵測並矯正您環境中的新興威脅。 若要使用雲端主控台，您必須首先註冊每個 Symantec Endpoint Protection Manager 網域。 請參閱第 498 頁的「Symantec Endpoint Protection 14.2 雲端主控台簡介」。 請參閱第 499 頁的「在 Symantec Endpoint Protection Manager Console 的雲端主控台中註冊 14.1/14.2 網域」。

Symantec Endpoint Protection 也隨附多項工具，可協助您提升安全性和管理產品。

請參閱第 718 頁的「Symantec Endpoint Protection 隨附的工具有哪些？」。

請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。

取得相關資訊的位置

表 1-4 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。

表 1-4 Symantec 網站資訊

資訊類型	網站連結
試用版	Trialware (14.x)

資訊類型	網站連結
手冊和說明文件更新	**英文：** ■ 賽門鐵克產品說明文件 ■ Symantec Endpoint Protection 12.1.x 所有版本的產品指南 ■ Symantec Endpoint Protection 14.x 所有版本的產品指南 **其他語言：** ■ 巴西葡萄牙文 ■ 簡體中文 ■ 繁體中文 ■ 法文 ■ 德文 ■ 義大利文 ■ 日文 ■ 韓文 ■ 西班牙文 *捷克文、波蘭文和俄文檔案位於英文頁面。
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 Security Center
訓練	■ 賽門鐵克教育服務 存取訓練課程、線上產品說明庫等。
Symantec Connect 論壇	Endpoint Protection

2

Symantec Endpoint Protection 入門指南

本章包含以下主題：

第一次在 Symantec Endpoint Protection 上啟動並執行

您應評估安全性需求，並判斷預設設定是否提供了所需的效能和安全性平衡。有一些效能增強作業可以於安裝 Symantec Endpoint Protection Manager 後立即進行。

立即執行下列工作以安裝和保護網路中的電腦：

- 步驟 3：新增群組、政策和位置
- 步驟 4：變更通訊設定以增加效能
- 步驟 5：啟用產品授權
- 步驟 6：決定用戶端部署方法
- 步驟 7：準備用戶端進行安裝
- 步驟 8：部署並安裝用戶端軟體
- 步驟 9：檢查電腦是否列於預期的群組中，以及用戶端是否可與管理伺服器進行通訊

請參閱第 54 頁的「安裝管理伺服器之後該做什麼？」。

步驟 1：規劃安裝結構

安裝產品之前，請考量網路的規模和地理分佈位置，以決定安裝架構。

為了確保維持良好的網路和資料庫效能，您需要評估數個因素。 這些因素包括需要防護的電腦數量、是否有任何電腦透過廣域網路連線，或排程內容更新的頻率。

- 如果網路規模很小、位於一個地理位置，而且少於 500 個用戶端，就只需要安裝一個 Symantec Endpoint Protection Manager。
- 如果您的網路非常龐大，則可安裝更多具有額外資料庫的網站，並將其架構為使用遠端複製來共用資料。 若要提供額外的備援，您可以安裝額外的網站，以支援容錯移轉或負載平衡。 容錯移轉和負載平衡只能搭配 Microsoft SQL Server 資料庫使用。
- 如果您的網路分散在不同地點，則可能需要針對負載平衡和頻寬分配目的，安裝額外的管理伺服器。

為了協助您規劃中型到大型安裝，請參閱：Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書。

請參閱第 71 頁的「網路架構考量」。

請參閱第 635 頁的「設定網站和遠端複製」。

請參閱第 629 頁的「設定容錯移轉和負載平衡」。

步驟 2：進行準備並安裝 Symantec Endpoint Protection Manager

1. 確定要安裝管理伺服器的電腦符合最低系統需求。

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

2. 若要安裝 Symantec Endpoint Protection Manager，您必須使用可授予本機管理員存取權的帳戶來登入。

3. 決定要安裝內嵌資料庫或使用 Microsoft SQL Server 資料庫。

   如果使用 Microsoft SQL Server 資料庫，安裝將會要求執行額外的步驟。 這些步驟包括但不限於，架構或建立資料庫實例，將該實例架構為使用混合模式或 Windows 驗證模式。

另外，還需要提供資料庫伺服器管理憑證，才能建立資料庫和資料庫使用者。這些會專門與管理伺服器搭配使用。

請參閱第 73 頁的「關於 SQL Server 組態設定」。

請參閱第 629 頁的「設定容錯移轉和負載平衡」。

4. 您首先要安裝 Symantec Endpoint Protection Manager。安裝之後，您需要使用「管理伺服器組態精靈」立即架構安裝。

   在架構管理伺服器時，決定以下項目：

   - 用於登入管理主控台的密碼
   - 可接收重要通知和報告的電子郵件地址
   - 加密密碼，根據安裝期間您所選取的選項可能需要使用這個密碼

   請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

   請參閱第 72 頁的「關於基本管理伺服器設定」。

   請參閱第 37 頁的「安裝後架構 Symantec Endpoint Protection Manager」。

步驟 3：新增群組、政策和位置

1. 群組可用來組織用戶端電腦，並將不同的安全層級套用到每個群組。您可以使用預設群組、匯入群組 (如果網路使用 Active Directory 或 LDAP 伺服器) 或新增群組。

   如果新增群組，您可以使用下列群組結構作為基礎：

   - 桌上型電腦
   - 筆記型電腦
   - 伺服器

   請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。

   請參閱第 202 頁的「如何設定群組結構」。

   請參閱第 203 頁的「新增群組」。

2. 您可以使用位置，根據特定準則將不同的政策和設定套用到電腦。例如，您可以根據電腦位於公司網路內部或外部，為電腦套用不同的安全政策。一般而言，與防火牆內部的電腦相比，從防火牆外部連線至網路的電腦需要更佳的安全性。

   此位置讓位於辦公室外的行動電腦從賽門鐵克的 LiveUpdate 伺服器自動更新其定義檔。

   請參閱 Symantec Endpoint Protection 位置偵測最佳實務。

   請參閱第 229 頁的「將位置新增到群組」。

3. 針對要使用不同政策或設定的群組或位置停用繼承。

依據預設，群組會從預設的父群組 **My Company** 繼承政策和設定。 如果您想要指派不同的政策給子群組，或想要新增位置，您必須先停用繼承。 然後就可以變更子群組的政策，或新增位置。

附註：Symantec Endpoint Protection Manager 政策繼承不會套用至從雲端接收到的政策。雲端政策會遵循在雲端中定義的繼承。

請參閱第 208 頁的「停用群組繼承」。

4. 針對每種類型的政策，您可以接受預設政策，或建立並修改新政策來套用到每個新群組或位置。 您必須將需求新增至預設主機完整性政策，才能使主機完整性檢查對用戶端電腦起作用。

步驟 4：變更通訊設定以增加效能

您可以在每個群組中修改下列用戶端伺服器通訊設定，以改善網路效能：

- 使用提取模式取代推送模式，控制用戶端於何時使用網路資源下載政策和內容更新。
- 增加活動訊號的間隔。 如果每部伺服器服務的用戶端數目少於 100，可將活動訊號間隔時間增加為 15-30 分鐘。 如果為 100 至 1,000 個用戶端，請將活動訊號間隔時間增加為 30-60 分鐘。 更大的環境可能需要更長的活動訊號間隔時間。 賽門鐵克建議您將**「讓用戶端立即上傳重大事件」**保留勾選狀態。
- 將下載隨機設定增加為活動訊號間隔時間的一到三倍。

請參閱第 177 頁的「從預設管理伺服器或群組更新提供者隨機進行內容下載」。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

步驟 5：啟用產品授權

產品安裝後的 60 日之內購買並啟用授權。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

請參閱第 67 頁的「Symantec Endpoint Protection 產品授權需求」。

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

步驟 6：決定用戶端部署方法

決定最適合用來在您環境中的電腦上安裝用戶端軟體的用戶端部署方法。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

- 針對 Linux 用戶端，您可以使用**「儲存套件」**或**「網路連結與電子郵件」**，但不能使用**「遠端推送」**。
- 針對 Windows 和 Mac 用戶端，如果您使用**「遠端推送」**，可能需要執行下列工作：

- 確認擁有遠端用戶端電腦的管理員存取權限。 修改任何現有的防火牆設定 (包括通訊埠和通訊協定) 以允許在 Symantec Endpoint Protection Manager 與用戶端電腦之間進行遠端部署。
  請參閱第 94 頁的「Symantec Endpoint Protection 的通訊埠」。
- 您必須使用可授予本機管理員存取權的帳戶來登入。
  如果用戶端電腦是 Active Directory 網域的一部分，您必須使用可授予用戶端電腦本機管理員存取權的帳戶登入裝載 Symantec Endpoint Protection Manager 的電腦。 針對不是 Active Directory 網域一部分的每個用戶端電腦，您都應該有管理員憑證可供使用。
  請參閱第 91 頁的「準備 Windows 和 Mac 電腦進行遠端部署」。

請參閱第 90 頁的「準備用戶端安裝」。

步驟 7：準備用戶端進行安裝

1. 確定要安裝用戶端軟體的電腦符合最低系統需求。 您也應將用戶端安裝在裝載 Symantec Endpoint Protection Manager 的電腦上。

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

2. 從 Windows 電腦手動解除安裝 Symantec Endpoint Protection 用戶端安裝程式無法解除安裝的任何第三方安全軟體程式。

   如需此功能移除的產品清單，請參閱：Symantec Endpoint Protection 中的第三方安全軟體移除支援

   您必須從 Linux 電腦或 Mac 電腦解除安裝任何現有的安全軟體。

   某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。

3. 自 14 起，您可以將安裝套件架構為移除未透過標準方法移除的 Windows Symantec Endpoint Protection 用戶端。該程序完成後，便會安裝 Symantec Endpoint Protection。

   請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

步驟 8：部署並安裝用戶端軟體

1. 針對 Windows 用戶端，執行下列工作：

   - 建立自訂用戶端安裝功能集，決定要在用戶端電腦上安裝的元件。您也可以使用其中一個預設用戶端安裝功能集。
     請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。
     若是工作站的用戶端安裝套件，請勾選環境中郵件伺服器所適用的電子郵件掃描程式防護選項。例如，如果您使用 Microsoft Exchange 郵件伺服器，則勾選**「Microsoft Outlook 掃描程式」**。
   - 更新自訂用戶端安裝設定，決定用戶端電腦上的安裝選項。 這些選項包括目標安裝資料夾、解除安裝第三方安全軟體，以及安裝完成後的重新啟動行為。 您也可以使用預設用戶端安裝設定。
     請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

2. 使用「用戶端部署精靈」，建立用戶端安裝套件，其中包含從可用選項所進行的選取，然後將它部署到用戶端電腦。您只能透過用戶端部署精靈部署至 Mac 或 Windows 電腦。

   請參閱第 52 頁的「使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端」。

   請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

   請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

   請參閱第 114 頁的「匯出用戶端安裝套件」。

賽門鐵克建議您不要在安裝 Symantec Endpoint Protection 的同時執行第三方安裝。任何進行網路層級或系統層級變更的第三方程式安裝都可能會在安裝 Symantec Endpoint Protection 時導致不理想的結果。如可能，請在安裝 Symantec Endpoint Protection 之前重新啟動用戶端電腦。

步驟 9：檢查電腦是否列於預期的群組中，以及用戶端是否可與管理伺服器進行通訊

在管理主控台中，於**「用戶端」**>**「用戶端」**頁面上：

1. 將檢視變更為**「用戶端狀態」**，確認每個群組中的用戶端電腦可與管理伺服器進行通訊。

   請查看以下各欄中的資訊：

   - 連線至管理伺服器的用戶端會於**「名稱」**欄中顯示綠點。
     請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。
   - **「上次狀態變更時間」**欄中會顯示每個用戶端上次與管理伺服器進行通訊的時間。
   - **「需要重新啟動」**欄中會顯示用戶端電腦是否需要重新啟動才能受到保護。
     請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。
   - **「政策序號」**欄中會顯示最新的政策序號。政策可能不會在一到兩個活動訊號時間範圍內進行更新。如果政策未立即更新，您可以在用戶端上手動更新政策。
     請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。
     請參閱第 268 頁的「更新用戶端政策」。

2. 變更為**「防護技術」**檢視，並確認**「防毒狀態」**和**「竄改防護狀態」**(含)之間欄的狀態設定為**「開啟」**。

   請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。

3. 在用戶端上，檢查用戶端是否已連線至伺服器，並檢查政策序號是否為最新序號。

   請參閱第 659 頁的「在用戶端電腦上檢查與管理伺服器的連線」。

請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

安裝 Symantec Endpoint Protection Manager

安裝管理伺服器及主控台時，您需要執行數項工作。在安裝精靈中，每個已完成的任務旁將顯示綠色核取記號。

如需最新系統需求，請參閱：所有 Endpoint Protection 版本的版本說明、新修正和系統需求

如果將 Symantec Endpoint Protection Manager 與其他產品安裝在相同的伺服器上，有些 Symantec 產品可能會與其發生衝突。如需這些產品中任何必要組態變更的相關資訊，請參閱：Symantec Endpoint Protection 的軟體相容性

另外，Symantec Endpoint Protection Manager 安裝和組態會檢查所需權限的安全政策，以讓虛擬服務帳戶正確執行。Symantec Endpoint Protection Manager 會自動變更本機安全政策，並警示您對網域安全政策進行必要的變更。您也可以在安裝之前變更安全政策。請參閱如何指派使用者權限給適用於 Symantec Endpoint Protection Manager 服務的 Windows 安全政策。

附註：如果在 IPv6 網路中安裝 Symantec Endpoint Protection Manager 14.2，您還必須針對 Java 提供 IPv4 堆疊，即使 IPv4 已停用。如果已解除安裝 IPv4 堆疊，Java 將無法運作，並且 Symantec Endpoint Protection Manager 安裝失敗。

安裝 Symantec Endpoint Protection Manager

1. 若已下載產品，請將完整的安裝檔案擷取至實體磁碟，例如：硬碟。從實體磁碟執行 **Setup.exe**。

   如果您有產品光碟，請將它插入光碟機。安裝作業應能自動啟動。若未自動開始，請開啟光碟，然後連按兩下 **Setup.exe**。

2. 在「**Symantec Endpoint Protection 安裝程式**」對話方塊上，依序按下「**安裝 Symantec Endpoint Protection**」和「**安裝 Symantec Endpoint Protection Manager**」。

3. 檢閱安裝事件的順序，然後按「**下一步**」開始。

4. 在「**授權許可協議**」畫面中，按下「**我接受授權許可協議中的條款**」，再按「**下一步**」。

5. 在「**目的資料夾**」畫面中，接受預設目的資料夾或指定其他的目的資料夾，再按「**下一步**」。

6. 按下「**安裝**」。

   Symantec Endpoint Protection Manager 管理伺服器和主控台的安裝程序即開始。安裝完成後，按「**下一步**」。

7. 初始安裝完成後，您便可以架構伺服器和資料庫。按「**下一步**」。

   「**管理伺服器組態精靈**」隨即啟動。

   請參閱第 37 頁的「安裝後架構 Symantec Endpoint Protection Manager」。

   請參閱第 38 頁的「使用自訂組態安裝 Symantec Endpoint Protection Manager」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 90 頁的「準備用戶端安裝」。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

安裝後架構 Symantec Endpoint Protection Manager

管理伺服器組態精靈會在安裝 Symantec Endpoint Protection Manager 後自動啟動。根據您的需求架構管理伺服器。

此外，在安裝後，您還可以隨時從**「開始」>「所有程式」> Symantec Endpoint Protection Manager >「Symantec Endpoint Protection Manager 工具」**啟動管理伺服器組態精靈。

安裝後架構 Symantec Endpoint Protection Manager

1. 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
2. 選取**「預設組態」**後，按**「下一步」**。
3. 輸入公司名稱、預設管理員 admin 的密碼和電子郵件地址。

   或者，您可以新增詳細資料以使用指定的郵件伺服器。
4. 按下**「傳送測試電子郵件」**。

   Symantec Endpoint Protection Manager 會將密碼復原資訊和其他重要通知傳送至此電子郵件帳戶，因此，如果您未收到這封電子郵件，將無法繼續架構。
5. 一旦確認您收到測試電子郵件，請按**「下一步」**。
6. 指示是否要在安裝過程中執行 LiveUpdate。如果在新安裝的過程中執行 LiveUpdate，內容會更方便於供您部署的用戶端使用。按**「下一步」**

   如果夥伴將管理您的賽門鐵克授權，您也可以新增選擇性**「夥伴資訊」**。
7. 指示是否希望賽門鐵克接收匿名資料，然後按**「下一步」**開始建立資料庫。
8. 資料庫建立完成後，按下**「完成」**以完成 Symantec Endpoint Protection Manager 架構。

   如果您勾選啟動 Symantec Endpoint Protection Manager 的選項，則會出現 Symantec Endpoint Protection Manager 主控台登入畫面。登入後，您便可以開始部署用戶端。

   請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

您可以在安裝 Symantec Endpoint Protection Manager 所在伺服器的下列位置尋找組態摘要：

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

請參閱第 72 頁的「關於選擇資料庫類型」。

使用自訂組態安裝 Symantec Endpoint Protection Manager

當您要將 Symantec Endpoint Protection Manager 與 Microsoft SQL Server 資料庫一起安裝且擁有超過 500 個用戶端時，應該選擇**「管理伺服器組態精靈」**中的**「自訂組態」**。選取此選項時，其他設定將可用於組態。

附註：若要提供與資料庫的連線，必須在執行 Symantec Endpoint Protection Manager 的伺服器上安裝 SQL Server 用戶端工具。

請參閱第 73 頁的「關於 SQL Server 組態設定」。

使用自訂組態安裝 Symantec Endpoint Protection Manager

1. 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
2. 在**「管理伺服器組態精靈」**中，按下**「自訂組態」**，然後按**「下一步」**。

   如果您的用戶端數目少於 500 個，賽門鐵克建議您按下**「預設組態」**。

   請參閱第 37 頁的「安裝後架構 Symantec Endpoint Protection Manager」。
3. 按下**「安裝我的第一個站台」**，然後按**「下一步」**。

   下列選項適用於進階安裝，且不適用於 Symantec Endpoint Protection Manager 的首次安裝。

   - 若需**「安裝額外的管理伺服器到現有站台」**，請參閱設定容錯移轉和負載平衡。
   - 若需**「安裝其他站台」**，請參閱：
     設定站台和複寫
     複寫的運作方式
4. 在此畫面上，您可以自訂下列設定，然後按**「下一步」**：
   - 站台名稱
   - 伺服器名稱
   - 埠號
     對預設 Symantec Endpoint Protection Manager 通訊埠組態進行變更之前，應該先聯絡網路管理員。
   - Symantec Endpoint Protection Manager 伺服器儲存資料夾的位置
     如果 Symantec Endpoint Protection Manager 安裝所在的磁碟機上沒有足夠的可用空間，請將伺服器儲存資料夾重新定位到替代磁碟機。
5. 在資料庫選取畫面上，按下**「Microsoft SQL Server 資料庫」**，然後按**「下一步」**。
   - 可選取含自訂組態的內嵌資料庫。但是，此步驟假設您選取 SQL Server 資料庫。

- 請洽詢 SQL 資料庫管理員以確認是否應啟用自動資料庫維護工作。
- 賽門鐵克建議您在單獨的實體伺服器上主控 SQL Server 和 Symantec Endpoint Protection Manager。
- 如需 Microsoft SQL Server 支援版本的相關資訊，請參閱 Symantec Endpoint Protection 的系統需求。

6 按下「**建立新的資料庫**」，然後按「**下一步**」。

附註：使用現有資料庫視為進階安裝選項，通常不適用於新安裝。

7 在「**步驟一: 驗證資料庫伺服器**」畫面上，填寫 Symantec Endpoint Protection Manager 連線之 SQL Server 的詳細資料，然後按下「**連線至資料庫**」。

如果資料庫連線成功，則「**步驟二: 建立新資料庫**」區段會變為可用。

8 在「**步驟二: 建立新資料庫**」下，填寫用於建立新資料庫的詳細資料，然後按「**下一步**」。

如需有關「**驗證資料庫伺服器**」或「**建立資料庫**」的問題，請聯絡 SQL Server 資料庫管理員。

9 輸入公司名稱、預設管理員 admin 的密碼和電子郵件地址。

或者，您可以新增詳細資料以使用指定的郵件伺服器。

10 按下「**傳送測試電子郵件**」。一旦確認您收到測試電子郵件，請按「**下一步**」。

Symantec Endpoint Protection Manager 會將密碼復原資訊和其他重要通知傳送至此電子郵件帳戶，因此，如果您未收到這封電子郵件，將無法繼續架構。

11 建立加密密碼或選擇使用隨機密碼，然後按「**下一步**」。

此密碼用於保護用戶端和 Symantec Endpoint Protection Manager 之間的通訊，並且將會儲存在 Symantec Endpoint Protection Manager 復原檔案中。

12 指示是否要在安裝過程中執行 LiveUpdate。如果在新安裝的過程中執行 LiveUpdate，內容會更方便於供您部署的用戶端使用。按「**下一步**」

如果夥伴將管理您的賽門鐵克授權，您也可以新增選擇性「**夥伴資訊**」。

13 指示是否希望賽門鐵克接收匿名資料，然後按「**下一步**」開始建立資料庫。

14 建立和初始化資料庫後 (可能需要幾分鐘的時間)，按下「**完成**」。

如果您勾選啟動 Symantec Endpoint Protection Manager 的選項，則會出現 Symantec Endpoint Protection Manager 主控台登入畫面。登入後，您便可以開始部署用戶端。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

您可以在安裝 Symantec Endpoint Protection Manager 所在伺服器的下列位置尋找組態摘要：

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

請參閱第 72 頁的「關於選擇資料庫類型」。

登入 Symantec Endpoint Protection Manager 主控台

您可以在安裝 Symantec Endpoint Protection Manager 之後登入 Symantec Endpoint Protection Manager 主控台。有兩種方式可以登入主控台：

- 透過本機，從安裝管理伺服器的電腦。
  本機登入主控台
  您也可以從連線至管理伺服器的獨立式網頁瀏覽器，存取報告功能。
  請參閱第 548 頁的「從獨立式網頁瀏覽器登入報告」。
- 透過遠端，從符合遠端主控台之系統需求並且可網路連線至管理伺服器的任何電腦。您可以登入遠端 Web 主控台或遠端 Java 主控台。
  遠端登入主控台

基於安全性，主控台最遲會在一小時後將您登出。您可以縮短這段時間。在 12.1.4 版及更早版本中，您可以停用逾時期間。

請參閱第 261 頁的「變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間」。

本機登入主控台

本機登入主控台

1. 移到**「開始」>「程式」> Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**。
2. 在 **Symantec Endpoint Protection Manager** 登入對話方塊中，輸入您在安裝期間所架構的使用者名稱 (預設為 `admin`) 和密碼。

   可選擇勾選**「記住我的使用者名稱」**和**「記住我的密碼」**(如果有的話) 中的一項或兩項。

   請參閱第 256 頁的「顯示「忘記了您的密碼?」連結，以便管理員可以重設遺失密碼」。

   - 若要使用 PIV 卡或 CAC 登入，請按下**「選項」**，然後勾選**「登入智慧卡」**(自 14.2 起)。在**「登入/PIN」**訊息中，輸入您的 PIN 號碼。
     請參閱第 248 頁的「架構 Symantec Endpoint Protection Manager 以驗證使用智慧卡登入的管理員」。
   - 若要使用雙因素驗證登入，請輸入密碼，後面緊接 Token。如果省略 Token，則登入嘗試會失敗。如果您使用 Symantec VIP 智慧型手機應用程式，請輸入密碼，然後在按下**「登入」**後核准應用程式上的要求。如果您未在兩分鐘內核准要求，則登入嘗試會失敗。
     請參閱第 247 頁的「使用 Symantec VIP 架構雙因素驗證」。

如果主控台有一個以上的網域，請按下**「選項」**，然後輸入網域名稱。請參閱第 264 頁的「新增網域」。

3 按下**「登入」**。

遠端登入主控台

若要遠端登入，您需要知道已安裝管理伺服器電腦的 IP 位址或主機名稱。 您還應該確定網頁瀏覽器的 Internet 選項允許您檢視來自要登入的伺服器的內容。

遠端登入時，可以執行與管理員本機登入時相同的工作。在主控台檢視哪些內容及執行哪些作業取決於您所屬的管理員類型。小型組織中的大多數管理員會以系統管理員身分登入。

附註：如果您安裝的遠端 Java 主控台上使用的是該產品的先前版本，必須在升級至更新版本後重新安裝主控台。

附註：對於 Windows Server 2016，請使用管理伺服器安裝所在電腦的主機名稱。

遠端登入主控台

1 開啟支援的網頁瀏覽器，然後在位址方塊中輸入下列位址：

http://*SEPMServer*:9090

其中 *SEPMServer* 是管理伺服器的主機名稱或 IP 位址。如需支援的網頁瀏覽器清單，請參閱：所有 Endpoint Protection 版本的版本說明、新修正和系統需求。

IP 位址包括 IPv4 和 IPv6。必須用方括弧括住 IPv6 位址。例如，**http://[*SEPMServer*]:9090**

2 在「Symantec Endpoint Protection Manager 主控台 Web 存取」頁面，按下所需的主控台類型。

如果按下**「Symantec Endpoint Protection Manager Web 主控台」**，將會載入一個安全的網頁，讓您從遠端登入而不使用 Java Runtime Environment (JRE)。

如果按下**「Symantec Endpoint Protection Manager 主控台」**，您登入時使用的電腦必須已安裝 JRE 才能執行 Java 用戶端。如果沒有，您必須下載並安裝該程式。請按照提示安裝 JRE，並按照提供的任何其他指示操作。

另一個選項不是遠端管理解決方案。您可按下**「Symantec Endpoint Protection Manager 憑證」**，系統會提示您下載管理主控台的憑證檔案。然後，您可以視需要將此檔案匯入網頁瀏覽器。

3 如果出現主機名稱訊息，請按下**「是」**。

此訊息表示您指定的遠端主控台 URL 與 Symantec Endpoint Protection Manager 憑證名稱不符。如果您登入並指定 IP 位址，而不是指定管理伺服器的電腦名稱，就會發生此問題。

如果出現網頁安全憑證警告，請按下**「繼續瀏覽此網站 (不建議)」**，然後新增自我簽署憑證。

4 遵照提示來完成登入程序。

如果這是您在安裝後第一次登入，請使用帳戶名稱 **admin**。

根據登入方法，您可能需要提供其他資訊。例如，如果主控台有多個網域，請按下**「選項」**，並提供所要登入之網域的名稱。

5 如果您使用的是 Java 型主控台，您可以選擇儲存使用者名稱和密碼。按下**「登入」**。

您可能會在遠端主控台啟動時，收到一或多個安全性警告訊息。如果確實如此，請按下**「是」**、**「執行」**、**「啟動」**，或同等功能的選項，然後繼續操作直到主控台出現。

您可能需要接受 Symantec Endpoint Protection Manager 主控台要求的自我簽署憑證。

請參閱第 259 頁的「授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取」。

請參閱第 258 頁的「在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息」。

請參閱第 258 頁的「關於接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證」。

啟用或匯入 Symantec Endpoint Protection 產品授權

您可以使用「授權啟用精靈」工作流程執行下列工作：

- 啟用新的付費授權。
- 將試用授權轉換為付費授權。
- 續購授權。
- 啟用其他已付費授權，以回應過度部署狀態。

您可以使用從以下來源收到的檔案或序號匯入並啟用授權：

- MySymantec
- 賽門鐵克合作夥伴或慣用經銷商
- 賽門鐵克銷售團隊
- Symantec Business Store (賽門鐵克商行)

您可以透過下列方式啟動「授權啟用精靈」：

- 安裝產品之後出現的「入門」畫面。
  您還可以透過**「說明」>「開始使用頁面」**存取「開始使用」畫面。
- Symantec Endpoint Protection Manager 主控台的**「管理員」**頁面。

如果從「入門」畫面啟用或匯入授權，您可以跳至步驟 3。

啟用或匯入 Symantec Endpoint Protection 產品授權

1 在 Symantec Endpoint Protection Manager 中，按下**「管理員」>「授權」**。

2 在**「工作」**下方，按下**「啟用授權」**。

3 按下**「啟用新授權」**，然後按**「下一步」**。 如果您沒看到此面板，請繼續下一個步驟。

4 在**「授權啟用」**面板上，選取符合您的情況的選項，再按**「下一步」**。

下表描述每個選項：

選項	敘述
我有序號	當您或您的賽門鐵克合作夥伴已購買授權時，您可能會收到授權序號。 如果您有授權序號，請選取此選項。 如果您是 eFlex (Symantec Enterprise 選項) 客戶，且擁有 eFlex 產生的序號，請選取**「我有賽門鐵克授權檔」**。
我有賽門鐵克授權檔 (.slf)	在大多數情況下，在您完成購買程序之後，很快就會收到賽門鐵克用電子郵件傳送給您的賽門鐵克授權檔 (.slf 檔)。 這個檔案會以 .zip 檔的形式隨通知電子郵件一併送達。 如果您已收到 .slf 檔，請選取此選項。 **附註：**您必須先從 .zip 檔解壓縮 .slf 檔，才能用它來啟用產品授權。 **警告：**.slf 檔包含您的授權專屬的資訊。 為避免損壞授權檔，請不要修改其內容。 您可以複製該檔案作為記錄。

您可以在下列網頁中找到 eFlex 的相關資訊：

Enterprise 選項

5 根據您在上一個步驟中選取的選項，執行下列其中一項工作：

- 如果您選取**「我有序號」**，請輸入序號，然後按下**「送出」**。 檢閱您新增的授權相關資訊，然後按**「下一步」**。

附註：若要使用序號啟用授權，您必須擁有作用中 Internet 連線並可連線至 賽門鐵克授權伺服器。如果連線成功，將載入賽門鐵克首頁。如果連線失敗，**請**參閱以下：

如何測試 Insight 與賽門鐵克授權伺服器的連線

- 如果您選取**「我有賽門鐵克授權檔 (.slf)」**，請按下**「新增檔案」**。瀏覽並選取您從隨附於賽門鐵克通知電子郵件之 .zip 檔解壓縮的 .slf 檔。 按下**「開啟」**，再按**「下一步」**。

6 輸入有關技術聯絡人和主要聯絡人的資訊，以及有關公司的資訊。 按一下認可披露聲明，然後按下**「送出」**。

如果您在購買授權時提供這項資訊，此面板就不會顯示。

7 按下**「完成」**。

請參閱第 81 頁的「關於試用授權」。

請參閱第 84 頁的「關於更新 Symantec Endpoint Protection 授權」。

請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

使用儲存套件安裝 Symantec Endpoint Protection 用戶端

如果您擁有較少數目的用戶端，請使用儲存套件方法在用戶端上部署和安裝安裝套件。

儲存套件會建立安裝套件，讓您可以手動安裝、使用第三方部署軟體安裝或使用登入程序檔安裝。

儲存套件包含下列工作：

- 選擇架構，然後建立用戶端安裝套件。
- 將安裝套件儲存到執行 Symantec Endpoint Protection Manager 之電腦的資料夾中。
  若是 Windows，安裝套件可為 32 或 64 位元作業系統。 安裝套件由一個 setup.exe 檔案或一組包含 setup.exe 檔案的多個檔案所組成。 對電腦使用者而言，單一 setup.exe 檔案通常較容易使用。

附註：Mac 和 Linux 用戶端安裝套件會自動匯出 `.zip` 封存檔案格式。 若要正確保留檔案權限，您應使用原生封存程式展開封存檔案，如 Mac「封存工具程式」或 `ditto` 指令。 在這些作業系統上，您不能使用 Mac 的 `unzip` 指令、第三方應用程式或任何 Windows 應用程式來展開檔案。

使用儲存套件安裝 Symantec Endpoint Protection 用戶端

1 在主控台中，啟動**「用戶端部署精靈」**。

按下**「說明」>「開始使用」頁面**，然後在**「所需工作」**下方，按下**「在您的電腦上安裝用戶端軟體」**。

2 在**「用戶端部署精靈」**中，執行下列其中一項工作：

- 按下**「新套件部署」**，再按**「下一步」**。「儲存套件」僅安裝新的安裝套件。
- 如果您想要在已安裝 Symantec Endpoint Protection 用戶端的電腦上更新 Windows 或 Mac 用戶端通訊設定，請按下**「通訊更新套件部署」**。按照畫面上的指示進行，然後移至步驟 4。

3 從可用選項 (隨安裝套件類型而異) 中選擇，再按**「下一步」**。

附註：若要移除 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。

請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

4 按下**「儲存套件」**，再按**「下一步」**。

5 按下**「瀏覽」**並指定要接收套件的資料夾。

如果是「通訊更新套件部署」或是 Mac 和 Linux 套件，請移至步驟 6。

如果是新的 Windows 套件，請勾選**「單一 .exe 檔案 (預設)」**或**「獨立檔案 (.MSI 必需)」**。

附註：除非您需要獨立檔案供第三方部署程式使用，否則使用**「單一 .exe 檔案」**。

---

6 按**「下一步」**。

7 檢閱設定摘要，然後按**「下一步」**，再按下**「完成」**。

8 將匯出的套件提供給電腦使用者。

使用下列方式將匯出的套件提供給使用者：電子郵件、將套件儲存於安全的共用網路位置，或使用第三方程式。

9 確認使用者下載並安裝用戶端軟體，以及確認用戶端的安裝狀態。

對於新的 Symantec Endpoint Protection 安裝，用戶端電腦在透過自動或是您或使用者採取的動作重新啟動之後，它們才會出現在 Symantec Endpoint Protection Manager 內。Mac 用戶端在安裝完成時會自動提示重新啟動。 Linux 用戶端不需要重新啟動。

請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 90 頁的「準備用戶端安裝」。

安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端

如果您無法使用或不想使用遠端推送，可以直接在 Mac 電腦上安裝 Symantec Endpoint Protection 用戶端。非受管或受管用戶端的安裝步驟差異不大。

安裝受管用戶端的唯一方式是使用透過 Symantec Endpoint Protection Manager 建立的套件。您可以隨時透過匯入用戶端伺服器通訊設定到 Mac 用戶端，將非受管用戶端轉換為受管用戶端。

附註：若要準備適用於 Mac 的 Symantec Endpoint Protection 用戶端以與第三方遠端部署軟體搭配使用，請參閱透過 Apple Remote Desktop 或 Casper 匯出及部署 Symantec Endpoint Protection 用戶端。

如果您下載了安裝檔案或接收了產品光碟

1. 執行下列其中一項作業：

   如果您下載了安裝檔案，請將內容解壓縮至 Mac 電腦上的資料夾中，然後開啟該資料夾。

   如果您接收了光碟，請將其插入電腦。

2. 開啟 `SEP_MAC`。
3. 將 `Symantec Endpoint Protection.dmg` 複製到 Mac 電腦的桌面上。
4. 連按兩下 `Symantec Endpoint Protection.dmg`，將檔案掛載為虛擬磁碟。 然後即可安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端。

如果您有用戶端安裝套件 .zip 檔

1. 如果您匯出安裝套件或從 MySymantec 下載了用戶端安裝程式套件，請將檔案複製到 Mac 電腦的桌面上。

   這個檔案的名稱可能是 `Symantec Endpoint Protection.zip` 或 `Symantec_Endpoint_Protection_`*`version`*`_Mac_Client.zip`，其中 *version* 是產品版本。

2. 在「**開啟檔案**」>「**封存公用程式**」上按下滑鼠右鍵，以解壓縮檔案的內容。
3. 開啟產生的資料夾。 然後即可安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端。

附註：產生的虛擬磁碟影像或資料夾包含應用程式安裝程式，以及一個稱為 **Additional Resources** 的資料夾。 兩個項目都必須存在於同一個位置才能成功安裝。 如果將安裝程式複製到另一個位置，則必須也複製 **Additional Resources**。

安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端

1. 連按兩下「**Symantec Endpoint Protection 安裝程式**」
2. 若要認可必要的重新啟動，請按下「**繼續**」。

3 若要檢閱授權許可協議，請按下**「檢視授權許可協議」**。

若要開始安裝，請按下**「同意並安裝」**。

4 出現提示時，輸入 Mac 管理帳戶的使用者名稱和密碼，然後按下**「安裝協助程式」**。

5 若要針對 macOS 10.13 授權 Symantec Endpoint Protection 核心延伸，請在安裝程式窗格中，按下**「系統偏好設定」**，然後在**「安全性與隱私權」**系統喜好設定窗格中，按下**「允許」**。您無須輸入密碼。

6 在安裝程式窗格中，按下**「關閉並重新啟動」**以完成安裝。

當您重新登入 Mac 電腦時，LiveUpdate 會啟動來更新定義檔。 LiveUpdate 會在背景中無訊息執行，且不會在螢幕上顯示其進度。

如果系統提示您授權核心延伸，但並未在步驟5中提示，則在電腦重新啟動後執行。您必須授權核心延伸才能使 Symantec Endpoint Protection 完全運作。

請參閱第 47 頁的「關於針對 macOS 10.13 或更新版本授權 Symantec Endpoint Protection 的核心延伸」。

請參閱第 114 頁的「匯出用戶端安裝套件」。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

關於針對 macOS 10.13 或更新版本授權 Symantec Endpoint Protection 的核心延伸

自 macOS 10.13 起，需要授權核心延伸 (kexts) 是一項新的安全功能。Symantec Endpoint Protection 14.0.1 新增了對 macOS 10.13 的支援。您必須授權核心延伸才能使 Symantec Endpoint Protection 完全運作。

在用戶端安裝期間，當**「系統偏好設定」**下的**「安全性與隱私權」**系統喜好設定窗格中出現提示時，按下**「允許」**。您無須輸入密碼。

「系統偏好設定」中允許 Symantec Endpoint Protection 核心延伸的選項會在 30 分鐘後消失。您可以透過以下方式重新取得該選項：

- 重新啟動 Mac。然後，可以開啟**「安全性與隱私權」**系統喜好設定。
- 在 Mac 上開啟 Symantec Endpoint Protection 用戶端使用者介面，然後按下**「核心延伸需要授權」**訊息旁的**「修正」**。此動作將會開啟**「安全性與隱私權」**系統喜好設定。

如果您之前已在 Mac 電腦上授權 Symantec Endpoint Protection 核心延伸，則無需重新授權。例如，如果您解除安裝並重新安裝用戶端，則無需重新授權核心延伸。如果將 Symantec Endpoint Protection 升級至 14.0.1 並將作業系統升級至 macOS 10.13，也無須明確授權。

不過，如果重新安裝作業系統，則需要重新授權核心延伸。如果您從早於 14.2 版的 Symantec Endpoint Protection 升級至 14.2 或更新版本，您也必須重新授權核心延伸。

請參閱第 48 頁的「部署適用於 Mac 的 Symantec Endpoint Protection 用戶端時管理核心延伸授權」。

請參閱第 46 頁的「安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端」。

部署適用於 Mac 的 Symantec Endpoint Protection 用戶端時管理核心延伸授權

如果大量部署適用於 Mac 的 Symantec Endpoint Protection 用戶端，您可能需要採取其他步驟，以確保已授權核心延伸。自 macOS 10.13 (High Sierra) 起，將適用此要求。作業系統指示必須在本機電腦上進行授權。您無法透過遠端存取授權核心延伸，也無法透過預先架構的磁碟影像儲存核心授權。

若要確保在 Mac 上已正確授權核心延伸，請執行下列其中一項：

- 指示 Mac 使用者核准必要的延伸。任何使用者都可以透過「安全性與隱私權」喜好設定窗格核准核心延伸，即使他們不具有管理員權限。
  請參閱第 47 頁的「關於針對 macOS 10.13 或更新版本授權 Symantec Endpoint Protection 的核心延伸」。
- 在 Mobile Device Management (MDM) 解決方案中註冊 Mac。即使您未主動使用此解決方案管理 Mac，核心延伸授權也會還原為 macOS 10.13 之前的強制執行方式。
- 自 macOS 10.13.2 版起，可以使用團隊識別碼透過 Mobile Device Management (MDM) 授權核心延伸。若要在 macOS 上針對 Symantec Endpoint Protection 授權核心延伸，請使用團隊識別碼 `9PTGMPNXZ2`。請查詢 MDM 套件的說明文件，以取得如何使用此團隊識別碼的相關指示。
- 如果您使用 **NetBoot**、**NetInstall** 或 **NetRestore**，請在準備用於部署的磁碟影像時使用下列指令：

  ```
  spctl kext-consent add 9PTGMPNXZ2
  ```

  此指令使用 Symantec 團隊識別碼來預先核准 Mac 上的 Symantec 核心延伸。
  透過此指令設定的團隊識別碼儲存在靜態隨機存取記憶體 (NVRAM) 中，即使 Mac 關閉電源，該記憶體仍存在。如果您重設 NVRAM，核心延伸需要重新核准。如果使用者還透過「安全性與隱私權」窗格核准了核心延伸，則不需要重新核准。

如需載入核心延伸的詳細資訊，請參閱以下 Apple 說明文件：

為 macOS High Sierra 中的核心延伸變更做準備

安裝 Linux 的 Symantec Endpoint Protection 用戶端

您可以直接在 Linux 電腦上安裝非受管或受管 Symantec Endpoint Protection 用戶端。您無法從遠端的 Symantec Endpoint Protection Manager 部署 Linux 用戶端。非受管或受管用戶端的安裝步驟差異不大。

安裝受管用戶端的唯一方式是使用您在 Symantec Endpoint Protection Manager 中建立的安裝套件。您可以隨時透過匯入用戶端伺服器通訊設定到 Linux 用戶端，將非受管用戶端轉換為受管用戶端。

如果 Linux 作業系統核心與預先編譯的自動防護核心模組不相容，此安裝程式會嘗試編譯相容的自動防護核心模組。自動編譯程序會視需要自動啟動。不過，此安裝程式可能無法編譯相容的自動防護核心模組。在這種情況下，自動防護會安裝，但處於停用狀態。如需詳細資訊，請參閱：

Symantec Endpoint Protection 支援的 Linux 核心

附註：您必須擁有進階使用者權限，才能在 Linux 電腦上安裝 Symantec Endpoint Protection 用戶端。此程序會使用 `sudo` 來提高權限。

安裝 Linux 的 Symantec Endpoint Protection 用戶端

1. 將您建立的安裝套件複製到 Linux 電腦。此套件是 .zip 檔。
2. 在 Linux 電腦上，開啟 Terminal 應用程式視窗。
3. 使用下列指令瀏覽到安裝目錄：

   `cd /directory/`

   其中 *directory* 是您將 .zip 檔複製到的目錄名稱。
4. 使用下列指令，將 .zip 檔的內容解壓縮到名為 `tmp` 的目錄中：

   `unzip "InstallPackage" -d sepfiles`

   其中 *`InstallPackage`* 是 .zip 檔的完整名稱，而 *`sepfiles`* 代表解壓縮程序將安裝檔案放入其中的目的資料夾。

   如果目的資料夾不存在，解壓縮程序會予以建立。
5. 使用下列指令瀏覽到 *`sepfiles`*：

   `cd sepfiles`

6 若要正確設定 `install.sh` 的執行檔案權限，請使用下列指令：

```
chmod u+x install.sh
```

7 使用下列指令，以內建指令碼安裝 Symantec Endpoint Protection：

```
sudo ./install.sh -i
```

出現提示時，輸入您的密碼。

此指令碼會起始安裝 Symantec Endpoint Protection 元件。預設安裝目錄如下：

`/opt/Symantec/symantec_antivirus`

LiveUpdate 的預設工作目錄如下：

`/opt/Symantec/LiveUpdate/tmp`

當傳回指令提示時，表示安裝完成。您無需重新啟動電腦，即可完成安裝。

若要驗證用戶端安裝，請按下 Symantec Endpoint Protection 黃色盾牌或在其上按下滑鼠右鍵，然後按下**「開啟 Symantec Endpoint Protection」**。黃色盾牌的位置隨 Linux 版本而有所不同。用戶端使用者介面會顯示程式版本、病毒定義檔、伺服器連線狀態，以及管理的相關資訊。

請參閱第 149 頁的「將用戶端伺服器通訊設定匯入 Linux 用戶端」。

請參閱第 90 頁的「準備用戶端安裝」。

使用遠端推送安裝 Symantec Endpoint Protection 用戶端

「遠端推送」會將用戶端軟體推送至依 IP 位址或電腦名稱指定的電腦。套件一旦複製到目標電腦之後，套件就會自動安裝。電腦使用者不需要開始安裝或具有管理員權限。

「遠端推送」包含下列工作：

- 選取現有的用戶端安裝套件、建立新的安裝套件，或建立套件以更新通訊設定。
- 如果是新的安裝套件，請架構並建立安裝套件。
- 指定您網路上要從 Symantec Endpoint Protection Manager 接收套件的電腦。
  「遠端推送」會找出使用您提供之 IP 號碼或範圍的特定電腦，或是透過瀏覽網路，找出所有可見的電腦。

附註：若要將用戶端安裝套件推送到**「瀏覽網路」**標籤中的 Mac 用戶端，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝 Bonjour 服務。請參閱下列文章：

安裝適用於 Symantec Endpoint Protection Manager 12.1.5 或更新版本的 Bonjour 服務

Bonjour 服務不支援 IPv6 網路。僅啟用 IPv6 網路的 Mac 無法顯示在**「瀏覽網路」**中。

- Symantec Endpoint Protection Manager 將用戶端軟體推送到指定的電腦。
  套件成功複製到目標電腦後，安裝會在電腦上自動開始。

附註：您無法使用遠端推送安裝 Linux 用戶端。

使用遠端推送安裝 Symantec Endpoint Protection 用戶端

1 在主控台中，啟動**「用戶端部署精靈」**。

  按下**「說明」>「開始使用」頁面**，然後在**「所需工作」**下方，按下**「在您的電腦上安裝用戶端軟體」**。

2 在**「用戶端部署精靈」**中，執行下列其中一項工作：

  - 按下**「新套件部署」**以建立新的安裝套件，然後按**「下一步」**。
  - 按下**「現有套件部署」**以使用先前建立的套件，然後按下**「瀏覽」**找出要安裝的套件。
    「用戶端部署精靈」會上傳套件，並將您導向至**「電腦選取」**面板 (步驟 5)。
  - 在**「通訊更新套件部署」**下，選擇是否要更新已安裝 Symantec Endpoint Protection 用戶端之電腦上的 Windows 或 Mac 用戶端通訊設定。按照畫面上的指示進行，然後移至步驟 4。
    使用此選項可將非受管用戶端轉換成受管用戶端。

  請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

3 若是新套件，請在**「選取群組並安裝功能集」**面板中，從可用選項 (隨安裝套件類型而異) 中進行選取。按**「下一步」**。

  附註：若要解除安裝 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。您也可以使用已架構為啟用此功能的現有用戶端安裝套件。

  請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

  請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

4 按下**「遠端推送」**，然後按**「下一步」**。

5 在**「電腦選取」**面板中，使用下列其中一種方法找出要接收軟體的電腦：

  - 若要瀏覽網路尋找電腦，按下**「瀏覽網路」**。
  - 若要依據 IP 位址或電腦名稱尋找電腦，按下**「搜尋網路」**，再按下**「尋找電腦」**。

  您可以設定逾時值，以限制伺服器套用至搜尋的時間長度。

6 按下 **> >**，將電腦新增至清單，若精靈提示驗證網域或工作群組，請相應執行。

  遠端推送安裝需要較高的權限。如果用戶端電腦是 Active Directory 網域的一部分，您應使用網域管理員帳戶。

7 按「**下一步**」，然後按「**傳送**」，將用戶端軟體推送至選取的電腦。

「**部署摘要**」面板指示成功部署後，安裝作業便會自動在用戶端電腦上開始。

安裝作業可能需要數分鐘的時間。

8 按「**下一步**」，然後按下「**完成**」。

9 在「**用戶端**」頁面上確認所安裝用戶端的狀態。

對於新的 Symantec Endpoint Protection 安裝，用戶端電腦在透過自動或是您或使用者採取的動作重新啟動之後，它們才會出現在 Symantec Endpoint Protection Manager 內。

請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。

附註：將用戶端安裝套件遠端安裝至 Mac 用戶端後，必須在用戶端電腦上確認已授權核心延伸。Symantec Endpoint Protection 需要核心延伸授權才能完全運作，如果需要授權，「遠端推送」不會提示您授權。在 Mac 上，勾選「**安全性與隱私權**」系統喜好設定，然後按下「**允許**」。

請參閱第 90 頁的「準備用戶端安裝」。

請參閱第 91 頁的「準備 Windows 和 Mac 電腦進行遠端部署」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端

「網路連結與電子郵件」選項會建立安裝套件和安裝套件的 URL。使用者以電子郵件的形式收到用於下載套件及安裝 Symantec Endpoint Protection 用戶端的 URL。使用者必須擁有管理員權限才能安裝套件。

網路連結與電子郵件包含下列工作：

- 選取、架構並建立用戶端安裝套件。
  從針對 Windows、Mac 和 Linux 用戶端安裝套件的架構顯示的選項中選擇。 所有用戶端安裝套件儲存於執行 Symantec Endpoint Protection Manager 的電腦內。
- 從 Symantec Endpoint Protection Manager 寄出電子郵件給電腦使用者，通知他們可以下載用戶端安裝套件。
  提供要接收電子郵件訊息的使用者清單，該訊息包含下載和安裝用戶端安裝套件的指示。使用者可依照指示安裝用戶端軟體。

附註：Mac 和 Linux 用戶端安裝套件會自動匯出 .zip 封存檔案格式。若要正確保留檔案權限，您應使用原生封存程式展開封存檔案，如 Mac「封存工具程式」或 ditto 指令。在這些作業系統上，您不能使用 Mac 的 unzip 指令、第三方應用程式或任何 Windows 應用程式來展開檔案。

在使用「網路連結與電子郵件」之前，請確保正確架構管理伺服器到郵件伺服器之間的連線。

請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。

使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端

1. 在主控台中，啟動**「用戶端部署精靈」**。

   按下**「說明」>「開始使用」頁面**，然後在**「所需工作」**下方，按下**「在您的電腦上安裝用戶端軟體」**。

2. 在**「用戶端部署精靈」**中，按下**「新套件部署」**，再按**「下一步」**。網路連結和電子郵件僅傳送新的安裝套件。

3. 從可用選項 (隨安裝套件類型而異) 中選擇，再按**「下一步」**。

   附註：若要移除 Windows 用戶端上的現有安全軟體，您必須先架構自訂「用戶端安裝設定」，再啟動「用戶端部署精靈」。

   請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

   請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

4. 按下**「網路連結與電子郵件」**，然後按**「下一步」**。

5. 在**「電子郵件收件者和訊息」**面板中，指定電子郵件收件者和主旨。

   若指定多位電子郵件收件者，請利用逗號分隔各電子郵件地址。管理主控台系統管理員會自動接收郵件的複本。

   您可以接受預設的電子郵件主旨和本文，也可以編輯文字。您也可以複製 URL 並將它貼到內部網路網頁等方便的線上安全位置。

6. 若要建立套件和透過電子郵件傳遞連結，請依序按**「下一步」**和**「完成」**。

7. 確認電腦使用者已收到電子郵件訊息並安裝用戶端軟體。

   用戶端電腦在透過自動或是您或使用者採取的動作重新啟動之後，它們才會出現在 Symantec Endpoint Protection Manager 內。Mac 用戶端在安裝完成時會自動提示重新啟動。Linux 用戶端不需要重新啟動。

   請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

   請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 90 頁的「準備用戶端安裝」。

安裝管理伺服器之後該做什麼？

表 2-1 顯示了安裝與架構產品後應執行以評估用戶端電腦上是否具有正確防護等級的工作。繼續定期執行這些工作 (每週或每月)。

表 2-1 安裝後要執行的工作

動作	敘述
修改病毒和間諜軟體防護政策	變更下列預設掃描設定： ■ 如果您建立伺服器群組，請將排程掃描時間變更為大多數使用者離線的某個時間。 請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。 ■ 在自動防護中啟用風險追蹤程式。 如需詳細資訊，請參閱文章：什麼是風險追蹤程式？ 風險追蹤程式具有以下前提條件： ■ 已啟用「網路威脅防護」。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。 ■ 已啟用 Windows 檔案及印表機共用。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。
修改遠端電腦群組和伺服器群組的防火牆政策	■ 確認異地位置的以下預設防火牆規則已啟用，增進遠端電腦的安全性： ■ **攔截對外部電腦的本機檔案共用** ■ **攔截遠端管理** ■ 確認下列防火牆規則已啟用，減弱伺服器群組的安全性：**「允許本機電腦共用本機檔案」**。 此防火牆規則會確保僅允許本機流量。 請參閱第 311 頁的「自訂防火牆規則」。 請參閱第 226 頁的「管理遠端用戶端的位置」。

動作	敘述
將應用程式和檔案排除在掃描範圍之外	您可以將用戶端架構為不掃描特定資料夾和檔案，以增強效能。 例如，用戶端會在每次排程掃描執行時掃描郵件伺服器目錄。 您應該從掃描範圍內排除郵件伺服器程式檔和目錄。 如需詳細資訊，請參閱文章：關於 Microsoft Exchange 伺服器和賽門鐵克產品的檔案和資料夾自動排除。 您可以排除已知會於接受掃描時造成問題的資料夾和檔案，以提升效能。 例如，Symantec Endpoint Protection 不應掃描專屬 Microsoft SQL Server 檔案。 您應該新增例外，防止掃描包含 SQL Server 資料庫檔案的資料夾。 這些例外可改善效能，並且避免發生損毀，或在 SQL Server 必須使用檔案時檔案遭到鎖定。 如需詳細資訊，請參閱知識庫文章：如何使用集中式例外排除 MS SQL 檔案和資料夾。 此外，應從掃描中排除誤報。 您也可以依副檔名排除 Windows 電腦上「自動防護」掃描的檔案。 請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。 請參閱第 403 頁的「自訂 Mac 用戶端的自動防護」。
在排程掃描後執行快速報告和排程報告	執行快速報告和排程報告，以檢視用戶端電腦是否具有正確的安全性層級。 請參閱第 549 頁的「關於 Symantec Endpoint Protection Manager 報告類型」。 請參閱第 559 頁的「執行和自訂快速報告」。 請參閱第 561 頁的「如何執行排程報告」。
請檢查確認排程掃描已成功且用戶端依預期執行	檢視監控器、日誌和用戶端電腦的狀態，確認每個群組都具有正確的防護等級。 請參閱第 539 頁的「監控端點防護」。
評估內容儲存和用戶端通訊頻寬需求	自 12.1.5 起，Symantec Endpoint Protection Manager 不再儲存多個完整內容版本。 相反地，系統只會儲存最新的完整版本，再加上增量差異。 這種方式意味著用戶端幾乎都是下載差異，而非完整套件。 只有在用戶端過時已久 (超過三個月) 的少數情況下，才需要完整下載最新的內容。 如果您的環境必須精確地控制網路頻寬，您也可以調節用戶端通訊。 如需詳細資訊，請參閱文章：Symantec Endpoint Protection 的用戶端通訊頻寬控制 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。 如需計算儲存空間和頻寬需求的詳細資訊，請參閱 Symantec Endpoint Protection 規模設定及擴充性最佳實務準則白皮書。

動作	敘述
針對單一風險爆發以及偵測到新風險的疫情架構通知	針對**「單一風險事件」**建立通知，並針對**「風險爆發」**修改通知。 針對這些通知，賽門鐵克建議您執行下列動作： **1** 將**「風險嚴重性」**變更為**「類別 1 (極低以上)」**，以避免接收有關追蹤 Cookie 的電子郵件。 **2** 將**「調節器」**設定保持為**「自動」**。 通知對於維護安全的環境而言非常重要，而且可以節省您的時間。 請參閱第 577 頁的「設定管理員通知」。 請參閱第 569 頁的「管理通知」。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

請參閱：Symantec Endpoint Protection 對保護企業環境安全的最佳實務準則建議

3

系統需求

本章包含以下主題：

- Symantec Endpoint Protection 的系統需求
- Symantec Endpoint Protection 產品授權需求
- 支援的虛擬安裝和虛擬化產品

Symantec Endpoint Protection 的系統需求

一般而言，Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端的系統需求與其支援的作業系統之系統需求相同。

附註：如需最新系統需求，請參閱：

Symantec Endpoint Protection 14.2 RU1 的系統需求

當資訊發生衝突時，應將網頁視為最準確。

- 請參閱第 58 頁的「Symantec Endpoint Protection Manager 系統需求」。
- 請參閱第 60 頁的「適用於 Windows 的 Symantec Endpoint Protection 用戶端系統需求」。
- 請參閱第 63 頁的「Windows Embedded 適用的 Symantec Endpoint Protection 用戶端系統需求」。
- 請參閱第 64 頁的「Mac 適用的 Symantec Endpoint Protection 用戶端系統需求」。
- 請參閱第 64 頁的「Linux 適用的 Symantec Endpoint Protection 用戶端系統需求」。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

請參閱第 66 頁的「國際化需求」。

Symantec Endpoint Protection Manager 系統需求

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

表 3-1 Symantec Endpoint Protection Manager 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 **附註：**不支援桌面作業系統。 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 65.x ■ Google Chrome 72.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 - SP2 ■ SQL Server 2016、RTM、SP1 ■ SQL Server 2017 **附註：**不支援 SQL Server Express 版本資料庫。 支援 Amazon RDS 上託管的 SQL Server 資料庫。 **附註：**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。此建議僅適用於 SQL Server 2008、2012 和 2014。 更多資訊： 適用於 Microsoft SQL Server 的 TLS 1.2 支援

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。

表 3-2 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 **附註：**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 **附註：**您的 Symantec Endpoint Protection Manager 伺服器可能需要額外的 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

附註：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。

請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

適用於 Windows 的 Symantec Endpoint Protection 用戶端系統需求

表 3-3 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)	■ 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) ■ Windows 10 April 2019 Update 請參閱第 63 頁的「Windows Embedded 適用的 Symantec Endpoint Protection 用戶端系統需求」。
作業系統 (伺服器)	■ Windows Server 2008 (32 位元、64 位元；RTM、R2、SP1 和 SP2) 包括 Windows Small Business Server 2008 (64 位元) 和 Windows Essential Business Server 2008 (64 位元) ■ Windows Small Business Server 2011 (64 位元) ■ 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

表 3-4 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)	■ 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 **附註：**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) **附註：**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： ■ 表 3-5 描述 Symantec Endpoint Protection 安裝到系統磁碟機時的硬碟機系統需求。 ■ 表 3-6 描述 Symantec Endpoint Protection 安裝到替代磁碟機時的硬碟機系統需求。 **附註：**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。

表 3-5 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

用戶端類型	需求
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。

表 3-6 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。

請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

Symantec Endpoint Protection 強化的系統需求

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

表 3-7 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 **附註：**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 Symantec Endpoint Detection and Response，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。 請參閱第 60 頁的「適用於 Windows 的 Symantec Endpoint Protection 用戶端系統需求」。
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

元件	需求
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)。

請參閱 Symantec Endpoint Protection 對 Windows Embedded 的支援。

請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

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

表 3-8 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	Mac OS X 10.10、10.11；macOS 10.12、10.13、10.14

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

表 3-9 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

元件	需求
作業系統	■ Amazon Linux ■ CentOS 6U3 - 6U9、7 - 7U5；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 ■ Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9、7 - 7U5 ■ 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；32 位元和 64 位元 如需受支援的作業系統核心清單，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` ■ 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 apt-get install libx11-6:i386 libgcc1:i386 libc6: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

請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

國際化需求

在非英文或混合語言環境中安裝 Symantec Endpoint Protection Manager 時，有某些特定限制。

表 3-10 國際化需求

元件	需求
電腦名稱、伺服器名稱及工作群組名稱	支援非英文字元時的限制如下： ■ 若主機或使用者使用雙位元字元集或高 ASCII 字元集，可能無法進行網路稽核。 ■ 在 Symantec Endpoint Protection Manager 主控台或用戶端使用者介面上，可能無法正常顯示雙位元字元集名稱或高 ASCII 字元集名稱。 ■ 較長的雙位元字元集或高 ASCII 字元集主機名稱長度不能超過 NetBIOS 的限制。如果主機名稱長度超過 NetBIOS 的限制，則 Symantec Endpoint Protection Manager 主控台不會出現「首頁」、「監視器」和「報告」頁面。
英文字元	下列情形必須使用英文字元： ■ 將用戶端套件部署至遠端電腦。 ■ 在「管理伺服器組態精靈」中定義伺服器儲存資料夾。 ■ 定義 Symantec Endpoint Protection Manager 的安裝路徑。 ■ 定義部署用戶端至遠端電腦時的憑證。 ■ 定義群組名稱。 您可以為包含非英文字元的群組名稱建立用戶端套件。但是，若群組名稱包含非英文字元，您可能無法使用「推動部署精靈」部署用戶端套件。 ■ 將非英文字元推送至用戶端電腦。 用戶端使用者介面可能無法正常顯示伺服器端產生的某些非英文字元。 例如，以非雙位元字元集命名的用戶端電腦，無法正常顯示雙位元字元集位置的名稱。
「使用者資訊」用戶端電腦對話方塊	安裝匯出的套件後，在**「使用者資訊」**用戶端電腦對話方塊中提供回應時，請勿使用雙位元字元或高 ASCII 字元。 請參閱第 222 頁的「收集使用者資訊」。
授權啟用精靈	請勿在下列欄位中使用雙位元字元： ■ **名** ■ **姓** ■ **公司名稱** ■ **城市** ■ **州/省** 請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

如需最新系統需求，請參閱：所有端點防護版本的版本說明、新修正和系統需求

Symantec Endpoint Protection 產品授權需求

如果您希望在試用期到期後使用 Symantec Endpoint Protection，則必須購買並啟用產品授權。

表 3-11 產品授權需求

產品	需求
Symantec Endpoint Protection 14 的已付費授權安裝	Symantec Endpoint Protection 內包含 60 天的試用授權。 試用授權到期時，您必須購買可涵蓋每個已部署用戶端的授權。一份授權可涵蓋所有用戶端，不論平台和版本為何。 請參閱第 85 頁的「我需要多少個 Symantec Endpoint Protection 授權？」。
Symantec Endpoint Protection 12.1 的已付費授權安裝	Symantec Endpoint Protection 可接受舊版賽門鐵克病毒防護軟體的授權檔。舊版授權到期時，您必須購買新授權。

下列術語適用於賽門鐵克產品授權：

序號
: 授權中有一個序號，可以獨特的方式辨識您的授權，並使授權與您的公司相關聯。此序號可用來啟用 Symantec Endpoint Protection 授權。

  請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

已部署
: 「已部署」表示受 Symantec Endpoint Protection 用戶端軟體保護的端點電腦。例如，「我們具有 50 個已部署基座」表示有 50 個端點安裝了用戶端軟體。

啟用
: 您可以啟用 Symantec Endpoint Protection 產品授權，以便對所有程式功能進行不受限制的存取。您可以使用「授權啟用精靈」完成啟用過程。

  請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

基座
: 一個基座是由 Symantec Endpoint Protection 用戶端軟體保護的一台端點電腦。授權須購買，僅對特定個數的基座有效。「有效基座個數」表示在所有的有效授權中指定的基座總數。

試用授權
: 試用授權表示具有完整功能的 Symantec Endpoint Protection，可在免費試用期內運作。如果要在試用期後繼續使用 Symantec Endpoint Protection，必須為您的安裝軟體購買並啟用授權。您不需要解除安裝軟體，即可將試用版軟體轉換為授權安裝。

  試用期是指自初始安裝 Symantec Endpoint Protection Manager 起 60 天內的時間。

  請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。

已過度部署
: 授權已過度部署是指已部署用戶端的數量超過授權基座個數的數量。

瞭解授權需求，是規劃 Symantec Endpoint Protection 安裝以及安裝後管理產品授權的一部分。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

支援的虛擬安裝和虛擬化產品

您可以在虛擬環境中執行的受支援作業系統上安裝 Symantec Endpoint Protection。請在客體作業系統 (而非主機) 上安裝 Symantec Endpoint Protection。

下列虛擬化產品支援 Symantec Endpoint Protection Manager、主控台和內嵌資料庫元件，以及適用於 Windows 和 Linux 的 Symantec Endpoint Protection 用戶端軟體：

- Microsoft Azure
- Amazon 工作區
- VMware WS 5.0 (工作站) 或更新版本
- VMware GSX 3.2 (企業) 或更新版本
- VMware ESX 2.5 (工作站) 或更新版本
- VMware ESXi 4.1 至 5.5
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1
- VMware ESXi 6.0 Update 2
- VMware ESXi 6.0 Update 3
- VMware ESXi 6.5
- VMware ESXi 6.5U1
- VMware ESXi 6.5U2
- VMware ESXi 6.7
- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V

- Citrix XenServer 5.6 或更新版本
- Virtual Box (由 Oracle 提供)

請參閱第 581 頁的「在虛擬基礎架構中使用 Symantec Endpoint Protection」。

請參閱第 409 頁的「隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能」。

部分 1

管理自訂安裝

4

規劃安裝

本章包含以下主題：

網路架構考量

您可以針對測試用途而安裝 Symantec Endpoint Protection，無需考量您的公司網路架構。您可以安裝 Symantec Endpoint Protection Manager 和數個用戶端，並熟悉其特點與功能。

當您準備好安裝正式用戶端時，您應根據您的組織架構和運算需求來規劃您的部署。

規劃部署時應考量下列要素：

- Symantec Endpoint Protection Manager
  管理員使用 Symantec Endpoint Protection Manager 管理安全性政策和用戶端電腦。針對已安裝 Symantec Endpoint Protection Manager 的電腦，您可能要考量到安全性與可用性。
- 遠端主控台
  管理員可以使用執行主控台軟體的遠端電腦來存取 Symantec Endpoint Protection Manager。管理員不在辦公室時可使用遠端電腦。您應確保遠端電腦符合遠端主控台需求。
- 本機及遠端電腦
  遠端電腦的網路連線可能較慢。您可能要使用有別於在本機電腦進行安裝的安裝方法。

- 如筆記型電腦等可攜式電腦
  可攜式電腦可能不會定期與網路連線。您可能會想確認可攜式電腦具有啟用 LiveUpdate 排程的 LiveUpdate 政策。未定期登入的可攜式電腦不會取得其他政策更新。
- 位於安全區域中的電腦
  位於安全區域的電腦可能需要與位於非安全區域的電腦不同的安全性設定。

確認您計畫安裝用戶端的電腦。賽門鐵克建議您在所有未受防護的電腦上安裝用戶端軟體，包括執行 Symantec Endpoint Protection Manager 的電腦。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

關於選擇資料庫類型

Symantec Endpoint Protection Manager 會使用資料庫來儲存用戶端及設定的相關資訊。進行架構程序時，會建立資料庫。您必須先決定要使用的資料庫，再安裝管理伺服器。使用資料庫的管理伺服器架構完畢之前無法使用主控台。

表 4-1 Symantec Endpoint Protection Manager 使用的資料庫

資料庫類型	說明
內嵌資料庫	內嵌資料庫包含在 Symantec Endpoint Protection Manager 之中。 內嵌資料庫不需要架構，是比較容易安裝的資料庫。內嵌資料庫最多支援 5,000 個用戶端。 請參閱第 72 頁的「關於基本管理伺服器設定」。
SQL Server 資料庫	如果選擇使用此選項，您必須在安裝 Symantec Endpoint Protection Manager 之前先安裝 SQL Server 和 SQL Server Native Client。為取得最佳相容性，請安裝與 SQL Server 版本等同的 SQL Server Native Client 版本。 您可考慮購買並安裝 SQL Server，原因如下： ■ 必須支援 5,000 個以上用戶端。使用 SQL Server 的每個管理伺服器最多可支援 18,000 個用戶端 (針對 14.x) 或 50,000 個用戶端 (針對 12.1.x)。如果您的組織有更多用戶端，則可安裝另一台管理伺服器。 ■ 需支援容錯移轉和負載平衡。 ■ 您需要將其他的管理伺服器設為網站夥伴。 請參閱第 641 頁的「判斷需要的網站數量」。 如果您建立的是 SQL Server 資料庫，則必須先安裝 SQL Server 實例。然後，您必須架構它，以便與管理伺服器進行通訊。 請參閱第 73 頁的「關於 SQL Server 組態設定」。

關於基本管理伺服器設定

當您安裝 Symantec Endpoint Protection Manager 時，下列值表示預設設定。

只有使用自訂組態安裝 Symantec Endpoint Protection Manager 時，才能架構部分下列值。

請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

請參閱第 94 頁的「Symantec Endpoint Protection 的通訊埠」。

表 4-2 基本伺服器設定

設定	預設	敘述
網站名稱	我的網站 (預設值) 網站 *本地主機名稱* (自訂)	出現在 Symantec Endpoint Protection Manager 中的網站名稱。網站名稱是用來架構所有功能並且在 Symantec Endpoint Protection Manager 內執行這些功能的最高層級容器。
伺服器名稱	*本地主機名稱*	執行 Symantec Endpoint Protection Manager 的電腦名稱。
伺服器儲存資料夾	*SEPM_Install*\data	Symantec Endpoint Protection Manager 放置資料檔案 (包括備份、遠端複製日誌和其他檔案) 的目錄。如果不存在，安裝程式會建立這個目錄。 *SEPM_Install* 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。
加密密碼	無	此密碼會加密 Symantec Endpoint Protection Manager 和用戶端之間的通訊。 如果您選擇預設組態，則系統會自動為您產生加密密碼。您可以從摘要畫面將這項資訊列印或複製到剪貼簿。 如果您選擇自訂組態，可以讓系統自動產生隨機密碼，或是建立自己的密碼。密碼可以是 6 至 32 個英數字元。 記下這個密碼並妥善保管。建立資料庫之後，您無法變更或復原密碼。如果您沒有可還原的備份資料庫，也必須輸入這個密碼，才能夠進行災難復原。 請參閱第 646 頁的「災難復原最佳實務準則」。
使用者名稱	admin	第一次登入 Symantec Endpoint Protection Manager 主控台時所使用的預設使用者名稱。這個值不可架構。
密碼	無	伺服器架構期間為管理員帳戶指定的密碼。 您需要原始管理員密碼才能在稍後重新架構管理伺服器。記下這個密碼並妥善保管。
電子郵件地址	無	系統通知會傳送到指定的電子郵件地址。

關於 SQL Server 組態設定

如果您安裝 Symantec Endpoint Protection Manager 搭配 SQL Server 資料庫使用，SQL Server 會有特定的架構需求。

建立資料庫之前，Symantec 建議您另外安裝符合 Symantec 安裝及架構需求的 SQL Server 實例。您可在現有實例內安裝資料庫，但必須正確架構此實例，否則資料庫安裝會失敗。 例如，如果選取區分大小寫的 SQL 定序，安裝會失敗。

警告：若要確保遠端 SQL Server 通訊的最高安全，請將兩台伺服器置於同一安全子網路中。

表 4-3 必要的 SQL Server 組態設定

架構設定	安裝需求
實例名稱	不要使用預設實例名稱。請建立如 SEPM 的名稱。 根據預設，安裝 Symantec Endpoint Protection Manager 時，會在 SQL Server 實例中建立名為 Sem5 的資料庫。預設名稱雖然受到支援，但如果您在同一電腦上安裝多個實例，就可能會造成混淆。
驗證架構	「混合模式」或「Windows 驗證」模式 請參閱第 76 頁的「關於 SQL Server 資料庫驗證模式」。
sa 密碼	設定「混合模式」驗證時，請設定此密碼。
啟用的通訊協定	TCP/IP
TCP/IP 的 IP 位址	啟用 IP1 和 IP2
IP1、IP2 及 IPALL 的 TCP/IP 埠號	將「TCP 動態通訊埠」留白，並指定 TCP 埠號。通常，預設通訊埠為 1433。請在建立資料庫時指定此埠號。 Symantec Endpoint Protection Manager 資料庫不支援動態通訊埠。
遠端連線	必須啟用。此外必須指定 TCP/IP 通訊協定。

如果您的資料庫位於遠端伺服器上，則也必須在執行 Symantec Endpoint Protection Manager 的電腦上安裝 SQL Server 用戶端元件。SQL Server 用戶端元件包含 `BCP.EXE`。SQL Server 用戶端元件的版本號碼應與您使用的 SQL Server 的版本號碼相同。如需安裝指示，請參閱 SQL Server 說明文件。

在安裝的 Symantec Endpoint Protection Manager 資料庫組態階段，您需要選取和輸入各種資料庫值。請瞭解您必須做的決定，以便能正確架構資料庫。

表 4-4 中顯示了您可能需要在開始安裝程序之前瞭解的設定。

表 4-4 SQL Server 資料庫設定

設定	預設	敘述
伺服器名稱	*本機主機名稱*	執行 Symantec Endpoint Protection Manager 的電腦名稱。

設定	預設	敘述
伺服器儲存資料夾	*SEPM_Install*\data	Symantec Endpoint Protection Manager 用來存放資料檔的資料夾，其中包括備份檔案、複寫檔案及其他 Symantec Endpoint Protection Manager 檔案。如果此資料夾不存在，安裝程式會自行建立。 *SEPM_Install* 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。
加密密碼	無	加密 Symantec Endpoint Protection Manager 和用戶端之間通訊的密碼。此密碼可以是 6 至 32 個英數字元，而且是必要的。 記下這個密碼並妥善保管。建立資料庫之後，您無法變更或還原密碼。如果您沒有可還原的備份資料庫，也必須輸入這個密碼，才能夠進行災害復原。 請參閱第 646 頁的「災難復原最佳實務準則」。
資料庫伺服器	*本地主機名稱*	已安裝 SQL Server 之電腦的名稱以及選擇性實例的名稱。如果資料庫伺服器是與未命名的預設實例一同安裝，則輸入*主機名稱*或主機的 *IP 位址*。如果資料庫伺服器是與已命名的實例一同安裝，則輸入*主機名稱**實例名稱*或 *IP 位址**實例名稱*。使用*主機名稱*只會對正確架構的 DNS 有效。 如果是安裝於遠端資料庫伺服器，必須先在執行 Symantec Endpoint Protection Manager 的電腦安裝 SQL Server 用戶端元件。
SQL Server 通訊埠	1433	用來與 SQL Server 傳送和接收流量的通訊埠。 不支援使用通訊埠 0。通訊埠 0 會指定隨機交涉的通訊埠。
資料庫名稱	sem5	已建立的資料庫名稱。
資料庫使用者名稱	sem5	已建立的資料庫使用者帳戶名稱。使用者帳戶是標準角色，有讀取及寫入存取權限。名稱可以是英數字元值和特殊字元 ~ # % _ + = | : . 的組合。不允許使用特殊字元 ` ! @ ' $ ^ & * ( ) - { } [ ] " \ / < ; > , ?。也不允許使用下列名稱：sysadmin、server admin、setupadmin、securityadmin、processadmin、dbcreator、diskadmin、bulkadmin。
資料庫密碼	無	與資料庫使用者帳戶相關聯的密碼。名稱可以是英數字元值和特殊字元 ~ # % _ + = | : . / 的組合。不允許使用特殊字元 ! @ * ( ) { } [ ] ; , ?。

設定	預設	敘述
SQL Server Native Client 資料夾	SQL Server 2008：*Install Directory*\100\Tools\Binn SQL Server 2012：*Install Directory*\110\Tools\Binn SQL Server 2014/2016：*Install Directory*\Client SDK\ODBC\110\Tools\Binn	包含 bcp.exe 的本機 SQL Native Client 目錄位置。 所顯示的安裝路徑表示 Microsoft SQL Server 的預設路徑。*Install directory* 表示 Microsoft SQL Server 的安裝磁碟機和目錄。 若要安裝 SQL Server Native Client，請參閱適用於 SQL Server 版本的 Microsoft TechNet 頁面： 安裝 SQL Server Native Client
伺服器使用者名稱	無	資料庫伺服器管理員帳戶的名稱，通常是 sa。
伺服器密碼	無	與資料庫伺服器管理員帳戶相關的密碼，通常是 sa。
資料庫儲存資料夾	按下**「預設值」**之後自動偵測。 SQL Server 2008：*Install Directory*\MSSQL10.MSSQLSERVER\MSSQL\Data SQL Server 2008 R2：*Install Directory*\MSSQL10_50.MSSQLSERVER\MSSQL\Data SQL Server 2012：*Install Directory*\MSSQL11.MSSQLSERVER\MSSQL\Data SQL Server 2014：*Install Directory*\MSSQL12.MSSQLSERVER\MSSQL\Data SQL Server 2016：*Install Directory*\MSSQL13.MSSQLSERVER\MSSQL\Data	SQL Server 資料資料夾的位置。如果您安裝至遠端伺服器，則磁碟區識別項必須符合遠端伺服器識別項。 所顯示的安裝路徑表示 Microsoft SQL Server 的預設路徑。 ■ 如果是安裝至 SQL Server 2008 的具名實例，則會在 MSSQL10 後面附加實例名稱。例如 \MSSQL10.*instance name*\MSSQL\Data ■ 如果是安裝至 SQL Server 2008 R2 的具名實例，則會在 MSSQL10_50 後面附加實例名稱。例如 \MSSQL10_50.*instance name*\MSSQL\Data ■ 如果是安裝至 SQL Server 2012 的具名實例，則會在 MSSQL11 後面附加實例名稱。例如 \MSSQL11.*instance name*\MSSQL\Data ■ 如果是安裝至 SQL Server 2014 的具名實例，則會在 MSSQL12 後面附加實例名稱。例如 \MSSQL12.*instance name*\MSSQL\Data ■ 如果是安裝至 SQL Server 2016 的具名實例，則會在 MSSQL13 後面附加實例名稱。例如 \MSSQL13.*instance name*\MSSQL\Data **附註：**如果輸入的是正確的資料庫伺服器和實例名稱，按下**「預設值」**就會顯示正確的安裝資料夾。如果按下**「預設值」**後未出現正確的安裝資料夾，則表示資料庫建立失敗。

請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

關於 SQL Server 資料庫驗證模式

Symantec Endpoint Protection Manager 支援兩種 SQL Server 資料庫驗證模式：

- Windows 驗證模式
- 混合模式

您可以架構 SQL Server 使用「Windows 驗證」或混合模式驗證。「混合」模式驗證可使用 Windows 或 SQL Server 認證。架構 SQL Server 使用混合模式時，就可設定 Symantec Endpoint Protection Manager 使用「Windows 驗證」或混合模式驗證。將 SQL Server 設為使用「Windows 驗證」模式時，也必須架構 Symantec Endpoint Protection Manager 使用「Windows 驗證」模式。

使用「Windows 驗證」模式的遠端資料庫連線需注意下列需求：

- 若是 Active Directory 環境中的部署，Symantec Endpoint Protection Manager 及 SQL Server 必須位於相同的 Windows 網域。
- 若是「工作群組」環境中的部署，本機電腦及遠端電腦的 Windows 帳戶認證必須相同。

請參閱第 73 頁的「關於 SQL Server 組態設定」。

移除 Symantec Endpoint Protection Manager

移除 Symantec Endpoint Protection Manager 時也會移除伺服器和主控台。在移除過程中，您可以選擇移除資料庫和資料庫備份檔案。若要移除 Symantec Endpoint Protection Manager，您可以使用 Windows「控制台」來移除、修復或變更應用程式，通常是使用**「程式和功能」**。

如果您打算重新安裝 Symantec Endpoint Protection Manager，則應於移除資料庫前先備份資料庫。

在某些情況下，您可能需要使用其他方法 (如 CleanWipe 公用程式) 來移除 Symantec Endpoint Protection Manager。請參閱：

移除 Symantec Endpoint Protection

請參閱第 648 頁的「備份資料庫和日誌」。

使用 CleanWipe 公用程式解除安裝 Symantec Endpoint Protection

您可以使用數種方法解除安裝 Symantec Endpoint Protection 產品元件，例如透過 Windows 控制台。如果這些通用方法不起作用，您可以使用 CleanWipe 公用程式。

警告：第一次您有解除安裝困難時，賽門鐵克技術支援不建議使用 CleanWipe。當常用解除安裝方法不成功時，您僅應使用 CleanWipe 作為最後一招。

您應永遠使用 CleanWipe 最新版本移除 Symantec Endpoint Protection。CleanWipe 可以解除安裝舊的 Symantec Endpoint Protection 安裝。但是，您不應使用舊版 CleanWipe 移除更新版本的 Symantec Endpoint Protection。此動作可能導致非預期結果。

附註：CleanWipe 會移除 Symantec 企業產品線的安全軟體安裝，例如 Symantec Endpoint Protection。若要移除 Norton 品牌的賽門鐵克消費者產品，請參閱：

下載並執行 Norton Remove and Reinstall 工具

自 14 版起，您還可以直接將 CleanWipe 功能併入 Symantec Endpoint Protection 用戶端套件。您可以透過用戶端安裝設定啟用此選項。如需詳細資訊，請參閱關於 Symantec Endpoint Protection 用戶端預先安裝移除功能。

如果您需要有關 CleanWipe 的協助，可直接聯絡技術支援。

若要從 MySymantec 下載 CleanWipe，請使用下列指南：

MySymantec 入門指南

使用 CleanWipe 公用程式解除安裝 Symantec Endpoint Protection

1. 將包含 Cleanwipe.exe 的資料夾複製到您要執行它所在的電腦。
2. 連按兩下 Cleanwipe.exe，然後按**「下一步」**。
3. 接受授權許可協議，然後按**「下一步」**。
4. 選取您要移除的賽門鐵克產品，然後按兩次**「下一步」**。
5. 當工具執行完時，可能會提示您重新啟動電腦。

   電腦重新啟動後，CleanWipe 重新開啟並繼續執行。
6. 按**「下一步」**。
7. 按下**「完成」**。

   將立即解除安裝您選取的賽門鐵克產品。

如需建議的解除安裝方法的相關資訊，請參閱：

解除安裝 Symantec Endpoint Protection

關於 Symantec Endpoint Protection 用戶端安裝失敗和 CleanWipe

5

管理產品授權

本章包含以下主題：

授權 Symantec Endpoint Protection

Symantec Endpoint Protection 試用期到期以後或您目前的授權到期時需要付費授權。 您可以將現有授權套用到產品升級。安裝 Symantec Endpoint Protection Manager 後，您有 60 天的時間來購買足夠的授權基座，以便涵蓋部署的所有用戶端。

若要管理授權，您必須以管理伺服器的系統管理員帳戶 (如預設帳戶 admin) 登入 Symantec Endpoint Protection Manager。您可使用「授權啟用精靈」啟用新授權或更新授權，或將試用授權轉換為付費授權。您可依據保護網站端點所需的用戶端的數目來授權 Symantec Endpoint Protection。

請參閱第 241 頁的「關於管理員帳戶和存取權限」。

表 5-1 授權工作

工作	敘述
檢查產品授權需求	瞭解所要保護電腦之授權需求的重要性。授權可讓您將 Symantec Endpoint Protection 用戶端安裝在特定數量的電腦上。授權可讓您從 LiveUpdate 下載病毒和間諜軟體定義檔，以及其他安全性內容。 請參閱第 67 頁的「Symantec Endpoint Protection 產品授權需求」。 請參閱第 85 頁的「我需要多少個 Symantec Endpoint Protection 授權？」。 請參閱第 87 頁的「關於多年授權」。
購買授權並將它儲存到管理伺服器	若有下列情形，表示您需要購買授權： ■ 您想購買 Symantec Endpoint Protection。 ■ 您的試用授權已到期。 ■ 您購買的授權已到期。 ■ 您的授權已過度部署。 購買授權之後，您會收到一封包含賽門鐵克授權檔 (.slf) 或授權序號的電子郵件。您可以使用該序號啟用安裝。您也可以使用該序號從 MySymantec 下載 .slf 檔案的複本。您不需要手動下載授權檔。 請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。 請參閱第 84 頁的「檢查 Symantec Endpoint Protection Manager 中的授權狀態」。 請參閱第 81 頁的「關於試用授權」。 請參閱第 83 頁的「關於管理授權」。
啟用所購買的授權	您可以使用 Symantec Endpoint Protection Manager 主控台中的「授權啟用精靈」來匯入和啟用賽門鐵克產品授權。 啟用授權之前，您必須具有下列任一項目： ■ Symantec 授權序號 ■ Symantec 授權檔 (.slf) 您在購買授權時會收到上述任一項目。 請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。 請參閱第 83 頁的「關於管理授權」。

工作	敘述
備份您的授權檔	備份您的授權檔，以便在資料庫或電腦硬碟損壞的情形下，仍能保有授權檔。 請參閱第 85 頁的「備份您的授權檔」。 請參閱第 86 頁的「復原刪除的授權」。
檢閱預先架構的授權通知	預先架構的授權通知會向管理員提出關於授權到期與其他授權問題的警示。 請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。
請記錄您的授權到期時間，並續購授權	檢查已匯入主控台的各項授權的狀態，以瞭解是否需要續購授權或購買更多授權。 請參閱第 84 頁的「檢查 Symantec Endpoint Protection Manager 中的授權狀態」。 請參閱第 84 頁的「關於更新 Symantec Endpoint Protection 授權」。

關於試用授權

透過試用授權可以在您的環境評估並測試 Symantec Endpoint Protection。

試用授權適用於下列 Symantec Endpoint Protection 元件：

- Symantec Endpoint Protection Manager
- Symantec Endpoint Protection 用戶端
- 存取 LiveUpdate 內容

試用授權到期後，您必須啟用已付費授權，才能保留完整的產品功能。您無需移除試用授權版，即可將 Symantec Endpoint Protection 安裝轉換為完整授權安裝。

此試用授權將會在您安裝 Symantec Endpoint Protection Manager 後 60 天到期。

請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。

關於購買 Symantec Endpoint Protection 授權

若有下列情形，表示您需要購買授權：

- 您的試用授權已到期。 Symantec Endpoint Protection 附有試用版授權，該授權允許您在您的環境中安裝及評估產品。
- 您目前的授權已到期。
- 您目前的授權已過度部署。 過度部署表示您部署的用戶端已超過目前授權允許的數目。

根據購買授權的方式，您將透過電子郵件收到產品授權序號或 Symantec 授權檔。 授權檔使用 .slf 副檔名。 透過電子郵件接收授權檔時，該檔案將以 .zip 檔案的形式附加到電子郵件。 您必須從 .zip 檔案解壓縮 .slf 檔案。

將授權檔儲存到可從 Symantec Endpoint Protection Manager 主控台進行存取的電腦。 許多使用者將授權儲存在裝載 Symantec Endpoint Protection Manager 的電腦上。 為了安全起見，許多使用者也將授權複本儲存到不同的電腦或抽取式儲存媒體上。

警告：為了避免授權檔損毀，請不要以任何方式開啟或改變檔案內容。 不過，您可以根據需要複製和儲存授權。

表 5-2 購買授權工作

工作	敘述
決定您的授權需求	請參閱第 67 頁的「Symantec Endpoint Protection 產品授權需求」。 請參閱第 85 頁的「我需要多少個 Symantec Endpoint Protection 授權？」。
找出購買產品授權的位置	您可以從以下來源購買賽門鐵克產品授權： ■ 賽門鐵克網路商店： http://store.symantec.com/ ■ 當地就近的賽門鐵克經銷商： 若要尋找經銷商，請使用 合作夥伴定位器。 若要瞭解有關賽門鐵克合作夥伴的更多資訊，請移至 https://www.symantec.com/partners ■ 賽門鐵克銷售團隊： 造訪 賽門鐵克訂購網站以取得銷售聯絡資訊。
瞭解有關從 Symantec Endpoint Protection 附帶的試用授權進行升級的更多資訊	請參閱第 81 頁的「關於試用授權」。
取得購買授權的協助，或詳細瞭解授權	https://support.symantec.com

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

必填的授權聯絡資訊

啟用程序會提示您提供任何漏填的授權聯絡資訊。精靈中提供的隱私權聲明會說明如何使用此資訊。您必須表示接受隱私權條件才能完成啟用程序。

表 5-3 授權聯絡資訊

資訊類型	說明
技術聯絡人	負責與安裝或維護端點安全性基礎架構有關的技術活動的人員的聯絡資訊。必須填寫聯絡人的姓名、電子郵件地址和電話號碼。

資訊類型	說明
主要聯絡人	代表公司的人員的聯絡資訊。必須填寫聯絡人的姓名、電子郵件地址和電話號碼。 **附註：** 按下該核取方塊以指定技術聯絡人和主要聯絡人為同一人。
公司資訊	包含公司名稱、地點、電話號碼和電子郵件地址。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

關於管理授權

您可以使用 MySymantec 來下載和啟用產品授權碼。不過，您也可以從 Symantec Endpoint Protection Manager 啟用授權，這個方式較簡單且更快。

Symantec 授權入口網站現在為 MySymantec 的一部分。如果您有 MySymantec 的現有憑證，可以透過「我的產品」標籤使用那些憑證來存取授權資訊。

如果您沒有 MySymantec 帳戶，則必須建立一個帳戶，才能存取授權管理。下列網站提供用於設定 MySymantec 存取權的詳細指示：

入門指南：就地執行所需的一切動作

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

關於產品升級和授權

賽門鐵克發行新版本的 Symantec Endpoint Protection 後，您可以將現有的使用中授權套用至新版本。您會收到電子郵件，通知您有新版本，郵件中還會包含有關下載 Symantec Endpoint Protection 新版本的指示。

在某些情況下，您可能不會收到通知電子郵件，而錯過了啟用新升級所需的所有重要資訊。如需授權和產品升級的詳細資訊，請參閱升級產品頁面上有關內部部署軟體升級的章節。

Symantec Endpoint Protection Manager 前後文相關說明提供關於您使用之 Symantec Endpoint Protection 版本特定的升級授權應用程式的其他協助。

請參閱第 119 頁的「升級至新版本」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

關於更新 Symantec Endpoint Protection 授權

如果您目前的授權即將到期，Symantec Endpoint Protection Manager 會開始向 Symantec Endpoint Protection 管理員傳送授權到期通知。賽門鐵克強烈建議您在授權到期前續購授權。

續購授權時，管理伺服器會移除過期授權，然後換成新授權。若要續購授權，請造訪賽門鐵克授權網路商店，或與您的賽門鐵克合作夥伴或當地就近的賽門鐵克經銷商聯絡。

如果您意外刪除了授權，可從 Symantec Endpoint Protection Manager 主控台還原授權。

請參閱第 81 頁的「關於購買 Symantec Endpoint Protection 授權」。

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

請參閱第 86 頁的「復原刪除的授權」。

檢查 Symantec Endpoint Protection Manager 中的授權狀態

您可以查看管理伺服器是使用試用版授權，還是已付費授權。對於已匯入主控台的所有已付費授權，您也可以取得下列相關授權資訊：

- 授權序號、基座總個數、到期日
- 有效基座個數
- 已部署的基座個數
- 已過期的基座個數
- 已過度部署的用戶端個數

試用版授權狀態僅提供與到期日期相關的有限資訊。

檢查您使用的是已付費授權還是試用授權

◆ 在主控台中，執行下列其中一項工作：

- 按下**「管理員」>「授權」**。
- 按下**「首頁」>「授權詳細資料」**。

檢查授權到期日

◆ 在主控台中，按下**「管理員」>「授權」**。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

我需要多少個 Symantec Endpoint Protection 授權？

Symantec Endpoint Protection 的授權數會根據下列規則強制執行：

表 5-4 授權強制執行規則

適用範圍	規則
授權期限	授權期限是指從啟用的日期時間開始，到授權期限的最後一天的午夜結束。 如果您有多個站台，則授權的到期日為地處最西邊的 Symantec Endpoint Protection Manager 資料庫的日期和時間。
Symantec Endpoint Protection 元件	Symantec Endpoint Protection 授權適用於 Symantec Endpoint Protection 用戶端。例如，在具有 50 部電腦的網路中，授權必須至少提供給 50 個基座個數。Symantec Endpoint Protection Manager 實例不需要授權。 Symantec Endpoint Protection Manager 不要求用戶端具有存取管理伺服器的授權。連線到管理伺服器的未授權用戶端都會獲得一個授權。您必須確保已購買足夠的授權基座，以便涵蓋每部用戶端電腦。
站台和網域	Symantec Endpoint Protection 產品授權適用於整個安裝，無論安裝所包含的複製站台或網域數目為多少。例如，具有 100 個基座個數的授權涵蓋兩個站台的安裝，其中每個站台各有 50 個基座個數。 如果您並未實作複寫，您可以部署相同的 .slf 檔案至多部 Symantec Endpoint Protection 管理伺服器。向管理伺服器報告的用戶端數量不得超過授權基座總數。
平台	授權基座會套用於任何平台上執行的用戶端，不論平台為 Windows、Mac 還是 Linux。
產品和版本	授權基座一視同仁適用於多個產品版本。

如需授權存取第三方伺服器軟體 (例如 Microsoft SQL Server) 的用戶端的相關資訊，請連絡軟體廠商。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

備份您的授權檔

賽門鐵克建議您備份您的授權檔。備份授權檔可以保留授權檔案，以備資料庫或主控台電腦的硬碟損壞時使用。

依據預設，當您使用授權啟用精靈匯入授權檔時，Symantec Endpoint Protection Manager 會在以下預設位置放入授權檔的複本：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\license

如果您忘記了原先下載或透過電子郵件收到的授權檔放在哪裡，可從賽門鐵克授權入口網站再次下載檔案。

備份您的授權檔

- 使用 Windows，從您儲存檔案的目錄中將 **.slf** 授權檔複製到您選取的另一台電腦。

  請參照貴公司備份檔案的程序。

請參閱第 42 頁的「啟用或匯入 Symantec Endpoint Protection 產品授權」。

請參閱第 83 頁的「關於管理授權」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

復原刪除的授權

如果您不小心刪除了授權檔，可以從 Symantec Endpoint Protection Manager 主控台進行還原。

還原刪除的授權

1. 在 Symantec Endpoint Protection Manager 主控台的**「管理」**頁面中，按下**「授權」**，然後在**「工作」**下方按下**「還原刪除的授權」**。
2. 在**「授權還原」**面板中，勾選要還原之已刪除授權旁的方塊，然後按下**「送出」**。

從資料庫清除過時的用戶端以使更多授權可用

Symantec Endpoint Protection Manager 可能會因為過時的用戶端，而錯誤地顯示過度部署的授權狀態。這些是受保護環境中不再與 Symantec Endpoint Protection Manager 進行通訊之用戶端的資料庫項目。用戶端可能會因為許多原因而呈現過時，例如當您升級作業系統、解除委任電腦，或變更硬體架構時。

如果授權報告顯示授權的基座個數大於已知的部署基座數，則應該清除過時用戶端的資料庫。過時的用戶端不利於產品授權，因此一旦建立過時用戶端，立即將其清除是很重要的。根據預設，每隔 30 天會進行一次清除。您可以縮短清除週期的間隔，以更快清除過時的用戶端。請在清除週期完成後，視需要重設間隔以符合長期需求。

在非持續虛擬桌面基礎架構 (VDI) 中，您可以設定一段單獨的時間用於清除非持續用戶端。此設定會清除您所設定期間內未連線的離線用戶端。非持續離線的用戶端不會影響授權計數。

從資料庫清除過時的用戶端以使更多授權可用

1. 在主控台的**「管理員」**頁面上，按下**「網域」**，在網域上按下滑鼠右鍵，然後按下**「編輯網域屬性」**。
2. 在**「一般」**標籤上，將**「刪除指定的時間內未連線的用戶端」**設定從預設值 **30** 變更為 **1**。

   您不需要因授權用途而設定清除非持續用戶端的選項。離線的非持續用戶端不會計算在授權總數內。

3 按下**「確定」**。

4 請在經過 24 小時之後，將設定復原為 30 天，或其他符合所需的間隔。

請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

關於多年授權

購買多年授權時，會根據授權有效的年數，收到等數的一組授權檔案。例如，三年授權會包含三個獨立授權檔。啟用多年授權時，會在同一個啟用階段作業中匯入所有的授權檔。Symantec Endpoint Protection Manager 會將獨立授權檔合併成一個啟用的授權，這個授權會在購買期限內有效。

未提供建議時，您可以啟用低於全數的授權檔。此時，Symantec Endpoint Protection Manager 會合併檔案，並套用最後到期之授權檔的持續期間。例如，僅啟用前兩個授權檔的三年授權，表示持續時間僅兩年。之後再啟用第三個檔案時，Symantec Endpoint Protection Manager 會精準報告授權的完整持續期間為三年。任何情況下，基座個數都會與所購買的基座個數一致。

當 Symantec Endpoint Protection Manager 合併檔案時，會刪除持續期間最短的檔案，並保留持續期間最長的檔案來進行內部授權保留功能。如果您認為某個授權遭到 Symantec Endpoint Protection Manager 不當刪除，請還原並重新啟用刪除的授權。

您可以查看與使用中授權相關聯且持續期間較短的授權序號。在**「管理員」**頁面上，按下**「授權」**，然後按下啟用的授權。相關聯的授權會出現在**「相關授權」**欄中。

請參閱第 86 頁的「復原刪除的授權」。

請參閱第 79 頁的「授權 Symantec Endpoint Protection」。

授權非受管 Windows 用戶端

非受管用戶端不需要手動安裝授權檔。但是，若要從非受管 Windows 用戶端傳送信譽資料，您必須在該非受管用戶端上安裝已付費授權。非受管 Mac 用戶端和 Linux 用戶端不會提交信譽資料。

授權非受管 Windows 用戶端

1 找到您目前的賽門鐵克授權檔 (.slf) 並建立該檔案的複本。

請使用您在 Symantec Endpoint Protection Manager 上用於啟用授權的相同檔案。

2 在用戶端電腦上，將複製的授權檔置於 Symantec Endpoint Protection 用戶端收件匣中。根據預設，收件匣所在的資料夾會處於隱藏狀態，因此請使用「資料夾選項」顯示隱藏的檔案和資料夾。

- 在使用 Vista 或更新版本的 Windows 用戶端上，收件匣預設位於：C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

- 在 Vista 版本之前的 Windows 上執行 12.1.x 的用戶端上，收件匣預設位於：C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

如果授權檔無效或授權安裝失敗，將會建立名為 `Invalid` 的資料夾且該無效授權將置於該資料夾中。如果授權檔有效，則系統會在處理該檔案後自動將其從收件匣移除。

3 若要確認是否正確套用授權，請檢查收件匣資料夾中不存在任何檔案。

4 請檢查 .slf 檔案位於下列其中一個資料夾中：

- 若是執行 Vista 或更新版本 Windows 的用戶端：C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config
- 若是在 Vista 版本之前的 Windows 上執行 12.1.x 的用戶端：C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

您也可以將 .slf 檔案納入第三方部署套件中。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

6

管理用戶端安裝

本章包含以下主題：

準備用戶端安裝

您必須在每個想要保護的電腦上安裝 Symantec Endpoint Protection 用戶端，無論該電腦為實體電腦還是虛擬電腦。

表 6-1　　用戶端電腦安裝工作

動作	敘述
確認用戶端電腦	確認您要安裝用戶端軟體的電腦。 檢查所有電腦是否執行支援的作業系統。 **附註：**賽門鐵克建議您也在裝載 Symantec Endpoint Protection Manager 的電腦上安裝用戶端。 如需最新系統需求，請參閱：所有端點防護版本的版本說明、新修正和系統需求
識別電腦群組 (選擇性)	確認要用戶端歸屬的電腦群組。 例如，您可以根據電腦類型來將用戶端分組，以遵從公司組織或所需的安全層級。 您可以在安裝用戶端軟體之前或之後建立這些群組。 您也可以匯入現有群組結構，如 Active Directory 結構。 請參閱第 201 頁的「管理用戶端群組」。 請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。
準備用戶端電腦進行部署和安裝	如果使用者沒有其電腦的管理權限，則您應該使用「遠端推送」遠端安裝用戶端軟體。「遠端推送」安裝會要求您輸入具有電腦本機管理權限的憑證。 請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。 準備電腦進行遠端用戶端部署以及在安裝之後成功與 Symantec Endpoint Protection Manager 進行通訊。 請參閱第 91 頁的「準備 Windows 和 Mac 電腦進行遠端部署」。

動作	敘述
確定功能並部署用戶端軟體	您可以使用其中一種可用方式來部署用戶端軟體。 您也可以匯出自訂用戶端套件以便稍後部署，或者使用第三方工具進行部署。 **附註：**賽門鐵克建議您不要在安裝 Symantec Endpoint Protection 的同時執行第三方安裝。 任何進行網路層級或系統層級變更的第三方程式安裝都可能會在安裝 Symantec Endpoint Protection 時導致不理想的結果。 如可能，請在安裝 Symantec Endpoint Protection 之前重新啟動用戶端電腦。 請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。 請參閱第 114 頁的「匯出用戶端安裝套件」。 請參閱第 697 頁的「使用第三方工具安裝 Windows 用戶端軟體」。 ■ 您可以決定要在用戶端電腦上安裝哪些功能。 匯出或部署安裝套件之前，請先架構自訂用戶端功能集與安裝設定。 安裝設定包含安裝資料夾以及重新啟動設定。 您也可以使用預設的用戶端功能集與安裝設定。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。 請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。 ■ 針對 Windows 用戶端，當您架構用戶端安裝設定時，可以選擇自動移除現有的第三方安全軟體。 請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。
驗證安裝狀態	確認成功安裝用戶端，且用戶端可與 Symantec Endpoint Protection Manager 進行通訊。 在重新啟動之前，受管型用戶端可能不會出現在主控台中。 請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。 請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

安裝完成後，您可以採取其他步驟來保護非受管電腦的安全，以及最佳化 Symantec Endpoint Protection 安裝的效能。

請參閱第 30 頁的「第一次在 Symantec Endpoint Protection 上啟動並執行」。

準備 Windows 和 Mac 電腦進行遠端部署

在從 Symantec Endpoint Protection Manager 部署 Symantec Endpoint Protection 之前，您必須採取一些步驟來準備電腦，才能確保遠端安裝成功。這些步驟僅與遠端安裝有關。您之後可以回復這些變更，但您必須再次套用它們，才能執行其他遠端安裝。

表 6-2 列出您必須在打算對其遠端部署 Symantec Endpoint Protection 用戶端之所有電腦上執行的工作。

表 6-3 列出您必須在 Windows 電腦上執行的其他工作。如需您不知如何執行之工作的更多資訊，請參閱您的 Windows 說明文件。

表 6-4 列出您必須在 Mac 電腦上執行的其他工作。如需您不知如何執行之工作的更多資訊，請參閱您的 Mac 說明文件。

附註：您無法從 Symantec Endpoint Protection Manager 將 Symantec Endpoint Protection 用戶端遠端部署至 Linux 電腦。

表 6-2　　準備所有電腦進行遠端部署的工作

工作	詳細資料
具有用戶端電腦的管理員權限	如果用戶端電腦是 Active Directory 網域的一部分，則您應該使用網域管理員帳戶憑證進行遠端推送安裝。否則，請為要在其中部署的每個電腦提供管理員憑證。
修改防火牆設定	修改防火牆設定以允許 Symantec Endpoint Protection 元件之間進行通訊。 請參閱第 94 頁的「Symantec Endpoint Protection 的通訊埠」。
解除安裝現有第三方安全軟體	解除安裝目前正在使用的所有第三方安全軟體。對於 Windows 電腦，Symantec Endpoint Protection 12.1 RU1 MP1 版及更新版本包含一種工具，可協助自動解除安裝選取的第三方安全軟體。您必須分別解除安裝此工具無法解除安裝的任何安全軟體。 **附註：**某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。 您可以在部署之前架構此工具，解除安裝程序在 Symantec Endpoint Protection 安裝之前進行。 請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。
解除安裝無法正常解除安裝的 Symantec Endpoint Protection 用戶端	自 14 版起，您可以解除安裝適用於 Windows 的 Symantec Endpoint Protection 用戶端的現有安裝。只有在現有 Symantec Endpoint Protection 安裝無法正常解除安裝時，才應使用此選項。請勿將此選項作為標準部署的一部分使用。 您可以在部署之前架構此工具，解除安裝程序在 Symantec Endpoint Protection 安裝之前進行。 請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。
解除安裝不支援的或消費性賽門鐵克安全軟體	解除安裝所有不支援的賽門鐵克安全軟體，如 Symantec AntiVirus 或 Symantec Client Security。不支援直接從這些產品進行移轉。 您也必須解除安裝所有消費者品牌的賽門鐵克安全產品，如 Norton Internet Security。 如需解除安裝的相關資訊，請參閱賽門鐵克軟體的說明文件。 請參閱第 122 頁的「最新版本 Symantec Endpoint Protection 14.x 支援的升級路徑」。

表 6-3 Windows 遠端部署準備工作

作業系統	工作
準備 Windows Vista、Windows 7 或 Windows Server 2008/2008 R2 電腦	Windows 的「使用者帳戶控制」會攔截本機管理員帳戶遠端存取遠端管理共用，如 C$ 和 Admin$。如果停用登錄機碼 LocalAccountTokenFilterPolicy，則不需要在遠端部署期間於用戶端電腦上完全停用「使用者帳戶控制」。 若要停用 UAC 遠端限制，請參閱： http://support.microsoft.com/kb/951016 請執行下列工作： ■ 停用「共用精靈」。 「共用精靈」可防範更進階的共用選項在遠端推送期間運作。 ■ 使用「網路和共用中心」啟用網路搜尋。 網路搜尋可讓您瀏覽網路。您無需它即可搜尋網路。 ■ 啟用內建管理員帳戶並指派密碼至此帳戶。 本機管理員帳戶擁有空白密碼時，遠端推送會失敗。 如果 Windows 用戶端電腦是 Active Directory 網域的一部分，請使用具備本機管理員權限的網域管理員帳戶憑證來進行遠端推送。 ■ 驗證您推送安裝的帳戶擁有管理員權限。 ■ 啟用並啟動遠端登錄服務。 ■ 停用或移除 Windows Defender。 請查詢作業系統的文件，以取得如何成功完成這些工作的相關指示。
準備 Windows 8/8.1 或更新版本，或者 Windows Server 2012/2012 R2 或更新版本的電腦	在您部署前，請執行下列工作： ■ 停用登錄機碼 LocalAccountTokenFilterPolicy。 若要停用 UAC 遠端限制，請參閱： http://support.microsoft.com/kb/951016 ■ 啟用並啟動遠端登錄服務。 ■ 停用或移除 Windows Defender。

表 6-4 Mac 遠端部署準備工作

作業系統	工作
準備任何支援作業系統上的 Mac 電腦	在部署前，請在 Mac 電腦上執行下列工作： ■ 按下「**系統喜好設定**」>「**共用**」>「**遠端登入**」，並且允許所有使用者進行存取，或僅允許特定使用者存取，如管理員。 ■ 如果使用 Mac 防火牆，請停用隱藏模式。啟用隱藏模式之後，遠端推送安裝將無法透過「**搜尋網路**」搜尋用戶端。 若要在 Mac 上停用隱藏模式，請參閱下列適用於您的 Mac 作業系統版本的文章。 macOS High Sierra：防止他人搜尋您的 Mac (10.13；Symantec Endpoint Protection 14.0.1) macOS Sierra：防止他人搜尋您的 Mac (10.12；Symantec Endpoint Protection 12.1.6 MP6 - 14.0.1) OS X El Capitan：防止他人搜尋您的 Mac (10.11；Symantec Endpoint Protection 12.1.6 MP2 - 14.0.1) OS X Yosemite：防止他人搜尋您的 Mac (10.10；Symantec Endpoint Protection 12.1.5 - 14.0.1) ■ 確保防火牆不會攔截安全 Shell (SSH) 使用的通訊埠。依據預設，此通訊埠為 TCP 通訊埠 22。此通訊埠允許進行遠端登入的必要通訊。 ■ Bonjour 服務不支援 IPv6 網路。若要確保「**瀏覽網路**」或「**搜尋網路**」顯示這些 Mac，請確定同時啟用了 IPv4 網路。

請參閱第 94 頁的「Symantec Endpoint Protection 的通訊埠」。

請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 90 頁的「準備用戶端安裝」。

Symantec Endpoint Protection 的通訊埠

如果執行 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端的電腦也執行第三方防火牆軟體或硬體，您必須開啟特定通訊埠。這些通訊埠用於遠端部署以及管理伺服器和用戶端之間的通訊。如需有關開啟通訊埠或允許應用程式使用通訊埠的指示，請參閱防火牆產品說明文件。

依據預設，Symantec Endpoint Protection 的防火牆元件已經允許這些通訊埠上的流量。

警告：依據預設，初始安裝時會停用 Symantec Endpoint Protection 用戶端的防火牆，直到電腦重新啟動為止。為確保受到防火牆防護，請讓用戶端上的 Windows 防火牆保持啟用，直到軟體安裝完成且用戶端重新啟動為止。Symantec Endpoint Protection 用戶端防火牆會在電腦重新啟動時自動停用 Windows 防火牆。

表 6-5 用戶端和伺服器安裝與通訊用通訊埠

通訊協定和通訊埠編號	用於	接聽程序	說明	適用版本
TCP 139、445 UDP 137、138	從 Symantec Endpoint Protection Manager 推送部署到 Windows 電腦	svchost.exe：	■ 由 Symantec Endpoint Protection Manager (clientremote.exe) 起始 ■ 無法架構 另也使用 TCP 暫時通訊埠。	全部
TCP 22	從 Symantec Endpoint Protection Manager 推送部署到 Mac 電腦	launchd	■ 由 Symantec Endpoint Protection Manager (clientremote.exe) 起始 ■ 無法架構	全部
TCP 2967	群組更新提供者 (GUP) Web 快取代理功能	ccSvcHst.exe	■ 由 Symantec Endpoint Protection 用戶端起始 ■ 可架構	全部
TCP 2968	WSS 流量重新導向用戶端驗證	ccSvcHst.exe	■ 由 Symantec Endpoint Protection 用戶端起始 ■ 可架構	自 14.2 版起
TCP 2638	內嵌式資料庫和 Symantec Endpoint Protection Manager 之間的通訊	dbsrv16.exe	■ 由 Symantec Endpoint Protection Manager 起始 ■ 可架構	全部
TCP 1433	遠端 SQL Server 資料庫和 Symantec Endpoint Protection Manager 之間的通訊	sqlserver.exe	■ 由 Symantec Endpoint Protection Manager 起始 ■ 可架構 Symantec Endpoint Protection Manager 管理伺服器也使用 TCP 暫時通訊埠。	全部

通訊協定和通訊埠編號	用於	接聽程序	說明	適用版本
TCP 8443	伺服器通訊 (HTTPS)	SemSvc.exe	所有登入資訊和管理通訊都是使用此安全通訊埠。 ■ 由 Java 型遠端主控台或網頁式遠端主控台起始，或是由遠端複製夥伴起始 ■ 可架構 Symantec Endpoint Protection Manager 會接聽此通訊埠。	全部
TCP 9090	Web 主控台通訊	SemSvc.exe	此通訊埠僅用於遠端管理主控台和 Symantec Endpoint Protection Manager 之間的初始 HTTP 通訊。此初始通訊包括安裝，僅顯示登入畫面。 ■ 由遠端 Web 主控台起始 ■ 可架構 另也使用 TCP 暫時通訊埠。	全部
TCP 8014	Symantec Endpoint Protection Manager (HTTP) 與 Symantec Endpoint Protection 用戶端之間的通訊	httpd.exe (Apache)	■ 由 Symantec Endpoint Protection 用戶端起始 ■ 可架構 用戶端也使用 TCP 暫時通訊埠。	全部
TCP 443	Symantec Endpoint Protection Manager (HTTPS) 與 Symantec Endpoint Protection 用戶端之間的通訊	httpd.exe (Apache)	■ 由 Symantec Endpoint Protection 用戶端起始 ■ 可架構 用戶端也使用 TCP 暫時通訊埠。	全部

通訊協定和通訊埠編號	用於	接聽程序	說明	適用版本
TCP 443	Symantec Endpoint Protection Manager 和雲端主控台之間的通訊	prunsvr.exe	如需新增至雲端主控台之代理略過清單的網域相關資訊，請參閱： 代理錯誤訊息顯示在 Endpoint Protection Manager 的「雲端」標籤 >「疑難排解」中	自 14.0.1 版起
HTTPS 443	Symantec Endpoint Protection 漫遊用戶端和雲端主控台之間的通訊	無	與 Symantec Endpoint Protection Manager 進行間歇性通訊的受管用戶端會將其重大事件直接上傳至雲端主控台。Symantec Endpoint Protection Manager 必須向雲端主控台註冊。 請參閱第 237 頁的「從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端」。	自 14.2 版起
HTTP 8081 HTTPS 8082	Symantec Endpoint Protection Manager 與 Content Analysis 伺服器硬體裝置之間的通訊	Symantec Endpoint Protection Manager	管理伺服器使用此通訊埠來與 Content Analysis 伺服器或 Malware Analysis 硬體裝置進行通訊。	自 14.2 版起
TCP 8445	由遠端報告主控台使用	httpd.exe (Apache)	■ 由報告主控台起始 ■ 可架構	全部
TCP 8446	Web 服務	semapisrv.exe	遠端管理應用程式使用此通訊埠透過 HTTPS 傳送 Web 服務流量。 ■ 由遠端監控與管理 (RMM) 和 EDR 起始 ■ 可架構 ■ 用於 Java 遠端主控台 (自 14.0.1 版起)	全部

通訊協定和通訊埠編號	用於	接聽程序	說明	適用版本
TCP 8447	程序啟動程式	semlaunchsrv.exe	此虛擬服務帳戶會啟動任何需要較高權限的 Symantec Endpoint Protection Manager 程序，如此其他服務就不需要具有這些程序。僅遵守 localhost 的要求。 ■ 由 Symantec Endpoint Protection Manager (SemSvc.exe) 起始 ■ 可架構	全部，自 12.1.5 版起
TCP 8765	伺服器控制	SemSvc.exe	由適用於 Tomcat Web 服務的 Symantec Endpoint Protection Manager 使用進行關機。 ■ 由 Symantec Endpoint Protection Manager 起始 ■ 可架構	全部
TCP 1100	主控端物件登錄	SemSvc.exe	指示 AjaxSwing 在哪個通訊埠上執行 RMI 登錄。 ■ 由 AjaxSwing 起始 ■ 無法架構	全部
UDP 514	將資料轉送至 Syslog 伺服器 (選擇性)	SemSvc.exe	■ Syslog 伺服器至 Symantec Endpoint Protection Manager 的離埠流量 ■ Syslog 伺服器的入埠流量 ■ 可架構 來往 Symantec Endpoint Protection Manager的流量會使用 UDP 暫時通訊埠。	

- Windows Vista 及更新版本包含預設已啟用的防火牆。若啟用防火牆，則可能無法遠端安裝或部署用戶端軟體。如果您在將用戶端部署到執行這些作業系統的電腦上時遇到問題，請架構其防火牆以允許所需流量。
- 如果決定在部署後使用 Windows 防火牆，您必須架構它以允許檔案和印表機共用 (通訊埠 445)。

如需架構 Windows 防火牆設定的詳細資訊，請參閱 Windows 說明文件。

請參閱第 72 頁的「關於基本管理伺服器設定」。

請參閱第 91 頁的「準備 Windows 和 Mac 電腦進行遠端部署」。

請參閱第 539 頁的「監控端點防護」。

請參閱第 90 頁的「準備用戶端安裝」。

如何選擇用戶端安裝類型

選擇用戶端安裝套件的用戶端類型。

版本 14.x 包含 Windows 用戶端安裝套件的啟用雲端的選項。這些選項會取代 12.1.x 標準大小和縮減大小用戶端安裝套件。啟用雲端的選項包括標準用戶端和內嵌式/VDI 用戶端。Symantec Endpoint Protection 還包括適用於未連線至雲端之用戶端的暗網安裝。

標準用戶端 (自 14 起)

- 使用雲端中的病毒和間諜軟體定義檔。
- 僅在磁碟上安裝最新的病毒和間諜軟體定義檔。標準用戶端在磁碟方面比舊版標準或暗網 Windows 用戶端小大約 80% 到 90%。
- 使用差量而非完整安裝處理「自動升級」。

暗網用戶端 (自 14 起)

- 無法使用雲端中的定義檔。
- 適用於具有間歇性雲端存取權或無雲端存取權的用戶端。
- 安裝一組完整的病毒和間諜軟體定義檔。
- 類似於舊版標準大小用戶端；如果已連線至雲端，則針對下載鑑識和 SONAR 使用信譽查詢。
- 使用差量而非完整安裝處理「自動升級」。

標準用戶端 (12.1.x)

- 無法使用雲端中的病毒和間諜軟體定義檔，但是可以針對下載鑑識和 SONAR 使用信譽查詢。
- 安裝一組完整的病毒和間諜軟體定義檔。
- 使用差量而非完整安裝處理「自動升級」。

內嵌式/VDI 用戶端 (自 14 起)

- 使用雲端中的病毒和間諜軟體定義檔。
- 僅安裝最新的病毒和間諜軟體定義檔。
  用戶端在磁碟方面比暗網 Windows 用戶端小大約 80% 到 90%。
- 與標準用戶端相較，內嵌式/VDI 用戶端包含更多大小最佳化：
  - 在安裝完成之後，安裝快取不會儲存。此變更表示您無法透過「控制台」來移除或修改安裝，除非您先將安裝套件複製到用戶端電腦。
  - 與標準用戶端相較，內嵌式用戶端會在更多的資料夾上利用 NTFS 壓縮。
- 使用完整安裝套件處理「自動升級」；無法使用差量。

內嵌式/VDI 用戶端 (自 12.1.6 起)

- 無法使用雲端中的病毒和間諜軟體定義檔。
- 僅安裝最新的病毒和間諜軟體定義檔。
  舊版用戶端在磁碟方面比舊版標準 Windows 用戶端小大約 80% 到 90%。
- 此用戶端提供的防護略少於 12.1.x 標準用戶端。賽門鐵克建議您安裝並啟用所有防護功能，其中包括防火牆、下載鑑識、入侵預防和 SONAR。為了取得最高層級的安全性，請使用系統鎖定功能。
- 包括與更新版內嵌式用戶端相同的大小最佳化。
- 使用完整安裝套件處理「自動升級」；無法使用差量
- 已在 12.1.6 中引入。

Symantec Endpoint Protection 對 Windows Embedded 的支援

請參閱第 63 頁的「Windows Embedded 適用的 Symantec Endpoint Protection 用戶端系統需求」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 114 頁的「匯出用戶端安裝套件」。

選擇使用用戶端部署精靈安裝用戶端的方法

安裝 Symantec Endpoint Protection Manager 後，請使用用戶端部署精靈安裝 Symantec Endpoint Protection 用戶端。

表 6-6 用戶端安裝方法

選項	敘述
儲存套件	此安裝選項會建立一個可執行安裝套件，供您儲存到管理伺服器，再派送至用戶端電腦。 然後，使用者會安裝用戶端軟體，因此這些使用者必須對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows、Mac 和 Linux 用戶端。 請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

選項	敘述
遠端推送	遠端推送安裝可將用戶端軟體推送至您指定的電腦。 用戶端電腦將自動開始安裝。 遠端推送安裝不需要使用者對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows 和 Mac 用戶端。 請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。 請參閱第 91 頁的「準備 Windows 和 Mac 電腦進行遠端部署」。
網路連結與電子郵件	使用者會收到其中包含下載及安裝用戶端軟體的連結的電子郵件訊息。 然後，使用者會安裝用戶端軟體，因此這些使用者必須對其電腦具有本機管理員權限。 您可以使用此選項安裝 Windows、Mac 和 Linux 用戶端。 請參閱第 52 頁的「使用網路連結與電子郵件安裝 Symantec Endpoint Protection 用戶端」。

執行「用戶端部署精靈」之前，應檢閱安裝選項，或對其進行自訂，然後選取安裝期間的選項。安裝選項包括要安裝的防護技術、安裝目的地資料夾以及安裝後的重新啟動行為。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

請參閱第 90 頁的「準備用戶端安裝」。

選擇要在用戶端上安裝哪些安全性功能

使用「用戶端部署精靈」部署 Windows 用戶端安裝套件時，必須選擇功能集。功能集指定在用戶端上安裝哪些防護元件。您可以選取預設功能集，也可以自訂功能集。依據電腦的角色以及電腦需要的安全層級或效能層級，決定要安裝哪些功能集。

安裝後，請確保所有防護處於啟用狀態。

表 6-7 用戶端安裝功能集 (Windows)

功能集	敘述
用戶端完整防護	建議用於工作站、桌上型電腦和筆記型電腦。 包含所有防護技術。 適用於筆記型電腦、工作站和桌上型電腦。 包含完整下載防護和郵件通訊協定防護。 如果可能，請使用完整防護以獲得最大的安全性。

功能集	敘述
伺服器完整防護	建議用於伺服器。 納入除電子郵件掃描程式防護以外的所有防護技術。適用於需要最高網路安全性的任何伺服器，包括 Symantec Endpoint Protection Manager 伺服器。
伺服器基本防護	建議用於高處理量伺服器。 包含病毒和間諜軟體防護以及基本下載防護。由於入侵預防可能導致高處理量伺服器上產生效能問題，因此，此選項適用於需要最高網路效能的任何伺服器。

Mac 用戶端安裝套件會安裝病毒和間諜軟體防護以及入侵預防。您無法為 Mac 用戶端安裝套件自訂功能。

Linux 用戶端安裝套件僅會安裝「病毒和間諜軟體防護」。

自訂功能集

如果您要安裝防護的子集，請建立自訂功能集。但是，賽門鐵克建議您安裝所有防護。

您無法自訂 Mac 或 Linux 用戶端安裝套件的功能。

建立自訂用戶端安裝功能集

1. 在主控台中，按下**「管理員」**>**「安裝套件」**。
2. 按下**「用戶端安裝功能集」**>**「新增用戶端安裝功能集」**。
3. 在**「新增用戶端安裝功能集」**對話方塊中，輸入名稱和說明，然後勾選要安裝在用戶端上的防護。
4. 按下**「確定」**。

請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 90 頁的「準備用戶端安裝」。

在 Symantec Endpoint Protection Manager 中建立自訂 Windows 用戶端安裝套件

您可以透過架構用戶端安裝設定和用戶端功能集，針對 Symantec Endpoint Protection for Windows 自訂用戶端安裝套件。除此之外，此自訂操作可讓您架構安裝路徑、安裝後的重新啟動行為，以及安裝套件是否移除第三方安全性產品。

附註：用戶端安裝設定和用戶端安裝功能集組態僅適用於 Windows 安裝套件。您可以透過**「管理」>「安裝套件」>「用戶端安裝套件」**匯出 Macintosh 或 Linux 安裝套件，但組態選項有所差異。

表 6-8 建立自訂 Windows 用戶端安裝套件的工作

工作	詳細資料
建立新的自訂用戶端安裝設定組態	使用**「用戶端安裝套件」**可定義安裝行為。 如果您要移除用戶端電腦上的現有安全軟體，請在此進行架構。 請參閱第 104 頁的「自訂用戶端安裝設定」。 請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。
建立新的自訂功能集	**「用戶端安裝功能集」**定義在用戶端電腦上安裝的防護技術。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。
建立新的自訂安裝套件	匯出用戶端安裝套件時，請從建立的自訂設定中進行選取。您也可以選擇儲存套件的位置，以及該套件為單一檔案 (.EXE) 還是包含多個檔案的資料夾。 也可以搭配「用戶端部署精靈」使用自訂安裝設定和自訂功能集。 請參閱第 114 頁的「匯出用戶端安裝套件」。 請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 90 頁的「準備用戶端安裝」。

關於 Windows 用戶端安裝設定

用戶端部署精靈會提示您指定 Windows 用戶端的用戶端安裝設定。 用戶端安裝設定定義安裝程序本身的選項。您可以定義目標安裝資料夾，是否停用安裝記錄，以及安裝後的重新啟動設定等選項。

您可以選擇預設用戶端安裝設定，或在**「管理」>「安裝套件」>「用戶端安裝設定」**下新增自訂**「用戶端安裝設定」**。 上下文說明可提供關於可架構設定的詳細資料。

您應該針對遠端部署使用無訊息安裝，以最大程度減少使用者干擾。 使用無訊息部署時，必須重新啟動加裝到 Symantec Endpoint Protection 的應用程式，如 Microsoft Outlook。

如果使用自動安裝 (**「僅顯示進度列」**)，則 Windows 可能會向使用者顯示一或多個彈出式視窗。 但是，即使使用者沒有注意到這些視窗，安裝應該也不會失敗。

您不應針對遠端部署使用互動安裝。 除非使用者與此安裝類型進行互動，否則安裝會失敗。同一作業系統上的安全性功能 (如 Windows 階段作業 0 隔離) 可能會造成不顯示互動安裝精靈。 您應該僅針對本機安裝使用互動安裝類型。 這些建議適用於 32 和 64 位元作業系統。

請參閱第 104 頁的「自訂用戶端安裝設定」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。

請參閱第 90 頁的「準備用戶端安裝」。

自訂用戶端安裝設定

您可以變更可套用至用戶端安裝套件以及用於自動升級的安裝設定。

例如，如果您想要將用戶端安裝至自訂安裝資料夾，或是重設用戶端伺服器通訊設定，您可以建立自訂的用戶端安裝設定。然後可以在匯出或部署套件時套用此自訂設定，或是設定自動升級。

自訂用戶端安裝設定

1. 在主控台中，按下**「管理員」>「安裝套件」>「用戶端安裝設定」**。
2. 在**「工作」**下方，按下**「新增用戶端安裝設定」**。

   無法修改預設的用戶端安裝設定檔。
3. 選擇該設定檔適用的作業系統。
4. 輸入名稱和說明。
5. 從以下標籤上的可用選項中進行選擇：
   - Windows：**基本設定**和**重新啟動設定**
   - Mac：**重新啟動設定**和**升級設定**

   附註：Mac 用戶端重新啟動和升級設定僅適用自動升級

   若需這些選項的詳細資訊，請按下**「說明」**。
6. 按下**「確定」**，儲存這些設定。

執行「用戶端部署精靈」或架構自動升級時，選取您從**「安裝設定」**旁的下拉式功能表建立的設定。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

架構用戶端套件來解除安裝現有安全軟體

您可以先架構並部署新的安裝套件來解除安裝現有安全軟體，然後再安裝 Symantec Endpoint Protection 用戶端。解除安裝現有的安全軟體可以讓 Symantec Endpoint Protection 用戶端的

執行更有效率。您可以移除現有第三方安全軟體或現有 Symantec Endpoint Protection 用戶端。

您可以建立或修改自訂用戶端安裝設定架構，來啟用安全軟體移除功能。然後，在部署期間選取這個自訂架構。

您可以使用此功能解除安裝第三方安全軟體。若要檢視用戶端套件會移除哪些第三方軟體，請參閱：Symantec Endpoint Protection 中的第三方安全軟體移除支援。某些程式可能具有特殊的解除安裝常式，或者可能需要停用自我防護元件。請參閱第三方軟體的說明文件。

您無法利用 Mac 或 Linux 用戶端套件移除第三方安全軟體。自 12.1.1 MP1 版起，您可以使用 Windows 用戶端套件移除第三方安全軟體。您必須先解除安裝第三方安全軟體，然後才能部署 Symantec Endpoint Protection 用戶端套件。

附註：對版本 14.2 之第三方安全軟體移除的變更，表示您無法為更早版本的安裝套件啟用此功能。例如，如果您從 Symantec Endpoint Protection Manager 14.2 版建立並從中部署 14.0.1 版用戶端套件，則無法為其啟用第三方安全軟體移除。

自第 14 版起，您也可以移除無法透過標準方法 (例如 Windows 控制台) 移除的現有 Symantec Endpoint Protection 安裝。此功能會以用戶端安裝設定中的獨立選項出現。

只有使用以下程序建立的套件才能移除現有安全軟體。

架構用戶端套件來解除安裝現有安全軟體

1 在主控台的**「管理員」**頁面上，按下**「安裝套件」**，再按下**「用戶端安裝設定」**。

2 在**「工作」**下方，按下**「新增用戶端安裝設定」**。

附註：如果您之前已建立自訂用戶端安裝設定架構，則可以在**「工作」**下進行修改，然後按下**「編輯用戶端安裝設定」**。修改現有的自動架構並不會修改之前匯出的安裝套件。

---

3 在**「基本設定」**標籤上，按下列其中一項：

- **自動移除現有的第三方安全軟體**
  若要檢視用戶端套件會移除哪些第三方軟體，請參閱 Endpoint Protection 的第三方安全軟體移除。
- **移除無法移除的現有 Symantec Endpoint Protection 用戶端軟體**
  請參閱第 106 頁的「關於 Symantec Endpoint Protection 用戶端預先安裝移除功能」。

4 閱讀所選選項的相關資訊，然後按下**「確定」**。

您也可以修改此組態的其他選項。關於這些選項的更多資訊，請按下**「說明」**。

5 按下**「確定」**以儲存組態。

部署用戶端套件來移除現有安全軟體

1 在主控台的**「首頁」**上，啟動**「用戶端部署精靈」**。

按下**「說明」>「開始使用」頁面**，然後在**「所需工作」**下方，按下**「在您的電腦上安裝用戶端軟體」**。

2 在**「用戶端部署精靈」**中，按下**「新套件部署」**，再按**「下一步」**。

您可以使用**「現有套件部署」**部署您先前建立的安裝套件。但是，您必須早已使用自訂用戶端安裝設定架構匯出這些套件，如上述程序所述。

3 在**「選取群組並安裝功能集」**中，選取 Windows 安裝套件。在**「安裝設定」**下拉式清單中，選取您在上述程序中所建立或修改的自訂用戶端安裝設定架構。按**「下一步」**。

4 按下您要使用的部署方法，然後按**「下一步」**繼續進行並完成您選擇的部署方法。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

請參閱第 90 頁的「準備用戶端安裝」。

關於 Symantec Endpoint Protection 用戶端預先安裝移除功能

自 14 起，您可以在 Symantec Endpoint Protection 安裝開始之前，移除用戶端電腦上的現有用戶端安裝。此功能可與 CleanWipe 公用程式相比，因此，不應該針對所有部署啟用此功能。相反地，您應該僅使用此功能來移除已損毀或未正常運作的 Symantec Endpoint Protection 用戶端安裝。

使用此功能前，請注意此重要資訊：

- 此功能會移除所有 Symantec Endpoint Protection 版本，直到並包含您建立的安裝套件版本。
  還會移除所有 Symantec Network Access Control 版本以及不支援的產品 (Symantec Endpoint Protection 11.x、Symantec AntiVirus 10.x 和 Symantec Client Security 3.x)。
- 雖然此功能會移除早於 14 的版本，但是您無法在為舊版建立安裝套件時將其啟用。例如，您無法為啟用此功能的 12.1.6 版 MP4 建立套件。
- 此功能無法移除高於隨附安裝套件的 Symantec Endpoint Protection 版本。例如，您無法在規劃的回復期間使用此功能。
- 如果您部署的錯誤套件類型已啟用此功能，則不會執行移除。例如，如果您將 32 位元套件部署到 64 位元電腦，則無法安裝。因此，它不會移除現有的 Symantec Endpoint Protection 安裝。
- 您無法將此功能用於直接使用 .MSI 檔案的安裝，例如透過 GPO 部署。
- 此功能不適用於自動升級。
- 此功能不會移除 Symantec Endpoint Protection Manager。

- 如果其他賽門鐵克產品皆未使用此功能，此選項僅會移除 Windows LiveUpdate。
- 在用戶端電腦上，此功能會以無訊息方式執行，且不顯示狀態畫面或使用者介面。
- 此選項會強制安裝類型為**「無訊息」**。
- 移除完成後，電腦會自動重新啟動。您無法架構此重新啟動延後或略過。

請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦

安裝用戶端軟體後，您需要重新啟動 Windows 用戶端電腦。儘管使用者可以延遲到第二天預先排定的時間重新啟動，但是依據預設，Windows 用戶端電腦還是會在安裝後自動重新啟動。匯出或部署安裝套件之前，您可以架構 Windows 用戶端安裝設定，以自訂安裝後重新啟動。您可以在某個群組上架構重新啟動選項，以控制在風險矯正或新用戶端下載後，用戶端電腦重新啟動的方式。

Mac 用戶端電腦會提示安裝後重新啟動。如果推送用戶端套件，並且沒有人登入 Mac 電腦，則安裝完成之後，會自動發生硬式重新啟動。您無法自訂此設定。

安裝後，Linux 用戶端電腦不需要重新啟動，也不會自動重新啟動。

您也可以透過從管理伺服器執行重新啟動指令，隨時重新啟動 Mac 和 Windows 用戶端電腦。您無法使用管理伺服器中的重新啟動指令來重新啟動 Linux 用戶端。您可以選擇將 Windows 用戶端電腦排程為在使用者方便的時間重新啟動。您可以強制立即重新啟動，或讓使用者選擇延後啟動。將重新啟動指令傳送給 Mac 用戶端電腦時，始終會執行硬式重新啟動。

在 Windows 用戶端電腦上架構風險矯正和新用戶端下載重新啟動選項

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面上選取群組，再按下**「政策」**。
3. 在**「政策」**標籤上，按下**「一般設定」**。
4. 在**「一般設定」**對話方塊的**「重新啟動設定」**標籤上，選取重新啟動方式和排程。

   某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。

   您也可以新增重新啟動前出現在用戶端電腦上的通知。預設訊息會告訴使用者安全風險矯正或新內容下載需要重新啟動。
5. 按下**「確定」**。

重新啟動所選用戶端電腦

1. 在主控台中，按下**「用戶端」**
2. 在**「用戶端」**頁面的**「用戶端」**標籤中，選取群組。

3 在「**用戶端**」標籤上，選取用戶端，在「**對電腦執行指令**」上按下滑鼠右鍵，然後按下「**重新啟動用戶端電腦**」。

4 按下「**是**」，指定您需要的重新啟動選項，然後按下「**確定**」。

某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。

重新啟動所選群組中的用戶端電腦

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面的「**用戶端**」標籤上選取群組，按下「**對群組執行指令**」，然後按下「**重新啟動用戶端電腦**」。

3 按下「**是**」，指定您需要的重新啟動選項，然後按下「**確定**」。

某些重新啟動選項僅適用於 Windows 用戶端。如需詳細資訊，請參閱前後文相關說明。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

請參閱第 215 頁的「什麼是可對用戶端電腦執行的指令？」。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

請參閱第 90 頁的「準備用戶端安裝」。

關於受管和非受管用戶端

您可以將用戶端軟體安裝為受管用戶端或非受管用戶端。在大多數情況下，您應該安裝受管用戶端。安裝非受管用戶端，以便使用者對電腦具有更多控制，例如測試電腦，或如果電腦主要為離站均可。請確認非受管用戶端使用者具有適當程度的知識，可以架構不同於預設設定的任何安全性設定。

您可以稍後將非受管用戶端轉換成受管用戶端，方法為取代用戶端電腦上的用戶端伺服器通訊檔案。

表 6-9 受管與非受管用戶端之間的差別

類型	說明
受管用戶端	受管用戶端會連線到 Symantec Endpoint Protection Manager。您可以從 Symantec Endpoint Protection Manager 主控台管理用戶端電腦。您可以使用主控台，更新受管用戶端電腦上的用戶端軟體、安全性政策，以及病毒定義檔。 受管用戶端可以透過 Symantec Endpoint Protection Manager、GUP、Internet 和 LiveUpdate 取得內容更新。 大多數情況下，會將用戶端軟體安裝為受管用戶端。 您可以採用下列其中一種方式安裝受管用戶端： ■ 初始產品安裝期間 ■ 安裝後則從主控台
非受管用戶端	主要電腦使用者必須管理用戶端電腦。非受管用戶端不會連線至 Symantec Endpoint Protection Manager，且無法從主控台進行管理。在大多數情況下，非受管客戶端會偶爾連線到網路，或是根本不連接到網路。主要電腦使用者必須更新非受管用戶端電腦上的用戶端軟體、安全性政策，以及病毒定義檔。 非受管用戶端可以透過 Internet 和 LiveUpdate 取得內容更新。您必須個別在每個用戶端上更新內容。 請參閱第 109 頁的「如何取得非受管用戶端安裝套件」。 請參閱第 110 頁的「安裝非受管 Windows 用戶端」。

請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。

請參閱第 145 頁的「如何在用戶端電腦上取代用戶端伺服器通訊檔案」。

請參閱第 90 頁的「準備用戶端安裝」。

如何取得非受管用戶端安裝套件

您可以透過以下其中一種方式取得非受管 Symantec Endpoint Protection 用戶端安裝套件：

- 從 MySymantec 下載獨立式安裝程式
  下載最新版的 Symantec Endpoint Protection
- 從安裝檔案 (從 MySymantec 下載或收到實體光碟) 內複製資料夾。
  SEP (32 位元) 或 SEPx64 (64 位元) 資料夾包含非受管 Windows 用戶端、SEP_MAC 包含非受管 Mac 用戶端、SEP_LINUX 包含非受管 Linux 用戶端。
- 使用預設政策和設定或使用自訂政策和設定，從 Symantec Endpoint Protection Manager 匯出非受管用戶端。

如需非受管用戶端的自訂政策和設定建議，請參閱非受管用戶端安裝套件的建議政策和設定。

請參閱第 114 頁的「匯出用戶端安裝套件」。

您無法使用群組政策匯出非受管 Mac 用戶端。

您要將用戶端安裝程式套件複製到用戶端電腦上以進行安裝。 如果檔案是 .zip 檔，您必須先解壓縮所有內容，然後進行安裝。

請參閱第 110 頁的「安裝非受管 Windows 用戶端」。

請參閱第 46 頁的「安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端」。

請參閱第 48 頁的「安裝 Linux 的 Symantec Endpoint Protection 用戶端」。

請參閱第 108 頁的「關於受管和非受管用戶端」。

安裝非受管 Windows 用戶端

非受管 (或自我管理) 用戶端通常會允許使用者透過用戶端使用者介面對 Symantec Endpoint Protection 設定擁有較多的控制。一般來說，您會將非受管 Symantec Endpoint Protection 用戶端直接安裝在 Windows 電腦上，而安裝需要使用者輸入才能完成。

請參閱第 108 頁的「關於受管和非受管用戶端」。

請參閱第 109 頁的「如何取得非受管用戶端安裝套件」。

附註：將受管 Windows 用戶端安裝套件直接安裝至用戶端電腦上時，安裝步驟是類似的。只有**「互動式」**安裝需要使用者輸入。用戶端安裝設定選項**「只顯示進度列」**或**「無訊息」**安裝不需要使用者輸入。

安裝非受管 Windows 用戶端

附註：使用自訂政策架構的非受管用戶端套件，於安裝期間可能不會顯示描述的部分面板。如果您沒有看到程序步驟描述的某個安裝面板，請跳到下一個步驟。

---

1 將安裝檔案或 Symantec Endpoint Protection Manager 資料夾複製到用戶端電腦，然後連按兩下 `Setup.exe`。按**「下一步」**。

如果您購買了實體光碟，並且想要安裝非受管用戶端，請插入光碟。安裝作業應能自動啟動。 若未自動啟動，連按兩下 `Setup.exe`。按下**「安裝非受管用戶端」**。

2 在**「授權許可協議」**畫面中，按**「我同意」**，再按**「下一步」**。

3 在「**安裝類型**」面板上，按下列其中一個選項：

按下包含最常用選項的「**典型**」，再按「**下一步**」。

按下「**自訂**」以架構安裝，然後按「**下一步**」，選取防護類型，接著按「**下一步**」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

4 如果安裝精靈顯示提示，請按下「**啟用自動防護**」和「**執行 LiveUpdate**」，再按「**下一步**」

5 在「**檔案信譽資料傳送**」面板上，如果您不想為賽門鐵克提供匿名檔案信譽資料，請取消勾選方塊，再按「**下一步**」。

如果沒有已付費授權，則即使您讓方塊保持勾選，非受管用戶端也不會傳送信譽資料。

請參閱第 87 頁的「授權非受管 Windows 用戶端」。

6 在「**已做好安裝程式的準備**」畫面上，按下「**安裝**」。

7 在「**精靈完成**」畫面上，按下「**完成**」。

請參閱第 46 頁的「安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端」。

請參閱第 48 頁的「安裝 Linux 的 Symantec Endpoint Protection 用戶端」。

請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。

請參閱第 90 頁的「準備用戶端安裝」。

移除適用於 Windows 的 Symantec Endpoint Protection 用戶端

您可以使用下列方式移除 Windows 用戶端：

- 透過使用 Windows「控制台」移除應用程式，通常是使用「**程式和功能**」。
- 透過架構和部署可移除 Symantec Endpoint Protection 用戶端的自訂用戶端安裝套件 (自 14 版起)。僅在使用 Windows「控制台」 進行移除沒有作用時，才使用此方法。
  請參閱第 106 頁的「關於 Symantec Endpoint Protection 用戶端預先安裝移除功能」。
- 如需移除 Symantec Endpoint Protection Manager 和其他元件的其他方法，請參閱移除 Symantec Endpoint Protection。

如果 Symantec Endpoint Protection 用戶端軟體使用攔截硬體裝置的政策，則政策會在您移除軟體之後攔截裝置。如果您在移除之前未依照政策停用裝置控制，請使用「Windows 裝置管理員」取消對裝置的攔截。

移除適用於 Windows 的 Symantec Endpoint Protection 用戶端

1 在主控台的「**管理員**」頁面上，按下「**安裝套件**」，再按下「**用戶端安裝設定**」。

2 在「**工作**」下方，按下「**新增用戶端安裝設定**」。

附註：如果您之前已建立自訂用戶端安裝設定架構，則可以在「**工作**」下進行修改，然後按下「**編輯用戶端安裝設定**」。修改現有的自動架構並不會修改之前匯出的安裝套件。

3 在「**基本設定**」標籤上，勾選「**移除無法移除的現有 Symantec Endpoint Protection 用戶端軟體**」。

4 閱讀訊息，然後按下「**確定**」。

5 按下「**確定**」。

請參閱第 112 頁的「解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端」。

請參閱第 113 頁的「移除適用於 Linux 的 Symantec Endpoint Protection 用戶端」。

解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端

您可以透過功能表列上的用戶端圖示解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端。解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端需要管理使用者認證。

附註：在解除安裝 Symantec Endpoint Protection 用戶端之後，會提示您重新啟動用戶端電腦以完成解除安裝。在開始之前，請確定您已儲存任何未完成的工作，或關閉所有開啟的應用程式。

解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端

1 在 Mac 用戶端電腦上，開啟 Symantec Endpoint Protection 用戶端，然後按下 **Symantec Endpoint Protection >「移除 Symantec Endpoint Protection」**。

2 再次按下「**解除安裝**」開始解除安裝作業。

3 看到提示時，使用您的 Mac 管理使用者名稱和密碼進行驗證。

可能還會提示您輸入密碼以移除用戶端。此密碼可能與 Mac 的管理密碼不同。

4 解除安裝完成後，按下「**立即重新啟動**」。

如果解除安裝失敗，您可能必須使用其他解除安裝方法。請參閱：

解除安裝 Symantec Endpoint Protection

請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。

移除適用於 Linux 的 Symantec Endpoint Protection 用戶端

您可以使用安裝作業提供的指令碼來移除 Linux 的 Symantec Endpoint Protection 用戶端。

附註：您必須擁有進階使用者權限，才能在 Linux 電腦上移除 Symantec Endpoint Protection 用戶端。 此程序會使用 `sudo` 來提高權限。

移除 Linux 的 Symantec Endpoint Protection 用戶端

1. 在 Linux 電腦上，開啟 Terminal 應用程式視窗。
2. 使用下列指令瀏覽到 Symantec Endpoint Protection 安裝資料夾：

   `cd /opt/Symantec/symantec_antivirus`

   此路徑是預設安裝路徑。
3. 使用下列指令，以內建指令碼移除 Symantec Endpoint Protection：

   `sudo ./uninstall.sh`

   出現提示時，輸入您的密碼。

   此指令碼會起始移除 Symantec Endpoint Protection 元件。
4. 在提示字元下，輸入 **Y**，然後按 **Enter** 鍵。

   當傳回指令提示時，表示移除完成。

   附註：在某些作業系統上，如果 `/opt` 資料夾的唯一內容是 Symantec Endpoint Protection 用戶端檔案，則移除程式指令碼也會一併刪除 `/opt`。 若要重新建立此資料夾，請輸入下列指令：**`sudo mkdir /opt`**

若要透過套件管理員或軟體管理員來執行移除作業，請參閱您的 Linux 發行版本特定的說明文件。

管理用戶端安裝套件

若要使用 Symantec Endpoint Protection Manager 管理用戶端，您必須匯出受管用戶端安裝套件，然後將套件檔案安裝到用戶端電腦上。您可以使用 Symantec Endpoint Protection Manager 或協力廠商部署工具來部署用戶端。

賽門鐵克有時會提供更新版的安裝檔案套件，一般是在發行新產品版本時。您可以使用「自動升級」功能，在群組中的所有受管 Windows 與 Mac 用戶端上自動更新用戶端軟體。您不需要使用安裝部署工具重新部署軟體。

表 6-10 用戶端安裝套件相關工作

工作	敘述
架構用戶端安裝套件	您可以選擇特定的用戶端防護技術進行安裝，也可指定安裝程序與一般使用者的互動方式。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。 請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。
匯出用戶端安裝套件	您可以為受管用戶端或非受管用戶端匯出套件。 您可以將這些套件匯出成單一可執行檔或是目錄中的一系列檔案。您選擇的方法取決於您的部署方法，以及您是否要升級群組中的用戶端軟體。一般而言，如果您使用 Active Directory 群組原則物件，則不選擇匯出至單一執行檔。 請參閱第 114 頁的「匯出用戶端安裝套件」。 請參閱第 109 頁的「如何取得非受管用戶端安裝套件」。 請參閱第 110 頁的「安裝非受管 Windows 用戶端」。
匯入用戶端安裝套件更新	您可以將用戶端安裝套件新增到資料庫，以使這些套件可從 Symantec Endpoint Protection Manager 進行散佈。您可以選擇性地在此程序期間匯出套件，以便將套件部署至沒有用戶端軟體的電腦。 請參閱第 116 頁的「將用戶端安裝套件匯入 Symantec Endpoint Protection Manager」。
在一或多個群組中升級 Windows 和 Mac 用戶端	您可以將匯出的套件一次安裝至一台電腦，也可以同時將匯出的檔案部署至多部電腦。 賽門鐵克提供用戶端安裝套件的更新時，您必須先將這些更新新增至 Symantec Endpoint Protection Manager，並且使這些更新可供匯出。但您不需要使用用戶端部署工具重新安裝這些更新。使用最新軟體更新 Windows 和 Mac 用戶端的最簡單方式是使用「自動升級」。您應該先更新測試電腦數量較少的群組。 請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。 如果您允許用戶端執行 LiveUpdate，而且「LiveUpdate 設定」政策允許更新，則您也可以使用 LiveUpdate 更新用戶端。
刪除用戶端安裝套件	您可以刪除舊的用戶端安裝套件來節省磁碟空間。但是，自動升級有時會使用較舊的用戶端安裝套件來建置升級套件。升級套件可使用戶端執行較小的下載。

請參閱第 90 頁的「準備用戶端安裝」。

匯出用戶端安裝套件

如果您需要在使用**「用戶端部署精靈」**中的**「儲存套件」**時不可用的那些選項，您可能需要匯出用戶端安裝套件。例如，您可能需要使用自訂政策建立非受管用戶端。您也可能僅需要適用於 Windows 的 32 位元或 64 位元安裝套件，或者需要適用於 Linux 的 DPKG 或 RPM 安裝套件。

匯出用戶端安裝套件後，即可部署該套件。**「用戶端部署精靈」**中的**「遠端推送」**可以部署您匯出的 Windows 和 Mac 套件。或者，您可以將匯出的套件直接安裝到用戶端，或使用第三方程式來部署套件。

您可以為受管用戶端或非受管用戶端建立安裝套件。這兩種類型的套件都包含您指定的功能、政策和設定。如果您建立受管用戶端的套件，則可使用 Symantec Endpoint Protection Manager 主控台管理這些用戶端。如果您建立非受管用戶端的套件，則無法從主控台管理這些用戶端。您隨時可以透過**「用戶端部署精靈」**的**「通訊更新套件部署」**，將非受管 Windows 或 Mac 用戶端轉換成受管用戶端。

附註：如果從遠端主控台匯出用戶端安裝套件，就會在執行遠端主控台的電腦建立套件。此外，如果您使用多個網域，則必須匯出各個網域的套件，否則這些套件不會顯示在適當的網域群組中。

匯出用戶端安裝套件

1. 在主控台中，按下**「管理員」**，再按下**「安裝套件」**。
2. 在**「安裝套件」**下方，按下**「用戶端安裝套件」**。
3. 在**「用戶端安裝套件」**窗格的**「套件名稱」**下，於要匯出的套件上按下滑鼠右鍵，然後按下**「匯出」**。
4. 按下**「瀏覽」**導覽至要包含匯出之套件的資料夾，選取它，然後按下**「確定」**。

   附註：「匯出套件」不支援包含雙位元組或高 ASCII 字元的目錄，並會阻止選取這些目錄。

   ---

5. 根據個人安裝需求設定其他選項。這些選項因匯出的安裝套件類型和平台而有所不同。

   若需此對話方塊中匯出選項的詳細資料，請按下**「說明」**。
6. 按下**「確定」**。

請參閱第 116 頁的「將用戶端安裝套件匯入 Symantec Endpoint Protection Manager」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

請參閱第 90 頁的「準備用戶端安裝」。

將用戶端安裝套件匯入 Symantec Endpoint Protection Manager

在以下情況中，您可能需要將用戶端安裝套件匯入 Symantec Endpoint Protection Manager：

使用已從舊版還原的資料庫升級至更新版本的 Symantec Endpoint Protection Manager。資料庫包括舊版用戶端安裝套件，並且您需要匯入更新的套件。

您應始終保持 Symantec Endpoint Protection Manager 版本與用戶端版本相同或更新。

附註：您可以直接匯入 .exe 或 .zip 檔案套件等執行檔套件，但不建議這麼做。.info 檔案包含描述套件以及確保透過差異更新正確移轉至 Symantec Endpoint Protection 用戶端之未來版次的資訊。另一方面，Symantec Endpoint Protection Manager Web 主控台不會匯入 .info 檔案格式。在 Web 主控台中，您只能在諸如 .zip 或 .exe 檔案格式的單一檔案中匯入或匯出套件。

將用戶端安裝套件匯入 Symantec Endpoint Protection Manager

1. 將匯入的安裝套件複製到執行 Symantec Endpoint Protection Manager 之電腦上的某個目錄中。

   用戶端安裝套件包含兩個檔案。一個檔案名稱為 *product_name*.dat，另一個檔案名稱為 *product_name*.info。這些檔案會在安裝或升級 Symantec Endpoint Protection Manager 期間自動匯入。您也可以從安裝檔案的 `SEPM/Packages` 資料夾中取得這些套件。

2. 在主控台中，按下**「管理員」**>**「安裝套件」**。
3. 在**「工作」**下方，按下**「新增用戶端安裝套件」**。
4. 在**「新增用戶端安裝套件」**對話方塊中，輸入套件的名稱和敘述。
5. 按下**「瀏覽」**。
6. 在**「選取資料夾」**對話方塊中，針對步驟 1 中複製的新套件找到並選取 *product_name*.info 檔案，然後按下**「選取」**。
7. 出現**「成功完成」**提示時，按下**「關閉」**。

   若要匯出安裝檔案並用於部署，請按下**「匯出這個套件」**，然後完成此程序。

   請參閱第 114 頁的「匯出用戶端安裝套件」。

   成功匯入套件後，可在「系統」>「管理日誌」中看到「套件已建立」事件。將使用類似「已透過 Symantec Endpoint Protection Manager 成功匯入 SEP 12.1 RU5 32 位元套件。此套件現在可供部署。」的文字描述該事件。

   請參閱第 563 頁的「檢視日誌」。

請參閱第 90 頁的「準備用戶端安裝」。

Windows 用戶端安裝套件和內容更新大小

用戶端安裝套件、產品修補程式以及內容更新也儲存於 Symantec Endpoint Protection 資料庫並影響儲存需求。產品修補程式包含用戶端套件的資訊，以及每一種語言或地區設定的資訊。請注意，修補程式也會建立新的、完整的用戶端版次。

表 6-11顯示用戶端安裝套件的大小，如果最大的用戶端記錄和防護技術層級已啟用。

表 6-11 Windows 用戶端安裝套件大小

用戶端類型/定義檔類型	*隨病毒定義檔一起安裝？	64 位元套件 (MB)	32 位元套件 (MB)
標準和內嵌 (14) CoreDefs-3**	是	188	175
	否	93	81
暗網 (14) CoreDefs-1.5	是	288	276
	否	93	80
標準 (12.1.6) CoreDefs-1	是	335	316
	否	86	70
縮減 (內嵌/VDI) (12.1.6) CoreDefs-3	是	182	165
	否	86	70

對於這些套件，您可以設定更大的活動訊號。這些大小不包括封包層級防火牆日誌，這些日誌不建議在生產環境中使用。如果用戶端記錄已停用，且沒有新政策或內容可從管理伺服器下載，則用戶端安裝套件較小。在這種情況下，您可以設定較小的活動訊號。

*如果您的網路具有低頻寬，請在沒有病毒定義檔的情況下安裝用戶端套件。只要用戶端連線至管理伺服器，就可接收完整的病毒定義檔集。

所有用戶端安裝套件皆包含所有功能，例如病毒和間諜軟體、防火牆、IPS、SONAR、系統鎖定、應用程式控制、主機完整性內容等。用戶端類型之間的差異在於病毒和間諜軟體定義檔的大小。

請參閱第 99 頁的「如何選擇用戶端安裝類型」。

在 12.1.5 及更新版本中，內容更新需要資料庫與檔案系統中較小的儲存空間。管理伺服器現在僅能儲存一個完整內容版本，外加增量差量，而不能儲存多個完整版本。在 12.1.6 中，完整內容更新需要 ~470 MB。

附註：自 14 版起，可使用 LiveUpdate 伺服器、管理伺服器或群組更新提供者，採用與其他內容相同的方式將安全修補程式下載到用戶端。在 12.1.6 及更早版本中，安全修補程式僅作為新版本以及使用自動升級之用戶端部署套件的一部分提供。請參閱第 197 頁的「將 Endpoint Protection 安全修補程式下載至 Windows 用戶端」。

7

升級 Symantec Endpoint Protection

本章包含以下主題：

升級至新版本

您可以升級至最新版的產品以使用新功能。若要安裝新版本的軟體，您必須執行某些工作，以確保升級成功。您也應檢查版本說明中的已知問題，瞭解有關升級的任何最新資訊。

本節特別針對在已安裝相容版本產品的環境中升級軟體。

進行升級之前，請先檢閱下列資訊：

- 系統需求
  如需最新系統需求，請參閱：所有 Endpoint Protection 版本的版本說明、新修正和系統需求
- 本版新功能
  Symantec Endpoint Protection 所有版本的新功能
- 升級最佳實務準則
  請參閱 Endpoint Protection 14.x 的升級最佳實務準則。
- 相容的 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端升級路徑
  請參閱第 122 頁的「最新版本 Symantec Endpoint Protection 14.x 支援的升級路徑」。

賽門鐵克建議您不要在升級 Symantec Endpoint Protection 的同時執行第三方安裝。任何進行網路層級或系統層級變更的第三方程式安裝都可能會在升級 Symantec Endpoint Protection 時導致不理想的結果。如可能，請在升級 Symantec Endpoint Protection 之前重新啟動用戶端電腦。

表 7-1 Symantec Endpoint Protection 的升級程序

工作	敘述
步驟 1：備份資料庫	備份 Symantec Endpoint Protection Manager 使用的資料庫，以確保用戶端資訊的完整性。 請參閱第 648 頁的「備份資料庫和日誌」。
步驟 2：中斷遠端複製關係 (選擇性)	如果要更新的管理伺服器會透過其他管理伺服器進行遠端複製，請中斷遠端複製關係。如果第二部管理伺服器或遠端複製夥伴，在升級期間啟動遠端複製，則可能會產生無法預測的結果。 **附註：**中斷管理伺服器之間的關係與移除遠端複製夥伴不同。您不會想要刪除整個遠端複製夥伴。 請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。
步驟 3：停止 Symantec Endpoint Protection Manager 服務	您必須先停止管理伺服器服務，才可以安裝更新版本。 請參閱第 128 頁的「停止及啟動管理伺服器服務」。
步驟 4：升級 Symantec Endpoint Protection Manager 軟體	在網路中的所有站台上，安裝新版本的 Symantec Endpoint Protection Manager。這會自動偵測現有版本，並且在升級時儲存所有的設定。 請參閱第 126 頁的「升級管理伺服器」。 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
步驟 5：升級之後還原遠端複製關係 (選擇性)	如果所更新的管理伺服器會透過其他管理伺服器進行遠端複製，請還原遠端複製關係。 請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

工作	敘述
步驟 6：升級 Symantec 用戶端軟體	準備並將用戶端軟體升級為最新版。如果您使用群組更新提供者，則必須先將它們升級。 請參閱第 130 頁的「選擇升級用戶端軟體的方法」。 請參閱第 135 頁的「升級群組更新提供者」。 請參閱第 90 頁的「準備用戶端安裝」。 賽門鐵克提供用戶端安裝套件的更新時，您必須先將這些更新新增至 Symantec Endpoint Protection Manager，並且使這些更新可供匯出。但您不需要使用用戶端部署工具重新安裝用戶端。使用最新軟體以群組方式更新 Windows 和 Mac 用戶端的最簡單方式是使用「自動升級」。您應該先更新測試電腦數量較少的群組，然後再更新整個生產網路。 請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

Symantec Endpoint Protection 的升級資源

表 7-2 升級資源

項目	資源
用戶端安裝套件設定和功能	您可以透過各種不同的設定和防護功能架構用戶端安裝套件。 請參閱第 270 頁的「安全政策類型」。 請參閱第 684 頁的「根據平台 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能」。 請參閱第 103 頁的「關於 Windows 用戶端安裝設定」。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。
功能和政策說明	請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。
功能相依性	請參閱第 682 頁的「針對 Windows 用戶端 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能相依性」。
管理產品授權	Symantec Endpoint Protection 是根據保護站台中電腦所需的用戶端數目進行授權。 請參閱第 67 頁的「Symantec Endpoint Protection 產品授權需求」。 請參閱第 83 頁的「關於產品升級和授權」。

項目	資源
其他資源	請參閱下列文章： ■ 升級至最新版本 Symantec Endpoint Protection 的最佳實務準則 ■ 下載最新版的 Symantec Endpoint Protection ■ Endpoint Protection 所有版本的版本說明、新修正和系統需求

請參閱第 119 頁的「升級至新版本」。

最新版本 Symantec Endpoint Protection 14.x 支援的升級路徑

Symantec Endpoint Protection Manager 和 Windows 用戶端

下列 Symantec Endpoint Protection Manager 版本和 Symantec Endpoint Protection Windows 用戶端版本可直接升級到 14.2.1：

- 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 (12.1.7445.7000)
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2332.0100) 或 14 MP1 重新整理版次 (14.0.2349.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.0.1 MP2 (14.0.3929.1200)
- 14.2 (14.2.770.0000)

附註：有效的 14.2 版 14.2.758.0000 和 14.2.760.0000 與相同的元件版本一起在短時間內可用。14.2.770.0000 取代了這些版本。

- 14.2 MP1 (14.2.1023.0100)

附註：有效的 14.2 MP1 版 14.2.1015.0100 與相同的元件版本一起在短時間內可用。14.2.1023.0100 會取代此版本。

Mac 用戶端

下列適用於 Mac 的 Symantec Endpoint Protection 用戶端版本可直接升級到 14.2.1：

- 12.1.4 - 12.1.6 MP9 (12.1.7369.6900)
  Mac 用戶端不會更新為版本 12.1.6 MP10。
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 或 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.2 (14.2.770.0000)

  附註：有效的 14.2 版 14.2.758.0000 和 14.2.760.0000 與相同的元件版本一起在短時間內可用。14.2.770.0000 取代了這些版本。

- 14.2 MP1 (14.2.1023.0100)

  附註：有效的 14.2 MP1 版 14.2.1015.0100 與相同的元件版本一起在短時間內可用。14.2.1023.0100 會取代此版本。

附註：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 14.2.1：

- 12.1.x，最高是 12.1.6 MP9 (12.1.7369.6900)
  Linux 用戶端不會更新為版本 12.1.6 MP10。
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 或 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)
- 14.0.1 MP1 (14.0.3876.1100)
- 14.0.1 MP2 (14.0.3929.1200)
- 14.2 (14.2.770.0000)

附註：有效的 14.2 版 14.2.758.0000 和 14.2.760.0000 與相同的元件版本一起在短時間內可用。14.2.770.0000 取代了這些版本。

- 14.2 MP1 (14.2.1023.0100)

附註：有效的 14.2 MP1 版 14.2.1015.0100 與相同的元件版本一起在短時間內可用。14.2.1023.0100 會取代此版本。

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。您必須先解除安裝下列產品，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。

降級路徑不受支援。例如，如果想要從 Symantec Endpoint Protection 14.2.1 移轉到 12.1.6 MP10，必須先解除安裝 Symantec Endpoint Protection 14.2.1。

升級前增加 Symantec Endpoint Protection Manager 可用磁碟空間

Symantec Endpoint Protection Manager 安裝需要最低可用磁碟空間量。 請確定任何目前版本伺服器或新硬體符合最低硬體需求。不過，升級時可能需要額外的可用磁碟空間才能建立暫存檔。

進行架構變更之前對資料庫進行備份。

請參閱第 648 頁的「備份資料庫和日誌」。

表 7-3 增加管理伺服器上磁碟空間的工作

工作	敘述
變更 LiveUpdate 設定以降低空間需求	1 移至**「管理員」>「伺服器」**，並在**「本機站台」**上按下滑鼠右鍵。選取**「編輯站台屬性」**。 2 在 **LiveUpdate** 標籤上，取消核取**「存儲經過解壓的用戶端套件以便為升級提供更高的網路性能」**。 **附註：**由於管理伺服器上的內容儲存有所改善，因此 12.1.5 版已移除這個選項。但是，仍應為升級 12.1.5 之前的版本以適當設定這個選項。 3 在 **LiveUpdate** 標籤上，減少要保留的內容修訂數量。對於升級，您可以將設定減少為 10。讓 Symantec Endpoint Protection Manager 有時間清除額外的修訂。不過，在比 12.1.5 更新的版本中，減少修訂數量可能會觸發從登入的用戶端下載完整更新。這些完整更新要求增加可能會對電腦效能產生負面的影響。 **附註：**自 12.1.5 版起，內容儲存的預設值和建議值也有所變更。但是，若要升級，您需要使用適用於所升級版本的值。 升級完成後不需要將修訂設定恢復為先前的值。Symantec Endpoint Protection Manager 儲存與管理內容的方式有所改善，與舊版本相比，耗用的磁碟空間更少，同時可容納的修訂更多。 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。
確定從 Symantec Endpoint Protection Manager 資料庫刪除未使用的病毒定義檔	1 移至**「管理員」>「伺服器」**，在資料庫伺服器上按下滑鼠右鍵，然後選取**「編輯資料庫屬性」**。 對於內嵌資料庫，請在 **localhost** 上按下滑鼠右鍵。對於 Microsoft SQL Server 資料庫，資料庫伺服器名稱會根據資料庫位置有所不同。 2 在**「日誌設定」**標籤上的**「風險日誌設定」**下，確定已勾選**「刪除未使用的病毒定義檔」**。
重新定位或移除共存的程式和檔案	■ 如果其他程式與 Symantec Endpoint Protection Manager 安裝於同一台電腦，請考慮將它們重新定位至其他伺服器。您可以移除未使用的程式。 ■ 如果佔用儲存較多的程式與 Symantec Endpoint Protection Manager 安裝於同一台電腦，請考慮使一台專用電腦僅支援 Symantec Endpoint Protection Manager。 ■ 移除暫存的 Symantec Endpoint Protection Manager 檔案。 如需瞭解可以移除的暫存檔清單，請參閱文章：Symantec Endpoint Protection Manager 目錄包含許多消耗大量磁碟空間的 .TMP 資料夾。 **附註：**移除程式和檔案之後，對硬碟進行磁碟重組。

工作	敘述
使用外部資料庫	如果 Symantec Endpoint Protection 資料庫與 Symantec Endpoint Protection Manager 位於同一台電腦，請考慮在另一台電腦上安裝 Microsoft SQL Server 資料庫。 會節省大量的磁碟空間，而且大多數情況下可提高效能。 請參閱第 72 頁的「關於選擇資料庫類型」。

附註：升級之前，請確定用戶端電腦也有足夠的磁碟空間。 檢查系統需求，並視需要移除不需要的程式和檔案，然後對用戶端電腦硬碟進行磁碟重組。

執行 Endpoint Protection 的電腦上發生錯誤：「磁碟空間不足」

如需最新系統需求，請參閱：所有端點防護版本的版本說明、新修正和系統需求

升級管理伺服器

升級任何用戶端前，必須先升級所有管理伺服器。

在支援負載平衡、容錯移轉或複寫的環境中升級管理伺服器時，必須按照特定順序準備和升級管理伺服器。

警告：您必須按照適用於您的安裝類型的方案操作，否則升級可能會失敗。

表 7-4 升級工作

工作	敘述
升級管理伺服器	檢閱系統需求和支援的升級路徑、升級管理伺服器，然後使用「管理伺服器組態精靈」進行架構。 自第 14 版起，Symantec Endpoint Protection Manager 升級適用下列幾點： ■ 不再支援 Windows Server 2003、所有桌面作業系統和 32 位元作業系統。 ■ 資料庫不再支援 SQL Server 2005。此外也停止支援 SQL Server 2008 SP4 之前的版本，以及 SQL Server 2008 R2 SP3 之前的版本。 ■ 現在必須在升級期間輸入 SQL Server 系統管理員認證。 **附註：**您可能需要編輯網域安全性政策，以允許虛擬服務帳戶在 Windows 7 / Server 2008 R2 或更新版本上正確執行。 請參閱： 在安裝或架構期間發生錯誤：「...服務需要使用者權限」或「...無法讀取使用者權限」 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。 請參閱第 122 頁的「最新版本 Symantec Endpoint Protection 14.x 支援的升級路徑」。 請參閱第 127 頁的「升級使用多個內嵌資料庫和管理伺服器的環境」。
登入管理伺服器	出現 Symantec Endpoint Protection Manager 登入畫面時，您可以使用您的登入認證登入主控台。 請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

附註：升級後不一定要重新啟動電腦，但是重新啟動電腦再登入後可提升效能。

請參閱第 629 頁的「設定容錯移轉和負載平衡」。

請參閱第 635 頁的「設定網站和遠端複製」。

升級使用多個內嵌資料庫和管理伺服器的環境

升級使用多個內嵌資料庫和管理伺服器的環境，將產生以下結果：

- 管理伺服器不會針對 Symantec Endpoint Protection 使用容錯移轉或負載平衡，因為內嵌資料庫不支援容錯移轉或負載平衡的伺服器。
- 管理伺服器是 Symantec Endpoint Protection 複寫夥伴。

所有的站台都有一台最先安裝管理伺服器的電腦。您必須先升級此管理伺服器，因為它包含加密金鑰或加密密碼等重要的站台資訊。然後再升級針對複寫所安裝的其他管理伺服器。

升級使用多個內嵌資料庫和管理伺服器的環境

1 驗證並登入安裝第一個 Symantec Endpoint Protection Manager 所在的電腦。

請勿登入 Symantec Endpoint Protection Manager。如果您使用複寫，則無需首先將其停用。如果產品版本不符，則 Symantec Endpoint Protection 不允許複寫。

2 升級管理伺服器。

請參閱第 126 頁的「升級管理伺服器」。

3 逐一升級所有其他的管理伺服器。

停止及啟動管理伺服器服務

在升級之前，您必須手動停止您網站中每部管理伺服器上的 Symantec Endpoint Protection Manager 服務。升級之後，服務會自動啟動。

警告：若不在伺服器升級前停止 Symantec Endpoint Protection Manager 服務，則有使現有 Symantec Endpoint Protection 資料庫損毀的風險。

附註：如果您停止管理伺服器服務，用戶端就無法再與之連線。如果用戶端需要與管理伺服器通訊以連線到網路，則在重新啟動此服務之後，才能允許這些用戶端存取。

例如，用戶端必須與管理伺服器通訊，才能通過「主機完整性」檢查。

請參閱第 119 頁的「升級至新版本」。

停止 Symantec Endpoint Protection Manager 服務

1 按下**「開始」>「設定」>「控制台」>「系統管理工具」>「服務」**。

2 在**「服務」**視窗的**「名稱」**下方，捲動至 **Symantec Endpoint Protection Manager**，然後按下滑鼠右鍵。

3 按下**「停止」**。

4 關閉「服務」視窗。

警告：關閉「服務」視窗，否則升級會失敗。

5 為所有 Symantec Endpoint Protection Manager 的安裝重複此程序。

附註：若要啟動 Symantec Endpoint Protection Manager 服務，請再次遵循此程序，並按下**「啟動」**而非**「停止」**。

使用指令行停止 Symantec Endpoint Protection Manager 服務

- 從指令提示處輸入：

```
net stop semsrv
```

使用指令行啟動 Symantec Endpoint Protection Manager 服務

- 從指令提示處輸入：

```
net start semsrv
```

在升級前後停用遠端複製和還原遠端複製

升級管理伺服器之前，您應該暫時中斷與架構為遠端複製夥伴之所有管理伺服器的夥伴關係。如果遠端複製夥伴在升級期間啟動遠端複製，可能會產生無法預期的結果。

警告：停用遠端複製與永久刪除遠端複製夥伴關係不同。如果您刪除關係，然後重新安裝管理伺服器，則管理伺服器會執行完整遠端複製而非增量遠端複製。請參閱第 645 頁的「刪除網站」。

停用遠端複製

您必須登入 Symantec Endpoint Protection Manager 並在至少兩個網站上停用遠端複製。

停用遠端複製

1. 在主控台中，按下**「管理員」>「伺服器」**。
2. 在**「本機網站」>「伺服器」**下方，展開**「遠端複製夥伴」**並選取管理伺服器。
3. 在管理伺服器上按下滑鼠右鍵，然後按下**「刪除遠端複製夥伴」**。
4. 按下**「是」**。
5. 在遠端複製資料的所有網站中重複此程序。

當網站已遠端複製時還原遠端複製夥伴

升級具有遠端複製關係的所有管理伺服器之後，重新新增遠端複製夥伴。還必須重新新增已架構用於容錯移轉和負載平衡的管理伺服器。

僅在最先升級管理伺服器的電腦上重新新增遠端複製夥伴。此外，升級的管理伺服器先前必須是相同網站陣列中的遠端複製夥伴。

重新新增遠端複製夥伴後，Symantec Endpoint Protection Manager 會使資料庫保持一致。不過，某些變更可能相互衝突。

請參閱第 639 頁的「如何解決遠端複製期間網站之間的資料衝突」。

如果您擁有兩個單獨的非遠端複製網站，亦可使用此選項將其中一個網站轉換為透過其他網站遠端複製的網站。

升級後還原遠端複製

1. 在主控台上，按下**「管理員」>「伺服器」**。
2. 在**「伺服器」**下方，展開**「本機網站」**，然後在**「工作」**下方，按下**「新增現有遠端複製夥伴」**。
3. 在「歡迎使用」面板中，按**「下一步」**。
4. 在**「遠端據點資訊」**面板中，輸入第二個管理伺服器的 IP 位址或主機名稱、系統管理員的登入資訊，然後按**「下一步」**。

   依據預設，系統管理員的使用者名稱為 `admin`。
5. 設定遠端複製排程，然後按**「下一步」**。
6. 檢查要遠端複製的項目，然後按**「下一步」**。

   用戶端套件遠端複製會使用大量的流量和硬碟空間。

   如果您按下**「是」**，則管理伺服器會在兩個遠端複製夥伴之間執行完整資料遠端複製。
7. 當出現一則訊息詢問是否已還原夥伴網站上的資料庫時，請按下列其中一個選項：
   - 按下**「否」**僅遠端複製自此夥伴關係停用之後變更的資料。賽門鐵克建議您選取此選項，尤其是在您的網路具有低頻寬的情況下。
   - 按下**「是」**在兩個遠端複製夥伴之間執行完整資料遠端複製。
8. 按下**「完成」**。
9. 為所有以此電腦遠端複製資料的電腦重複這個程序。

請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。

Endpoint Protection 14 的升級最佳實務準則

請參閱第 119 頁的「升級至新版本」。

選擇升級用戶端軟體的方法

您可以利用多種方式來升級用戶端。您應採用的方法視環境和目標而定。例如，您可能擁有大量用戶端或群組，或者執行不同用戶端版本的電腦。

某些方法可能耗時達 30 分鐘。 因此，您可以在大多數使用者未登入其電腦時，升級用戶端軟體。

表 7-5 升級用戶端軟體的方法

方法	何時使用	何時不使用
自動升級 (建議較小的環境使用)	■ 當您擁有的用戶端數目較少時，例如 5,000 個或更少的用戶端。 ■ 當您需要將升級排程為在升級不中斷使用者工作的情況下執行時。 ■ 當您使用 Symantec Endpoint Protection Manager (而非第三方應用程式) 部署用戶端安裝套件時。 ■ 當您需要升級 Windows 或 Mac 用戶端，但不升級 Linux 用戶端時。 ■ 當您想要採用簡單的升級方法時。 請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。	■ 當您擁有大量用戶端時。此方法不夠靈活。 ■ 當您擁有大量群組時，因為在精靈中個別按下每個群組相當耗時。 ■ 當您設定複雜的升級排程 (需要較高精細度) 時。 ■ 當您需要升級 Linux 用戶端時。如何將 Symantec Endpoint Protection Linux 用戶端部署為已複製磁碟機影像的一部分
匯出用戶端安裝套件 (建議較大的環境使用)	■ 當您手動 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端安裝套件時。 ■ 當您使用現有第三方部署應用程式 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端安裝套件時。若要使用此方法，您應已安裝此基礎架構。 ■ 當您需要升級 Windows 用戶端、Mac 用戶端及 Linux 用戶端時。 請參閱第 114 頁的「匯出用戶端安裝套件」。 請參閱第 697 頁的「使用第三方工具安裝 Windows 用戶端軟體」。	■ 當您通常使用 Symantec Endpoint Protection Manager 更新用戶端時。
用戶端部署精靈	■ 當您擁有的用戶端數目較少時，例如 250 個以下用戶端。 ■ 當您使用 Symantec Endpoint Protection Manager (而非第三方應用程式) 部署用戶端時。 ■ 當您想要採用較簡單的升級方法時。 使用**「新套件部署」**。 請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。	■ 當您擁有大型網路環境時，因為此方法不夠靈活。

方法	何時使用	何時不使用
從 MySymantec 下載用戶端安裝檔案	■ 當您想要在少數特定情況下一次升級數個用戶端時。例如： ■ 如果某個問題在數個安裝有舊版用戶端的電腦上出現，更新版本修正了該問題。 ■ 如果您要升級較少數目的用戶端，但不想升級管理伺服器。 ■ 當您需要升級 Windows、Mac 及 Linux 用戶端時。 ■ 當您必須直接在電腦上部署或使用第三方部署應用程式 (而非使用 Symantec Endpoint Protection Manager) 部署用戶端時。 您可以從 MySymantec 下載獨立的**「所有用戶端」**安裝檔案。 MySymantec 入門指南 請參閱第 110 頁的「安裝非受管 Windows 用戶端」。	如果您升級具有現有受管用戶端之電腦上的用戶端，這些受管用戶端會保持受管狀態。但是，如果您部署至不含現有用戶端的新電腦，此方法會僅安裝非受管用戶端。您必須稍後將用戶端轉換為受管用戶端，才能連線至管理伺服器。 請參閱第 145 頁的「如何在用戶端電腦上取代用戶端伺服器通訊檔案」。 請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

請參閱第 119 頁的「升級至新版本」。

使用自動升級來升級用戶端軟體

自動升級可讓您自動升級群組中所有 Windows 或 Mac 用戶端上的 Symantec Endpoint Protection 用戶端軟體。

Windows 標準用戶端可使用自動升級接收 Symantec Endpoint Protection Manager 建立的差量升級套件。此套件比完整安裝套件小。Windows Embedded 或 VDI 用戶端始終接收完整安裝套件。這些用戶端不會在安裝程式快取中保留安裝程式複本。Mac 用戶端始終接收完整安裝套件。

使用下列最佳實務來使用自動升級：

- 嘗試在產品網路中升級大量用戶端之前，先測試自動升級程序。如果沒有測試網路，您可以在正式網路中建立一個測試群組。 針對這類測試，您可以將幾個非至關重要的用戶端新增至測試群組，然後使用「自動升級」來升級這些用戶端。
- 若要減少尖峰時間的頻寬，請在**「使用套件升級用戶端」**精靈中，排程在營業時間後執行「自動升級」，尤其是針對含縮減大小用戶端的用戶端群組。 針對廣域網路，您應該也設定遠端用戶端，以從遠端 Web 伺服器接收升級套件。
- 因為自動升級最初包含在具有 Symantec Endpoint Protection 14 的 Mac 用戶端中，因此您無法從 14 版之前的 Symantec Endpoint Protection 版本使用自動升級進行升級。
- 升級 Symantec Endpoint Protection Manager 後，在主控台中至少執行一次 LiveUpdate，然後使用自動升級來升級用戶端。

請參閱第 162 頁的「確認 Symantec Endpoint Protection Manager 具有最新內容」。

- 僅當符合下列條件時，自動升級才會在用戶端電腦上安裝應用程式強化功能：
  - 當您執行**「使用套件升級用戶端」**時，必須啟用**「更新時保留現有用戶端功能」**。此設定預設為啟用。
  - 用戶端電腦無法安裝 Symantec Data Center Security 代理程式。
  - 病毒和間諜軟體防護功能目前已安裝，並選取進行升級。

請參閱第 130 頁的「選擇升級用戶端軟體的方法」。

使用自動升級來升級用戶端軟體

1. 在主控台中，按下**「管理員」**>**「安裝套件」**。
2. 在**「工作」**下方，按下**「使用套件升級用戶端」**。
3. 在**「升級用戶端精靈」**面板中，按**「下一步」**，選取適當的用戶端安裝套件，然後按**「下一步」**。
4. 選取包含您要升級之用戶端電腦的群組，然後按**「下一步」**。
5. 從下列選項中選取用戶端應從何處下載套件：
   - 若要從 Symantec Endpoint Protection Manager 伺服器進行下載，請按下**「從管理伺服器下載」**。
   - 若要從位於需要更新之電腦本機的 Web 伺服器進行下載，請按下**「從下列 URL (http 或 https) 下載」**。在提供的欄位中輸入用戶端安裝套件的 URL。
6. 按下**「升級設定」**以指定升級選項。
7. 在**「一般」**標籤的**「用戶端設定」**下，從下列選項 (視用戶端作業系統而定) 中選擇：
   - 對於 Windows，請使用下拉式功能表選取**「更新時保留現有用戶端功能」**和**「安裝設定」**的選項。

     附註：如果取消選取**「更新時保留現有用戶端功能」**，您可以選擇在升級時新增或移除功能。
   - 對於 Mac，請使用下拉式功能表選取**「安裝設定」**的選項。
   - 對於 Windows，**「內容選取」**可讓您在安裝套件中包含內容。如果包含內容，套件雖然較大但用戶端在安裝後就能立即擁有最新內容。如果不包含內容，套件雖然較小但用戶端必須在安裝後取得內容更新。

   您也可以新增選擇性升級排程。如果未設定排程，自動升級程序會在精靈完成後開始。
8. 在**「通知」**標籤上，自訂使用者通知設定。

   您可以自訂升級時用戶端電腦上顯示的訊息。您也可以允許使用者延後升級。

9 按下「**確定**」，再按「**下一步**」。

10 在「**升級用戶端精靈完成**」面板中，按下「**完成**」。

確認用戶端軟體的版本號碼

- 升級完成後，您可以透過下列其中一種方式檢查版本以確認升級是否成功：
  - 在主控台中，按下「**用戶端**」>「**用戶端**」，選取適當的群組，並將檢視變更為「**用戶端狀態**」。
  - 在 Windows 用戶端上，於 Symantec Endpoint Protection 用戶端介面中按下「**說明**」>「**關於**」。
  - 在 Mac 用戶端上，開啟 Symantec Endpoint Protection 用戶端介面。在功能表列中，按下 **Symantec Endpoint Protection** >「**關於 Symantec Endpoint Protection**」。

升級後，用戶端電腦必須重新啟動。依據預設，用戶端會在安裝後重新啟動。您可以在群組的一般設定中架構重新啟動選項，以控制群組中的用戶端在自動升級後的重新啟動方式。您也可以從管理伺服器執行重新啟動指令，隨時重新啟動用戶端。

請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

請參閱第 134 頁的「將升級設定套用至其他群組」。

將升級設定套用至其他群組

您可以將現有自動升級用戶端安裝套件的升級設定從一個群組複製到另一個群組。如果複製升級設定，則無須為每個群組個別建立套件設定。

此選項會複製下列用戶端安裝套件設定：

- 用戶端功能集
- 「**更新時保留現有用戶端功能**」已啟用還是已停用
- 用戶端安裝設定
- 內容選取
- 下載來源
- 升級排程
- 「**通知**」標籤中的設定和訊息文字

在自動升級期間，Windows 設定會套用至 Windows 用戶端，Mac 設定會套用至 Mac 用戶端。這些設定也會套用至任何加入群組的新用戶端。

如果將已複製設定套用至已指派給目標群組的套件，則已複製設定會覆寫目標群組的現有設定。如果目標群組沒有指派套件，則此選項會使用已複製設定新增用戶端安裝套件。

套用升級設定到其他群組

1 在主控台中，執行下列其中一項工作：

- 按下**「用戶端」**>**「安裝套件」**，選取群組，然後在**「工作」**下，按下**「套用目前的部署設定到其他群組」**。
- 按下**「用戶端」**，在群組上按下滑鼠右鍵，然後按下**「複製部署設定」**。

2 在**「複製部署設定」**對話方塊中，按下新群組，按下**「確定」**，然後按下**「是」**。

請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。

升級群組更新提供者

使用此程序升級屬於「群組更新提供者」的用戶端。

升級群組更新提供者用戶端

1 將 Symantec Endpoint Protection Manager 伺服器升級為新版軟體。

2 將屬於「群組更新提供者」的用戶端升級為新版用戶端軟體。

3 將其餘的用戶端更新為新版用戶端軟體。

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

請參閱第 119 頁的「升級至新版本」。

部分 2

管理用戶端伺服器通訊和更新內容

8

管理用戶端伺服器通訊

本章包含以下主題：

管理用戶端伺服器連線

安裝用戶端後，管理伺服器會自動連線到用戶端電腦。

表 8-1 管理伺服器和用戶端之間的連線管理工作

動作	敘述
檢查用戶端是否連線至管理伺服器	您可以在用戶端與管理主控台中檢查用戶端狀態圖示。狀態圖示會顯示用戶端和伺服器之間是否通訊。 請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。 電腦可能已安裝用戶端軟體，但沒有正確的通訊檔案。 請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。 請參閱第 145 頁的「如何在用戶端電腦上取代用戶端伺服器通訊檔案」。
檢查用戶端是否取得政策更新	檢查用戶端和管理主控台的政策序號，確認用戶端電腦是否取得最新的政策更新。如果用戶端能夠與伺服器進行通訊，並且接收定期的政策更新，則政策序號應該相符。 您可以執行手動政策更新，然後比對政策序號。 請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。 請參閱第 268 頁的「更新用戶端政策」。
變更用來下載政策與內容至用戶端的方式	您可以將管理伺服器架構為下推政策至用戶端，或由用戶端提取管理伺服器的政策。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。
決定是否使用預設的管理伺服器清單	您可以針對容錯移轉和負載平衡使用其他管理伺服器清單。管理伺服器清單可提供用戶端可連線至多個管理伺服器的清單資訊。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。
架構位置的通訊設定	您可以針對位置和群組分別架構通訊設定。 請參閱第 234 頁的「架構位置的通訊設定」。
排除管理伺服器連線問題	若管理伺服器與用戶端無法連線，您可以解決兩者連線的問題。 請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

如需詳細資訊，請參閱以下文章：關於 Symantec Endpoint Protection 使用的通訊埠

檢查用戶端是否已連線至管理伺服器且受保護

在您安裝用戶端後，請檢查用戶端是否為線上狀態且已連線至 Symantec Endpoint Protection Manager。您可以在主控台和用戶端上檢查連線狀態。

在 Symantec Endpoint Protection 用戶端上檢查用戶端管理伺服器連線

- 在用戶端電腦上，執行下列其中一項工作：

- 電腦工作列中的用戶端保護盾帶有綠點。

- 開啟用戶端並查看「狀態」畫面，其指出**「您的電腦已受到防護」**並顯示綠色核取記號。

- 開啟用戶端並按下**「說明」**>**「疑難排解」**。

請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。

在 Symantec Endpoint Protection Manager 中檢查用戶端管理伺服器連線

1 在主控台中，按下**「用戶端」**，然後選取目標群組。

2 在**「用戶端」**標籤上，已連線的用戶端在**「名稱」**欄中會顯示帶有綠點的圖示，並顯示**「線上」**運作狀態。

附註：透過 Symantec Endpoint Protection Manager 連線的用戶端可能不會立即在雲端主控台中顯示正確的線上狀態。在線上狀態變更後，可能需要 5-10 分鐘才能看到目前狀態的準確反映。

版本 14

版本 12.1.x

表 8-2顯示**「名稱」**欄中的以下圖示表示什麼。

表 8-2 管理主控台中的用戶端狀態圖示

14	12.1.x	敘述
		用戶端軟體安裝失敗。
		■ 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。運作狀態為**「線上」**。 ■ 用戶端處於電腦模式。
		■ 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。運作狀態為**「離線」**。 ■ 用戶端處於電腦模式。 ■ 可能已使用主控台新增用戶端，但可能尚未安裝任何 Symantec 用戶端軟體。

14	12.1.x	敘述
		■ 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於電腦模式。 ■ 用戶端為非受管偵測程式。
		■ 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於電腦模式。 ■ 用戶端為非受管偵測程式。
		■ 用戶端能夠與 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於使用者模式。
		■ 用戶端無法與 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於使用者模式。 ■ 可能已使用主控台新增用戶端，但可能尚未安裝任何 Symantec 用戶端軟體。
		■ 用戶端能夠與另一網站上的 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於電腦模式。
		■ 用戶端能夠與另一網站上的 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於電腦模式。 ■ 用戶端為非受管偵測程式。
		■ 用戶端能夠與另一網站上的 Symantec Endpoint Protection Manager 進行通訊。 ■ 用戶端處於使用者模式。

請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。

Symantec Endpoint Protection 用戶端狀態圖示

您可以檢查用戶端上的通知區域圖示，判斷用戶端是否連線至管理伺服器以及獲得適當保護。通知區域圖示有時又稱為系統匣圖示。

該圖示位於用戶端電腦桌面的右下角。您還可以滑鼠右鍵按下此圖示，顯示常用指令。

表 8-3 用戶端狀態圖示

圖示	敘述
	用戶端執行時未發生問題。該用戶端可能離線或為非受管用戶端。非受管用戶端並未連線到管理伺服器。

圖示	敘述
	用戶端執行時未發生問題。該用戶端已連線到伺服器，並與其通訊。安全性政策的所有元件都可保護電腦。
	用戶端發生次要問題。例如，病毒定義檔可能過期。
	用戶端未執行、發生了重大問題、具有過期的授權，或至少有一個防護技術停用。

您還能檢查管理伺服器，以檢視電腦的連線狀態。

請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。

請參閱第 137 頁的「管理用戶端伺服器連線」。

使用推送模式或提取模式更新用戶端上的政策和內容

決定要使用提取模式還是推送模式來進行 Symantec Endpoint Protection Manager 與用戶端之間的連線

在管理伺服器上架構政策時，需要將更新後的政策下載到用戶端電腦。您可以在主控台中將用戶端電腦架構為使用以下任一更新方法：

提取模式　用戶端電腦會根據活動訊號設定的頻率，定期連線至管理伺服器。用戶端電腦會在用戶端連線時檢查管理伺服器的狀態。

推送模式　用戶端電腦會與管理伺服器建立持續的 HTTP 連線。每當管理伺服器的狀態發生變更，就會立刻通知用戶端電腦。

無論使用哪一種模式，用戶端電腦都會根據管理伺服器狀態的變更來採取相應的動作。由於必須持續連線的關係，推送模式需要較大的網路頻寬。架構為使用提取模式的用戶端電腦需要較小的頻寬。

活動訊號通訊協定定義用戶端電腦上傳資料的頻率，例如上傳日誌項目和下載政策等。用戶端啟動後會立刻出現首次活動訊號。依照您所設定的活動訊號頻率會出現下次活動訊號。

活動訊號頻率是決定 Symantec Endpoint Protection Manager 可支援多少個用戶端的重要因素。如果您將活動訊號頻率設為 30 分鐘 (含) 以下，那麼 Symantec Endpoint Protection Manager 可支援的用戶端總數就會受限制。如果部署的用戶端數為 1,000 或更多，賽門鐵克建

議盡可能地將活動訊號頻率設定為最長時間。賽門鐵克建議您使用仍符合公司安全性需求的最長時間間隔。例如，如果您想要每天更新政策並收集日誌，可以將活動訊號頻率設為 24 小時。評估您網路環境所需的正確組態、硬體及網路架構。

附註：您也可以在用戶端電腦上手動更新政策。

請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。

請參閱第 94 頁的「Symantec Endpoint Protection 的通訊埠」。

架構群組的推送模式或提取模式

可以指定是 Symantec Endpoint Protection Manager 將政策下推至用戶端，還是用戶端從 Symantec Endpoint Protection Manager 提取政策。 預設設定為推送模式。 若選取提取模式，則依據預設，用戶端每隔五分鐘就會連線到管理伺服器，但可以變更此預設活動訊號間隔。

請參閱第 268 頁的「執行適用於所有政策的工作」。

可以設定群組或位置的模式。

架構群組的推送或提取模式

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下，選取您要為其指定推送或提取政策的群組。
3. 按下**「政策」**。
4. 取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。
5. 在**「與位置無關的政策與設定」**窗格的**「設定」**下方，按下**「通訊設定」**。
6. 在**「<群組名稱> 的通訊設定」**對話方塊中，確認已勾選**「下載」**下方的**「從管理伺服器下載政策和內容」**。
7. 執行下列其中一項工作：
   - 按下**「推送模式」**。
   - 按下**「提取模式」**，然後在**「活動訊號間隔時間」**下，設定分鐘數或小時數。
8. 按下**「確定」**。

為位置指定推送模式或提取模式

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下，選取您要為其指定推送或提取政策的群組。
3. 按下**「政策」**。
4. 取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。
5. 在**「位置限定的政策與設定」**下，針對要修改的位置找出**「位置限定的政策」**，然後展開**「位置限定的設定」**。

6 在「**位置限定的設定**」下方，按下「**通訊設定**」右側的「**工作**」，然後取消勾選「**使用群組通訊設定**」。

7 在「**通訊設定**」的右側，按下「**本機 - 推送**」或 (「**本機 - 提取**」)。

8 執行下列其中一項工作：

- 按下「**推送模式**」。
- 按下「**提取模式**」，然後在「**活動訊號間隔時間**」下，設定分鐘數或小時數。

9 按下「**確定**」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

使用政策序號檢查用戶端伺服器通訊

若要檢查伺服器和用戶端是否通訊，請檢查主控台和用戶端上的政策序號。如果用戶端與管理伺服器進行通訊，並且接收定期的政策更新，則序號應該相符。

如果政策序號不符，您可以嘗試在用戶端電腦上手動更新政策，並且檢查疑難排解日誌。

請參閱第 268 頁的「更新用戶端政策」。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

檢視主控台中的政策序號

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」下，選取相關群組。

政策序號與政策日期會出現在程式視窗的右上角。

附註：政策序號與政策日期還會顯示在「**詳細資料**」標籤上的詳細資料清單的底部。

檢視用戶端電腦上的政策序號

◆ 在用戶端電腦上的用戶端中，按下「**說明**」>「**疑難排解**」。

在「**管理**」標籤上，檢視政策序號。

此序號應與用戶端電腦所在群組的主控台上的序號相符合。

請參閱第 268 頁的「執行適用於所有政策的工作」。

用戶端電腦和管理伺服器的通訊方式?

Symantec Endpoint Protection Manager 使用通訊檔 Sylink.xml 連線至用戶端。Sylink.xml 檔案含有通訊設定，例如，管理伺服器的 IP 位址和活動訊號間隔。在您安裝用戶端安裝套件到用戶端電腦後，用戶端和伺服器會自動通訊。

Sylink 檔案會在活動訊號期間執行大多數功能。活動訊號是用戶端電腦將日誌上傳到管理伺服器，並下載政策和指令的頻率。

Sylink 檔案包含：

- 所有管理伺服器的公開憑證。
- KCS 或加密金鑰。
- 每個用戶端所屬的網域 ID。

附註：請勿編輯 Sylink 檔案。如果您變更設定，管理伺服器會在用戶端下次連線至管理伺服器時覆寫大部分設定。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

疑難排解 Sylink 通訊

在版本 14.2 中，通訊模組已升級，並包含新的日誌檔。您可以使用此資訊來疑難排解 Symantec Endpoint Protection Manager 與用戶端之間的通訊問題。

14.2 通訊模組適用於所有用戶端類型 (包括 Windows、Mac 和 Linux)，並且已改進 IPv6 支援。

附註：自 14.2 版起，通訊模組僅遵守系統代理資訊。

檢視通訊模組的日誌檔

◆ 在 Windows 用戶端上的下列資料夾中：

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data`

您可以檢視下列檔案：

- **對於用戶端註冊：**
  - `RegistrationInfo.xml`
    用戶端提交至 Symantec Endpoint Protection Manager 的用戶端註冊中繼資料。
  - `Registration.xml`
    Symantec Endpoint Protection Manager 傳回用戶端的用戶端註冊中繼資料。
  - `State.xml`
    包含內部設定，例如管理伺服器 IP 位址。
- **對於通訊模組日誌：**
  `\Logs\cve.log` 和 `\Logs\cve-actions.log`
  您可以使用這些日誌來疑難排解 Symantec Endpoint Protection Manager 與用戶端之間的通訊。如果系統要求，請將這些日誌傳送至技術支援。

- **對於 Opstate 狀態：**
  顯示在 \Pending 和 \Sent 資料夾中的日誌中

架構通訊模組日誌

1 開啟 Windows 登錄編輯程式，按下**「開始」>「執行」**，輸入 regedit，然後按下**「確定」**。

2 若要啟用 cve.log 或 cve-actions.log，請開啟下列 Windows 登錄機碼：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint
Protection\SMC\SYLINK\SyLink REG_DWORD: CVELogLevel
```

使用下列任一值：

- 1 = 除錯
- 2 = 告知
- 3 = 警告
- 4 = 錯誤
- 5 = 嚴重

如果登錄機碼不存在或不具有有效值，則預設值為 4。安裝預設值也是 4。

例如，您可以輸入：

32 位元：`[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001`

64 位元：`[HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001`

3 若要控制這些日誌的大小，請使用下列登錄值：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint
Protection\SMC\SYLINK\SyLink] REG_DWORD: CVELogSizeDB
```

預設大小為 250 MB。

如何在 Endpoint Protection 14.2 中啟用通訊模組記錄

如何在用戶端電腦上取代用戶端伺服器通訊檔案

何時應在用戶端電腦上取代用戶端伺服器通訊檔案？

通常您不需要取代 Sylink.xml 檔案。不過，您可能需要在下列情況下取代用戶端電腦上的現有 Sylink.xml 檔案：

- 用戶端和伺服器沒有通訊。如果用戶端失去與管理伺服器之間的通訊，則必須使用新的檔案來取代舊的 Sylink.xml 檔案。

請參閱第 659 頁的「在用戶端電腦上檢查與管理伺服器的連線」。

- 您想要將非受管用戶端轉換成受管用戶端。如果使用者從安裝檔案安裝用戶端，該用戶端即為非受管用戶端，不會與管理伺服器進行通訊。您也可以在電腦上重新安裝用戶端軟體成為受管電腦。
  請參閱第 108 頁的「關於受管和非受管用戶端」。
- 您想要管理以前遺棄的用戶端。例如，如果安裝在管理伺服器上的硬碟損毀，您必須重新安裝管理伺服器。您可以更新遺棄的用戶端上的 Sylink.xml 檔案，以與其重新建立通訊。
  請參閱第610頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。
  請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。
- 您想要從多個群組移動大量的用戶端到單一群組。例如，您可能想要將遠端群組和桌上型電腦群組中的用戶端電腦移動到測試群組。一般來說，必須一次移動一個用戶端電腦群組。
  請參閱第 209 頁的「將用戶端電腦移至其他群組」。

如何在用戶端電腦上取代用戶端伺服器通訊檔案

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

如何將適用於 Macintosh 用戶端的非受管 Symantec Endpoint Protection 轉換為受管

如何在用戶端電腦上取代用戶端伺服器通訊檔案

如果您需要在用戶端電腦上取代用戶端伺服器通訊檔案 (Sylink.xml)，您可以使用以下方法：

- 建立新的用戶端安裝套件，並將其部署在用戶端電腦上。如果在大型環境中手動匯入 Sylink.xml 是實際無法進行的作業，且要求管理存取權時，請使用這個方法。
  請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。
- 撰寫執行 SylinkDrop 工具的程序檔，該工具位於安裝檔案的 \Tools 資料夾中。賽門鐵克建議針對大量用戶端使用這個方法。如果您使用軟體管理工具下載用戶端軟體到電腦，那麼也應該使用 SylinkDrop 工具。軟體管理工具的優點是，只要一般使用者開啟用戶端電腦，它就會下載 Sylink.xml 檔案。相較之下，用戶端安裝套件只會在用戶端電腦連線至管理伺服器時，才會下載新的 Sylink.xml 檔案。
  請參閱第 663 頁的「使用 SylinkDrop 工具還原用戶端伺服器通訊設定」。
- 將 Sylink.xml 檔案匯出至用戶端電腦，然後手動在用戶端電腦上將它匯入。如果您想要使用軟體管理工具，賽門鐵克建議使用此方法。利用軟體管理工具，只要使用者啟動電腦，工作就會佇列並完成。使用其他方法時，用戶端電腦將必須連線。
  表 8-4 顯示匯出和匯入 Sylink.xml 檔案至用戶端電腦的程序。

表 8-4 匯出和匯入通訊檔案的步驟

步驟	敘述
步驟 1：針對要使用戶端出現在其中的群組，匯出包含全部通訊設定的檔案。	預設檔案名稱為 *group name*_sylink.xml。 請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

步驟	敘述
步驟 2：將檔案部署至用戶端電腦。	您能夠將檔案儲存於網路位置，也能夠傳送至用戶端電腦的個別使用者。
步驟 3：在用戶端電腦上匯入檔案。	您或使用者可以在用戶端電腦上匯入檔案。 請參閱第 149 頁的「將用戶端伺服器通訊設定匯入 Windows 用戶端」。 非受管用戶端未使用密碼保護，因此不需要在用戶端上輸入密碼。不過，如果您嘗試將某個檔案匯入至受密碼保護的受管用戶端，則必須輸入密碼。此密碼與用來匯入或匯出政策的密碼相同。 請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。 您不需重新啟動用戶端電腦。
步驟 4：驗證用戶端上的用戶端和伺服器通訊。	用戶端會立即連線至管理伺服器。管理伺服器會將用戶端放置於通訊檔案中指定的群組。用戶端會以群組的政策和設定進行更新。用戶端與管理伺服器進行通訊後，用戶端電腦工作列將顯示帶有綠點的通知區域圖示。 請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

請參閱第 667 頁的「用戶端與伺服器通訊檔案」。

請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。

使用「通訊更新套件部署」還原用戶端伺服器通訊

如果用戶端伺服器通訊中斷，您可以取代用戶端電腦上的 Sylink.xml 檔案，迅速還原通訊。您可以部署通訊更新套件來取代 Sylink.xml 檔案。請將此方法用於大量電腦、您實際上無法輕易存取的電腦或需要管理存取的電腦。

請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。

使用「通訊更新套件部署」還原用戶端伺服器通訊設定

1. 在主控台中，啟動**「用戶端部署精靈」**。

   按下**「說明」>「開始使用」頁面**，然後在**「所需工作」**下方，按下**「在您的電腦上安裝用戶端軟體」**。

2. 在**「用戶端部署精靈」**的**「通訊更新套件部署」**下方，選取想要適用於 Windows 還是 Mac 用戶端的套件，然後按**「下一步」**。

3. 選取您要套用政策的群組，然後按**「下一步」**。

   僅針對 Windows 用戶端，您可以設定密碼防護。

   請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。

4. 選擇下列其中一種部署方法，然後按**「下一步」**：

   - 按下**「遠端推送」**並移至下列程序中的**「電腦選取」**步驟。

請參閱第 50 頁的「使用遠端推送安裝 Symantec Endpoint Protection 用戶端」。

- **「儲存套件」**並移至下列程序中的**「瀏覽器」**步驟。
  請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

5 套用通訊更新套件之後，請確認電腦與 Symantec Endpoint Protection Manager 成功通訊。

請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。

手動匯出用戶端伺服器通訊檔案 (Sylink.xml)

如果用戶端與伺服器之間的通訊中斷，您可能需要在用戶端電腦上取代 Sylink.xml 檔案才能還原通訊。您可以根據群組從 Symantec Endpoint Protection Manager 手動匯出 Sylink.xml 檔案。

在用戶端上取代 Sylink.xml 的最常見原因如下：

- 將非受管用戶端轉換成受管用戶端。
- 將先前遺棄的用戶端重新連接到管理伺服器。
  請參閱第610頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。

請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。

如果您需要更新大量用戶端的用戶端伺服器通訊，請部署「通訊更新套件」，而非使用這個方法。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

手動匯出用戶端伺服器通訊檔案

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下，選取要使用戶端在其中出現的群組。

3 在群組上按下滑鼠右鍵，然後按下**「匯出通訊設定」**。

4 在**「匯出 <群組名稱> 的通訊設定」**對話方塊中，按下**「瀏覽」**。

5 在**「選取匯出檔案」**對話方塊中，找出要將 .xml 檔案匯出至的資料夾，然後按下**「確定」**。

6 在 **「偏好政策模式」**中，確定已核取**「電腦模式」**。

7 按下**「匯出」**。

如果檔案名稱已經存在，請按下**「確定」**以覆寫檔案，或按下**「取消」**以新的檔案名稱儲存檔案。

若要結束轉換，您或使用者必須匯入用戶端電腦的通訊設定。

請參閱第 149 頁的「將用戶端伺服器通訊設定匯入 Windows 用戶端」。

將用戶端伺服器通訊設定匯入 Windows 用戶端

匯出用戶端伺服器通訊設定之後，即可將這些設定匯入 Windows 用戶端。您可以使用此方式，將非受管用戶端轉換為受管用戶端，或重新連線先前遺棄的用戶端至 Symantec Endpoint Protection Manager。

將用戶端伺服器通訊設定檔案匯入 Windows 用戶端

1. 開啟電腦中您要轉換為受管用戶端的 Symantec Endpoint Protection。
2. 在右上角，按下**「說明」**，再按下**「疑難排解」**。
3. 在**「疑難排解」**對話方塊的**「管理」**窗格中，按下**「匯入」**。
4. 在**「匯入群組註冊設定」**對話方塊中，找出 <群組名稱_sylink>.xml 檔案，然後按下**「開啟」**。
5. 按下**「關閉」**，關閉**「疑難排解」**對話方塊。

   匯入通訊檔案後，用戶端與管理伺服器進行通訊時，電腦工作列將顯示帶有綠點的通知區域圖示。綠點表示用戶端與管理伺服器互相通訊中。

請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

將用戶端伺服器通訊設定匯入 Linux 用戶端

為 Linux 用戶端安裝非受管 Symantec Endpoint Protection 後，您可將其轉換為受管用戶端，以便利用 Symantec Endpoint Protection Manager 集中管理用戶端的政策和狀態。受管用戶端會與 Symantec Endpoint Protection Manager 通訊，並向其報告狀態和其他資訊。

您也可以使用此程序，將先前遺棄的用戶端重新與 Symantec Endpoint Protection Manager 連線。

附註：您必須具有進階使用者權限才能執行此程序。必要時，此程序會使用 `sudo` 來提高權限。

文字 *path-to-sav* 代表 sav 指令的路徑。預設路徑為 /opt/Symantec/symantec_antivirus/。

將用戶端伺服器通訊設定檔案匯入 Linux 用戶端

1 您或 Symantec Endpoint Protection Manager 管理員必須先從 Symantec Endpoint Protection Manager 匯出通訊設定檔案，然後再將檔案複製到 Linux 電腦上。確認檔案名稱是 `sylink.xml`。

請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

2 在 Linux 電腦上，開啟終端機視窗，然後輸入下列指令：

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

其中 ***path-to-sylink*** 代表您要將 `sylink.xml` 複製到的路徑。

例如，如果您將檔案複製到使用者設定檔的桌面，請輸入：

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

3 傳回「確定」即表示匯入成功。若要進一步驗證受管狀態，請輸入下列指令，它會顯示成功匯入的政策序號：

```
path-to-sav/sav manage -p
```

請參閱第 48 頁的「安裝 Linux 的 Symantec Endpoint Protection 用戶端」。

9

更新用戶端上的內容

本章包含以下主題：

- 將 Endpoint Protection 安全修補程式下載至 Windows 用戶端

如何更新用戶端上的內容和定義檔

依據預設，Symantec Endpoint Protection Manager 從公用 Symantec LiveUpdate 伺服器下載內容更新。Symantec Endpoint Protection 用戶端接著會從 Symantec Endpoint Protection Manager 下載這些更新。該內容包括病毒定義檔、入侵預防特徵和主機完整性範本等。

表 9-1 更新 Symantec Endpoint Protection 用戶端上的內容的步驟

工作	敘述
請確保管理伺服器具有來自 LiveUpdate 的最新內容 (建議使用)	依據預設，在 Symantec Endpoint Protection Manager 安裝過程中，LiveUpdate 會執行。遇到下列情況時，您可能需要手動執行 LiveUpdate： ■ 在安裝期間略過了 LiveUpdate。 ■ 您必須執行 LiveUpdate 才能下載主機完整性範本和入侵預防特徵。 ■ 您想要在下一個排程更新之前執行 LiveUpdate。 請參閱第 162 頁的「確認 Symantec Endpoint Protection Manager 具有最新內容」。 您也可以在 Symantec Endpoint Protection Manager 上使用 .jdb 檔案更新內容。 下載 .jdb 檔案以更新 Endpoint Protection Manager 的定義檔 此外，如果您使用遠端複製，則可以在本機站台與夥伴站台之間遠端複製內容和政策。 請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。
變更用戶端電腦取得更新的方式 (選擇性)	依據預設，Windows 用戶端電腦將從管理伺服器取得內容更新。 其他傳送方法包括群組更新提供者、內部 LiveUpdate 伺服器或第三方工具派送。您可能需要變更傳送方法以支援不同的用戶端平台、大量的用戶端或網路限制。 請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。 請參閱第 157 頁的「選擇派送方法以根據平台來更新用戶端上的內容」。
變更管理伺服器的 LiveUpdate 設定 (選擇性)	您可以自訂 LiveUpdate 階段作業的頻率、下載的防護元件等。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。
減少網路超載 (建議使用)	如果管理伺服器收到太多來自用戶端的關於完整定義套件的並行要求，網路可能會超載。 您可以降低這些超載的風險，並阻止用戶端下載完整定義。 請參閱第 176 頁的「減少用戶端更新要求的網路超載」。

工作	敘述
改善效能 (建議使用)	為了協助降低下載對網路頻寬的影響，可以隨機下載內容，這樣，所有用戶端就不會同時取得更新。 請參閱第 176 頁的「關於隨機化同時內容下載」。 請參閱第 177 頁的「從預設管理伺服器或群組更新提供者隨機進行內容下載」。 請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。 為了緩解下載對用戶端電腦效能的影響，您可以讓用戶端電腦在閒置時下載內容更新。 請參閱第 178 頁的「將 Windows 用戶端更新架構為在用戶端電腦閒置時執行」。
讓您的端點使用者管理他們自己的更新 (選擇性)	依據預設，用戶端電腦上的使用者可以隨時執行 LiveUpdate。您可以決定給予使用者對其內容更新的控制範圍。 請參閱第 175 頁的「架構使用者對 LiveUpdate 的控制能力」。 您也可以在用戶端電腦上使用智慧型更新小幫手 (Intelligent Updater) 來更新定義檔。 請參閱第 191 頁的「使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容」。
在賽門鐵克發布測試引擎更新之前測試更新 (選擇性)	賽門鐵克將每季發布引擎更新。在使用特定的 Symantec LiveUpdate 伺服器發布引擎更新之前，您可以先下載這些更新。然後，在引擎內容遞送到生產環境之前，可以測試內容。 請參閱第 180 頁的「在 Windows 用戶端上發布之前測試引擎更新」。

選擇派送方法以更新用戶端上的內容

您可能需要變更用戶端的預設更新方法，視用戶端平台、網路組態、用戶端數目或是您公司的安全政策和存取政策而定。

表 9-2 內容派送方法及使用時機

方法	敘述	使用時機
Symantec Endpoint Protection Manager 至用戶端電腦 (預設值) (Windows、Mac、Linux)	預設管理伺服器會自動更新所管理的用戶端電腦。 請勿定義從管理伺服器到用戶端之更新的排程。用戶端根據通訊模式和活動訊號頻率從管理伺服器下載內容。 請參閱第 180 頁的「將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容」。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。	賽門鐵克建議您使用此方法，除非網路限制或是您公司的政策需要替代方法。 如果您有大量用戶端或頻寬問題，可以搭配使用此方法和「群組更新提供者」。 要讓 Mac 或 Linux 電腦從管理伺服器接收內容更新，則必須架構 Apache Web 伺服器。 使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

方法	敘述	使用時機
「群組更新提供者」至用戶端電腦 (僅限 Windows)	「群組更新提供者」是從管理伺服器接收更新的用戶端電腦。然後，「群組更新提供者」會將更新轉送到群組中的其他用戶端電腦。「群組更新提供者」可以更新多個群組。 「群組更新提供者」可以派送除用戶端軟體更新之外的所有類型的 LiveUpdate 內容。「群組更新提供者」也無法用於更新政策。	「群組更新提供者」可讓您減輕管理伺服器的負載，而且比內部 LiveUpdate 伺服器更容易架構。 對於位於最小頻寬的遠端位置的群組，請使用「群組更新提供者」。 請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。 請參閱第 640 頁的「決定是否要設定多個網站和遠端複製」。
內部 LiveUpdate 伺服器至用戶端電腦 (Windows、Mac、Linux)	用戶端電腦可以直接從內部 LiveUpdate 伺服器下載更新，內部 LiveUpdate 伺服器從 Symantec LiveUpdate 伺服器接收其更新。 如有必要，您可以設定幾個內部 LiveUpdate 伺服器，並將此清單散佈到用戶端電腦。 您可以將下載排程從 LiveUpdate 伺服器變更為管理伺服器。 請參閱第 173 頁的「針對用戶端電腦架構 LiveUpdate 下載排程」。 如需設定內部 LiveUpdate 伺服器的詳細資訊，請參閱「LiveUpdate Administrator User's Guide」，網址為： 下載 LiveUpdate Administrator	內部 LiveUpdate 伺服器可讓您減輕大型網路中管理伺服器的負載。在較小型網路中，請考量「群組更新提供者」是否能夠滿足組織的需要。 請考慮在下列情況下使用內部 LiveUpdate 伺服器： ■ 如果管理大型網路 (超過 10,000 個用戶端) ■ 如果管理不應連線至外部 LiveUpdate 伺服器的 Mac 或 Linux 用戶端 ■ 如果您組織部署的多項賽門鐵克產品也使用 LiveUpdate 派送內容到用戶端電腦 **附註：**您不應該將管理伺服器與內部 LiveUpdate 伺服器安裝在同一個實體硬體或虛擬機器上。安裝在同一台電腦上可能導致重大的伺服器效能問題。 如需詳細資訊，請參閱： 相同電腦上的 LiveUpdate Administrator 2.x 和 Symantec Endpoint Protection Manager 請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

方法	敘述	使用時機
外部 Symantec LiveUpdate 伺服器透過 Internet 與用戶端電腦連線 (Windows、Mac、Linux)	用戶端電腦可以直接從 Symantec LiveUpdate 伺服器接收更新。	如果您需要排程用戶端更新內容的時間或者 Symantec Endpoint Protection Manager 與用戶端之間的可用頻寬受限，則可以使用外部 Symantec LiveUpdate 伺服器。 Symantec Endpoint Protection Manager 和排程更新預設會啟用。使用預設設定時，用戶端一律從管理伺服器取得更新，除非管理伺服器在較長時間內無回應。 **附註：**請勿將大量的受管理網路用戶端架構為從外部 Symantec LiveUpdate 伺服器提取更新。此組態會耗用不必要的頻寬。 請參閱第 171 頁的「架構用戶端從外部 LiveUpdate 伺服器下載內容」。
第三方工具派送 (僅限 Windows)	Microsoft SMS 等第三方工具可將特定的更新檔案派送至用戶端。	此方法可讓您在派送更新檔案之前先行測試。如果您備有第三方工具派送基礎架構，則可能也適用。 請參閱第 195 頁的「使用第三方派送工具派送內容」。
智慧型更新小幫手 (Intelligent Updater) (僅限 Windows)	智慧型更新小幫手 (Intelligent Updater) 檔案包含可用於手動更新用戶端的病毒和安全風險內容以及入侵預防內容。 您可以從賽門鐵克網站下載智慧型更新小幫手 (Intelligent Updater) 自動解壓縮檔案。	如果 LiveUpdate 無法使用，可以使用智慧型更新小幫手 (Intelligent Updater) 檔案。 請參閱第 191 頁的「使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容」。 若要更新其他種類的內容，您必須設定和架構管理伺服器以下載和預備更新檔案。 請參閱第 192 頁的「使用第三方派送工具更新用戶端電腦」。

圖 9-1 顯示較小型網路的派送架構範例。

圖 9-1 較小型網路的派送架構範例

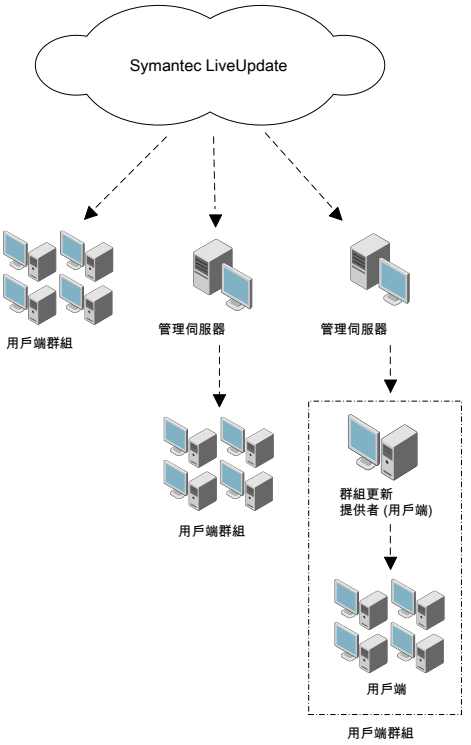
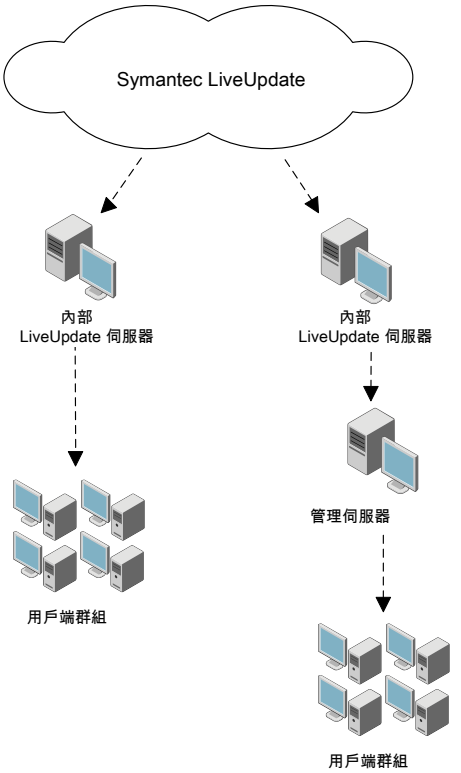


圖 9-2 顯示較大型網路的派送架構範例。

圖 9-2 較大型網路的派送架構範例



請參閱第 157 頁的「選擇派送方法以根據平台來更新用戶端上的內容」。
請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。
請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

選擇派送方法以根據平台來更新用戶端上的內容

可用於將病毒定義檔和其他內容派送到用戶端電腦的方法視用戶端平台而定。

表 9-3 根據 Windows、Mac 和 Linux 用戶端的內容派送方法

平台	方法
Windows	依據預設，Windows 用戶端會從管理伺服器取得內容。 Windows 用戶端也可以從下列來源取得更新： ■ LiveUpdate 伺服器 (外部或內部) 請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。 請參閱第 171 頁的「架構用戶端從外部 LiveUpdate 伺服器下載內容」。 ■ 外部 LiveUpdate 伺服器 (僅測試) 請參閱第 180 頁的「在 Windows 用戶端上發布之前測試引擎更新」。 ■ 群組更新提供者 請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。 ■ 協力廠商散佈工具 請參閱第 195 頁的「使用第三方派送工具派送內容」。 ■ 智慧型更新小幫手 (Intelligent Updater) 請參閱第 191 頁的「使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容」。 請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。 對於 Windows 用戶端，您也可以自訂下列設定： ■ 用戶端接收的內容類型 ■ 用戶端是否能從多個來源取得定義檔 ■ 如果管理伺服器只能提供完整定義檔套件，則用戶端是否能從 LiveUpdate 取得較小的套件 (增量) 完整定義檔套件非常龐大。 下載過多完整套件可能會使您的網路超載。 增量通常小很多，對網路頻寬的影響也很少。 請參閱第 176 頁的「減少用戶端更新要求的網路超載」。
Mac 或 Linux	■ LiveUpdate 伺服器 (外部或內部) ■ 架構為反向代理的 Apache Web 伺服器 使 Mac 或 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

請參閱第 163 頁的「關於 LiveUpdate 下載的內容類型」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager

架構管理伺服器下載 LiveUpdate 內容時，必須做幾個決定。將內容下載至 Symantec Endpoint Protection Manager 時，可以下載站台上所有管理伺服器的內容。

關於下載內容的決定

表 9-4 關於內容下載的決定

決定	敘述
LiveUpdate 伺服器應該提供什麼內容給站台？	您可以指定外部 Symantec LiveUpdate 伺服器 (建議)，也可以指定先前已安裝和架構的一台或多台內部 LiveUpdate 伺服器。 您不應該將 Symantec Endpoint Protection Manager 與內部 LiveUpdate 伺服器安裝在同一個實體硬體或虛擬機器上。安裝在同一台電腦上可能導致重大的伺服器效能問題。 如果您決定使用一台或多台內部 LiveUpdate 伺服器，則可能要將賽門鐵克公共 LiveUpdate 伺服器新增為最後一個項目。如果您的用戶端無法連線清單上的任何伺服器，它們仍可從 Symantec LiveUpdate 伺服器進行更新。 **附註：**Symantec Endpoint Protection Manager 不再包括 LiveUpdate Administrator 1.x 舊版支援。若要繼續使用內部 LiveUpdate 伺服器，您應升級至最新版 LiveUpdate Administrator。 下載 LiveUpdate Administrator 請參閱第 171 頁的「架構用戶端從外部 LiveUpdate 伺服器下載內容」。 請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。 請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

決定	敘述
站台要儲存多少內容修訂？	管理伺服器上儲存的 LiveUpdate 內容修訂與 12.1.5 之前的 Symantec Endpoint Protection Manager 版本不同。舊版儲存了每個修訂的完整內容。現在，該伺服器僅儲存最近的完整內容套件，以及您在此處所指定數目的修訂的遞增增量。 這種方法可減少在伺服器上儲存多個內容修訂所需的磁碟空間。 您在安裝 Symantec Endpoint Protection Manager 期間選取的用戶端數目將定義伺候器儲存的修訂數目。 對於每個 LiveUpdate 內容類型，預設值如下： 對於 14 版： ■ 如果您不勾選**「管理伺服器將管理少於 500 個用戶端」**，Symantec Endpoint Protection Manager 將儲存 21 個修訂。 ■ 如果您勾選**「管理伺服器將管理少於 500 個用戶端」**，Symantec Endpoint Protection Manager 將儲存 90 個修訂。 對於早於 14 版但晚於 12.1.5 版的版本，或是從早於 14 版的升級： ■ 如果選取的用戶端少於 100 個，Symantec Endpoint Protection Manager 會儲存 12 個修訂。 ■ 如果選取 100 至 500 個用戶端，Symantec Endpoint Protection Manager 會儲存 21 個修訂。 ■ 如果選取 500 至 1,000 個用戶端，Symantec Endpoint Protection Manager 會儲存 42 個修訂。 ■ 如果選取的用戶端超過 1,000 個，則 Symantec Endpoint Protection Manager 會儲存 90 個修訂。 在升級期間的大部分實例中，安裝會增加修訂數目以符合這些新預設值。 如果您在升級之前擁有的修訂數目少於新的最小預設值 (根據上述準則)，則會發生這種增加的情況。 請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。
站台檢查 LiveUpdate 內容更新的頻率為何？	讓 Symantec Endpoint Protection Manager 每四小時執行一次 LiveUpdate 的預設排程是最佳實務準則。
我將下載哪些作業系統的內容？	LiveUpdate 僅下載適用於指定作業系統的內容。
可下載至站台和用戶端的內容類型有哪些？	請確定站台可下載用戶端 LiveUpdate 內容政策中指定的所有內容更新。 請參閱第 163 頁的「關於 LiveUpdate 下載的內容類型」。 請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。
應該為產品更新下載哪些語言？	這個設定僅套用於產品更新；會自動下載所有語言的內容更新。

決定	敘述
應該為定義檔下載哪些內容大小？	14 版標準和內嵌式/VDI 用戶端使用啟用雲端的縮減大小定義檔集 (僅限最新)。這些用戶端上的掃描會自動使用在雲端的延伸定義檔集。 14 版還包括下載整個定義檔集的暗網用戶端。 12.1.x 版標準用戶端需要舊版標準大小內容，其中包括整個定義檔集。 12.1.6.x 版內嵌式/VDI 用戶端需要舊版縮減大小內容。 **警告：**管理伺服器必須為您網路中的用戶端類型下載正確內容。如果管理伺服器不下載已安裝用戶端所需的內容，用戶端將無法從管理伺服器取得更新。
應在發布引擎更新之前測試這些更新？	若為大型組織，您應該先測試新引擎更新和定義檔，然後將其遞送到所有用戶端電腦。您想要以最少的中斷次數和停機時間測試新引擎更新。 請參閱第 180 頁的「在 Windows 用戶端上發布之前測試引擎更新」。

將 LiveUpdate 伺服器中的內容下載至 Symantec Endpoint Protection Manager

將內容下載至管理伺服器時，可以針對站台內所有管理伺服器進行下載。

架構站台以下載內容

1. 在主控台中，按下**「管理員」>「伺服器」**。
2. 在**「伺服器」**下，於**「本機站台」**上按下滑鼠右鍵，然後按下**「編輯站台屬性」**。
3. 在 **LiveUpdate** 標籤上，從下列可用選項中進行選擇。
4. 在**「LiveUpdate 來源伺服器」**下，按下**「編輯來源伺服器」**，然後檢查目前用於更新管理伺服器的 LiveUpdate 伺服器。此伺服器預設為 Symantec LiveUpdate 伺服器。然後執行下列其中一個動作：
   - 若要使用現有的 LiveUpdate 來源伺服器，按下**「確定」**。
   - 若要使用內部 LiveUpdate 伺服器，請按下**「使用指定的內部 LiveUpdate 伺服器」**，然後按下**「新增」**。

   如果已選取**「使用指定的內部 LiveUpdate 伺服器」**，請在**「新增 LiveUpdate 伺服器」**對話方塊中填寫可識別 LiveUpdate 伺服器的資訊，然後按下**「確定」**。

   出於容錯移轉目的，您可以新增多台伺服器。如果一個伺服器離線，其他伺服器會提供支援。您還可以將賽門鐵克公共 LiveUpdate 伺服器新增為清單中的最後一台伺服器。如果新增公共伺服器，請使用 URL **http://liveupdate.symanteclive update.com**。

附註：如果使用 UNC 伺服器，則 LiveUpdate 會要求您在使用者名稱中使用網域或工作群組。

如果電腦位於網域中，請使用格式*網域名稱\使用者名稱*。

如果電腦位於工作群組中，請使用格式*電腦名稱\使用者名稱*。

在**「LiveUpdate 伺服器」**對話方塊中，按下**「確定」**。

5 在**「用於下載的磁碟空間管理」**下方，輸入要保留的 LiveUpdate 內容修訂號碼。

6 在**「下載排程」**群組方塊中，按下**「編輯排程」**，設定伺服器應檢查更新頻率的選項。按下**「確定」**。

7 在**「要下載的平台」**下，按下**「變更平台」**，然後檢查平台清單。取消核取您不想將內容下載到哪些平台。

8 在**「要下載的內容類型」**下，檢查已下載的更新類型清單。

若要新增或刪除更新類型，請按下**「變更選定內容」**、修改清單，然後按下**「確定」**。

此清單應與包含在用戶端電腦的 LiveUpdate 內容政策中的內容類型清單相符合。

9 在**「要為用戶端類型下載的內容」**下，決定要為標準和內嵌式/VDI 用戶端還是暗網用戶端下載和儲存內容。如果在網路中執行 12.1.x 版用戶端，您還應該下載和儲存縮減大小內容或標準大小內容。

警告：您必須為網路中的用戶端類型下載內容。如果沒有下載已安裝的用戶端所需的內容，則用戶端無法從管理伺服器取得更新。

若要修改設定，請按下**「變更選定內容」**，修改選定內容，然後按下**「確定」**。

10 在**「要下載的語言」**之下，檢查已下載更新類型的語言清單。

若要新增或刪除語言，按下**「變更選定內容」**，修改清單，然後按下**「確定」**。

11 按下**「確定」**以儲存您的選定內容並關閉視窗。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

確認 Symantec Endpoint Protection Manager 具有最新內容

LiveUpdate 會按排程將定義檔和其他內容下載至 Symantec Endpoint Protection Manager。但是，如果 Symantec Endpoint Protection Manager 沒有最新版本，您可以隨時下載內容。然後 Symantec Endpoint Protection Manager 會透過預設的 LiveUpdate 政策提供此內容給用戶端電腦。

確認 Symantec Endpoint Protection Manager 具有最新內容

1 在主控台中，按下「**首頁**」。

2 在「端點狀態」群組方塊中的「**Windows 定義檔**」下，比較「**管理程式最新定義檔**」以及「**Symantec 最新定義檔**」的日期。

3 如果日期不相符，請按下「**管理員**」>「**伺服器**」>「**本機站台 (我的站台)**」。

4 在「**工作**」下方，按下「**下載 LiveUpdate 內容**」>「**下載**」。

如果您無法透過 LiveUpdate 更新 Symantec Endpoint Protection Manager 上的內容，則可以從賽門鐵克安全機制應變中心下載 .jdb 檔案。Symantec Endpoint Protection Manager 會處理這些檔案的內容，並使其可供用戶端下載。

下載 .jdb 檔案以更新 Endpoint Protection Manager 的定義檔

將內容從 LiveUpdate 下載至 Symantec Endpoint Protection Manager 時檢查

您可以確定內容在 LiveUpdate 中的 Symantec Endpoint Protection Manager 上的最近更新日期和時間。

檢查從 LiveUpdate 下載到 Symantec Endpoint Protection Manager 的內容

1 在主控台中，按下「**管理員**」。

2 在「**管理員**」頁面的「**工作**」下，按下「**伺服器**」，然後選取相應站台。

3 執行下列其中一項工作：

- 若要檢查下載狀態，請按下「**顯示 LiveUpdate 狀態**」。
- 若要檢查 Symantec Endpoint Protection Manager 所使用的目前內容版本，請按下「**顯示 LiveUpdate 狀態**」。

4 按下「**關閉**」。

疑難排解 Endpoint Protection Manager 的 LiveUpdate 和定義檔問題

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

關於 LiveUpdate 下載的內容類型

依據預設，Symantec Endpoint Protection Manager 會從公用 Symantec LiveUpdate 伺服器下載所有類型的內容。然後，LiveUpdate 內容政策會從 Symantec Endpoint Protection Manager 將所有類型的內容下載至 Windows 和 Mac 用戶端。

如果您從網站排除某個內容類型，但從 LiveUpdate 內容政策移除此內容，則此內容不會傳送至用戶端。通常，不需要排除 Symantec Endpoint Protection Manager 下載的內容。如果不確定是否需要，請不要排除某個類型的內容。

請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。

LiveUpdate 不會下載已更新的政策。指派新政策給群組或編輯現有政策時，Symantec Endpoint Protection Manager 會將政策更新至用戶端。

表 9-5 可從 LiveUpdate 下載到 Symantec Endpoint Protection Manager 的內容類型

內容類型	敘述
用戶端產品更新	賽門鐵克建議您保持此設定為取消勾選狀態。 產品更新指的是對已安裝之用戶端軟體的改進。但是，雖然可以透過使用 LiveUpdate 來取得產品更新，Symantec Endpoint Protection 一般也不會使用此方法。相反，賽門鐵克會透過 MySymantec 發行新版軟體。然後，可以升級管理伺服器軟體和用戶端軟體。 您可以使用**「用戶端部署精靈」**透過**「網路連結與電子郵件」**和**「儲存套件」**選項更新 Mac 和 Linux 用戶端。 請參閱第 119 頁的「升級至新版本」。 請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。
用戶端安全修補程式	防範 Windows 用戶端中已公開發佈的安全漏洞。例如，攻擊者可能會略過 Symantec Endpoint Protection 防護功能。 **「LiveUpdate 設定」**政策 > **「其他設定」**標籤上的**「用戶端安全修補程式設定」**核取方塊，可讓您透過 LiveUpdate、管理伺服器或群組更新提供者更新安全修補程式。
病毒和間諜軟體定義檔	x86 及 x64 平台分別有適用的病毒定義套件。此內容類型也包括自動防護入口網站清單以及 Power Eraser 定義檔。
SONAR 啟發式特徵	防範零時差攻擊的威脅。
入侵預防特徵	防範網路威脅和主機漏洞。支援入侵預防、偵測引擎和記憶體攻擊緩和。
主機完整性內容	包括預先定義需求的範本，這些範本會強制在用戶端電腦上執行更新的修補程式與安全措施。LiveUpdate 會針對執行 Windows 作業系統和 Mac 作業系統的電腦下載範本。 請參閱第 532 頁的「從範本新增自訂需求」。
傳送控制特徵	控制傳送至賽門鐵克安全機制應變中心的流程。
信譽設定	包含對用於防護的信譽資料的更新。
延伸檔案屬性和特徵	用於使更新憑證和下載鑑識更加受到資料驅動。這些資料驅動的下載有助於賽門鐵克使用定義檔式更新來更新信任的特徵清單。
Endpoint Detection and Response	Endpoint Detection and Response (EDR) 元件用以偵測和調查主機與端點上的可疑活動和問題的定義檔。EDR 會提供此蒐證資訊給各種產品元件，包括提交和 EDR 伺服器。
通用網路傳輸程式庫和組態	整個產品用以接收網路傳輸和遙測的定義檔。這些定義檔是信譽查詢以及提交和與 EDR 通訊所必需的定義檔。此類別中的定義檔包括 SEPM STIC 和 SEPC STIC，分別用於 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端。

內容類型	敘述
進階機器學習	定義檔供使用低頻寬政策的用戶端用於病毒和間諜軟體掃描 (新增於 14.0.1 版)。對具有慢速 Internet 連線網路的標準用戶端和內嵌用戶端使用低頻寬模式。在低頻寬模式中，LiveUpdate 會每週下載一次定義檔或以更不頻繁的頻率下載。若要使用低頻寬模式，您必須註冊使用雲端並啟用「低頻寬」政策。暗網用戶端無法使用低頻寬模式。 如果您不在雲端主控台中註冊管理伺服器，或不想要使用低頻寬政策，請停用此選項以節省部分頻寬和 Symantec Endpoint Protection Manager 上的磁碟空間。 請參閱第 512 頁的「在低頻寬環境中更新用戶端」。
WSS 流量重新導向	Web Security Services (WSS) 流量重新導向功能所使用的定義檔。WSS 流量重新導向使用 WSS 伺服器，以針對網頁瀏覽器提供安全的代理設定。(新增於 14.0.1 MP1 版。)
應用程式控制內容	應用程式控制引擎用於應用程式控制政策的定義檔。此選項應隨時保持在啟用狀態。 此內容僅在 14.2 及更新版本的用戶端上執行。在舊版 Windows 用戶端中，您必須先升級至 14.2。
政策指令處理常式	由政策指令處理程式引擎使用的內容。
Endpoint Threat Defense for AD 資料	由 Active Directory 防禦引擎使用的內容。針對 14.2 RU1 新增。
Symantec Endpoint Protection Manager 14.2 RU1 中繼資料	Symantec Endpoint Protection Manager 顯示政策選項所需的資料驅動資訊。除了疑難排解目的外，您應當保持啟用此內容。針對 14.2 RU1 新增。

無法在 LiveUpdate 內容政策中停用下列內容類型，其中包括**「延伸檔案屬性和特徵」**、**Endpoint Detection and Response**、**「通用網路傳輸程式庫和組態」**。

表 9-6　　功能及其需要的更新內容

安裝非受管用戶端時	更新時，您必須下載這些類型的內容
病毒和間諜軟體防護	■ 病毒和間諜軟體定義檔 ■ SONAR 定義檔 在「網站屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 ■ 集中式信譽設定 在「網站屬性」中架構下載的內容類型時，這個內容類型稱為「信譽設定」。 ■ 撤銷資料 (依據預設下載，無法從 Symantec Endpoint Protection Manager 架構) ■ 賽門鐵克許可清單 ■ 傳送控制特徵 ■ 自動防護入口網站清單 ■ Power Eraser 定義檔 ■ 延伸檔案屬性和特徵 ■ Endpoint Detection and Response ■ 通用網路傳輸程式庫和組態 ■ 進階機器學習
「病毒和間諜軟體防護」>「下載防護」	■ 病毒和間諜軟體定義檔 ■ SONAR 定義檔 在「網站屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 ■ 集中式信譽設定 ■ 撤銷資料 ■ 賽門鐵克許可清單 ■ 入侵預防特徵 選取這個下載選項時，同時包含入侵預防特徵和入侵預防引擎的更新。 ■ 傳送控制特徵 ■ 自動防護入口網站清單 ■ Power Eraser 定義檔 ■ 延伸檔案屬性和特徵 ■ Endpoint Detection and Response ■ 通用網路傳輸程式庫和組態

安裝非受管用戶端時	更新時，您必須下載這些類型的內容
「病毒和間諜軟體防護」>「Outlook 掃描程式」	■ 病毒和間諜軟體定義檔 ■ SONAR 定義檔 在「網站屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 ■ 集中式信譽設定 ■ 撤銷資料 ■ 賽門鐵克許可清單 ■ 傳送控制特徵 ■ 自動防護入口網站清單 ■ Power Eraser 定義檔 ■ 延伸檔案屬性和特徵 ■ Endpoint Detection and Response ■ 通用網路傳輸程式庫和組態 ■ 進階機器學習
「病毒和間諜軟體防護」>「Notes 掃描程式」	■ 病毒和間諜軟體定義檔 ■ SONAR 定義檔 在「網站屬性」中架構下載的內容類型時，這些定義檔稱為 SONAR 啟發式特徵。 ■ 集中式信譽設定 ■ 撤銷資料 ■ 賽門鐵克許可清單 ■ 傳送控制特徵 ■ 自動防護入口網站清單 ■ Power Eraser 定義檔 ■ 延伸檔案屬性和特徵 ■ Endpoint Detection and Response ■ 通用網路傳輸程式庫和組態
「主動型威脅防護」>SONAR	SONAR 定義檔 傳送控制特徵 延伸檔案屬性和特徵 進階機器學習
「主動型威脅防護」>「應用程式控制」	傳送控制特徵 延伸檔案屬性和特徵 應用程式控制內容 (自 14.2 起)
整合政策	WSS 流量重新導向 (自 14.0.1 MP1 起)

安裝非受管用戶端時	更新時，您必須下載這些類型的內容
「防網路和主機刺探利用」>「入侵預防」	■ 入侵預防特徵 選取這個下載選項時，同時包含入侵預防特徵和入侵預防引擎的更新。 ■ 傳送控制特徵 ■ 延伸檔案屬性和特徵
「防網路和主機刺探利用」>「防火牆」	傳送控制特徵 延伸檔案屬性和特徵
主機完整性	主機完整性內容 傳送控制特徵 延伸檔案屬性和特徵

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。

將用戶端架構為從內部 LiveUpdate 伺服器下載內容

依據預設，Windows 用戶端將從管理伺服器取得其更新。 如果您選取預設管理伺服器，且您的環境包括 Mac 和 Linux 電腦，則 Mac 和 Linux 用戶端會從預設 LiveUpdate 伺服器取得其更新。

如果您管理大量的用戶端，您可能希望對 Windows 用戶端使用「群組更新提供者」(GUP)。GUP 會減輕管理伺服器的負載，而且比內部 LiveUpdate 伺服器容易設定。

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

如果您不想使用預設管理伺服器或「群組更新提供者」進行用戶端更新，則可以：

- 設定內部 LiveUpdate 伺服器。
- 使用位於網路外部的 Symantec LiveUpdate 伺服器。

若要使用內部 LiveUpdate 伺服器，您必須執行下列工作：

- 安裝內部 LiveUpdate 伺服器。
  如需有關使用內部 LiveUpdate 伺服器的詳細資訊，請參閱「LiveUpdate Administrator 指南」。

附註：Symantec Endpoint Protection Manager 不再包括 LiveUpdate Administrator 1.x 舊版支援。若要繼續使用內部 LiveUpdate 伺服器，您應升級至最新版 LiveUpdate Administrator。 對 LiveUpdate Administrator 2.x 和更新版本的支援始終處於啟用狀態。

- 使用 LiveUpdate 設定政策將您的用戶端架構為使用該內部 LiveUpdate 伺服器。

附註：您可以為連線至內部 LiveUpdate 伺服器以檢查更新的用戶端指定代理設定。代理設定僅適用於更新，不適用於用戶端使用的其他外部通訊類型。您必須另外為其他類型的用戶端外部通訊架構代理。

請參閱第 172 頁的「指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器」。

將 Windows 用戶端架構為使用內部 LiveUpdate 伺服器

1. 在「**政策**」下方，按下 **LiveUpdate**。
2. 在「**LiveUpdate 設定**」標籤上，在所要的政策上按滑鼠右鍵，然後按下「**編輯**」。
3. 在「**Windows 設定**」下方，按下「**伺服器設定**」。
4. 在「**伺服器設定**」窗格中，勾選「**使用 LiveUpdate 伺服器**」。
5. 按下「**使用指定的內部 LiveUpdate 伺服器**」，再按下「**新增**」。
6. 在「**新增 LiveUpdate 伺服器**」對話方塊中，鍵入識別所要使用的伺服器並與之通訊所需的資訊。

   例如，對於 URL：

   - 如果您使用的是 FTP 方法 (建議)，請輸入伺服器的 FTP 位址。 例如：
     ftp://myliveupdateserver.com
   - 如果您使用的是 HTTP 方法，請輸入伺服器的 URL。 例如：
     網域名稱：http://myliveupdateserver.com
     IPv4 位址：http://192.168.133.11/Export/Home/LUDepot
     IPv6 位址：http://[fd00:fe32::b008]:80/update
   - 如果您使用的是 LAN 方法，請輸入伺服器的 UNC 路徑名稱。例如，
     \\myliveupdateserver\LUDepot
7. 如果需要，請鍵入伺服器的使用者名稱和密碼。

附註：如果您使用 UNC 伺服器，則 LiveUpdate 會要求除使用者名稱之外，還要使用網域或工作群組。 如果電腦是網域的一部分，請使用格式*網域名稱\使用者名稱*

如果電腦是工作群組的一部分，請使用格式*電腦名稱\使用者名稱*。

8 在「**LiveUpdate 政策**」下，按下「**排程**」透過 LiveUpdate 為更新設定排程。

請參閱第 173 頁的「針對用戶端電腦架構 LiveUpdate 下載排程」。

9 按下「**確定**」。

10 按下「**進階設定**」。

決定要保留還是變更預設的使用者設定、產品更新設定和非標準標頭設定。一般來說，您不希望讓使用者修改更新設定。但是，如果用戶端太多而無法支援，您不妨讓使用者手動啟動 LiveUpdate 階段作業。

請參閱第 175 頁的「架構使用者對 LiveUpdate 的控制能力」。

11 按下「**確定**」。

將 Mac 用戶端架構為使用內部 LiveUpdate 伺服器

1 在「**政策**」下方，按下 **LiveUpdate**。

2 在「**LiveUpdate 設定**」標籤上，在所要的政策上按滑鼠右鍵，然後按下「**編輯**」。

3 在「**Mac 設定**」下方，按下「**伺服器設定**」。

4 按下「**使用指定的內部 LiveUpdate 伺服器**」，再按下「**新增**」。

5 在「**新增 LiveUpdate 伺服器**」對話方塊中，鍵入識別所要使用的伺服器並與之通訊所需的資訊。

例如，對於 URL：

- 如果您使用的是 FTP 方法 (建議)，請輸入伺服器的 FTP 位址。例如：
  ftp://myliveupdateserver.com
- 如果您使用的是 HTTP 方法，請輸入伺服器的 URL。例如：
  網域名稱：http://myliveupdateserver.com
  IPv4 位址：http://192.168.133.11/Export/Home/LUDepot
  IPv6 位址：http://[fd00:fe32::b008]:80/update

6 如果需要，請鍵入伺服器的使用者名稱和密碼，然後按下「**確定**」。

7 如果您的伺服器使用 FTP，請按下「**進階伺服器設定**」。

8 按下伺服器使用的 FTP 模式「**主動**」或「**被動**」，然後按下「**確定**」。

9 在「**Mac 設定**」下，按下「**進階設定**」。

如果您要讓用戶端電腦透過 LiveUpdate 取得產品更新設定，請按下「**使用 LiveUpdate 伺服器下載 Symantec Endpoint Protection 產品更新**」。

10 按下「**確定**」。

將 Linux 用戶端架構為使用內部 LiveUpdate 伺服器

1 在「**政策**」下方，按下 **LiveUpdate**。

2 在「**LiveUpdate 設定**」標籤上，在所要的政策上按滑鼠右鍵，然後按下「**編輯**」。

3 在「**Linux 設定**」下方，按下「**伺服器設定**」。

4 按下「**使用指定的內部 LiveUpdate 伺服器**」，再按下「**新增**」。

5 在「**新增 LiveUpdate 伺服器**」對話方塊中，鍵入識別所要使用的伺服器並與之通訊所需的資訊。

例如，對於 URL：

- 如果您使用的是 FTP 方法 (建議)，請輸入伺服器的 FTP 位址。 例如：
  ftp://myliveupdateserver.com。
- 如果您使用的是 HTTP 方法，請輸入伺服器的 URL。 例如：
  網域名稱：http://myliveupdateserver.com
  IPv4 位址：http://192.168.133.11/Export/Home/LUDepot
  IPv6 位址：http://[fd00:fe32::b008]:80/update

6 如果您的伺服器使用 FTP 或 HTTPS，請按下「**進階伺服器設定**」。

7 選取伺服器使用的 FTP 或 HTTPS 模式，然後按下「**確定**」。

8 按下「**確定**」。

請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。

請參閱第 178 頁的「將 Windows 用戶端更新架構為在用戶端電腦閒置時執行」。

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

架構用戶端從外部 LiveUpdate 伺服器下載內容

依據預設，Symantec Endpoint Protection Manager 會為 Windows 用戶端提供更新。為了協助降低 Windows 用戶端更新的網路負載，您還應讓用戶端從 LiveUpdate 伺服器取得更新。Linux 和 Mac 用戶端必須從 LiveUpdate 伺服器取得更新，或者您可以將 Apache Web 伺服器設為反向代理來從管理伺服器下載更新。

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

附註：您可能需要建立代理伺服器與 Symantec Endpoint Protection Manager 之間的通訊，以便它可以連線至賽門鐵克訂購授權服務。 代理伺服器可以在您的站台和外部 Symantec LiveUpdate 伺服器之間提供多一層的保護。

請參閱第 172 頁的「架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容」。

架構用戶端從外部 LiveUpdate 伺服器下載內容

1 在主控台中，開啟 LiveUpdate 政策，然後按下「**編輯**」。

2 在「**Windows 設定**」、「**Mac 設定**」或「**Linux 設定**」下方，按下「**伺服器設定**」。

3 按下「**使用預設 Symantec LiveUpdate 伺服器**」，或指定另一台 LiveUpdate 伺服器。如有需要，請指定代理架構。

4 按下「**確定**」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容

您可以將 Symantec Endpoint Protection Manager 架構為通過代理伺服器以連線至 Internet。Proxy 伺服器可以增加一層安全性，原因是只有 Proxy 伺服器直接連線到 Internet。

架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容

1 在主控台中，按下「**管理員**」，再按下「**伺服器**」。

2 在「**伺服器**」下，選取您要將 Proxy 伺服器連接至的管理伺服器。

3 在「**工作**」下方，按下「**編輯伺服器屬性**」。

4 在「**Proxy 伺服器**」標籤的「**HTTP Proxy 設定**」或「**FTP Proxy 設定**」下，為「**Proxy 使用**」選取「**使用自訂 Proxy 設定**」。

5 鍵入 Proxy 設定。

如需這些設定的詳細資訊，請按下「**說明**」。

6 按下「**確定**」。

請參閱第 172 頁的「指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器」。

指定用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的代理伺服器

您可以指定用戶端用來與內部 LiveUpdate 伺服器通訊的 Proxy 伺服器。 Proxy 設定不會影響群組更新提供者的任何設定。

附註：其他用戶端通訊的 Proxy 設定則需另行架構。

指定 Windows 電腦或 Linux 電腦用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的 Proxy 伺服器

1. 在主控台中，按下「**政策**」。
2. 在「**政策**」下方，按下「**LiveUpdate**」，然後按下「**LiveUpdate 設定**」標籤。
3. 在所需的政策上按下滑鼠右鍵，再選取「**編輯**」。
4. 在「**Windows 設定**」下或「**Linux 設定**」下，按下「**伺服器設定**」。
5. 在「**LiveUpdate Proxy 架構**」下方，按下「**架構 Proxy 選項**」。
6. 執行下列其中一個動作：
   - 對於 Windows 用戶端，在「**HTTP 或 HTTPS**」標籤上，選取所需的選項。還可以指定 FTP 的 Proxy 設定。
   - 對於 Linux 用戶端，在「**HTTP**」標籤上，選取所需的選項。

   如需這些選項的詳細資訊，請參閱線上說明。
7. 按下對話方塊中的「**確定**」。
8. 按下「**確定**」。

指定 Mac 電腦用戶端用來與 Symantec LiveUpdate 或內部 LiveUpdate 伺服器通訊的 Proxy 伺服器

1. 在主控台中，按下「**用戶端**」>「**政策**」。
2. 在「**與位置無關的政策與設定**」下方的「**設定**」下，按下「**外部通訊設定**」。
3. 在「**Proxy 伺服器 (Mac)**」標籤上，選取所需的選項。

   如需這些選項的詳細資訊，請參閱線上說明。
4. 按下「**確定**」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

針對用戶端電腦架構 LiveUpdate 下載排程

LiveUpdate 用戶端排程設定在「LiveUpdate 設定」政策中進行定義。 這些設定會套用至 LiveUpdate 階段作業，以從 Symantec LiveUpdate 伺服器或內部 LiveUpdate 伺服器取得最新的更新。

請參閱第 171 頁的「架構用戶端從外部 LiveUpdate 伺服器下載內容」。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

若要儲存頻寬，您可以讓您的用戶端只在符合下列任一條件時執行排定的 LiveUpdate 階段作業：

- 用戶端電腦上的病毒和間諜軟體定義檔已超過 2 天。

- 用戶端電腦與 Symantec Endpoint Protection Manager 中斷連線已超過 8 小時。

附註：若要確保任何不常與您的網路連線的用戶端電腦取得最新的更新，請讓這些電腦從 Symantec LiveUpdate 伺服器取得更新。 這些伺服器是公用的，因此用戶端不根據與您的網路連線來取得更新。

架構 LiveUpdate 下載至 Windows 用戶端電腦的排程

1. 按下「**政策**」，然後按下 **LiveUpdate**。
2. 在「**LiveUpdate 設定**」標籤上，在所需的政策上按下滑鼠右鍵，然後按下「**編輯**」。
3. 在「**Windows 設定**」下方，按下「**排程**」。
4. 確認已勾選「**啟用 LiveUpdate 排程**」。 此選項預設為啟用。
5. 指定頻率。

   如果選取「**每日**」，請同時設定要執行的時間。如果選取「**每週**」，請同時設定要在星期幾和哪個時間執行。
6. 如果選取「**連續**」之外的任何頻率，請指定「**重試時段**」。

   「**重試時段**」是當排程的 LiveUpdate 因故失敗時，用戶端電腦嘗試執行 LiveUpdate 的小時數或天數。
7. 請視需要設定任何其他選項。如果定義檔已過期，或是用戶端最近未連線至管理伺服器，賽門鐵克建議您保留執行 LiveUpdate 的預設值。
8. 按下「**確定**」。

請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。

架構 LiveUpdate 下載至 Mac 用戶端電腦的排程

1. 按下「**政策**」，然後按下 **LiveUpdate**。
2. 在「**LiveUpdate 設定政策**」標籤上，在所要的政策上按滑鼠右鍵，然後按下「**編輯**」。
3. 在「**Mac 設定**」下方，按下「**排程**」。
4. 指定頻率。

   如果選取「**每日**」，請同時設定要執行的時間。如果選取「**每週**」，請同時設定要在星期幾和哪個時間執行。
5. 完成後，請按下「**確定**」。

架構 LiveUpdate 下載至 Linux 用戶端電腦的排程

1. 在「**LiveUpdate 設定政策**」標籤上，在所要的政策上按滑鼠右鍵，然後按下「**編輯**」。
2. 在「**Linux 設定**」下方，按下「**排程**」。

3 勾選「**啟用 LiveUpdate 排程**」。此選項預設為啟用。

附註：您不應取消核取此方塊。如果您停用「**LiveUpdate 排程**」，Linux 用戶端不會取得最新更新。

4 指定頻率。

如果選取「**每日**」，請同時設定要執行的時間。如果選取「**每週**」，請同時設定要在星期幾和哪個時間執行。

5 如果選取「**連續**」之外的任何頻率，請指定「**重試時段**」。

「**重試時段**」是當排程的 LiveUpdate 失敗時，用戶端電腦嘗試執行 LiveUpdate 的小時數或天數。

您也可以隨機進行內容下載。

6 按下「**確定**」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

架構使用者對 LiveUpdate 的控制能力

您可能想要讓出差的使用者可以使用 Internet 連線，直接從 Symantec LiveUpdate 伺服器取得更新。您也可以讓使用者修改您為內容下載設定的 LiveUpdate 排程。

附註：如果非受管用戶端具有在建立安裝套件時向其指派的 LiveUpdate 設定政策，當使用者重新啟動電腦後，該政策設定一律會優先於使用者的變更。若要安裝非受管用戶端，並在電腦重新啟動後，保留使用者對 LiveUpdate 設定所做的變更，請從安裝檔案安裝用戶端。不要使用從 Symantec Endpoint Protection Manager 匯出的用戶端安裝套件。

架構使用者對 LiveUpdate 的控制能力

1 在主控台中，按下「**政策**」。

2 在「**政策**」下方，按下 **LiveUpdate**。

3 在「**LiveUpdate 設定**」標籤上，在所需的政策上按下滑鼠右鍵，然後按下「**編輯**」。

4 在「**Windows 設定**」下方，按下「**進階設定**」。

5 在「**使用者設定值**」窗格下，勾選「**允許使用者手動啟動 LiveUpdate**」。

6 您也可以勾選「**允許使用者修改 LiveUpdate 排程**」。

7 按下「**確定**」。

請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。

請參閱第 173 頁的「針對用戶端電腦架構 LiveUpdate 下載排程」。

減少用戶端更新要求的網路超載

當有過多用戶端同時從管理伺服器或「群組更新提供者」要求一組完整的病毒和間諜軟體定義檔時，您必須針對這種重大但不常見的情況管理網路。如果管理伺服器發生錯誤或磁碟空間不足，以致用戶端上的下載和更新定義檔失敗，就可能發生這種情況。如果管理伺服器不下載定義檔套件，然後用戶端要求此特定差量，也可能會發生此情況。不論是哪種情況，用戶端接著都必須從管理伺服器或「群組更新提供者」要求包含一組完整定義檔的套件。

為了協助防止網路超載，管理伺服器提供下列功能：

- 當管理伺服器在指定期間內收到對一組完整定義檔提出的指定數目要求時，會發出通知。您可以根據造成環境超載的原因，設定此通知的條件。若要架構通知，請新增**「網路負載: 病毒和間諜軟體完整定義檔的要求」**通知條件。
  請參閱第 577 頁的「設定管理員通知」。
- 在管理伺服器只能提供一組完整定義檔的情況下，讓用戶端能夠從 LiveUpdate 伺服器取得病毒和間諜軟體定義檔的差量。在 LiveUpdate 設定政策中，按下**「進階設定」>「從 LiveUpdate 伺服器下載較小的用戶端安裝套件」**。
- 攔截用戶端，使其無法從管理伺服器下載一組完整的病毒和間諜軟體定義檔。
  如果您收到網路超載的通知，可以攔截任何從管理伺服器進一步下載完整套件的動作。但是，您無法停止任何已在進行中的下載作業。此選項的架構方式是：按下**「管理」>「伺服器」>***server_name* **>「編輯伺服器屬性」>「完整定義檔下載」>「防止用戶端下載完整定義檔套件」**。

關於隨機化同時內容下載

Symantec Endpoint Protection Manager 支援從預設管理伺服器或「群組更新提供者」，隨機將內容同時下載至您的用戶端。這也支援從 LiveUpdate 伺服器隨機將內容下載至您的用戶端。隨機化可減少尖峰網路流量，並且預設為啟動。

您可以啟用或停用隨機化功能。已啟用預設設定。您也可以架構隨機化視窗。管理伺服器會使用隨機化視窗錯開內容下載的時間。一般而言，您應該不需要變更預設的隨機化設定。

然而，在某些狀況下，可能需要提高隨機化視窗值。例如，在執行管理伺服器的相同實體電腦上，您可能在多個虛擬機器上執行 Symantec Endpoint Protection 用戶端。較高的隨機化值可以改善伺服器的效能，但是會延遲虛擬機器的內容更新。

當您有多部實體用戶端電腦連線至執行管理伺服器的單一伺服器時，也可能需要增加隨機化視窗。一般而言，用戶端與伺服器的比例愈高，可能需要設定愈多的隨機化視窗。較高的隨機化值可減少伺服器的尖峰負載，但是會延遲用戶端電腦的內容更新。

有較少用戶端且需要快速的內容傳送時，可以將隨機化視窗設定為較低的值。較低的隨機化值會增加伺服器的尖峰負載，但是可加速用戶端的內容傳送。

若是從預設管理伺服器或「群組更新提供者」進行下載，您可以在選取的群組的**「通訊設定」**對話方塊中架構隨機化設定。 這些設定不是 LiveUpdate 設定政策的一部分。

如果是從 LiveUpdate 伺服器下載至用戶端，您可以將隨機化設定架構為 LiveUpdate 設定政策的一部分。

請參閱第 177 頁的「從預設管理伺服器或群組更新提供者隨機進行內容下載」。

請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

從預設管理伺服器或群組更新提供者隨機進行內容下載

多個用戶端電腦嘗試同時從您的預設管理伺服器或「群組更新提供者」下載內容時，預設管理伺服器或「群組更新提供者」可能會遭遇效能下降。您可以在用戶端電腦所屬群組的通訊設定中設定隨機化時段。每台用戶端電腦會嘗試在該時段內的隨機時間下載內容。

附註：通訊設定不會控制用戶端電腦從 LiveUpdate 伺服器下載內容的隨機化設定。您可以在 LiveUpdate 設定政策中變更這些電腦的隨機化設定。

請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。

從預設管理伺服器或群組更新提供者隨機進行內容下載

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下方，按下您所要的群組。
3. 在**「政策」**標籤的**「與位置無關的政策與設定」**下，按下**「設定」**下的**「通訊設定」**。
4. 在**「通訊設定」**對話方塊的**「下載隨機化」**下，勾選**「啟用隨機化」**。
5. 或者，可以變更隨機化時段持續時間。
6. 按下**「確定」**。

請參閱第 176 頁的「關於隨機化同時內容下載」。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

從 LiveUpdate 伺服器隨機進行內容下載

多個用戶端電腦嘗試從 LiveUpdate 伺服器下載內容時，您的網路可能會遇到流量擁塞。您可以在 Windows 或 Linux 用戶端上架構更新排程以包含隨機化時段。每台用戶端電腦會嘗試在該時段內的隨機時間下載內容。

附註：對於從預設管理伺服器或從「群組更新提供者」下載內容的用戶端電腦，LiveUpdate 設定政策中的排程設定不控制隨機化。您可以在這些電腦所屬群組的**「通訊設定」**對話方塊中變更這些電腦的隨機化設定。

請參閱第 177 頁的「從預設管理伺服器或群組更新提供者隨機進行內容下載」。

從 LiveUpdate 伺服器隨機進行內容下載

1. 按下**「政策」**。
2. 在**「政策」**下方，按下 **LiveUpdate**。
3. 在**「LiveUpdate 設定」**標籤上，在要編輯的政策上按滑鼠右鍵，然後按下**「編輯」**。
4. 在**「Windows 設定」**、**「Mac 設定」**或**「Linux 設定」**下方，按下**「排程」**。
5. 在**「下載隨機化選項」**下，勾選**「隨機設定開始時間為 + 或 - (小時)」**。

   附註：如果您選取**「每週」**更新，則此設定以天為單位。

6. 或者，可以變更隨機開始時間的持續時間。
7. 按下**「確定」**。

請參閱第 176 頁的「關於隨機化同時內容下載」。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

將 Windows 用戶端更新架構為在用戶端電腦閒置時執行

為緩和 Windows 用戶端電腦效能問題，您可以架構內容下載在用戶端電腦閒置時執行。此設定預設為開啟。會以使用者、CPU 和磁碟動作等數個條件，判斷電腦何時處於閒置狀態。

如果已啟用**「閒置偵測」**，則應進行特定更新時，下列狀況可能會延遲工作階段：

- 使用者並未處於閒置狀態。
- 電腦使用電池電力。
- CPU 處於忙碌狀態。
- 磁碟輸入/輸出處於忙碌狀態。
- 沒有網路連線。

一小時後，該攔截設定會變為只有 CPU 忙碌、磁碟輸入/輸出忙碌，或沒有網路連線等狀況會延遲更新。當排程的更新逾期兩個小時後，不論閒置狀態為何，只要有網路連線，就會執行排程的 LiveUpdate。

將 Windows 用戶端更新架構為在用戶端電腦閒置時執行

1 按下「**政策**」。

2 在「**政策**」下方，按下 **LiveUpdate**。

3 在「**LiveUpdate 設定**」標籤上，在要編輯的政策上按滑鼠右鍵，然後按下「**編輯**」。

4 在「**Windows 設定**」下，按下「**排程**」。

5 勾選「**延遲排程的 LiveUpdate，直到電腦變成閒置為止。逾期階段作業將無條件執行**」。

6 按下「**確定**」。

請參閱第 173 頁的「針對用戶端電腦架構 LiveUpdate 下載排程」。

請參閱第 179 頁的「將 Windows 用戶端更新架構為在定義檔太舊或電腦已中斷連線時執行」。

將 Windows 用戶端更新架構為在定義檔太舊或電腦已中斷連線時執行

您可以確保 Windows 用戶端在定義檔太舊或電腦於一段指定時間內中斷網路連線時進行更新。

附註：如果同時勾選兩個可用的選項，則用戶端電腦必須同時符合兩個條件。

架構 Windows 用戶端在定義檔太舊或電腦與管理程式中斷連線時進行更新

1 按下「**政策**」。

2 在「**政策**」下方，按下 **LiveUpdate**。

3 在「**LiveUpdate 設定**」標籤上，在要編輯的政策上按滑鼠右鍵，然後按下「**編輯**」。

4 在「**Windows 設定**」下方，按下「**排程**」。

5 勾選「**只有在病毒和間諜軟體定義檔的時間早於以下時間時才執行 LiveUpdate:**」，然後設定小時數或天數。

6 勾選「**僅於用戶端與 Symantec Endpoint Protection Manager 斷線超過以下時間時才執行 LiveUpdate:**」，然後設定分鐘數或小時數。

7 按下「**確定**」。

請參閱第 173 頁的「針對用戶端電腦架構 LiveUpdate 下載排程」。

請參閱第 178 頁的「將 Windows 用戶端更新架構為在用戶端電腦閒置時執行」。

將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容

將內容下載至用戶端的預設方法是使用管理伺服器。

請勿定義從管理伺服器到用戶端之更新的排程。用戶端根據通訊模式和活動訊號頻率從管理伺服器下載內容。

將用戶端架構為從 Symantec Endpoint Protection Manager 下載內容

1. 在主控台中，開啟 LiveUpdate 政策，然後按下「**編輯**」。
2. 在「**Windows 設定**」下方，按下「**伺服器設定**」。
3. 確保已核取「**使用預設管理伺服器**」。
4. 按下「**確定**」。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

在 Windows 用戶端上發布之前測試引擎更新

Symantec Endpoint Protection 包含多個執行其部分功能的引擎。這些引擎是二進位檔案 (.dll 或 .exe)，會隨安全性定義檔一起傳送。賽門鐵克會更新這些引擎的功能，以強化 Symantec Endpoint Protection 功能並回應新威脅。

雖然賽門鐵克每天更新病毒定義檔多次，但引擎內容按季更新。賽門鐵克使用 LiveUpdate 提供引擎更新。

自 14.0.1 MP1 版起，賽門鐵克會提供特殊的伺服器，可讓您在將引擎內容遞送到生產環境之前下載並測試內容。賽門鐵克會在早期採用者伺服器 (EAS) 上發布這些更新。引擎更新會在引擎可供在公用 LiveUpdate 伺服器上進行一般發布之前的幾週內發布。

您可使用 EAS 下載引擎更新，在實驗室環境中加以嘗試，並告知賽門鐵克您遇到的任何衝突。此程序可讓賽門鐵克在一般發布之前修正這些衝突。

您可以使用下列程序來測試引擎更新：

步驟 1：建立一組測試電腦來接收內容

步驟 2：將測試電腦架構為從早期採用者伺服器接收搶鮮版內容

步驟 3：將測試和非測試電腦架構為特定引擎版本

步驟 4：設定新引擎版本的通知 (選擇性)

步驟 5：發布引擎內容後，監控測試電腦

步驟 1：建立一組測試電腦來接收內容

最準確的引擎相容性測試是在實際執行工作的生產系統下進行的。透過使用下列準則選取一組用戶端電腦來接收 EAS 內容，以建立永久測試群組：

- 識別您環境內各種類型的重要系統。這些系統可能因硬體、軟體或功能而有所不同。例如，可在其他要測試的重要系統之間識別零售系統，例如金級桌面影像、銷售點系統和Web伺服器。
- 由於某些軟體衝突可能僅間歇性地出現，因此，請使用每種類型的多個系統。選擇已具備您通常使用且執行代表工作負載的已安裝軟體的生產系統。
- 架構用於接收較早版本內容的測試用戶端電腦，例如非測試的生產電腦。測試及非測試的兩個用戶端應安裝相同的 Symantec Endpoint Protection 功能並使用相同的政策。

如果您不希望將生產電腦用於透過 EAS 進行測試，您可以使用以實驗室為基礎的系統。在此情況下，您可能想要撰寫自動化，以在測試和模擬負載下運用系統功能。

對於用戶端電腦數量較少的客戶，您只需要一個 Symantec Endpoint Protection Manager 和一個 Windows 適用的 Symantec Endpoint Protection 用戶端。

步驟 2：將測試電腦架構為從早期採用者伺服器接收搶鮮版內容

針對測試群組，透過執行下列步驟，將 LiveUpdate 架構為從賽門鐵克早期採用者伺服器下載內容。

將站台架構為從賽門鐵克早期採用者 LiveUpdate 伺服器下載內容

1. 在主控台中，按下「**管理員**」>「**伺服器**」。
2. 在「**伺服器**」下，於「**本機站台**」上按下滑鼠右鍵，然後按下「**編輯站台屬性**」。
3. 在「**LiveUpdate 來源伺服器**」下，按下「**編輯來源伺服器**」。
4. 在「**LiveUpdate 伺服器**」對話方塊中，按下「**使用 Symantec LiveUpdate 伺服器取得搶鮮版內容**」，然後按下「**確定**」>「**確定**」。

將受管用戶端架構為使用搶鮮版賽門鐵克早期採用者 LiveUpdate 伺服器

1. 在主控台中，開啟新的 LiveUpdate 設定政策，然後按下「**政策**」> **LiveUpdate**。
2. 在「**Windows 設定**」下，按下「**伺服器設定**」>「**使用 LiveUpdate 伺服器**」>「**使用 Symantec LiveUpdate 伺服器取得搶鮮版內容**」。
3. 按下「**確定**」，然後將政策指派給測試群組。

只要您的 LiveUpdate 設定政策從 EAS 取得內容，測試用戶端就會繼續接收搶鮮版內容。

附註：對於非測試群組，始終對您通常使用的LiveUpdate伺服器架構LiveUpdate設定政策。在引擎可供一般發布之後，所有用戶端電腦會接收 LiveUpdate 內容，視您將用戶端電腦架構為接收此內容的方式而定。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

請參閱第 171 頁的「架構用戶端從外部 LiveUpdate 伺服器下載內容」。

步驟 3：將測試和非測試電腦架構為特定引擎版本

架構多個 LiveUpdate 內容政策，以便：

- 測試群組會收到最新版本的安全性定義檔及引擎。此群組會下載所有未來的內容修訂以及其中的搶鮮版引擎。
- 非測試群組會收到現有的安全引擎版本。
  自 14.0.1 MP1 起，您也可以鎖定引擎版本。藉由此選項，用戶端會繼續收到與特定引擎相關聯的最新安全性定義檔，而不是最新引擎版本。
  請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。
  對於通常具有搶鮮版內容的測試群組功能感到滿意之後，您可以手動選擇這些非測試群組的下一個引擎版本。

步驟 4：設定新引擎版本的通知 (選擇性)

若要取得 LiveUpdate 下載至 Symantec Endpoint Protection Manager 的計劃引擎版本的通知，請執行下列其中一項工作：

- 新增何時已將新內容下載至 Symantec Endpoint Protection Manager 的通知。自 14.0.1 MP1 起，新內容的通知包括新引擎版本以及安全性定義檔。只有在依引擎版本指定內容修訂的一或多個 LiveUpdate 內容政策因可用引擎更新而鎖定時，您才會收到通知。
  若要檢視通知，請在**「首頁」**頁面的**「安全狀態」**窗格中，按下**「檢視通知」**。

  附註：EAS 與定期 LiveUpdate 伺服器的更新頻率相同。如果您認為收到這些通知的頻率過高，請架構為不顯示通知。

  請參閱第 577 頁的「設定管理員通知」。
- 若為較舊版本，請登入客戶訂購授權入口網站。
  PCS 客戶如何註冊警示和通知

步驟 5：發布引擎內容後，監控測試電腦

當賽門鐵克將引擎更新發布到 EAS 之後，開始監控架構為接收此內容的電腦。監控下列項目：

- 確認測試電腦執行搶鮮版引擎更新。
  驗證用戶端電腦上所執行的引擎和定義檔
- 開機時間、伺服器上的可用資源，及其他使用 Microsoft System Center Operations Manager 等工具的重要基礎架構。
- 在用戶端電腦上執行的應用程式，用於確保其如預期般繼續執行。
- Symantec Endpoint Protection 用戶端狀態，用於確保其仍會連線至管理伺服器且受到保護。
  請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

此外，在修改政策後執行用戶端或執行掃描，以確保電腦如預期般運作。

如果您發現任何非預期行為，或懷疑引擎更新存在軟體衝突，請聯絡支援以取得協助。通常，如果賽門鐵克在開始進行分階段遞送之前確認存在軟體衝突，賽門鐵克會重新排程發布，並與您一起修正問題。然後，賽門鐵克會將更新的引擎重新發布至 EAS。

還原為舊版 Symantec Endpoint Protection 安全更新

依據預設，從 LiveUpdate 伺服器下載至管理伺服器的最新版本內容會自動下載至 Windows 用戶端。LiveUpdate 內容政策會指定允許用戶端檢查和安裝的內容類型。

不過，在下列情況下，您可能需要下載舊版內容：

- 最新的定義檔集或引擎導致用戶端電腦上發生軟體衝突。
- 您需要時間在內容發布至生產之前測試控制群組上的新引擎。

附註：請謹慎使用此功能。取消核取內容類型意味著用戶端上的此功能不會保持最新。這可能會將您的用戶端置於較大的風險中。

還原為舊版 Symantec Endpoint Protection 安全更新

1. 在主控台中，按下**「政策」> LiveUpdate**，然後開啟 LiveUpdate 內容政策。
2. 在**「Windows 設定」**下，按下**「安全性定義檔」**。

   無法回復 Mac 用戶端或 Linux 用戶端的內容。
3. 若要將內容回復為特定版本，請按下下列其中一個選項：
   - **「選取修訂版本」>「編輯」**，然後選取修訂編號。
     此選項會將用戶端鎖定至一組特定的安全性定義檔。用戶端不會收到任何新的安全性定義檔。
   - **「選取引擎版本」>「編輯」**，然後選取引擎版本。
     自 14.0.1 MP1 起，此選項會將用戶端鎖定到一個特定引擎，但仍繼續派送與該引擎相關聯的最新安全性定義檔。如果您知道目前在環境中運作的引擎，而且您需要在發布前測試其他群組中的較新引擎，請選取引擎版本。或者，按下**「使用最新的可用群組更新提供者」**，讓用戶端持續收到該內容類型的最新引擎版本和定義檔。14.0.1 和更早版本會忽略此設定。
4. 按下**「確定」**。

   無須重新啟動用戶端電腦，即可更新內容。
5. 在您解決任何疑難排解問題之後，請在**「Windows 設定」**下，針對每種內容類型按下**「安全性定義檔」>「使用最新的可用群組更新提供者」**。

請參閱第 180 頁的「在 Windows 用戶端上發布之前測試引擎更新」。

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

使用群組更新提供者將內容散佈至用戶端

群組更新提供者 (GUP) 係為一部可直接將內容更新派送給其他用戶端的用戶端電腦。

GUP 的優勢包括：

- 可透過將處理負載轉移到 GUP，以保留頻寬和管理伺服器資源。
- 可有效地將更新傳送至網路連線受限或緩慢的用戶端。
- 比內部 LiveUpdate 伺服器容易設定。

表 9-7 使用群組更新提供者的工作

步驟	敘述
步驟 1：瞭解您可以架構的各種群組更新提供者類型之間的區別	您可以設定單一、多個或跨子網路群組更新提供者。您設定的群組更新提供者類型取決於您的網路及該網路上的用戶端。各「群組更新提供者」類型之間並不會互斥。您可以對每個政策架構一或多種類型的「群組更新提供者」。 請參閱第 185 頁的「關於群組更新提供者的類型」。 請參閱第 189 頁的「關於在您的網路中架構一種以上類型群組更新提供者的影響」。
步驟 2：確認用戶端的通訊	架構群組更新提供者前，請確認用戶端電腦可接收伺服器的內容更新。解決任何用戶端伺服器通訊問題。 您可以在**「監視器」**頁面的**「日誌」**標籤上檢視「系統日誌」中的用戶端伺服器活動。 請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。
步驟 3：在一個或多個「LiveUpdate 設定」政策中架構群組更新提供者	在「LiveUpdate 設定」政策中架構群組更新提供者。 請參閱第 187 頁的「將用戶端架構為從群組更新提供者下載內容」。
步驟 4：將「LiveUpdate 設定」政策指派給群組	您可以指派「LiveUpdate 設定」政策給使用「群組更新提供者」的群組。您也必須指派政策給內含「群組更新提供者」的群組。 針對單一「群組更新提供者」，您需要為每個網站的每個群組指派一個「LiveUpdate 設定」政策。 針對多個「群組更新提供者」和明確的「群組更新提供者」清單，您需要跨子網路指派一個「LiveUpdate 設定」政策給多個群組。 請參閱第 275 頁的「指派政策給群組或位置」。

步驟	敘述
步驟 5：確認用戶端已指定為群組更新提供者	若要檢視被指定為群組更新提供者的用戶端電腦，請執行下列其中一項工作： ■ 按下「**用戶端**」>「**用戶端**」標籤 > 在用戶端上按下滑鼠右鍵，然後按下「**編輯屬性**」。「群組更新提供者」欄位為 **True** 或 **False**。 ■ 請參閱第 189 頁的「搜尋作為群組更新提供者的用戶端」。

關於群組更新提供者的類型

您可以在「LiveUpdate 設定」政策中架構多種類型的群組更新提供者。您使用的群組更新提供者的類型取決於網路的設定方式。您可以對每個政策架構一或多種類型的群組更新提供者；這些類型並不互斥。

表 9-8 何時使用特定群組更新提供者類型

「群組更新提供者」類型	使用時機
單一	單一群組更新提供者係指可為一個或多個用戶端群組提供內容的專屬用戶端電腦。架構單一群組更新提供者會將單一用戶端變成群組更新提供者。單一群組更新提供者可以是任一群組中的某台用戶端電腦。 當您要對所有用戶端電腦使用相同的「群組更新提供者」時，使用單一「群組更新提供者」。 您可以使用單一「LiveUpdate 設定」政策，為單一群組更新提供者指定靜態 IP 位址或主機名稱。但是，如果用作單一群組更新提供者的用戶端變更位置，您必須變更政策中的 IP 位址。 如果您要在不同的群組中使用不同的單一群組更新提供者，則必須為每個群組建立個別的「LiveUpdate 設定」政策。

「群組更新提供者」類型	使用時機
多個	多個群組更新提供者會使用一組規則或準則選出為本身所擁有子網路中用戶端群組提供服務的提供者。所有用戶端電腦位於相同的子網路中。 您可以指定用戶端電腦作為群組更新提供者所必須符合的準則。如果用戶端電腦符合準則，管理伺服器會將此用戶端新增至全域群組更新提供者清單。然後，管理伺服器會對網路中的所有用戶端提供全域清單。用戶端可查看清單並選擇位於本身所擁有子網路內的群組更新提供者。 架構多個群組更新提供者會將多個用戶端變成群組更新提供者。 針對下列任一情況使用多個群組更新提供者： ■ 您擁有多個群組，而且想要在每個群組中使用不同的群組更新提供者。 您可以使用一項政策指定多個「群組更新提供者」的選擇規則。 如果用戶端變更位置，您不需要更新「LiveUpdate 設定」政策。 Symantec Endpoint Protection Manager 會結合各站台與網域的多個「群組更新提供者」。 您網路中各群組的所有用戶端便可使用此份清單。 ■ 多個「群組更新提供者」亦具備容錯移轉機制的功能。 使用多個「群組更新提供者」可確保在每個子網路中至少都有一個「群組更新提供者」可以使用。
明確清單	如果您希望用戶端能夠連線到位於用戶端本身所屬子網路以外的其他子網路上的「群組更新提供者」，請使用明確的「群組更新提供者」清單。 變更位置的用戶端可以漫遊到清單上最近的「群組更新提供者」。 明確的群組更新提供者清單不會將用戶端變成群組更新提供者。 當您架構明確的清單時，可以指定 IP 位址在特定子網路的用戶端應使用特定群組更新提供者。用戶端可能有多個 IP 位址，管理伺服器在比對要使用的群組更新提供者時，會將用戶端的所有 IP 位址列入考量。因此，政策比對的 IP 位址不一定繫結至用戶端用來與群組更新提供者通訊的介面。 例如，假設用戶端有 IP 位址 A，用來與管理伺服器和群組更新提供者通訊。這一個用戶端也有 IP 位址 B，這個位址符合您在「LiveUpdate 設定」政策中針對此用戶端架構的「明確群組更新提供者」。這個用戶端可以選擇使用根據位址 B 的「群組更新提供者」，儘管該位址並不是它用來與「群組更新提供者」通訊的位址。

在「LiveUpdate 設定」政策中架構單一或多個「群組更新提供者」時，會執行下列功能：

- 指定具有此政策的哪些用戶端作為「群組更新提供者」。
- 指定具有此政策的用戶端應使用哪些群組更新提供者來進行內容更新。

架構明確的群組更新提供者清單時，就只會執行一項功能：

- 指定具有此政策的用戶端應使用哪些群組更新提供者來進行內容更新。
  雖然它不會將用戶端變成「群組更新提供者」，不過您仍可以架構和套用僅包含一個明確提供者清單的政策。 不過，您接著必須在 Symantec Endpoint Protection Manager 中的其他政策架構單一「群組更新提供者」或多個「群組更新提供者」。 或者，您可以在其他政策中同時架構這兩種類型。

如果用戶端無法透過任何群組更新提供者取得其更新，則可能會選擇性地嘗試從 Symantec Endpoint Protection Manager 更新。

請參閱第 189 頁的「關於在您的網路中架構一種以上類型群組更新提供者的影響」。

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

請參閱第 187 頁的「將用戶端架構為從群組更新提供者下載內容」。

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

將用戶端架構為從群組更新提供者下載內容

您可以使用「LiveUpdate 設定」政策，使用戶端只從群組更新提供者取得更新，永遠不從管理伺服器取得更新。您可以設定單一、多個或跨子網路群組更新提供者。您設定的群組更新提供者類型取決於您的網路及該網路上的用戶端。

請參閱第 185 頁的「關於群組更新提供者的類型」。

將用戶端架構為從群組更新提供者下載內容

1. 在主控台中，按下**「政策」**。
2. 在**「政策」**下方，按下 **LiveUpdate**。
3. 在**「LiveUpdate 設定」**標籤上，在所要的政策上按滑鼠右鍵，然後按下**「編輯」**。
4. 在**「LiveUpdate 設定政策」**視窗中，按下**「伺服器設定」**。
5. 在**「內部或外部 LiveUpdate 伺服器」**下，勾選**「使用預設管理伺服器」**。
6. 在**「群組更新提供者」**下，勾選**「使用群組更新提供者」**。
7. 按下**「群組更新提供者」**。
8. 執行下列其中一項工作：
   - 按照架構單一「群組更新提供者」中的步驟作業。
   - 按照架構多個「群組更新提供者」中的步驟作業。
   - 按照架構「群組更新提供者」明確清單中的步驟作業。
9. 在**「群組更新提供者設定」**下，架構控制群組更新提供者電腦下載與儲存內容方式的選項。

   按下**「說明」**可獲得內容下載相關資訊。
10. 按下**「確定」**。

架構單一「群組更新提供者」

1 在**「群組更新提供者」**對話方塊中，勾選**「單一群組更新提供者 IP 位址或主機名稱」**，然後輸入用作單一群組更新提供者之用戶端電腦的 IP 位址或主機名稱。

若需 IP 位址或主機名稱的相關資訊，請按下**「說明」**。

2 返回此程序架構「群組更新提供者」。

架構多個「群組更新提供者」

1 在**「群組更新提供者」**對話方塊中，勾選**「多個群組更新提供者」**，然後按下**「架構群組更新提供者清單」**。

2 在**「群組更新提供者清單」**對話方塊中，選取樹狀結構節點**「群組更新提供者」**，然後按下**「新增」**以新增規則集。

3 在**「指定群組更新提供者的規則準則」**對話方塊的**「選取」**下拉式清單中，選取下列選項目之一：

- **電腦 IP 位址或主機名稱**
- **登錄機碼**
- **作業系統**

4 若選取了**「電腦 IP 位址或主機名稱」**或**「登錄機碼」**，請按下**「新增」**。

5 輸入或選取 IP 位址或主機名稱、Windows 登錄機碼或作業系統資訊。

若需架構規則的相關資訊，請按下**「說明」**。

6 按下**「確定」**，直到返回**「群組更新提供者清單」**對話方塊，您可以在此對話方塊中選擇新增更多規則集。

7 按下**「確定」**。

8 返回此程序架構「群組更新提供者」。

架構「群組更新提供者」明確清單

1 在**「群組更新提供者」**對話方塊中，勾選**「漫遊用戶端的明確群組更新提供者」**，然後按下**「架構明確群組更新提供者清單」**。

2 按下**「新增」**。

3 在**「新增明確群組更新提供者」**對話方塊中，輸入要這些群組更新提供者對應至的用戶端子網路。

按下**「指定用戶端子網路遮罩」**以一次新增多個用戶端子網路。

4 根據 IP 位址、主機名稱或群組更新提供者的網路位址，選取要設定的對應**類型**。

針對選取的對應類型輸入必要的設定。

5 按下**「確定」**。

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

搜尋作為群組更新提供者的用戶端

您可以先確認用戶端是否可作為「群組更新提供者」。在**「用戶端」**標籤進行搜尋即可檢視「群組更新提供者」清單。

附註：您也可查看用戶端屬性。屬性中包括一項說明用戶端是否可作為「群組更新提供者」的欄位。

搜尋作為「群組更新提供者」的用戶端

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**標籤上的**「檢視」**方塊中，選取**「用戶端狀態」**。
3. 在**「工作」**窗格中，按下**「搜尋用戶端」**。
4. 在**「尋找」**下拉式清單中，選取**「電腦」**。
5. 在**「在群組中」**方塊中指定群組名稱。
6. 在**「搜尋條件」**下方，按下**「搜尋欄位」**欄並選取**「群組更新提供者」**。
7. 在**「搜尋條件」**下方，按下**「比較運算子」**欄並選取**「=」**。
8. 在**「搜尋條件」**下方，按下**「值」**欄並選取 **True**。

   若需搜尋條件的相關資訊，請按下**「說明」**。
9. 按下**「搜尋」**。

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

關於在您的網路中架構一種以上類型群組更新提供者的影響

如果您在政策中架構一或多個「群組更新提供者」，則 Symantec Endpoint Protection Manager 會撰寫已經登入的所有提供者的全域清單。 此檔案預設為：

64 位元作業系統：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml`

32 位元作業系統：`C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml`。

Symantec Endpoint Protection Manager 提供此全域清單給任何要求此清單的用戶端，因此用戶端可以決定自身應該使用的「群組更新提供者」。 由於存在此程序，因此如果單一提供者滿足明確對應準則，政策僅架構了多個或明確「群組更新提供者」的用戶端也可以使用單一「群

組更新提供者」。 此現象可能發生，因為單一提供者是用戶端從其 Symantec Endpoint Protection Manager 取得的全域提供者清單的一部分。

因此，在 Symantec Endpoint Protection Manager 上任何政策中架構的所有「群組更新提供者」均有可能為用戶端使用。如果您將僅包含明確的「群組更新提供者」清單的政策套用到群組中的用戶端，則群組中的所有用戶端均會嘗試使用 Symantec Endpoint Protection Manager 全域「群組更新提供者」清單中滿足明確對應準則的「群組更新提供者」。

附註：Symantec Endpoint Protection 用戶端可能有多個 IP 位址。 當 Symantec Endpoint Protection 符合某「群組更新提供者」時，會考量所有 IP 位址。 因此，政策符合的 IP 位址不是永遠繫結至用戶端用於與 Symantec Endpoint Protection Manager 和「群組更新提供者」通訊的介面。

如果所有類型的「群組更新提供者」均在 Symantec Endpoint Protection Manager 上的政策中架構，則用戶端會嘗試連接到全域清單中的「群組更新提供者」，順序如下：

- **「多個群組更新提供者」**清單中依序列出的提供者
- **「明確的群組更新提供者」**清單中依序列出的提供者
- 架構為**「單一群組更新提供者」**的提供者

您可以架構以下類型的明確對應準則：

- IP 位址：子網路 A 中的用戶端應該使用 IP 位址為 ***x.x.x.x*** 的「群組更新提供者」。
- 主機名稱：子網路 A 中的用戶端應該使用主機名稱為 ***xxxx*** 的「群組更新提供者」。
- 子網路網路位址：子網路 A 中的用戶端應該使用位於***子網路 B*** 中的任何「群組更新提供者」。

可將多個對應準則用於單一政策中明確的「群組更新提供者」清單。 賽門鐵克建議您小心架構多個對應準則，避免發生意外結果。例如，如果您對明確對應架構不當，在無法取得更新時就可能中斷用戶端。

可以考量在單一政策中架構的以下多個明確對應準則，作為方案：

- 如果用戶端在子網路 10.1.2.0 中，請使用 IP 位址為 10.2.2.24 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用 IP 位址為 10.2.2.25 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用主機名稱為 **SomeMachine** 的「群組更新提供者」
- 如果用戶端在子網路 10.1.2.0 中，請使用子網路 10.5.12.0 上的任何「群組更新提供者」
- 如果用戶端在子網路 10.6.1.0 中，請使用子網路 10.10.10.0 上的任何「群組更新提供者」

有了這個明確的「群組更新提供者」政策，如果用戶端在子網路 10.1.2.0 中，前四個規則適用；第五個規則不適用。 如果未指定任何對應給用戶端所在的子網路，例如 10.15.1.0，則沒有規則適用於該用戶端。 用戶端的政策指出使用一個明確的「群組更新提供者」清單，但是根

據這些規則，沒有用戶端可以使用的對應。 如果您也禁止了該用戶端從 Symantec Endpoint Protection Manager 和 Symantec LiveUpdate 伺服器下載更新，則該用戶端沒有可用的更新方法。

請參閱第 185 頁的「關於群組更新提供者的類型」。

請參閱第 187 頁的「將用戶端架構為從群組更新提供者下載內容」。

使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容

賽門鐵克建議用戶端電腦使用 LiveUpdate 來更新 Symantec Endpoint Protection 用戶端上的內容。但是，如果您不想使用 LiveUpdate 或 LiveUpdate 無法使用，則可以使用智慧型更新小幫手 (Intelligent Updater) 檔案更新用戶端。Windows 適用的智慧型更新小幫手 (Intelligent Updater) .exe 檔案僅為更新用戶端設計。智慧型更新程式檔案並不包含 Symantec Endpoint Protection Manager 更新其受管用戶端所需的資訊。

Windows 適用的智慧型更新小幫手 (Intelligent Updater) 檔案是包含病毒和間諜軟體定義檔的自動執行檔案。其他智慧型更新小幫手 (Intelligent Updater) 檔案可供 SONAR 定義檔與入侵預防特徵使用。針對 Mac 和 Linux，您可以下載病毒和間諜軟體定義檔。

下載檔案後，您可以採用偏好的派送方法，將更新派送到用戶端。

附註：智慧型更新小幫手 (Intelligent Updater) 不提供任何其他類型內容的更新。 例如，智慧型更新小幫手(Intelligent Updater)不支援延伸檔案屬性和特徵、自動防護入口網站清單、Power Eraser 定義檔或縮減大小定義檔。

下載智慧型更新小幫手 (Intelligent Updater) 檔案

1. 使用網頁瀏覽器，前往下列頁面：

   https://www.symantec.com/security_response/definitions.jsp

2. 從下拉式清單，選取下列其中一個可用的 Symantec Endpoint Protection 選項：

   - Symantec Endpoint Protection 12.1 (Windows 和 Linux)
   - Symantec Endpoint Protection 12.1.2 (Windows 和 Linux)
   - Symantec Endpoint Protection 12.1.3 (或更新版本) (Windows 和 Linux)
   - Symantec Endpoint Protection 14 (Windows 和 Linux)
   - Symantec Endpoint Protection for Macintosh 12.x

- Symantec Endpoint Protection for Macintosh 14.x

頁面會重新整理，以顯示可供該版本使用的內容。

3 在「**檔案型防護·(傳統防毒)**」、「**網路型防護·(IPS)**」·(僅限 Windows) 或「**行為型防護**」(僅限 Windows) 下方，於「**下載**」旁按下「**定義檔**」。

4 按下您要更新的用戶端版本的適當檔案名稱。

附註：針對 Linux 病毒定義檔，按下「**Unix 平台**」標籤。

5 當系統提示您提供儲存檔案的位置時，請在硬碟上選取一個資料夾。

6 使用偏好的派送方法將檔案派送至用戶端電腦。

如果您需要其他檔案，可以重複此程序。

在用戶端電腦上安裝病毒定義檔和安全更新檔

1 請在用戶端電腦上尋找已派送至用戶端的智慧型更新小幫手 (Intelligent Updater) 檔案。

2 執行下列其中一個動作：

- 若為 Windows：連按兩下 .exe 檔案，然後按照畫面上的指示操作。
- 若為 Mac：連按兩下 .zip 檔案，連按兩下 .pkg 檔案，然後按照畫面上的指示操作。
- 若為 Linux：驗證檔案具有可執行權限，驗證已安裝 uudecode 和 uncompress，然後使用進階使用者權限執行 .sh 檔案。請參閱下列各項以取得詳細資訊：
  如何使用智慧型更新小幫手 (Intelligent Updater) 定義檔更新 Linux 系統電腦

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

使用第三方派送工具更新用戶端電腦

某些大型企業依賴第三方派送工具 (例如 IBM Tivoli 或 Microsoft SMS) 將內容更新派送到用戶端電腦。Symantec Endpoint Protection 支援使用第三方派送工具，更新執行 Windows 作業系統的受管用戶端和非受管用戶端。Mac 和 Linux 用戶端僅能從內部或外部 LiveUpdate 伺服器收到內容更新。

在您準備使用第三方派送工具之前，必須安裝 Symantec Endpoint Protection Manager 以及要更新的用戶端電腦。

表 9-9 準備使用第三方派送工具進行更新前要執行的工作

工作	敘述
將 Symantec Endpoint Protection Manager 架構為接收內容更新。	您可以將管理伺服器架構為自動或手動接收內容更新。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。
將群組的 LiveUpdate 設定政策架構為允許派送第三方內容更新。	如果要使用第三方派送工具更新受管用戶端，則您必須將群組的 LiveUpdate 設定政策架構為允許執行該作業。 請參閱第 193 頁的「將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端」。
為非受管用戶端進行準備，以透過第三方派送工具接收更新。	如果要使用第三方派送工具更新非受管用戶端，必須先在每個非受管用戶端上建立登錄機碼。 請參閱第 194 頁的「準備非受管用戶端以從第三方派送工具接收更新」。
尋找、複製與派送內容。	每個 Symantec Endpoint Protection Manager 用戶端群組都有 index2.dax 檔案，該檔案位於執行 Symantec Endpoint Protection Manager 的電腦上。 依據預設，這些檔案位於 *SEPM_Install*\data\outbox\agent 資料夾下的子資料夾中。若要更新用戶端，您需要使用 index2.dax 檔案。 *SEPM_Install* 的預設位置為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。 請參閱第 195 頁的「使用第三方派送工具派送內容」。

將 LiveUpdate 設定政策架構為允許將第三方內容派送至受管用戶端

如果要使用第三方派送工具更新受管用戶端，則您必須將用戶端群組的 LiveUpdate 設定政策架構為允許執行該作業。 您可以選擇是否要停用讓用戶端使用者手動執行 LiveUpdate 的功能。

完成此程序後，群組的用戶端電腦的以下位置會顯示資料夾：

- Vista 及更新版本作業系統
  C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Vista 之前的作業系統 (針對舊版 12.1.x 用戶端)
  C:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

使用 LiveUpdate 政策啟用派送第三方內容給受管用戶端的功能

1. 在主控台中，按下「**政策**」。
2. 在「**政策**」下方，按下 **LiveUpdate**。
3. 在「**LiveUpdate 設定**」標籤的「**工作**」下方，按下「**新增 LiveUpdate 設定政策**」。
4. 在「**LiveUpdate 政策**」視窗的「**政策名稱**」和「**敘述**」文字方塊中，輸入名稱和敘述。
5. 在「**Windows 設定**」下方，按下「**伺服器設定**」。
6. 在「**第三方管理**」下，勾選「**啟用第三方內容管理**」。
7. 取消勾選其他所有 LiveUpdate 來源選項。
8. 按下「**確定**」。
9. 在「**指派政策**」對話方塊中，按下「**是**」。

   您也可以取消此程序，稍後再指派政策。
10. 在「**指派 LiveUpdate 政策**」對話方塊中，選取一個或多個要指派此政策的群組，然後按下「**指派**」。

請參閱第 168 頁的「將用戶端架構為從內部 LiveUpdate 伺服器下載內容」。

準備非受管用戶端以從第三方派送工具接收更新

如果您從安裝檔案安裝非受管用戶端，則無法立即使用第三方派送工具，向其派送 LiveUpdate 內容或政策更新。作為安全措施，根據預設，這些用戶端電腦既不信任也不處理第三方派送工具傳送給其的內容。

若要成功使用第三方派送工具傳送更新，您必須先在每個非受管用戶端上建立 Windows 登錄機碼。此機碼可讓您使用非受管用戶端上的收件匣資料夾，以便使用第三方派送工具來派送 LiveUpdate 內容和政策更新。

收件匣資料夾顯示在非受管用戶端的以下位置：

- Vista 及更新版本作業系統
  C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Vista 之前的作業系統 (針對舊版 12.1.x 用戶端)
  C:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

登錄機碼一經建立，您便可以使用第三方派送工具，複製內容或政策更新到此資料夾。然後，Symantec Endpoint Protection 用戶端軟體便會信任並處理更新。

準備非受管用戶端以從第三方派送工具接收更新

1. 請在每台用戶端電腦上，使用 regedit.exe 或其他 Windows 登錄編輯工具新增下列 Windows 登錄機碼之一：

- 在 64 位元電腦上的 12.1.5 及更新版本用戶端上，新增 **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState**
- 在 32 位元電腦上的 12.1.5 及更新版本用戶端和其他所有 12.1 用戶端上，新增 **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState**

2 將登錄機碼的值類型設定為 DWORD (32 位元) 或 QWORD (64 位元)，並將值設定為十六進位數字 80，如下所示：

```
0x00000080 (128)
```

3 儲存登錄機碼，然後結束登錄編輯工具。

請參閱第 192 頁的「使用第三方派送工具更新用戶端電腦」。

請參閱第 195 頁的「使用第三方派送工具派送內容」。

使用第三方派送工具派送內容

若要使用第三方派送工具將內容派送到用戶端電腦，您需要使用 index2.dax 檔案。 index2 檔案中與 LiveUpdate 相關的內容，包含一組稱為內容 Moniker 的 GUID 及其關聯的序號。 每個內容 Moniker 對應一個特定的內容類型。 index2 檔案中的每個序號都對應於特定內容類型的修訂。 視已安裝的防護功能而定，您必須判斷需要哪些內容類型。

請參閱第 163 頁的「關於 LiveUpdate 下載的內容類型」。

附註：內容 Moniker 通常隨每個主要版本而異。 有時，也可能變更次要版本的內容 Moniker。賽門鐵克通常不會變更版本更新或維護修補程式的 Moniker。

您可以開啟 ContentInfo.txt 檔案來查看 Moniker 與其內容類型的相同映射內容。 依據預設，ContentInfo.txt 檔案位於 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\。

例如，您可能會看見以下項目：

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions
Win32 12.1 RU6 - MicroDefsB.CurDefs - SymAllLanguages
```

每個 Symantec Endpoint Protection Manager 用戶端群組有其自己的 index2 檔案。 每個用戶端群組的 index2 檔案都可在該群組的資料夾中找到。 依據預設，用戶端群組的資料夾位於 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\。用戶端群組的資料夾名稱與群組政策序號相對應。您可以在**「群組屬性」**對話方塊中或**「用戶端」**頁面的**「詳細資料」**標籤上找到序號。每個群組政策序號的前四個十六進位值與該群組資料夾中的前四個十六進位值相符合。

受管用戶端使用的 index2.dax 檔案已加密。 若要檢視該檔案的內容，請開啟同一資料夾中的可用 index2.xml 檔案。 index2.xml 檔案提供了內容 Moniker 及其序 (版本) 號清單。 例如，您可能會看見以下項目：

```
<File Checksum="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

群組的 LiveUpdate 內容政策會指定特定版本的內容或最新內容。 index2 檔案中的序號必須與對應於群組的 LiveUpdate 內容政策中的內容規範的序號相符合。 例如，如果所有內容類型的政策均架構為**「使用最新的可用群組更新提供者」**，則每種類型的序號即為最新的可用內容。 在此範例中，派送僅在 index2 檔案調出對應於最新內容修訂的序號 (修訂號) 時才執行。 如果序號對應到任何其他改版編號，則此發布無效。

附註：您必須使用 Copy 指令將檔案放入用戶端的 \inbox 資料夾。使用 Move 指令不會觸發更新處理，而且更新會失敗。如果將內容壓縮至單一封存檔以供派送，不應該將它直接解壓縮至 \inbox 資料夾。

使用第三方派送工具將內容派送至用戶端

1. 在執行 Symantec Endpoint Protection Manager 的電腦上，建立工作資料夾 (如 \Work_Dir)。
2. 執行下列其中一項動作：
   - 對於受管用戶端，請在主控台的**「用戶端」**標籤上，於要更新的群組上按下右鍵，然後按下**「屬性」**。
   - 對於非受管用戶端，請在主控台的**「用戶端」**標籤上，右鍵按下**「我的公司」**，然後按下**「屬性」**。
3. 記下**「政策序號」**的前四位十六進位值，例如 7B86。
4. 瀏覽到以下資料夾：

   SEPM_Install\data\outbox\agent

   其中 *SEPM_Install* 表示 Symantec Endpoint Protection Manager 的安裝資料夾。預設安裝資料夾為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。
5. 找到包含與**「政策序號」**相符合的前四位十六進位值的資料夾。
6. 開啟該資料夾，然後將 `index2.dax` 檔案複製到您的工作資料夾。
7. 瀏覽到以下資料夾：

   SEPM_Install\Inetpub\content

   其中 *SEPM_Install* 表示 Symantec Endpoint Protection Manager 的安裝資料夾。預設安裝資料夾為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

8 開啟並讀取 `ContentInfo.txt`，搜尋每個 *target moniker* 資料夾包含的內容。

每個目錄的內容會採用下列格式：*target moniker**sequence number*\full.zip|full。

9 將每個 *target moniker* 資料夾的內容複製到您的工作資料夾 (如 \Work_Dir)。

10 將每一個 *target moniker* 中的所有檔案和資料夾刪除，只在您的工作資料夾中保留下列資料夾結構和檔案：

\\Work_Dir*target moniker**latest sequence number*\full.zip

現在，您的工作資料夾包含要派送至用戶端的資料夾結構和檔案。

11 使用第三方派送工具將工作資料夾的內容派送至每個用戶端的 \\Symantec Endpoint Protection\inbox\ 資料夾。

最後的結果須類似如下：

\\Symantec Endpoint Protection\inbox\index2.dax

\\Symantec Endpoint Protection\inbox*target moniker**latest sequence number*\full.zip

然後，會刪除已成功處理的檔案。 未能成功處理的檔案則會移至名為 Invalid 的子資料夾中。 如果您在 **inbox** 資料夾下的 **Invalid** 資料夾中看到檔案，則必須重新處理這些檔案。

請參閱第 192 頁的「使用第三方派送工具更新用戶端電腦」。

請參閱第 194 頁的「準備非受管用戶端以從第三方派送工具接收更新」。

將 Endpoint Protection 安全修補程式下載至 Windows 用戶端

什麼是安全修補程式以及運作方式為何？

安全修補程式是適用於 Symantec Endpoint Protection 用戶端的軟體修補程式，可修正用戶端程式碼中存在的弱點。由於新弱點成為已知弱點，賽門鐵克會傳送安全修補程式以修正弱點並將其上傳至 LiveUpdate 伺服器。從 14 版開始，您可以從 LiveUpdate 伺服器下載安全修補程式至管理伺服器。然後，可使用 LiveUpdate 伺服器、管理伺服器或群組更新提供者 (GUP)，採用與其他內容相同的方式將修補程式下載到用戶端。

附註：在早於 14 的版本中，安全修補程式僅作為新版本以及使用自動升級之用戶端部署套件的一部分提供。在 14 中，當 Symantec Endpoint Protection Manager 和用戶端已安裝相同版本時，您可以使用自動升級在這些用戶端上安裝安全修補程式。

安全修補程式不適用於 12.1.x 用戶端。

請參閱第 153 頁的「選擇派送方法以更新用戶端上的內容」。

如果用戶端和管理伺服器版本相符，則用戶端可從 LiveUpdate 伺服器、管理伺服器或 GUP 取得安全修補程式。如果用戶端和管理伺服器版本不相符，則用戶端只能從 LiveUpdate 伺服器取得安全修補程式，正如管理伺服器管理具有多個版本的用戶端時一樣。如果您想要使用管理伺服器或 GUP 下載修補程式，則必須更新用戶端或管理伺服器版本使其版本相同。

此外，用戶端的語言必須與管理伺服器相符。例如，管理法文、德文和簡體中文版用戶端的法文版管理伺服器僅向法文版用戶端提供安全修補程式。

請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。

附註：安全修補程式與維護修補程式不同。安全修補程式只解決可能的安全問題，並透過 LiveUpdate 傳送。維護修補程式可提供其他更新 (例如，為新的作業系統提供支援)，並透過 MySymantec 以完整安裝下載形式傳送。

關於 Endpoint Protection 發行類型和版本

表 9-10顯示了用戶端是否可以根據 Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 用戶端的版本號碼從管理伺服器接收安全修補程式的範例。

表 9-10　　哪些用戶端版本下載哪些安全修補程式的範例

管理伺服器版本	用戶端版本	用戶端是否從管理伺服器下載修補程式？
14.2	14.2	是
14.2	14.0.1 MP2	否
14.0.1 MP2	14.0.1 MP2	是
14.0.1 MP2	14.0.1 MP1	否
14.0.1 MP2	14.2	否

在 Windows 用戶端上安裝安全修補程式

依據預設，LiveUpdate 會將安全修補程式下載至 Symantec Endpoint Protection Manager，反過來又根據為其他內容類型架構的派送方法將修補程式安裝在用戶端上。

在用戶端下載和安裝安全修補程式後，會繼續執行未經修正的舊版用戶端，直到用戶端重新啟動。您必須重新啟動用戶端才能執行最新的修補程式。用戶端一般使用者必須重新啟動電腦，或者您必須從管理伺服器執行重新啟動指令。管理伺服器會向您傳送一個通知，指示哪些用戶端需要重新啟動。

在 Windows 用戶端上安裝安全修補程式

1 在主控台中，確認已將 LiveUpdate 架構為下載安全修補程式至管理伺服器。

在**「要下載的內容類型」**對話方塊中，確保已核取**「用戶端安全修補程式」**。

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

2 若要執行報告以找出用戶端電腦上安裝哪些版本，請執行**「防護內容版本」**報告。

請參閱第 543 頁的「產生網路中安裝的 Symantec Endpoint Protection 版本的清單」。

3 確認已將 LiveUpdate 設定政策架構為下載修補程式至用戶端。

在 LiveUpdate 設定政策中，於**「Windows 設定」**下方，按下**「進階設定」**。確保已勾選**「下載安全修補程式可修正最新版本 Symantec Endpoint Protection 用戶端中的漏洞」**。

請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。

4 收到通知後，請重新啟動用戶端電腦。

請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。

部分 3

管理群組、用戶端和管理員

10

管理用戶端電腦群組

本章包含以下主題：

管理用戶端群組

在 Symantec Endpoint Protection Manager 中，群組用作執行用戶端軟體的端點的配置區。這些端點可以是電腦或使用者。您可以將具有類似安全需求的用戶端分門別類為群組，以便於管理網路安全。

Symantec Endpoint Protection Manager 包含下列預設群組：

- **My Company** 群組為頂層或父群組，其中包含子群組的平面樹狀結構。
- **Default Group** 是 **My Company** 的子群組。除非用戶端屬於預先定義的群組，否則以 Symantec Endpoint Protection Manager 率先登錄時，會先指定到 **Default Group**。 您無法在 **Default Group** 下建立子群組。

附註：預設群組無法重新命名或者刪除。

如果您在雲端主控台中重新命名**「我的公司」**，Symantec Endpoint Protection Manager 中的群組名稱不會變更。

表 10-1 群組管理動作

工作	敘述
新增群組	請參閱第 202 頁的「如何設定群組結構」。 請參閱第 203 頁的「新增群組」。
匯入現有群組	若您的組織已有現成的群組結構，可匯入該群組作為組織單位。 **附註：**您無法以管理 Symantec Endpoint Protection Manager 中建立的群組的相同方式來管理匯入的組織單位。 請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。
停用子群組繼承	根據預設，子群組會從父群組繼承相同的安全性設定。您可以停用繼承。 請參閱第 208 頁的「停用群組繼承」。
在群組內建立位置	您可以設定代理程式，在用戶端實體位置變更時，自動切換成另一安全性政策； 請參閱第 226 頁的「管理遠端用戶端的位置」。 某些安全設定屬於群組特定，而某些設定屬於位置特定。您可以自訂位置特定的任何設定。 請參閱第 234 頁的「架構位置的通訊設定」。
管理群組的安全性政策	您可以根據各群組的需要建立安全性政策。然後，您可以將不同的政策指派到不同的群組或位置。 請參閱第 272 頁的「新增政策」。 請參閱第 275 頁的「指派政策給群組或位置」。 請參閱第 268 頁的「執行適用於所有政策的工作」。
執行群組維護	您可以移動群組以方便管理，並在群組之間移動用戶端。您還可以攔截用戶端，使其無法新增到特定群組。 請參閱第 209 頁的「將用戶端電腦移至其他群組」。 請參閱第 208 頁的「防止用戶端電腦被加入至群組」。

如何設定群組結構

您可以建立多個群組和子群組，以符合公司的組織結構和安全性。亦可根據功能、角色、地理位置或單項準則組合等群組結構進行。

表 10-2 群組建立準則

準則	敘述
功能	您可以根據欲管理的電腦類型建立群組，例如筆記型電腦、桌上型電腦以及伺服器。或者也可以根據使用類型建立多個群組。例如，您可以為出差使用的用戶端電腦建立遠端群組，以及為辦公室內的用戶端電腦建立本機群組。
角色	您可以根據各部門角色建立群組，例如銷售、工程、財務以及行銷等部門。
地理位置	您可以根據辦公室、城市、州、地區或國家等電腦所處位置建立群組。
組合	您可以根據準則組合建立群組。例如可以合併功能與角色兩者。 您可以根據角色新增父群組，然後根據功能新增子群組，如下所示： ■ 銷售，底下設有筆記型電腦、桌上型電腦和伺服器的子群組。 ■ 工程，底下設有筆記型電腦、桌上型電腦和伺服器的子群組。

在您將用戶端電腦組成群組之後，可以將適量的安全性套用到該群組。

例如，假設公司有電話行銷和會計部門。這些部門分別在紐約、倫敦和法蘭克福分公司都有職員。這兩個部門的所有電腦都指派給相同的群組，因此可以從相同來源接收病毒及安全風險定義檔更新。但是，IT 報告指出電話銷售部門比會計部門更容易受到風險的威脅。因此，系統管理員建立了獨立的電話行銷和會計群組。電話行銷用戶端會共用嚴格限制使用者與病毒和安全風險防護互動方式的架構設定。

建立群組結構最佳實務準則

請參閱第 268 頁的「執行適用於所有政策的工作」。

請參閱第 201 頁的「管理用戶端群組」。

新增群組

您可以在定義組織的群組結構之後，新增群組。

群組敘述最多可包含 1024 個字元。群組名稱可包含除下列字元之外的任何字元：[" / \ * ? < > | :] 群組敘述則不受此限。

附註：您無法在預設群組中新增群組。

請參閱第 202 頁的「如何設定群組結構」。

新增群組

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下方，選取要新增子群組的群組。

3 在「**用戶端**」標籤的「**工作**」下方，按下「**新增群組**」。

4 在「**新增*群組名稱*的群組**」對話方塊中，輸入群組名稱和敘述。

5 按下「**確定**」。

從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦

如果您的公司使用 Active Directory 或 LDAP 伺服器管理群組，您可以將群組結構匯入 Symantec Endpoint Protection Manager。然後，您可以從管理主控台管理群組和電腦。

表 10-3 列出在您可以管理群組之前，必須執行的工作以匯入群組結構。

表 10-3 匯入現有群組和電腦

步驟	敘述
步驟 1：將 Symantec Endpoint Protection Manager 連線至您公司的目錄伺服器	您可以將 Symantec Endpoint Protection Manager 連線至 Active Directory 或 LDAP 相容伺服器。新增伺服器時應啟用同步。 請參閱第 205 頁的「關於從目錄伺服器匯入組織單位」。 請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。 請參閱第 206 頁的「連線至遠端複製網站上的目錄伺服器」。
步驟 2：匯入整個組織單位或容器	您也可以從 Active Directory 或 LDAP 匯入現有群組結構至 Symantec Endpoint Protection Manager。您也可以將個別帳戶從匯入的群組結構複製到現有的 Symantec Endpoint Protection Manager 群組結構。 請參閱第 207 頁的「從目錄伺服器匯入組織單位」。
步驟 3：將匯入的電腦或使用者帳戶保留在他們自己的群組中，或複製匯入的帳戶到現有群組	在您匯入組織單位後，您可以執行下列任一動作： ■ 將匯入的組織單位或帳戶保留在他們自己的群組中。在您匯入組織單位或個別帳戶後，可指派政策到組織單位或群組。 ■ 複製匯入的帳戶到現有的 Symantec Endpoint Protection Manager 群組。複製的帳戶會遵循 Symantec Endpoint Protection Manager 群組，而非匯入的組織單位的政策。 請參閱第 203 頁的「新增群組」。 請參閱第 275 頁的「指派政策給群組或位置」。 請參閱第 270 頁的「安全政策類型」。

步驟	敘述
步驟 4：變更管理員帳戶的驗證方法 (選擇性)	對於您在 Symantec Endpoint Protection Manager 中新增的管理員帳戶，變更驗證方法以使用目錄伺服器驗證，而不是預設的 Symantec Endpoint Protection Manager 驗證。您可以使用管理員帳戶驗證您匯入的帳戶。當管理員登入 Symantec Endpoint Protection Manager 時，管理伺服器會從資料庫擷取使用者名稱，從目錄伺服器擷取密碼。 請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。 請參閱第 250 頁的「檢查目錄伺服器驗證」。

關於從目錄伺服器匯入組織單位

Microsoft Active Directory 和 LDAP 伺服器使用組織單位來管理電腦和使用者的帳戶。您可以將組織單位及其帳戶資料匯入 Symantec Endpoint Protection Manager，然後在管理主控台中管理該帳戶資料。由於 Symantec Endpoint Protection Manager 會將組織單位視為群組，因此您接著可以將安全性政策指派給組織單位群組。

您也可以藉由複製帳戶的方式，將帳戶從組織單位移入 Symantec Endpoint Protection Manager 群組。如此一來，Symantec Endpoint Protection Manager 群組和組織單位便存在相同的帳戶。由於 Symantec Endpoint Protection Manager 群組的優先順序高於組織單位，因此複製的帳戶會採用 Symantec Endpoint Protection Manager 群組的政策。

如果您從目錄伺服器刪除已複製到 Symantec Endpoint Protection Manager 群組的帳戶，該帳戶名稱仍會留在 Symantec Endpoint Protection Manager 群組中。您必須從管理伺服器手動移除該帳戶。

如果您需要修改組織單位中的帳戶資料，請在目錄伺服器上，而不是在 Symantec Endpoint Protection Manager 中執行這項工作。例如，您可以從管理伺服器刪除組織單位，此舉並不會永久刪除目錄伺服器中的該組織單位。您必須將 Symantec Endpoint Protection Manager 與 Active Directory 伺服器進行同步處理，這些變更才能自動更新於 Symantec Endpoint Protection Manager。設定連線至目錄伺服器時，可以啟用同步處理。

附註：同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

您也可以將選取的使用者匯入 Symantec Endpoint Protection Manager 群組，而不是匯入整個組織單位。

請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。

請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。

請參閱第 207 頁的「從目錄伺服器匯入組織單位」。

將 Symantec Endpoint Protection Manager 連線至目錄伺服器

您必須先將 Symantec Endpoint Protection Manager 連線至公司的目錄伺服器，然後才能匯入包含電腦帳戶或使用者帳戶的組織單位。

您無法修改管理伺服器中組織單位內的帳戶，只能在目錄伺服器中修改這些帳戶。不過，您可以同步處理 Active Directory 伺服器與管理伺服器間的帳戶資料。您在 Active Directory 伺服器上所做的任何變更，均會在 Symantec Endpoint Protection Manager 中自動更新。您在 Active Directory 伺服器上所做的任何變更，不會立即出現在先前匯入至管理伺服器的組織單位中。延遲的時間視同步處理頻率而定。在您架構連線時，請啟用同步處理，並設定同步處理頻率。

如果您從 Symantec Endpoint Protection Manager 中刪除目錄伺服器連線，則必須先刪除與該連線關聯的任何已匯入組織單位。然後，您便可以同步處理伺服器間的資料。

附註：同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

將 Symantec Endpoint Protection Manager 連線至目錄伺服器

1. 在主控台中，按下**「管理員」**>**「伺服器」**。
2. 在**「伺服器」**和**「本機網站」**下方，選取管理伺服器。
3. 在**「工作」**下方，按下**「編輯伺服器屬性」**。
4. 在**「伺服器屬性」**對話方塊的**「目錄伺服器」**標籤中，按下**「新增」**。
5. 在**「新增目錄伺服器」**對話方塊中，輸入目錄伺服器的名稱。
6. 勾選 **Active Directory** 或 **LDAP**，然後輸入 IP 位址、主機名稱或網域名稱。

   新增 LDAP 伺服器時，若 LDAP 伺服器的通訊埠編號必須與預設值不同，則變更埠號。
7. 如果想要使用加密連線，請勾選**「使用安全連線」**。
8. 按下**「確定」**。
9. 在**「目錄伺服器」**標籤上，勾選**「與目錄伺服器同步處理」**，然後在**「排程」**下，設定同步處理排程。
10. 按下**「確定」**。

請參閱第 207 頁的「從目錄伺服器匯入組織單位」。

連線至遠端複製網站上的目錄伺服器

如果某網站使用遠端複製 Active Directory 或 LDAP 伺服器，則可以將 Symantec Endpoint Protection Manager 連線至主要目錄伺服器和遠端複製伺服器。如果主要目錄伺服器連線中斷，管理伺服器仍會與遠端複製目錄伺服器保持連線。

然後，Symantec Endpoint Protection Manager 可以驗證管理員帳戶，並同步本機網站與遠端複製網站的所有 Active Directory 伺服器上的組織單位。

請參閱第 635 頁的「設定網站和遠端複製」。

附註：同步處理僅適用於 Active Directory 伺服器。Symantec Endpoint Protection 不支援與 LDAP 伺服器進行同步處理。

連線至遠端複製網站上的目錄伺服器

1. 在主控台中，按下**「管理員」**>**「伺服器」**。
2. 在**「伺服器」**下方，選取管理伺服器。
3. 在**「工作」**下方，按下**「編輯伺服器屬性」**。
4. 在**「伺服器屬性」**對話方塊的**「目錄伺服器」**標籤中，按下**「新增」**。
5. 在**「新增目錄伺服器」**對話方塊的**「遠端複製伺服器」**標籤中，按下**「新增」**。
6. 在**「新增遠端複製伺服器」**對話方塊中，輸入目錄伺服器的 IP 位址、主機名稱或網域名稱，然後按下**「確定」**。
7. 按下**「確定」**。
8. 按下**「確定」**。

請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。

從目錄伺服器匯入組織單位

當您從 Active Directory 或 LDAP 伺服器匯入電腦帳戶或使用者帳戶時，會作為組織單位匯入這些帳戶。您接著便可以將安全性政策套用到該組織單位。您也可以將這些帳戶複製到現有的 Symantec Endpoint Protection Manager 群組。

您可以將組織單位匯入成 **My Company** 群組或您所建立群組的子群組，但不能是 **Default Group** 的子群組。您不能建立群組作為組織單位的子群組。您不能將組織單位置於多個 Symantec Endpoint Protection Manager 群組中。

如果您不想將組織單位或容器內的所有帳戶新增至 Symantec Endpoint Protection Manager，仍然必須將其匯入。一旦匯入完成，可將要管理的帳戶複製到現有用戶端群組。

附註：將組織單位匯入 Symantec Endpoint Protection Manager 之前，您必須先轉換電腦名稱或使用者名稱前面的一些特殊字元。您可以在目錄伺服器中執行這項工作。如果不轉換特殊字元，管理伺服器就不會匯入這些帳戶。

您必須轉換下列特殊字元：

- 出現在項目開頭的空格或井字號字元 (#)。

- 出現在項目結尾的空格字元。
- 逗號 (,)、加號 (+)、雙引號 (")、小於或大於符號 (< 或 >)、等號 (=)、分號 (;)、反斜線 (\)。

若要允許匯入包含這些字元的名稱，您必須在每個字元前面加上反斜線字元 (\)。

從目錄伺服器匯入組織單位

1 將 Symantec Endpoint Protection Manager 連線至目錄伺服器。

請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。

2 在主控台中按下**「用戶端」**，然後在**「用戶端」**下方，選取要新增組織單位的群組。

3 在**「工作」**下方，按下**「匯入組織單位或配置區」**。

4 在**「網域」**下拉式清單中，選擇您在步驟 1 中建立的目錄伺服器名稱。

5 選取網域或子群組。

6 按下**「確定」**。

請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。

請參閱第 205 頁的「關於從目錄伺服器匯入組織單位」。

停用群組繼承

在群組結構中，子群組起初會自動從其父群組繼承位置、政策及設定。依據預設，每個群組會啟用繼承。您可以停用繼承，如此就能為子群組架構獨立的安全性設定。如果您在執行變更後又啟用繼承，則會覆寫子群組設定中的所有變更。

來自雲端的政策不會遵循 Symantec Endpoint Protection Manager 政策繼承組態。相反地，它們會遵循在雲端中定義的繼承規則。

請參閱第 201 頁的「管理用戶端群組」。

停用群組繼承

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**頁面的**「用戶端」**下，選取要停用或啟用繼承的群組。

您可以選擇頂層群組 My Company 以外的任何群組。

3 在**「<群組名稱>」**窗格的**「政策」**標籤上，取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。

防止用戶端電腦被加入至群組

您可以設定已定義群組成員資格的用戶端安裝套件。如果您在套件中定義了群組，則用戶端電腦會自動新增至相關群組。第一次新增用戶端時，會連線至管理伺服器。

請參閱第 113 頁的「管理用戶端安裝套件」。

如果您不希望用戶端在連線至網路時自動新增到特定群組，可以攔截用戶端。您可以攔截新用戶端新增至用戶端安裝套件中指派給使用者的群組。 在此情況下，該用戶端會新增至預設群組。 您可以手動將電腦移到攔截的群組。

攔截用戶端電腦加入至群組

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下方，在群組上按下滑鼠右鍵，再按下**「屬性」**。
3. 在**「詳細資訊」**標籤的**「工作」**下方，按下**「編輯群組屬性」**。
4. 在**「<*群組名稱*> 的群組屬性」**對話方塊中，按下**「攔截新用戶端」**。
5. 按下**「確定」**。

請參閱第 209 頁的「將用戶端電腦移至其他群組」。

將用戶端電腦移至其他群組

若您的用戶端電腦位於不正確的群組內，則可將其移至其他群組內。

若要將用戶端從多個群組移至單一群組中，您可以重新部署用戶端安裝套件。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

將用戶端電腦移至其他群組

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面上，選取群組。
3. 在**「用戶端」**標籤中選取的群組內，選取電腦，然後在**「移動」**上按下滑鼠右鍵。

   使用 Shift 鍵或 Control 鍵可選取多台電腦。
4. 在**「移動用戶端」**對話方塊中，選取新的群組。
5. 按下**「確定」**。

請參閱第 201 頁的「管理用戶端群組」。

11

管理用戶端

本章包含以下主題：

管理用戶端電腦

表 11-1 管理用戶端電腦的工作

工作	敘述
檢查電腦上是否安裝了用戶端軟體	■ 您可以在各群組中顯示尚未安裝用戶端軟體的電腦。 請參閱第 213 頁的「搜尋未安裝用戶端軟體的用戶端」。 ■ 您可以架構用戶端電腦以偵測未安裝用戶端軟體的其他裝置。部分這些裝置可能是未受保護的電腦。 然後，您可以將用戶端軟體安裝到這些電腦上。 請參閱第 220 頁的「將用戶端架構為偵測非受管裝置」。 ■ 您可以將用戶端新增至群組，稍後再安裝用戶端軟體。 請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。
檢查用戶端是否連線至管理伺服器	您可以在管理主控台和用戶端中檢查用戶端狀態圖示。狀態圖示會顯示用戶端和伺服器之間是否通訊。 請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。 請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。 電腦可能已安裝用戶端軟體，但本身是非受管用戶端。您無法管理未受管用戶端。請改為將未受管用戶端轉換成受管用戶端。 請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。
架構用戶端與伺服器之間的連線	安裝用戶端軟體後，用戶端電腦會在下一次活動訊號時自動連線至管理伺服器。您可以變更伺服器與用戶端電腦進行通訊的方式。 請參閱第 137 頁的「管理用戶端伺服器連線」。 您可以疑難排解任何連線問題。 請參閱第 664 頁的「Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題疑難排解」。
檢查用戶端電腦是否擁有正確的防護等級	■ 您可以檢視用戶端電腦上各項防護技術的狀態。 請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。 請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。 ■ 您可以執行報告或檢視日誌，看是否必須提高防護等級或改善效能。 例如，掃描可能導致誤報。 您也可以識別需要防護的用戶端電腦。 請參閱第 539 頁的「監控端點防護」。 ■ 您可以根據用戶端軟體或用戶端電腦的特定屬性來修改防護。 請參閱第 214 頁的「搜尋用戶端電腦相關資訊」。

工作	敘述
調整用戶端電腦的防護功能	如果您認為用戶端未擁有正確的防護等級，可以調整防護設定。 ■ 您可以根據報告和日誌的結果，來增減各種類型的防護功能。 請參閱第 270 頁的「安全政策類型」。 請參閱第 23 頁的「Symantec Endpoint Protection 技術如何保護您的電腦」。 ■ 您可以要求在用戶端上使用密碼。 請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。
在群組之間移動端點來修改防護 (選擇性)	若要變更某用戶端電腦的防護等級，您可以將它移到提供較多或較少防護的群組。 請參閱第 209 頁的「將用戶端電腦移至其他群組」。 當您部署用戶端安裝套件時，會指定用戶端要歸屬於哪個群組。您可以將用戶端移至其他群組。如果用戶端遭到刪除或中斷連線，然後又重新加入且重新連線，則用戶端會回到原始群組。若要讓用戶端留在最後歸屬的群組中，請架構重新連線喜好設定。您可以在**「通訊設定」**對話方塊的**「用戶端」**>**「政策」**標籤上架構這些設定。
決定使用者是否可以控制電腦防護 (選擇性)	您可以指定使用者對用戶端電腦上的防護功能具有何種控制。 ■ 對於病毒和間諜軟體防護、主動型威脅防護以及記憶體攻擊緩和，您可以在政策內鎖定或解除鎖定核取方塊，以指定使用者是否能夠變更個別設定。 ■ 針對防火牆政策和 IPS 政策，以及部分用戶端使用者介面設定，您可以更廣泛地變更使用者控制等級。 請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。 ■ 如果使用者需要用戶端的完整控制權限，您可以安裝非受管用戶端。 請參閱第 143 頁的「用戶端電腦和管理伺服器的通訊方式?」。
從解除委任的電腦移除 Symantec Endpoint Protection 用戶端軟體 (選擇性)	如果您已解除委任用戶端電腦，並且想要將授權用於其他電腦，則可以解除安裝 Symantec Endpoint Protection 用戶端軟體。對於未連線的受管用戶端，Symantec Endpoint Protection Manager 預設會在 30 天後從資料庫刪除用戶端。 您可以變更時段，在該時段之後，Symantec Endpoint Protection Manager 即會從資料庫中刪除用戶端。刪除用戶端後，您也會省下資料庫的空間。 請參閱第 111 頁的「移除適用於 Windows 的 Symantec Endpoint Protection 用戶端」。 請參閱第 112 頁的「解除安裝適用於 Mac 的 Symantec Endpoint Protection 用戶端」。 請參閱第 113 頁的「移除適用於 Linux 的 Symantec Endpoint Protection 用戶端」。 請參閱第 86 頁的「從資料庫清除過時的用戶端以使更多授權可用」。

檢視用戶端電腦的防護狀態

您可以檢視網路中用戶端與電腦的即時操作狀態和防護狀態的相關資訊。

您可以檢視：

- 未安裝用戶端的受管用戶端電腦清單。

您可以檢視電腦名稱、網域名稱，以及登入使用者名稱。

- 已啟用和已停用的防護。
- 擁有最新政策和定義檔的用戶端電腦。
- 群組的政策序號和用戶端的版本號碼。
- 有關用戶端電腦網路元件的資訊，例如電腦使用的網路卡 MAC 位址。
- 有關用戶端電腦的系統資訊，例如，可用磁碟空間量和作業系統版本號碼。

瞭解特定用戶端的狀態後，即可解決用戶端電腦的任何安全問題。您可以透過對群組執行指令來解決多種問題。例如，您可以更新內容或啟用「自動防護」。

附註：如果您管理任何執行舊版 Symantec Endpoint Protection 的用戶端，某些較新的防護技術可能會列為**「未報告」**。這是預期狀況。這並不表示您需要對這些用戶端採取動作。

請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

請參閱第 213 頁的「搜尋未安裝用戶端軟體的用戶端」。

檢視用戶端電腦的防護狀態

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面的**「用戶端」**下，找出需要相關資訊的用戶端所在群組。
3. 在**「用戶端」**標籤上，按下**「檢視」**下拉式清單。然後選取類別。

   您可以在右下角的文字方塊中輸入頁碼，直接移至特定的頁面。

搜尋未安裝用戶端軟體的用戶端

您可根據下列準則搜尋群組中的用戶端：

- 已安裝用戶端軟體。
- 在 Windows、Mac 或 Linux 電腦上執行用戶端。
- Windows 用戶端處於電腦模式或使用者模式。
- 在虛擬桌面基礎架構中，用戶端處於非持續且離線狀態。

請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。

請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。

搜尋未安裝用戶端軟體的用戶端

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」窗格中，選擇要搜尋的群組。

3 在「**用戶端**」標籤的「**工作**」下方，按下「**設定顯示過濾器**」。

4 在「**設定顯示過濾器**」對話方塊中，勾選「**已建立但尚未安裝用戶端軟體的新使用者或電腦**」。

5 按下「**確定**」。

搜尋用戶端電腦相關資訊

您可以搜尋用戶端、用戶端電腦和使用者的資訊，以便在充分掌握資訊的狀況下，決定網路的安全。

例如，您可以找出 Sales 群組的哪些電腦執行最新的作業系統。 您可以找出 Finance 群組的哪些用戶端電腦需要安裝最新的病毒定義檔。

附註：若要搜尋大多數關於使用者的資訊，您必須在用戶端軟體安裝期間，或此後收集使用者資訊。這項使用者資訊也會顯示在用戶端「編輯屬性」對話方塊的「一般」標籤和「使用者資訊」標籤上。

請參閱第 222 頁的「收集使用者資訊」。

搜尋用戶端電腦相關資訊

1 在主控台中，按下「**用戶端**」。

2 在「**工作**」下方，按下「**搜尋用戶端**」。

3 在「**搜尋用戶端**」對話方塊的「**尋找**」下拉式清單中，按下「**電腦**」或「**使用者**」。

4 按下「**瀏覽**」可選取預設群組以外的其他群組。 按下以選取群組，然後按下「**確定**」。

5 在「**搜尋條件**」下方，按下「**搜尋欄位**」顯示下拉式清單，然後選取搜尋條件。

若要尋找內嵌式用戶端，您可以搜尋使用中的寫入過濾器類型。按下「**加強型寫入過濾器**」、「**檔案型寫入過濾器**」或「**統一寫入過濾器**」，搜尋它們是已安裝、已啟用還是兩者皆是。 您也可以搜尋縮減大小用戶端。 按下「**安裝類型**」以搜尋「**縮減大小**」的值。

6 按下「**比較運算子**」下拉式清單，然後選取比較運算子。

您可以在搜尋條件中使用標準的布林運算子。如需關於選項的詳細資訊，請按下「**說明**」。

7 在「**值**」儲存格中，輸入搜尋字串。

8 按下「**搜尋**」。

您可以將結果匯出至文字檔。

9 按下「**關閉**」。

您可以將查詢中包含的資料匯出至文字檔。

請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。

什麼是可對用戶端電腦執行的指令？

您可以從主控台，對個別用戶端或整個群組執行遠端指令。

若要查看任何指令的結果，請按下「**監視器**」頁面>「**日誌**」>「**指令狀態**」。您也可以從「**類型**」下拉式清單執行某些指令。

系統管理員和網域管理員可自動執行這些指令。對於限制的管理員，可個別啟用或停用每個指令的存取權限。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

表 11-2 可對用戶端電腦執行的指令

指令	敘述
分析 (雲端主控台)	從雲端主控台執行「**分析**」指令。「**分析**」指令會顯示您從雲端主控台提交至 Content Analysis 系統 (CAS) 以進行分析的所有要求的進度。 架構 Symantec Endpoint Protection 以使用 Symantec Content Analysis 系統
取消有害證據掃描	開始或取消您在第三方遠端監控與管理上使用的掃描。
掃描	在用戶端電腦上執行隨選掃描。 如果您執行掃描指令，並選擇「**自訂**」掃描，掃描會使用您在「**管理員定義掃描**」頁面上架構的指令掃描設定。 指令使用的是「病毒和間諜軟體防護」政策 (套用於選取的用戶端電腦) 的設定。 請參閱第 374 頁的「在用戶端電腦上執行隨選掃描」。
更新內容	在用戶端電腦初始化 LiveUpdate 階段作業，以更新用戶端的內容。 用戶端會從 Symantec LiveUpdate 接收最新的內容。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。
更新內容和掃描	初始化 LiveUpdate 階段作業，以更新內容，然後在用戶端電腦執行隨選掃描。

指令	敘述
「啟動 Power Eraser 分析」	在選取的電腦上執行 Power Eraser 分析。 一般來說，您應當僅在一台或少數幾台電腦上執行 Power Eraser。 應當僅在電腦呈現不穩定狀態或持續發生問題時執行 Power Eraser。 Power Eraser 和其他掃描不同，並不會自動矯正任何潛在威脅。 您必須檢閱日誌中的偵測結果，並指定要移除或略過的風險。 **附註：**Mac 和 Linux 用戶端電腦不會處理此指令。 請參閱第 678 頁的「從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析」。
重新啟動用戶端電腦	重新啟動用戶端電腦。 如果使用者登入至用戶端，根據管理員為該用戶端所架構的重新啟動選項，使用者會看見警告。 您可以在**「一般設定」**頁面上架構用戶端的重新啟動選項。 **附註：**重新啟動選項僅適用於 Windows 用戶端電腦。 Mac 用戶端電腦始終執行硬式重新啟動。 Linux 用戶端電腦會忽略此指令。 請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。 **附註：**您可以確保 Windows 用戶端不會重新啟動。 您可以在用戶端新增登錄機碼，使其即使管理員發出重新啟動指令也不會重新啟動。 請參閱第 218 頁的「確保用戶端不會重新啟動」。
啟用自動防護	為用戶端電腦上的檔案系統啟用「自動防護」。 預設會為檔案系統啟用「自動防護」。 賽門鐵克建議您始終保持自動防護為啟用狀態。您可以鎖定此設定，讓用戶端電腦上的使用者無法停用「自動防護」。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。 請參閱第 403 頁的「自訂 Mac 用戶端的自動防護」。 如果電子郵件的自動防護已停用，可在病毒和間諜軟體防護政策中加以啟用。
啟用網路威脅防護和**停用網路威脅防護**	啟用或停用用戶端電腦上的防火牆和啟用入侵預防。 **附註：**Linux 用戶端電腦不會處理此指令。 請參閱第 288 頁的「管理防火牆防護」。
「啟用下載鑑識」和**「停用下載鑑識」**	啟用或停用用戶端電腦上的「下載鑑識」。 **附註：**Mac 和 Linux 用戶端電腦不會處理此指令。 請參閱第 380 頁的「管理「下載鑑識」偵測」。
從隔離所刪除	從隔離所刪除所有檔案。此指令僅出現在**「風險日誌」>「動作」**下拉式清單中。 如何從 Symantec Endpoint Protection Manager 刪除隔離項目

指令	敘述
收集檔案指紋清單	從所選用戶端產生無法編輯的檔案指紋清單。 收集的指紋清單會顯示在**「政策元件」>「檔案指紋清單」**下方的**「政策」**標籤上。 通常，您可以在單一電腦或小型電腦群組上執行此指令。 如果選取多台電腦，則指令會收集每台電腦的個別清單。 **附註：**Mac 和 Linux 用戶端電腦不會處理此指令。
「將用戶端放置在隔離所中」和**「從隔離所中移除用戶端」**	可讓您新增用戶端，或從隔離所中移除用戶端。這些指令僅在您啟用「欺敵」時可用。

請參閱第 684 頁的「根據平台 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能」。

在用戶端電腦上從主控台執行指令

您可以隨時在用戶端電腦上手動執行指令，例如，啟動掃描或取消掃描。在受管用戶端上，從管理伺服器執行的指令會覆寫使用者執行的指令。指令在用戶端電腦上的處理順序，根據指令的不同而有所差異。無論在何處啟動指令，處理指令的方式一樣。

請參閱第 215 頁的「什麼是可對用戶端電腦執行的指令？」。

您從下列位置執行這些指令：

- **「用戶端」**頁面。
- **「電腦狀態」**日誌。您僅可以從**「電腦狀態」**日誌執行**「取消全部掃描」**和**「啟動 Power Eraser 分析」**指令。
- **風險**日誌。您僅可以從**「風險」**日誌執行**「從隔離所刪除」**指令。
  如何從 Symantec Endpoint Protection Manager 刪除隔離項目

開始掃描後，您也可以立即將其取消。

在用戶端電腦上從「用戶端」頁面執行指令

1. 在主控台中，按下**「用戶端」**。
2. 對群組或電腦執行下列其中一項動作：
   - 在左側窗格中，在群組上按下滑鼠右鍵，然後按下**「對群組執行指令」> *command***
   - 按下**「用戶端」**標籤，在電腦上按下滑鼠右鍵，然後按下**「對電腦執行指令」> *指令***
3. 在出現的訊息中，按下**「是」**。

從電腦狀態日誌執行指令

1 按下**「監視器」**>**「日誌」**>**「電腦狀態」**日誌類型，然後按下**「檢視日誌」**。

2 從**「指令」**清單方塊中選取指令，並選取電腦，然後按下**「啟動」**。

附註：透過從指令清單按下**「取消全部掃描」**，即可以取消進行中的排程掃描或您開始的掃描。

如果指令未成功佇列，您可能需要重複此程序。您可以檢查伺服器是否停機。如果主控台失去與伺服器的連線，您可以登出主控台後再重新登入看看是否有幫助。

檢視指令結果

1 按下**「監視器」**。

2 在**「指令狀態」**標籤上，從清單中選取一個指令，然後按下**「詳細資訊」**。

附註：您也可透過按下掃描指令**「指令」**欄中的**「取消掃描」**圖示，來取消進行中掃描。

確保用戶端不會重新啟動

您可以使用以下程序，來確保任何 Symantec Endpoint Protection 用戶端電腦不會重新啟動。例如，您可能想要在執行 Symantec Endpoint Protection 用戶端的伺服器上設定此值。設定此登錄機碼可確保當管理員從主控台於自己所屬的群組上發出「重新啟動電腦」指令時，伺服器不會重新啟動。

確保用戶端不會重新啟動

1 在用戶端電腦中開啟登錄編輯程式。

2 瀏覽到 HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC。

3 將下面這一行新增至登錄：

```
DisableRebootCommand   REG_DWORD   1
```

在使用者模式和電腦模式之間切換 Windows 用戶端

您可依照將政策套用至群組中用戶端的方式，將 Windows 用戶端新增為使用者模式或電腦模式。將使用者或電腦新增至群組後，系統會採用先前指派至該群組的政策。

新增用戶端時，預設為使用優先於使用者模式的電腦模式。賽門鐵克建議您使用電腦模式。Linux 用戶端和 Mac 用戶端僅以電腦模式安裝。

模式	敘述
電腦模式	用戶端電腦會從電腦所屬的群組取得政策。不論哪個使用者登入電腦，用戶端都會以相同的政策防護電腦。政策會以電腦所在的群組為準。電腦模式為預設設定。多數組織多數於電腦模式架構用戶端。您可能會想要依照網路環境架構幾個擁有特殊要求的使用者用戶端。 若電腦名稱已位於其他群組中，您無法將使用者模式切換為電腦模式。切換至電腦模式時，會從群組中刪除用戶端的使用者名稱，並將用戶端的電腦名稱新增至該群組。 加入於電腦模式的用戶端可啟用為非受管偵測程式，並且用於偵測未經授權的裝置。 請參閱第 220 頁的「將用戶端架構為偵測非受管裝置」。
使用者模式	用戶端電腦會從使用者所屬的群組取得政策。政策會根據登入用戶端的使用者而變更。政策會以使用者為準。 如果您將現有群組結構從 Microsoft Active Directory 或 LDAP 目錄伺服器匯入 Symantec Endpoint Protection Manager 以按使用者編排用戶端，則使用使用者模式。 如果使用者登入名稱與電腦名稱已存於任何群組中，您無法將電腦模式切換為使用者模式。切換至使用者模式時，會從群組中刪除用戶端的電腦名稱。然後，將用戶端的使用者名稱新增至群組。 請參閱第 204 頁的「從 Active Directory 或 LDAP 伺服器匯入現有群組和電腦」。

當您部署用戶端安裝套件時，會指定用戶端要歸屬於哪個群組。您稍後可以將用戶端指定為使用者模式或電腦模式。若用戶端稍後被刪除或失去連線，然後又將其重新新增和重新連線，用戶端將回到原群組。不過，您可以架構用戶端留在其上次移至使用者模式或電腦模式時所在的群組。例如，新的使用者可能登入架構為使用者模式的用戶端。用戶端接著會留在先前使用者所在的群組。

您可以按下**「用戶端」**>**「政策」**，再按下**「通訊設定」**，來架構這些設定。

在使用者模式和電腦模式之間切換 Windows 用戶端

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面的**「用戶端」**下方，選取包含使用者或電腦的群組。
3. 在**「用戶端」**標籤上，在表格中的電腦或使用者名稱上按下滑鼠右鍵，然後選取**「切換至電腦模式」**或**「切換至使用者模式」**。

   此模式是屬於切換設定，因此始終會切換顯示其中一種模式。表格中的資訊會隨新設定而變更。

將用戶端架構為偵測非受管裝置

未授權裝置能夠以多種方式連線至網路，例如，會議室的實體存取或非授權無線網路存取點。若要在各個端點強制執行政策，您必須能夠迅速偵測出網路中是否有新的裝置出現。您必須判斷這些裝置是否安全。您可以啟用任何用戶端作為非受管偵測程式，以偵測不明裝置。不明裝置是未執行 Symantec Endpoint Protection 用戶端軟體的非受管裝置。如果非受管裝置是電腦，您可以在該電腦上安裝 Symantec Endpoint Protection 用戶端軟體。

裝置啟動時，作業系統會將下列流量傳送至網路，以告知其他電腦有裝置出現：

- 位址解析通訊協定 (ARP) 流量 (ICMPv4)
- 芳鄰搜尋通訊協定 (NDP) 流量 (ICMPv6)

啟用成為非受管偵測程式的用戶端會收集此封包資訊，然後傳送至管理伺服器。管理伺服器會在封包中搜尋裝置的 MAC 位址和 IP 位址。伺服器會將這些位址與伺服器資料庫中的現有 MAC 位址與 IP 位址清單相互比對。如果伺服器找不到相符的位址，伺服器會記錄該裝置為新裝置。然後您可以決定該裝置是否安全。由於用戶端只傳輸資訊，因此不會使用額外的資源。

您可以架構非受管偵測程式忽略某些裝置，例如印表機。您也可以設定電子郵件通知，以便在非受管偵測程式偵測出不明裝置時通知您。

若要架構用戶端成為非受管偵測程式，必須執行下列動作：

- 啟用網路威脅防護。
  請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。
- 將用戶端切換為電腦模式。
  請參閱第 218 頁的「在使用者模式和電腦模式之間切換 Windows 用戶端」。
- 任何時間都在執行不間斷的電腦上安裝用戶端。

架構用戶端偵測未授權裝置

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下，選取包含要啟用為非受管偵測程式的用戶端的群組。
3. 在**「用戶端」**標籤上，在要啟用成為非受管偵測程式的用戶端上按下滑鼠右鍵，然後按下**「啟用為非受管偵測程式」**。
4. 若要指定一個或多個裝置由非受管偵測程式排除在偵測之外，請按下**「架構非受管偵測程式」**。
5. 在**「<用戶端名稱> 發生非受管偵測程式例外」**對話方塊中，按下**「新增」**。
6. 在**「新增非受管偵測程式例外」**對話方塊中，按下下列其中一個選項：
   - **「排除偵測 IP 位址範圍」**，然後輸入多個裝置的 IP 位址範圍。
   - **「排除偵測 MAC 位址」**，然後輸入裝置的 MAC 位址。

7 按下「**確定**」。

8 按下「**確定**」。

顯示用戶端偵測的未授權裝置清單

1 在主控台中，按下「**首頁**」。

2 在「**首頁**」頁面的「**安全狀態**」區段中，按下「**更多詳細資料**」。

3 在「**安全狀態詳細資料**」對話方塊中，捲動至「**不明裝置失敗**」表格。

4 關閉對話方塊。

防止和允許使用者變更用戶端的使用者介面

使用者可以在用戶端使用者介面上變更哪些項目？

以管理員身分設定使用者控制等級，以判斷使用者是否能夠對用戶端進行變更。例如，您可以防止使用者開啟用戶端使用者介面或通知區域圖示。針對使用者管理的使用者介面功能稱為受管設定。使用者無法存取所有用戶端功能，例如密碼防護。

請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。

如何架構使用者介面設定？

如果您執行下列任一項工作，則可以架構 用戶端上的使用者介面設定：

- 將用戶端的使用者控制層級設定為伺服器控制。
- 將用戶端的使用者控制層級設定為混合控制，並將「**用戶端/伺服器控制設定**」標籤上的父系功能設定為「**伺服器**」。
  例如，您可以將「**顯示/隱藏通知區域圖示**」選項設定為「**用戶端**」。通知區域圖示會出現在用戶端上，而使用者可以選擇顯示或隱藏圖示。如果您將「**顯示/隱藏通知區域圖示**」選項設定為「**伺服器**」，則可以選擇是否要在用戶端上顯示通知區域圖示。

附註：這些設定大部分僅適用於 Windows 用戶端。您只能在伺服器控制中架構 Mac 用戶端上的幾個選項。

在混合控制中架構使用者介面設定

1 按下「**用戶端**」>「**政策**」標籤。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

2 在「***<位置名稱>*的用戶端使用者介面控制設定**」對話方塊中，按下「**混合控制**」旁的「**自訂**」。

3 在「**用戶端使用者介面混合控制設定**」對話方塊的「**用戶端/伺服器控制設定**」標籤上，執行下列其中一個動作：

- 鎖定某個選項，這樣您就只能從伺服器架構它。針對要鎖定的選項，按下**「伺服器」**。您在此對「伺服器」設定的任何病毒及間諜軟體防護設定，會覆寫用戶端上的設定。
- 解除鎖定某個選項，讓使用者可以在用戶端上架構它。針對所要的選項，按下**「用戶端」**。 預設會針對所有設定選取用戶端，但不包含病毒及間諜軟體設定。

4 針對一些已設定為**「伺服器」**的選項，請按下**「用戶端使用者介面設定」**標籤架構這些選項：

如需瞭解在主控台何處架構其餘設定為**「伺服器」**的選項，請按下**「說明」**。例如，若要啟用防火牆設定，請在「防火牆」政策中架構設定。

請參閱第 320 頁的「為網路服務啟用通訊而非新增規則」。

請參閱第 330 頁的「啟用網路入侵預防或瀏覽器入侵預防」。

5 在**「用戶端使用者介面設定」**標籤上，勾選選項的核取方塊，這樣就能在用戶端上使用選項。

6 按下**「確定」**。

7 按下**「確定」**。

在伺服器控制中架構使用者介面設定

1 將使用者控制等級變更為伺服器控制。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

2 在**「用戶端使用者介面設定」**對話方塊中，勾選要顯示在用戶端上的選項。

3 按下**「確定」**。

4 按下**「確定」**。

請參閱第 319 頁的「架構混合控制的防火牆設定」。

收集使用者資訊

在進行用戶端軟體安裝程序或政策更新時，您可以提示用戶端電腦的使用者輸入自己的相關資訊。您可以收集有關員工的資訊，包括行動電話號碼、工作職稱和電子郵件地址等。收集此資訊之後，您必須手動維護和更新資訊。

附註：用戶端電腦上第一次出現啟用訊息後，如果使用者已回應所需的資訊，訊息則不會再次出現。即使使用者編輯任何欄位，或停用並再次啟用訊息，用戶端也不會顯示新訊息。然而，使用者可以隨時編輯資訊，而且管理伺服器也可擷取該資訊。

請參閱第 113 頁的「管理用戶端安裝套件」。

收集使用者資訊

1 在主控台中，按下**「管理員」**，再按下**「安裝套件」**。

2 在**「安裝套件」**窗格，按下**「用戶端安裝套件」**。

3 在**「工作」**下方，按下**「設定使用者資訊收集」**。

4 在**「設定使用者資訊收集」**對話方塊中，勾選**「收集使用者資訊」**。

5 在**「彈出式訊息」**文字方塊中，輸入您想要使用者在收到提示資訊時閱讀的訊息。

6 如果您想要讓使用者能延後收集使用者資訊，請勾選**「啟用稍後提醒我」**，然後以分鐘為單位設定時間。

7 在**「選取要顯示來讓使用者輸入的欄位」**下，選擇要收集的資訊類型，然後按下**「新增」**。

按 Shift 鍵或 Ctrl 鍵可同時選擇一個或多個欄位。

8 在「非必填」欄位中，在您要定義為使用者選填的欄位旁勾選核取方塊。

9 按下**「確定」**。

用密碼保護 Symantec Endpoint Protection 用戶端

您可以要求用戶端電腦在使用者每次執行特定工作時都啟用密碼防護，以提高企業安全性。

您可以要求使用者在嘗試執行下列其中一個動作時必須輸入密碼：

- 開啟用戶端的使用者介面。
- 停止用戶端服務。
- 解除安裝用戶端。
  自 14.0.1 起，您可以要求 Mac 使用者輸入密碼來解除安裝用戶端。
- 匯入和匯出用戶端通訊設定。

請參閱第 221 頁的「防止和允許使用者變更用戶端的使用者介面」。

使用密碼保護用戶端

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下方，選取要設定密碼防護的群組。

3 在**「政策」**標籤的**「與位置無關的政策與設定」**下方，按下**「密碼」**。

4 在**「用戶端密碼設定」**視窗中，勾選任何或所有核取方塊。

如果方塊顯示為灰色，此群組會從父群組繼承政策。必須先編輯父群組中的政策，或停用此群組的繼承，才能繼續。

請參閱第 208 頁的「停用群組繼承」。

5 在**「密碼」**和**「確認密碼」**文字方塊中，輸入同一密碼。

您可以建立介於 6 到 256 個字元長度的密碼。

如果您看到密碼強度不可接受的訊息，請考慮增加您的密碼強度。不過，您可能仍無法儲存密碼。

勾選**「將密碼設定套用至非繼承的子群組」**，以修改不會從父系繼承其設定的任何子群組的密碼防護設定。僅為父群組顯示此設定。

6 按下**「確定」**。

12

管理遠端用戶端

本章包含以下主題：

管理遠端用戶端

您的網路可能會包含一些從不同位置連線到網路的用戶端。管理這些用戶端的方式，可能與管理僅從網路內部連線之用戶端的方式不同。您可能需要管理一些始終透過 VPN 遠端連線的用戶端，或由於員工出差而從多個位置進行連線的用戶端。您也可能需要為一些不在管理控制範圍內的電腦管理安全性。例如，您可能會提供客戶、承包商、供應商或業務夥伴有限的網路存取權限。部分員工可能會使用自己的個人電腦連線到您的網路，因此，您可能需要以不同的方式管理這些用戶端。

在所有上述情況下，您都必須應付更大的安全性風險。連線或用戶端電腦的安全性可能會比較低，而且您對部分用戶端的控制權可能會較少。為了將這些風險對整體網路安全性的影響降至最低，您應評估各個用戶端對網路的不同類型遠端存取權限。然後，您就可以根據評估套用更嚴格的安全性政策。

若要基於安全性風險的差異以不同方式管理連線到網路的用戶端，您可以使用 Symantec Endpoint Protection 的位置偵測功能。

您需要根據用戶端的位置，為可能對網路造成較大風險的用戶端套用不同的政策。Symantec Endpoint Protection 中的位置會定義成用戶端電腦用於連線到網路的連線類型。位置也可以包含有關連線位於公司網路內部或外部的資訊。

您可以為用戶端群組定義位置。然後為每個位置指派不同的政策。部分安全性設定可以指派給整個群組，不論位置為何。而部分設定則會視位置而有所不同。

表 12-1 管理遠端用戶端

工作	敘述
根據安全性風險評估設定群組	請參閱第 201 頁的「管理用戶端群組」。
設定遠端用戶端群組的位置	請參閱第 226 頁的「管理遠端用戶端的位置」。
架構各位置的通訊設定	請參閱第 234 頁的「架構位置的通訊設定」。
加強安全性政策	請參閱第 235 頁的「關於加強遠端用戶端的安全性政策」。
開啟用戶端通知	請參閱第 236 頁的「關於開啟遠端用戶端的通知」。
自訂用戶端日誌管理設定	自訂遠端用戶端的日誌設定，特別是如果用戶端離線多天。若要減少頻寬和管理伺服器負載，請進行下列變更： ■ 將用戶端設定為不上傳其日誌到管理伺服器。 ■ 將用戶端設定為僅上傳用戶端安全日誌。 ■ 將過濾日誌事件設定為僅上傳指定事件。 建議要上傳的事件包括定義更新，否則會對修復故障有副作用。 ■ 延長日誌的存留時間。 較長的存留時間可以讓您檢閱更多的病毒和間諜軟體事件資料。
監控遠端用戶端	請參閱第 236 頁的「關於從管理伺服器監控遠端用戶端」。 請參閱第 237 頁的「從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端」。

管理遠端用戶端的位置

設定需要管理的群組後，請新增位置。如果您的安全策略有此需求，則每個群組可以有不同的位置。您可在 Symantec Endpoint Protection Manager 主控台中設定依照位置觸發自動政策切

換的條件。位置偵測功能會根據用戶端符合的位置條件，自動將您指定的安全性政策套用到用戶端。

位置條件可依據數個準則。 這些準則包含 IP 位址、網路連線類型，以及用戶端電腦是否可以連線到管理伺服器等。您可以根據指定的準則，允許或攔截用戶端連線。

位置可以套用到您為其建立的群組，也可套用到從該群組繼承的任何子群組。因此最好能夠在 My Company 群組層級建立任何用戶端都可以使用的位置。然後，在子群組層級上為特定的群組建立位置。

如果您建立的群組和位置的數目較少，安全性政策和設定的管理會比較簡單。不過，, 由於網路的複雜性和其安全性需求，可能需要更多的群組和位置。視您所需要的不同安全設定、日誌相關設定、通訊設定和政策數目而定，會決定您建立多少群組和位置。

您想為遠端用戶端自訂的部分組態選項是與位置無關的。這些選項可以從父群組繼承，也可以獨立設定。如果您建立單一群組來包含所有遠端用戶端，則對群組中的用戶端來說，與位置無關的設定都是相同的。

下列設定與位置無關：

- 自訂入侵預防特徵
- 系統鎖定設定
- 網路應用程式監控設定
- LiveUpdate 內容政策設定
- 用戶端日誌設定
- 用戶端伺服器通訊設定
- 一般安全性相關設定，包括位置偵測和竄改防護

若要自訂上述任何與位置無關的設定，例如處理用戶端日誌的方式，就需要建立不同的群組。

某些設定會視位置而定。

基於最佳實務，請勿允許使用者關閉下列防護：

- 自動防護
- SONAR
- 竄改防護
- 您所建立的防火牆規則

表 12-2 可執行的位置偵測工作

工作	敘述
規劃位置	您應該衡量環境中所需的各種安全性政策類型，藉此決定應使用的位置。然後，即可判斷定義每個位置所要使用的準則。最好同時規劃群組和位置。 請參閱第 201 頁的「管理用戶端群組」。 以下範例可能對您很有用： 請參閱第 231 頁的「設定第一種狀況的位置偵測條件」。 請參閱第 232 頁的「設定第二種狀況的位置偵測條件」。
啟用位置偵測	若要根據用戶端的連線位置來控制指派給用戶端的政策，您可以啟用位置偵測。 請參閱第 228 頁的「啟動用戶端位置偵測」。
新增位置	可新增群組位置。 請參閱第 229 頁的「將位置新增到群組」。
指派預設位置	所有群組都必須有個預設位置。安裝主控台後，僅有一個名為「預設值」的位置。建立新群組後，預設位置永為「預設值」。稍後新增其他位置之後，您可以變更預設位置。 如果發生下列情形之一，會使用預設位置： ■ 多個位置中有一個符合位置準則，且上一個位置不符合位置準則。 ■ 您正在使用位置偵測，而所有位置都不符合準則。 ■ 位置在政策中已重新命名或變更。用戶端接收新政策時會復原為預設位置。 請參閱第 230 頁的「變更預設位置」。
架構各位置的通訊設定	您也可以根據位置，架構管理伺服器與用戶端之間的通訊設定。 請參閱第 234 頁的「架構位置的通訊設定」。

請參閱文章 Symantec Endpoint Protection 位置偵測的最佳實務準則。

請參閱第 225 頁的「管理遠端用戶端」。

啟動用戶端位置偵測

如果要根據用戶端的連線位置來指定用戶端政策，您可啟動用戶端位置偵測。

勾選**「記住上次的位置」**後，當用戶端連線至網路時，將從上次使用的位置指定政策。如果啟用位置偵測，用戶端會在幾秒後自動切換至適當的政策。與特定位置關聯的政策會判斷用戶端的網路連線。如果停用了位置偵測，即使用戶端是在伺服器控制中，用戶端仍可手動切換至任意位置。如果啟用隔離所位置，用戶端可能會在幾秒後切換至隔離所政策。

如果取消勾選**「記住上次的位置」**後，當用戶端連線至網路時，將從預設位置指定政策。用戶端無法連接到最後使用的位置。如果啟用位置偵測，用戶端會在幾秒後自動切換至適當的政策。與特定位置關聯的政策會判斷用戶端的網路連線。如果停用了位置偵測，即使用戶端是在伺服器控制中，使用者仍可手動切換至任意位置。如果啟用隔離所位置，用戶端可能會在幾秒後切換至隔離所政策。

啟動用戶端位置偵測

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面的**「用戶端」**下，選取要實作自動位置切換的群組。
3. 在**「政策」**標籤中，取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。
4. 在**「與位置無關的政策和設定」**下方，按下**「一般設定」**。
5. 在**「一般設定」**對話方塊之**「一般設定」**標籤的**「位置設定」**下，勾選**「記住上次的位置」**。

   此選項預設為啟用。用戶端一開始會指派給與用戶端最後連線至網路的位置相關聯的政策。
6. 勾選**「啟用位置偵測」**。

   依據預設，會啟用位置偵測。用戶端會自動指派給使用者嘗試連接至網路位置相關聯的政策。
7. 按下**「確定」**。

請參閱第 226 頁的「管理遠端用戶端的位置」。

請參閱第 229 頁的「將位置新增到群組」。

將位置新增到群組

將位置新增到群組時，您可以指定觸發該群組中的用戶端切換到該位置的條件。您也必須將適當的政策和設定套用到各位置，位置偵測才會有效。

將位置新增到群組

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面的**「用戶端」**下，選取要新增一個或多個位置的群組。
3. 在**「政策」**標籤中，取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。

   您只能針對未繼承父群組政策的群組新增位置。

   您也可以按下**「新增位置」**來執行**「新增位置」**精靈。
4. 在**「用戶端」**頁面的**「工作」**下方，按下**「管理位置」**。
5. 在**「管理位置」**對話方塊的**「位置」**下方，按下**「新增」**。
6. 在**「新增位置」**對話方塊中，輸入新位置的名稱和敘述，然後按下**「確定」**。

7 在「**切換至這個位置的狀況**」方塊的右側，按下「**新增**」。

8 在「**類型**」清單中選取條件，然後選取該條件所適用的定義。

若用戶端電腦符合指定的準則，便會切換到該位置。

9 按下「**確定**」。

10 若要新增更多條件，請按下「**新增**」，然後選取**含 AND 關係的準則**」或「**含 OR 關係的準則**」。

11 重複步驟 8 到步驟 9。

12 按下「**確定**」。

請參閱第 201 頁的「管理用戶端群組」。

請參閱第 235 頁的「關於加強遠端用戶端的安全性政策」。

變更預設位置

首次安裝 Symantec Endpoint Protection Manager 時，只有名為「預設值」的單一位置存在。這時，所有群組的預設位置都是「預設值」。每個群組都必須有個預設位置。建立新群組時，Symantec Endpoint Protection Manager 主控台會自動將其預設位置設為「預設值」。

新增其他位置後，您便可指定其他位置作為某群組的預設位置。您或許偏好指定如家裡 (Home) 或出差 (Road) 的位置為預設位置。

如果發生下列情形之一，會使用群組的預設位置：

- 多個位置中有一個符合位置準則，且上一個位置不符合位置準則。
- 您正在使用位置偵測，而所有位置都不符合準則。
- 位置在政策中已重新命名或變更。用戶端接收新政策時會復原為預設位置。

變更預設位置

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面的「**用戶端**」下方，按下要指派不同預設位置的群組。

3 在「**政策**」標籤中，取消勾選「**從父群組 <群組名稱> 繼承政策和設定**」。

4 在「**工作**」下方，按下「**管理位置**」。

5 在「**管理位置**」對話方塊的「**位置**」下，選取要作為預設位置的位置。

6 在「**敘述**」下，勾選「**如果發生衝突則設定此位置為預設位置**」。

在為群組指派另一個位置前，預設位置通常會是預設位置。

7 按下「**確定**」。

請參閱第 226 頁的「管理遠端用戶端的位置」。

設定第一種狀況的位置偵測條件

如果您使用遠端用戶端，在最單純的狀況下，通常是使用 My Company 群組與三個位置。這是第一種狀況。

若要管理這種狀況下的用戶端安全性，您可以在 My Company 群組之下建立下列位置以便使用：

- 登入辦公室的辦公室用戶端。
- 從遠端透過 VPN 登入公司網路的遠端用戶端。
- 從遠端未透過 VPN 登入 Internet 的遠端用戶端。

由於沒有 VPN 連線的遠端位置最不安全，因此會有最安全的政策。最佳實務準則是，請一律將這個位置設為預設位置。

附註：如果您關閉 My Company 群組繼承，然後新增群組，則新增的群組不會繼承您針對 My Company 群組設定的位置。

下列建議是第一種狀況的最佳實務做法。

針對位在辦公室中的用戶端設定辦公室位置

1. 在「**用戶端**」頁面上，選取要新增位置的群組。
2. 在「**政策**」標籤的「**工作**」下方，按下「**新增位置**」。
3. 在「**新增位置精靈**」中，按「**下一步**」。
4. 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「**下一步**」。
5. 在清單方塊中，按下清單中的「**用戶端可以連線到管理伺服器**」，然後按「**下一步**」。
6. 按下「**完成**」，然後按下「**確定**」。
7. 在「**工作**」下方，按下「**管理位置**」，然後選取您建立的位置。
8. 按下「**新增**」，再按下「**含 AND 關係的準則**」。
9. 在「**指定位置條件**」對話方塊的「**類型**」清單中，按下「**網路連線類型**」。
10. 按下「**如果用戶端電腦不使用下方指定的網路連線類型**」。
11. 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下「**確定**」。
12. 按下「**確定**」結束「**管理位置**」對話方塊。

針對透過 VPN 登入的用戶端設定遠端位置

1. 在「**用戶端**」頁面上，選取要新增位置的群組。
2. 在「**政策**」標籤的「**工作**」下方，按下「**新增位置**」。
3. 在「**新增位置精靈**」中，按「**下一步**」。

4 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「**下一步**」。

5 在清單方塊中，按下「**網路連線類型**」。

6 在「**連線類型**」清單方塊中，選取您的組織使用的VPN用戶端名稱，然後按「**下一步**」。

7 按下「**完成**」。

8 按下「**確定**」。

為未透過 VPN 登入的用戶端設定遠端位置

1 在「**用戶端**」頁面上，選取要新增位置的群組。

2 在「**政策**」標籤的「**工作**」下方，按下「**新增位置**」。

3 在「**新增位置精靈**」中，按「**下一步**」。

4 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「**下一步**」。

5 在清單方塊中，保留「**無特定條件**」，然後按「**下一步**」。

使用這些設定之後，此位置的政策會最為嚴格且安全，可作為預設的位置政策。

6 按下「**完成**」，然後按下「**確定**」。

請參閱第 232 頁的「設定第二種狀況的位置偵測條件」。

請參閱第 225 頁的「管理遠端用戶端」。

設定第二種狀況的位置偵測條件

在第二種狀況中，您可以使用第一種狀況中指定的兩個遠端位置，以及兩個辦公室位置，這樣總共有四個位置。

您會新增下列辦公室位置：

- 透過乙太網路連線登入的辦公室用戶端。
- 透過無線連線登入的辦公室用戶端。

這可簡化管理程式，使所有的用戶端處於預設的伺服器控制模式。如果要對使用者進行與不可進行的細部控制，有經驗的管理員可使用混合控制。一般使用者可控制混合控制設定的某些安全性設定，但必要時，您可以覆寫使用者所做的變更。「用戶端控制」讓使用者控制更多項目，但是也相對提高網路安全風險。

賽門鐵克建議您只在下列狀況使用用戶端控制：

- 使用者必須相當瞭解電腦安全性。
- 絕對必要時。

附註：辦公室中的某些用戶端使用乙太網路連線，某些用戶端使用無線連線。因此，程序的最後一項條件設為無線連線。這項條件可供您建立乙太網路位置防火牆政策規則，以在同時使用兩種連線時，攔截所有的無線連線流量。

針對透過乙太網路登入的用戶端設定辦公室位置

1 在「**用戶端**」頁面上，選取要新增位置的群組。

2 在「**工作**」下方，按下「**新增位置**」。

3 在「**新增位置精靈**」中，按「**下一步**」。

4 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「**下一步**」。

5 在清單方塊中，選取「**用戶端可以連線到管理伺服器**」，然後按「**下一步**」。

6 按下「**完成**」。

7 按下「**確定**」。

8 在「**工作**」下方，按下「**管理位置**」，然後選取您建立的位置。

9 在「**切換至這個位置的狀況**」旁，按下「**新增**」，然後選取「**含 AND 關係的準則**」。

10 在「**指定位置條件**」對話方塊的「**類型**」清單中，按下「**網路連線類型**」。

11 按下「**如果用戶端電腦不使用下方指定的網路連線類型**」。

12 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下「**確定**」。

13 按下「**新增**」，再按下「**含 AND 關係的準則**」。

14 在「**指定位置條件**」對話方塊的「**類型**」清單中，按下「**網路連線類型**」。

15 按下「**如果用戶端電腦使用下方指定的網路連線類型**」。

16 在底部清單方塊中，選取「**乙太網路**」，然後按下「**確定**」。

17 按下「**確定**」結束「管理位置」對話方塊。

針對透過無線連線登入的用戶端設定辦公室位置

1 在「**用戶端**」頁面上，選取要新增位置的群組。

2 在「**工作**」下方，按下「**新增位置**」。

3 在「**新增位置精靈**」中，按「**下一步**」。

4 輸入位置的名稱，另外可選擇新增位置的敘述，然後按「**下一步**」。

5 在清單方塊中，按下「**用戶端可以連線到管理伺服器**」，然後按「**下一步**」。

6 按下「**完成**」。

7 按下「**確定**」。

8 在「工作」下方，按下「**管理位置**」，然後選取已建立的位置。

9 在「切換至這個位置的狀況」旁按下**「新增」**，然後按下**「含 AND 關係的準則」**。

10 在**「指定位置條件」**對話方塊的**「類型」**清單中，按下**「網路連線類型」**。

11 按下**「如果用戶端電腦不使用下方指定的網路連線類型」**。

12 在底部清單方塊中，選取您組織使用的 VPN 用戶端名稱，然後按下**「確定」**。

13 按下**「新增」**，再按下**「含 AND 關係的準則」**。

14 在**「指定位置條件」**對話方塊的**「類型」**清單中，按下**「網路連線類型」**。

15 按下**「如果用戶端電腦不使用下方指定的網路連線類型」**。

16 在底部清單方塊中，按下**「乙太網路」**，然後按下**「確定」**。

17 按下**「新增」**，再按下**「含 AND 關係的準則」**。

18 在**「指定位置條件」**對話方塊的**「類型」**清單中，按下**「網路連線類型」**。

19 按下**「如果用戶端電腦使用下方指定的網路連線類型」**。

20 在底部清單方塊中，按下**「無線」**，然後按下**「確定」**。

21 按下**「確定」**結束**「管理位置」**對話方塊。

請參閱第 231 頁的「設定第一種狀況的位置偵測條件」。

請參閱第 225 頁的「管理遠端用戶端」。

架構位置的通訊設定

預設情況下，您可以在群組層級架構管理伺服器與用戶端之間的通訊設定。但是，您也可以為群組中的各個位置架構這些設定。例如，對於用戶端電腦透過 VPN 進行連線的位置，您可以使用個別的管理伺服器。若要將同時連線至管理伺服器的用戶端數目降至最低，您可以針對各個位置指定不同的活動訊號。

您可以針對位置架構下列通訊設定：

- 用戶端執行所用的控制模式。
- 用戶端使用的管理伺服器清單。
- 用戶端執行所用的下載模式。
- 是否要收集在用戶端上執行的全部應用程式的清單，並將此清單傳送到管理伺服器。
- 用戶端進行下載的活動訊號間隔時間。
- 管理伺服器是否會隨機從預設管理伺服器或群組更新提供者下載內容。

附註：這些設定中只有一部分可以針對 Mac 用戶端進行架構。

架構位置的通訊設定

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面上，選取群組。

3 在「**政策**」標籤的「**位置限定的政策與設定**」下，展開某位置下方的「**位置限定的設定**」。

4 在「**通訊設定**」右邊，按下「**工作**」，然後取消勾選「**使用群組通訊設定**」。

5 再次按下「**工作**」，然後按下「**編輯設定**」。

6 在「**<位置名稱> 的通訊設定**」對話方塊中，僅修改指定位置的設定。

7 按下「**確定**」。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

請參閱第 226 頁的「管理遠端用戶端的位置」。

請參閱第 201 頁的「管理用戶端群組」。

關於加強遠端用戶端的安全性政策

當您管理遠端使用者時，基本上會採取下列其中一種方式：

- 保留預設政策，以免妨礙遠端使用者使用電腦。
- 加強預設安全性政策，以進一步保護網路，即使這會限制遠端使用者可執行的動作。

在大多數情況下，最佳實務是加強遠端用戶端的安全性政策。

您可以建立共用或非共用政策，然後將政策指派給群組或位置。共用政策是套用到任何群組和位置的政策，而且可以繼承。非共用政策則是套用到群組中特定位置的政策。一般來說，最佳實務是建立共用政策，因為這可以方便變更多個群組和位置的政策。但是，當您需要建立特定位置專屬的政策，就需要建立非共用政策，或將政策轉換為非共用政策。

請參閱第 225 頁的「管理遠端用戶端」。

針對遠端用戶端之防火牆政策設定的最佳實務準則

表 12-3 說明了一些範例和最佳實務建議。

表 12-3 防火牆政策最佳實務

範例	建議
使用者不使用 VPN 進行登入的遠端位置	■ 將最嚴格的安全政策指派給不使用 VPN 進行遠端登入的用戶端。 ■ 啟用 NetBIOS 防護。 **附註：**對於遠端用戶端透過 VPN 登入公司網路的位置，請勿啟用 NetBIOS 防護。此規則僅適用於遠端使用者連線到網際網路的狀況，不適用於連線到公司網路的狀況。 ■ 為提升安全性，攔截 NetBIOS 通訊埠 135、139 及 445 上的所有本機 TCP 流量。
使用者透過 VPN 登入的遠端位置	■ 維持各項攔截所有配接卡上流量的規則。請勿變更這些規則。 ■ 維持各項允許所有配接卡上 VPN 流量的規則。請勿變更此規則。 ■ 對於各項使用「允許」動作的規則，請將「配接卡」欄的「全部配接卡」變更為您使用的 VPN 配接卡名稱。 ■ 啟用攔截其他所有流量的規則。 **附註：**如果要避免透過 VPN 分割通道，您需要進行所有上述變更。
使用者透過乙太網路或無線連線登入的辦公室位置	使用您的預設防火牆政策。對於無線連線，請確定已啟用允許無線 EAPOL 的規則。802.1x 會使用 LAN 延伸驗證通訊協定 (EAPOL) 進行連線驗證。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 320 頁的「為網路服務啟用通訊而非新增規則」。

關於開啟遠端用戶端的通知

對於未透過 VPN 登入的遠端用戶端，最好在下列狀況開啟用戶端通知：

- 入侵偵測
  您可以使用特定位置的伺服器開啟這些通知，也可以在**「用戶端使用者介面控制設定」**中選取**「混合控制」**。您可以在**「用戶端使用者介面設定」**標籤上自訂此設定。
- 病毒和安全風險
  您可以在「病毒和間諜軟體防護」政策開啟這些通知。

當您開啟這些通知，出現安全性問題時，會通知遠端使用者。

請參閱第 225 頁的「管理遠端用戶端」。

關於從管理伺服器監控遠端用戶端

通知和日誌是維護安全環境所不可或缺的。一般來說，監控遠端用戶端的方式應與監控其他用戶端的方式相同。您應隨時檢查防護是否為最新，而且網路目前未受到攻擊。如果網路遭受攻擊，那麼需要找出是誰發出攻擊以及攻擊的方式。

首頁的喜好設定會決定 Symantec Endpoint Protection Manager 顯示資料的期間。根據預設，首頁上的資料僅表示過去 12 小時內連線的用戶端。如果有許多用戶端經常離線，最佳的監控方式是查看日誌和報告。在日誌和報告中，您可以過濾資料，只包含離線用戶端。

即使您限制了行動用戶端可以上傳的部分用戶端日誌資料，還是可以檢查下列顯示畫面。

表 12-4 監控遠端用戶端安全性的顯示畫面

顯示畫面	說明
首頁 > 端點狀態	顯示內容是否最新，或檢視是否有任何防護已關閉。 您可以檢查下列狀態條件： ■ 內容日期和版本號碼 ■ 用戶端連線 ■ 已啟用和已停用的防護 您可以按下**「詳細資料」**，檢視各用戶端的狀態。
首頁 > 安全狀態	顯示系統安全性概觀。檢視**「病毒和風險活動摘要」**，查看網路是否受到攻擊。 您可以按下**「詳細資料」**，檢視各安全防護技術的狀態。
首頁 > 病毒和風險活動摘要	顯示偵測到的病毒和風險活動，以及採取的動作，如已清除、已攔截或已隔離。
監視器 > 摘要類型 > 網路威脅防護	顯示攻擊類型和來源的相關資訊。

請參閱第 225 頁的「管理遠端用戶端」。

請參閱第 237 頁的「從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端」。

從雲端主控台監控漫遊 Symantec Endpoint Protection 用戶端

漫遊 Symantec Endpoint Protection 用戶端是偶爾連線至管理伺服器的用戶端。漫遊用戶端會在風險較高的其他位置存取 Internet，例如機場、旅館或其他公司。Symantec Endpoint Protection Manager 可使用位置偵測對這些用戶端電腦提供網路內和網路外防護。

在 14.1 及更早版本中，漫遊用戶端僅在連線時將嚴重事件傳送至管理伺服器。自 14.2 版起，如果漫遊用戶端無法連線至管理伺服器，用戶端會自動將嚴重事件傳送至雲端主控台。漫遊用戶端重新連線至管理伺服器後，會傳送管理伺服器上任何新的重大事件。此外，不會再將此用戶端視為漫遊用戶端。

使用嚴重事件清單作為加強 Symantec Endpoint Protection Manager 安全政策的方式。例如，假設當 Employee1 位於特定旅館時，Employee1 的用戶端會遭受更多的阻斷服務攻擊。因此，您可以建立該旅館的位置，並在防火牆政策中啟用阻斷服務偵測。

雲端主控台顯示的嚴重事件有哪些？

請參閱第 236 頁的「關於從管理伺服器監控遠端用戶端」。

Endpoint Protection 的位置偵測最佳實務準則

尋找漫遊用戶端和嚴重事件

若要找出漫遊的用戶端，請尋找下列項目：

- 裝置是否直接連線到雲端主控台而非管理伺服器。
- Symantec Endpoint Protection Manager 位置偵測政策中所定義的位置
- 用戶端的外部 IP 位址。

尋找漫遊用戶端和嚴重事件

1. 在雲端主控台中，移至**「警示和事件」**。
2. 在**「安全事件」**標籤上的**「連線類型」**下方，按下**「雲端」**以顯示用戶端傳送至雲端主控台的事件。

   若要顯示管理伺服器傳送的事件，請按下 **Symantec Endpoint Protection Manager**。
3. 在**「嚴重性」**下方，按下**「嚴重」**。

   雲端主控台僅過濾和顯示漫遊用戶端偵測到的嚴重安全事件。
4. 若要尋找位置和外部 IP 位址，請選取該裝置並尋找裝置位置項目。

雲端主控台顯示的嚴重事件有哪些？

漫遊用戶端將下列安全事件上傳到雲端主控台：

- 通訊埠掃描事件
- Mac 詐騙
- 阻斷服務
- 卡納里群島
- IPS
- 欺敵
- 記憶體攻擊緩和
- 主機完整性合規

漫遊用戶端將下列安全事件上傳到雲端主控台：

- 防毒
- SONAR

13

管理管理員帳戶和密碼

本章包含以下主題：

管理管理員帳戶

您可以使用管理員帳戶管理 Symantec Endpoint Protection Manager 資料中心。管理員可登入 Symantec Endpoint Protection Manager 來變更政策設定、管理群組、執行報告、安裝用戶端軟體以及執行其他管理工作。

預設帳戶是系統管理員帳戶，可供存取所有功能。您也可以針對需要執行一部分工作的管理員，新增有較多限制的管理員帳戶。

針對小公司，您可能只需要一個管理員和一個網域。如果大公司擁有多個站台和 Windows 網域，則很可能需要多個管理員，某些管理員比其他人擁有更多的存取權。您可能也需要在 Symantec Endpoint Protection Manager 中新增多個網域。

您可以在**「管理員」**頁面上管理網域和管理員帳戶及其密碼。

表 13-1 帳戶管理

工作	敘述
決定是否新增多個網域	決定是否新增網域。 請參閱第 263 頁的「關於網域」。 請參閱第 264 頁的「新增網域」。 請參閱第 265 頁的「切換至目前的網域」。
新增管理員帳戶	針對需要存取 Symantec Endpoint Protection Manager 主控台的管理員新增帳戶。 **1** 新增所需的管理員帳戶類型和存取權限層級。 請參閱第 241 頁的「關於管理員帳戶和存取權限」。 請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。 **2** 選擇在管理員登入 Symantec Endpoint Protection Manager 時進行驗證的方法 (選擇性)。依據預設，Symantec Endpoint Protection Manager 資料庫會驗證管理員的憑證。 請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。
解除鎖定或鎖定管理員帳戶	根據預設，在使用者嘗試使用管理員帳戶登入 Symantec Endpoint Protection Manager 太多次後，Symantec Endpoint Protection Manager 會鎖定管理員。您可以架構這些設定，增加鎖定管理員的嘗試次數或時間。 如果管理員的帳戶遭到鎖定，則必須等待指定的時間，然後再次登入。鎖定時間間隔內，您無法解除鎖定帳戶。 請參閱第 260 頁的「在嘗試太多次登入後解除鎖定管理員的帳戶」。
變更並重設遺失密碼	■ 變更您的帳戶密碼或其他管理員的帳戶密碼。 請參閱第 254 頁的「變更管理員帳戶或內嵌資料庫的密碼」。 ■ 使用出現在管理伺服器登入畫面上的**「忘記了您的密碼?」**連結重設遺失密碼。管理員會收到包含用於啟用暫時密碼的連結的電子郵件。 請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。 請參閱第 256 頁的「顯示「忘記了您的密碼?」連結，以便管理員可以重設遺失密碼」。 ■ 允許管理員在管理伺服器登入畫面上儲存他們的使用者名稱和密碼。 請參閱第 259 頁的「在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊」。 ■ 強制管理員的登入密碼在一定天數後到期。 請參閱第 259 頁的「在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊」。

工作	敘述
為 Symantec Endpoint Protection Manager 架構登入選項	您可以為每種管理員類型架構下列登入選項： ■ 顯示管理員要在登入前閱讀的訊息。 請參閱第 258 頁的「在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息」。 ■ 允許或攔截管理主控台的登入存取，以限制某些管理員是否能夠從遠端登入。 請參閱第 259 頁的「授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取」。 ■ 變更管理員可保持登入管理伺服器的期限。 請參閱第 261 頁的「變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間」。 請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

關於管理員帳戶和存取權限

安裝 Symantec Endpoint Protection Manager 時，會建立一個名為 admin 的預設系統管理員帳戶。該系統管理員帳戶可讓管理員存取 Symantec Endpoint Protection Manager 中的所有功能。

您可以新增其他系統管理員帳戶、網域管理員帳戶與限制的管理員帳戶，協助您管理安全性。網域管理員與限制的管理員可存取 Symantec Endpoint Protection Manager 的部分功能。

您可根據公司需要的角色類型與存取權選擇所需的帳戶。例如，大公司可能會使用下列角色類型：

- 安裝管理伺服器和用戶端安裝套件的管理員。安裝產品後，負責接管作業的管理員。這些管理員很可能是系統管理員。
- 作業管理員，維護伺服器、資料庫，和安裝修正程式。如果您具有單一網域，作業管理員可以是獲得完全授權來管理站台的網域管理員。
- 防毒管理員，在用戶端上建立和管理「病毒和間諜軟體防護」政策和 LiveUpdate 政策。此管理員很可能是限制的管理員。
- 桌面管理員，負責用戶端安全和為用戶端建立、維護「防火牆」政策和「入侵預防」政策。此管理員很可能是網域管理員。
- 服務台管理員，建立報告，和擁有政策唯讀存取權。防毒管理員和桌面管理員會讀取服務台管理員傳送的報告。服務台管理員很可能是獲得報告權限和政策權限的限制的管理員。

表 13-2　　管理員角色與責任

管理員角色	責任
系統管理員	系統管理員可以登入 Symantec Endpoint Protection Manager 主控台，且擁有對所有功能與工作的完整不受限制的存取權。 系統管理員可以建立並管理其他系統管理員帳戶、網域管理員帳戶與限制的管理員帳戶。 系統管理員可以執行下列工作： ■ 管理所有網域。 ■ 管理授權。 ■ 檢視和管理所有主控台設定。 ■ 管理資料庫和管理伺服器。
管理員	管理員是可檢視並管理單一網域的網域管理員。網域管理員具有與系統管理員一樣的權限，但僅限單一網域。 依預設，網域管理員具有管理網域 (而非站台) 的完整系統管理員權限。您必須明確地授予單一網域內的站台權限。雖然網域管理員無法修改自己的站台權限，但可以修改其他管理員與限制的管理員的站台權限。 網域管理員可以執行下列工作： ■ 建立和管理單一網域內的管理員帳戶和限制的管理員帳戶。 網域管理員無法修改自己的站台權限。此功能必須由系統管理員執行。 ■ 執行報告、管理站台及重設密碼。 ■ 無法管理授權。只有系統管理員可以管理授權。 請參閱第 263 頁的「關於網域」。
限制的管理員	限制的管理員可以有限的存取權登入 Symantec Endpoint Protection Manager 主控台。根據預設，限制的管理員沒有存取權。系統管理員角色必須明確地授予可讓限制的管理員執行工作的存取權。 當您限制存取權限時，部分管理伺服器使用者介面無法供限制的管理員使用。例如： ■ 不具報告權限的限制管理員無法檢視**「首頁」**、**「監視器」**或**「報告」**頁面。 ■ 不具政策權限的限制管理員無法檢視或修改政策。此外，他們也不能套用、取代或撤銷政策。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。
請參閱第 239 頁的「管理管理員帳戶」。

新增管理員帳戶和設定存取權限

系統管理員可以新增其他系統管理員、管理員或限制的管理員。網域內的管理員可以新增存取權限與自己相當或較不受限制的其他管理員。 管理員可以新增限制的管理員並架構其存取權限。

新增管理員帳戶

1 在主控台中，按下「**管理員**」>「**管理員**」。

2 在「**工作**」下，按下「**新增管理員**」。

3 在「**新增管理員**」對話方塊的「**一般**」標籤中，輸入使用者名稱和電子郵件地址。

4 在「**存取權限**」標籤上，指定管理員帳戶的類型。

如果您新增限制的管理員帳戶，也必須指定管理員的存取權限。未被授予任何存取權限的限制管理員帳戶是在停用狀態下建立的，且限制的管理員無法登入管理伺服器。

請參閱第 241 頁的「關於管理員帳戶和存取權限」。

5 在「**驗證**」標籤的「**Symantec Endpoint Protection Manager 驗證**」下，輸入管理員用來登入的密碼。

當管理員登入 Symantec Endpoint Protection Manager 時，Symantec Endpoint Protection Manager 會使用資料庫驗證使用者名稱與密碼是否正確。

請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。

6 按下「**確定**」。

選擇管理員帳戶的驗證方法

您可以從管理伺服器在登入前，用來檢查管理員憑證的多個驗證方法中進行選擇。

若為第三方驗證方法，Symantec Endpoint Protection Manager 在資料庫中會有管理員帳戶的相關項目，但由第三方伺服器來驗證使用者名稱與密碼。

表 13-3 驗證方法

類型	使用時機
Symantec Endpoint Protection Manager 驗證 (預設)	透過儲存在 Symantec Endpoint Protection Manager 資料庫中的管理員使用者名稱和密碼，來驗證管理員。當管理員登入管理伺服器時，管理伺服器會使用資料庫驗證使用者名稱與密碼是否正確。 您可以顯示「**密碼永久有效**」選項，這樣一來管理員的帳戶將不會過期。 請參閱第 257 頁的「使 Symantec Endpoint Protection Manager 登入密碼永久有效」。
雙因素驗證	使用智慧型手機上的 Symantec VIP 驗證來驗證管理員。管理員在登入時除了提供密碼，還必須提供一次性的唯一驗證碼。 為了讓此選項可供使用，您必須先新增適當的 PKCS 金鑰儲存區檔案和金鑰儲存區的密碼。 請參閱第 247 頁的「使用 Symantec VIP 架構雙因素驗證」。

類型	使用時機
RSA SecurID 驗證	使用 RSA SecurID Token (而非軟體 RSA Token)、RSA SecurID 卡或 RSA 鍵台卡 (而非 RSA 智慧卡)，驗證管理員。 若要驗證使用 RSA SecurID 機制的管理員，請先安裝 RSA Authentication Manager 伺服器，並啟用 RSA SecurID 加密驗證。 請參閱第 245 頁的「搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證」。
目錄伺服器驗證	使用 LDAP 伺服器或 Microsoft Active Directory 伺服器驗證管理員。 若要使用 Active Directory 或 LDAP 目錄伺服器驗證管理員，您需要在目錄伺服器上設定帳戶。 您還必須建立目錄伺服器與 Symantec Endpoint Protection Manager 之間的連線。 如果您沒有建立連線，便無法從 Active Directory 伺服器匯入使用者，也無法與它們進行同步處理。 **附註：**同步處理僅適用於 Active Directory 伺服器。不支援與 LDAP 伺服器進行同步處理。 請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。 請參閱第 250 頁的「檢查目錄伺服器驗證」。
智慧卡驗證	驗證在美國聯邦機構以平民或軍事人員身分工作且必須使用 PIV 卡或 CAC 登入的管理員。 請參閱第 248 頁的「架構 Symantec Endpoint Protection Manager 以驗證使用智慧卡登入的管理員」。

選擇管理員帳戶的驗證方法

1. 新增管理員帳戶。

   請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

2. 在**「驗證」**標籤上，如果您不想使用**「Symantec Endpoint Protection Manager 驗證」**(預設)，則選取驗證方法。
3. 按下**「確定」**。
4. 在**「確認變更」**對話方塊中，輸入您用來登入 Symantec Endpoint Protection Manager 的密碼，然後按下**「確定」**。

   在切換驗證方法時，必須輸入管理員帳戶的密碼。

搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證

附註：在 IPv6 環境中，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝並啟用 IPv4 堆疊以使用 RSA SecurID 驗證。

架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員

如果您要使用 RSA SecurID 驗證使用 Symantec Endpoint Protection Manager 的管理員，必須先架構與 RSA Authentication Manager 伺服器的連線來啟用加密的驗證。

架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員

1. 必要時，安裝 RSA Authentication Manager 伺服器。使用 RSA Authentication Manager 8.1。
2. 在 Symantec Endpoint Protection Manager 伺服器上安裝並適當架構 RSA Authentication Agent，以連線至 RSA 伺服器。使用 RSA Authentication Agent 7.x。

   請參閱第 245 頁的"架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員"。
3. 確保 Symantec Endpoint Protection Manager 伺服器在 RSA Authentication Manager 伺服器上註冊為有效的主機。
4. 確定可以在網路上存取 RSA Authentication Manager 伺服器上的 `sdconf.rec` 檔案。
5. 將同步化的 SecurID 卡或密鑰卡指派給管理伺服器帳戶；在 RSA Authentication Manager 伺服器上啟用登入名稱。
6. 確保管理員有可使用的 RSA PIN 或密碼。

賽門鐵克支援下列的 RSA 登入類型：

- RSA SecurID Token (非軟體 RSA Token)
- RSA SecurID 卡
- RSA 鍵台卡 (非 RSA 智慧卡)

若要以 RSA SecurID 登入管理伺服器，管理員需有登入名稱、Token (硬體) 和 PIN。

安裝 RSA Authentication Agent 並將 Symantec Endpoint Protection Manager 伺服器架構為使用 RSA SecurID 驗證

若要搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID，您必須在 Symantec Endpoint Protection Manager 伺服器上安裝 RSA Authentication Agent，並將其架構為 SecurID 驗證用戶端。

安裝 RSA Authentication Agent

1 在 Symantec Endpoint Protection Manager 伺服器上安裝 RSA Authentication Agent 的軟體。您可以從 RSA Authentication Agent 安裝檔案或 CD 執行 Windows .msi 檔案來安裝軟體。

2 將 `sdconf.rec` 檔案從 RSA Authentication 伺服器複製到 Symantec Endpoint Protection Manager 伺服器。

若為舊版 RSA Authentication Agent，請複製 `nodesecret.rec`、`sdconf.rec` 和 `agent_nsload.exe`。

架構 Symantec Endpoint Protection Manager 伺服器使用 RSA SecurID 驗證

1 登入 Symantec Endpoint Protection Manager 主控台，然後按下**「管理員」>「伺服器」**。

2 在**「伺服器」**下方的**「本機站台」**下，按下管理伺服器。

3 在**「工作」**下，按下**「架構 SecurID 驗證」**。

4 在**「歡迎使用架構 SecurID 驗證精靈」**畫面中，按**「下一步」**。

5 在**「架構 SecurID 驗證精靈」**的**「資格」**畫面中，閱讀先決條件，並確認符合所有要求。

6 按**「下一步」**。

7 在**「架構 SecurID 驗證精靈」**的**「上傳 RSA 檔案」**畫面中，瀏覽尋找 sdconf.rec 檔案所在的資料夾。

您也可以鍵入路徑名稱。

8 按**「下一步」**，然後按下**「測試」**來測試您的架構。

9 在**「測試架構」**對話方塊中，鍵入 SecurID 的使用者名稱和密碼，然後按下**「測試」**。

現在已成功驗證。

新增使用 RSA SecurID 驗證的 Symantec Endpoint Protection Manager 管理員

新增使用 RSA SecurID 驗證的 Symantec Endpoint Protection Manager 管理員

1 新增管理員帳戶。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

2 在**「驗證」**標籤上，按下「RSA SecurID 驗證」。

如果無法使用此選項，請參閱架構準則。

請參閱第 245 頁的"架構 RSA SecurID 驗證 Symantec Endpoint Protection Manager 管理員"。

3 按下**「確定」**。

您也可以將現有管理員帳戶變更為使用 RSA SecurID 驗證，不過並不建議採取這種做法，尤其是預設管理員帳戶 admin。如果您在編輯現有使用者時提供了無效的資訊，則會較難復原該使用者。

不過，如果要修改現有管理員帳戶，請在**「確認變更」**對話方塊中，輸入您用來登入 Symantec Endpoint Protection Manager 的密碼，然後按下**「確定」**。

在切換驗證方法時，必須輸入管理員帳戶的密碼。

請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。

使用 Symantec VIP 架構雙因素驗證

如果您的環境中使用 Symantec VIP 雙因素驗證，您可以將 Symantec Endpoint Protection Manager 管理員架構為向其進行驗證。

雙因素驗證可為登入程序的安全增添多一層保護。如果啟用雙因素驗證，您在登入時除了提供密碼，還必須提供唯一的一次性驗證碼。您可以透過語音、文字或使用免費的 Symantec VIP Access 應用程式收到此驗證碼。建議您使用此應用程式，因為它最安全且方便易用。如需 Symantec VIP 的快速總覽，請參閱：

Symantec VIP：讓所有人輕鬆進行企業級驗證

您可以針對使用 Symantec Endpoint Protection Manager 驗證的每一個個別管理員管理個別的雙因素驗證設定。使用 RSA SecurID 或目錄驗證進行驗證的管理員無法使用雙因素驗證。

附註：透過 IPv6 或在啟用 FIPS 的環境中，不支援雙因素驗證。

架構 Symantec Endpoint Protection Manager 以使用 Symantec VIP 進行雙因素驗證

1. 在主控台中，按下**「管理員」>「伺服器」**，然後再按下本機伺服器名稱。
2. 在**「工作」**下方，按下**「架構 VIP 驗證」**。
3. 瀏覽至 PKCS 金鑰儲存區檔案加以選取，輸入金鑰儲存區的密碼，然後按下**「確定」**。

   憑證會自動傳播至同一網站中的其他 Symantec Endpoint Protection Manager 主控台，而不需要遠端複製。您不需要手動將憑證新增到網站上的每個 Symantec Endpoint Protection Manager。

   若要將憑證傳播至其他網站上的 Symantec Endpoint Protection Manager，這些網站必須是遠端複製夥伴。

架構管理員以使用 Symantec VIP 進行雙因素驗證

1 請確認 Symantec Endpoint Protection Manager 管理員在 Symantec VIP Manager 上具有包括大小寫在內，完全相符的對應使用者名稱。這兩個使用者名稱的密碼不一定要相符。

請參閱 Symantec VIP Manager 說明文件，以瞭解如何架構使用者名稱。

Symantec VIP Access Manager 3.0 管理指南

2 在主控台中，按下**「管理員」>「伺服器」>「管理員」**。

3 選取現有的管理員，然後按下**「編輯管理員」**。

您也可以新增管理員以進行架構。

4 在**「驗證」**標籤上，按下**「使用 VIP 啟用雙因素驗證」**。

架構 Symantec Endpoint Protection Manager 以驗證使用智慧卡登入的管理員

自版本 14.2 起，在美國聯邦機構工作的管理員可以使用智慧卡登入 Symantec Endpoint Protection Manager。

若要設定智慧卡驗證，管理員需要執行下列步驟：

步驟 1：針對智慧卡驗證架構 Symantec Endpoint Protection Manager

步驟 3：新增管理員帳戶並註冊智慧卡

步驟 3：新增管理員帳戶並註冊智慧卡

步驟 4：使用智慧卡登入 Symantec Endpoint Protection Manager

關於智慧卡

美國聯邦機構現在針對 HSPD-12 需求使用允許智慧卡驗證的軟體系統。美國聯邦智慧卡包含將被授予聯邦機構和資訊系統存取權的持卡人的必要資料。此存取權可確保所有適用的聯邦應用程式享有適當的安全層級。

某些 Windows 用戶端電腦或工作站的鍵盤中已內建 PIV 或 CAC 讀取裝置。

Symantec Endpoint Protection Manager 會驗證使用下列類型智慧卡的管理員：

- 個人身分驗證 (PIV) 卡 (適用於平民)
- 通用存取卡 (CAC) (適用於軍事人員)
- 在 FIPS 模式下：Symantec Endpoint Protection Manager 不支援使用 ECDSA 和 RSASSA-PSS 簽署的智慧卡。
- 在非 FIPS 模式下：Symantec Endpoint Protection Manager 不支援使用 RSASSA-PSS 簽署的智慧卡。

請參閱：HSPD-12

步驟 1：針對智慧卡驗證架構 Symantec Endpoint Protection Manager

此步驟會驗證由正確授權中心核發的卡憑證。之後，在管理員登入時，管理伺服器讀取智慧卡的憑證，並對照這些 CA 憑證進行驗證。

若要驗證憑證檔案，管理伺服器會確認此憑證檔案是否未列於 Internet 上的憑證撤銷清單 (CRL) 中。

請確定所有根檔案和中間檔案皆位於管理員的電腦上，否則他們無法登入。

針對智慧卡驗證架構 Symantec Endpoint Protection Manager

1. 在主控台中，按下**「管理員」>「伺服器」**，然後選取本機管理伺服器名稱。
2. 在**「工作」**下，按下**「架構智慧卡驗證」**。
3. 在**「指定根憑證檔案及 (或) 中間憑證檔案的路徑」**文字方塊中，瀏覽至一或多個憑證檔案，然後按下**「確定」**。

   選取需要檢查是否撤銷的所有憑證檔案。若要選取多個檔案，請按下 **Ctrl**。

   附註：選擇性：如果管理員登入的管理伺服器無法存取 Internet，請在**「指定憑證撤銷清單的路徑」**文字方塊中新增 .crl 或 .pem 檔案。還必須在這些管理伺服器上執行下列工作。步驟 2 (選擇性)：將管理伺服器架構為執行撤銷檢查 (暗網所需)

4. 按下**「確定」**。
5. 如果管理員使用 Web 主控台遠端登入 Symantec Endpoint Protection Manager，則必須重新啟動 Symantec Endpoint Protection Manager 服務與 Symantec Endpoint Protection Manager Web 服務。

   請參閱第 128 頁的「停止及啟動管理伺服器服務」。

步驟 2 (選擇性)：將管理伺服器架構為執行撤銷檢查 (暗網所需)

如果管理伺服器沒有 Internet 存取權，您必須將其架構為改成檢查管理伺服器電腦上的 CRL 檔案。如果未執行此檢查，管理員仍可登入，但管理伺服器無法檢查 CRL 檔案，可能會導致安全問題。

將管理伺服器架構為執行撤銷檢查 (僅限暗網)

1. 在此管理伺服器上，開啟下列檔案：*`Symantec Endpoint Protection Manager 安裝路徑`*\tomcat\etc\conf.properties
2. 在 `conf.properties` 檔案中新增 **smartcard.cert.revocation.ocsp.crldp.enabled=false** 並儲存檔案。
3. 重新啟動管理伺服器服務。

   請參閱第 128 頁的「停止及啟動管理伺服器服務」。

步驟 3：新增管理員帳戶並註冊智慧卡

此步驟透過設定 PIV 驗證，將管理員驗證為智慧卡的使用者。PIV 驗證需要用來確認 PIV 憑證由授權實體核發的憑證和金鑰組尚未到期，且未遭到撤銷。PIV 憑證還會識別向其核發相同個別憑證的管理員。

此步驟也可確保使用者只需輸入其使用者名稱、插入卡，然後輸入智慧卡 PIN 即可登入 Symantec Endpoint Protection Manager。他們無需輸入 Symantec Endpoint Protection Manager 密碼。

附註：不支援透過 IPv6 進行智慧卡驗證。

新增管理員帳戶並註冊智慧卡

1. 在主控台中，按下**「管理員」>「伺服器」>「管理員」**。
2. 新增管理員，或編輯現有管理員。

   請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。
3. 在**「驗證」**標籤上，按下 **「啟用智慧卡驗證」**。
4. 瀏覽至該管理員的 PIV 卡或 CAC 的驗證憑證檔案，然後按下**「確定」**。
5. 在**「確認變更」**對話方塊中，輸入管理員的密碼，然後按下**「確定」**。

對於使用智慧卡登入 Symantec Endpoint Protection Manager 的每個管理員，請遵循此步驟。

步驟 4：使用智慧卡登入 Symantec Endpoint Protection Manager

若要登入 Symantec Endpoint Protection Manager，管理員會將卡插入智慧卡讀取裝置，並輸入 PIN 號碼。當智慧卡管理員登入和使用管理伺服器時，必須始終將智慧卡插入讀取裝置。如果管理員移除智慧卡，Symantec Endpoint Protection Manager 會在 30 秒內將管理員登出。

Java 主控台和 Web 主控台支援智慧卡驗證。RMM 主控台和 REST API 不支援智慧卡驗證。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

疑難排解和遠端複製

如果兩個站台彼此遠端複製，則具有最近架構的 CA 檔案的站台會覆寫所有其他站台上的 CA 檔案。

請參閱第 637 頁的"遠端複製如何運作？"。

檢查目錄伺服器驗證

您可以檢查 Active Directory 或 LDAP 伺服器是否驗證您所建立的管理員帳戶的使用者名稱和密碼。此次檢查會評估您新增的使用者名稱和密碼是否正確，以及目錄伺服器上是否存在此帳戶名稱。

您在 Symantec Endpoint Protection Manager 中會與您在目錄伺服器中一樣，為管理員帳戶使用相同的使用者名稱和密碼。當管理員登入管理伺服器時，目錄伺服器會驗證管理員的使用者名稱和密碼。 管理伺服器會使用您所新增的目錄伺服器組態，搜尋目錄伺服器上的帳戶。

您也可以檢查 Active Directory 或 LDAP 伺服器是否會驗證沒有使用者名稱和密碼的管理員帳戶。沒有使用者名稱或密碼的帳戶是匿名存取。您應該使用匿名存取建立一個管理員帳戶，讓管理員永遠不會因為目錄伺服器上的密碼變更而遭到鎖定。

附註：在 Windows 2003 Active Directory 伺服器中，預設會停用匿名驗證。 因此，如果您將沒有使用者名稱的目錄伺服器新增至管理員帳戶，然後按下**「檢查帳戶」**，就會顯示**「帳戶驗證失敗」**錯誤訊息。若要解決這個問題，請建立兩個目錄伺服器項目，一個用於測試，另一個用於匿名存取。管理員仍然可以使用有效的使用者名稱和密碼登入管理伺服器。

表 13-4　測試管理員帳戶的目錄伺服器驗證的步驟

步驟	工作	敘述
步驟 1	新增多個目錄伺服器連線	若要讓測試更容易進行匿名存取，請至少新增兩個目錄伺服器項目。使用其中一個項目測試驗證，另一個項目測試匿名存取。 這些項目全部都使用具有不同組態的相同目錄伺服器。 根據預設，除非移到不同的組織單位，否則多數使用者位於 CN=Users。LDAP 目錄伺服器中的使用者是以 CN=Users、DC=<*sampledomain*>、DC=local 所建立。若要找出使用者在 LDAP 中的位置，請使用 ADSIEdit。 使用下列資訊設定此範例的目錄伺服器： ■ CN=John Smith ■ OU=test ■ DC=<*sampledomain*> ■ DC=local 此範例會使用預設的 Active Directory LDAP (389)，但也可以使用安全 LDAP (636)。
步驟 2	新增多個管理員帳戶	您要新增多個系統管理員帳戶。 匿名存取的帳戶沒有使用者名稱或密碼。 請參閱第 252 頁的「使用目錄伺服器項目新增管理員帳戶」。

新增目錄伺服器連線以檢查 Active Directory 和 LDAP 伺服器驗證

1. 在主控台上，按下**「管理員」**>**「伺服器」**，選取預設伺服器，然後按下**「編輯伺服器屬性」**。
2. 在**「目錄伺服器」**標籤上，按下**「新增」**。
3. 在**「一般」**標籤上，新增下列目錄伺服器組態，然後按下**「確定」**。

   目錄伺服器 1：

   - **名稱:** `<sampledomain> Active Directory`

- **伺服器類型: Active Directory**
- **伺服器 IP 位址或名稱:** server01。<*sampledomain*>.local
- **使用者名稱:** <*sampledomain*>\administrator
- **密碼:** <*directory server password*>

目錄伺服器 2：

- **名稱:**<*sampledomain*> LDAP with User Name
- **伺服器類型: LDAP**
- **伺服器 IP 位址或名稱:** server01。<*sampledomain*>.local
- **LDAP 通訊埠: 389**
- **LDAP BaseDN:** DC=<*sampledomain*>, DC=local
- **使用者名稱:** <*sampledomain*>\administrator
- **密碼:** <*directory server password*>

目錄伺服器 3 (用於匿名驗證)：

- **名稱:** <*sampledomain*> LDAP without User Name
- **伺服器類型: LDAP**
- **伺服器 IP 位址或名稱:** server01。<*sampledomain*>.local
- **LDAP 通訊埠: 389**
- **LDAP BaseDN:** <empty>
  當您使用匿名存取時，請將此欄位留空。
- **使用者名稱:** <empty>
- **密碼:** <empty>
  按下**「確定」**之後，會出現一個警告。但是目錄伺服器是有效的。
  當您嘗試新增沒有使用者名稱和密碼的 BaseDN 時，會出現警告。

使用目錄伺服器項目新增管理員帳戶

1 在主控台上，按下**「管理員」**>**「管理員」**，然後在**「一般」**標籤上，新增步驟 2 中的管理員帳戶。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。

2 在您新增每個管理員帳戶並按下**「檢查帳戶」**選項之後，您會看到一則訊息。在某些情況下，這個訊息似乎會使帳戶資訊無效。 但是，管理員仍然可以登入 Symantec Endpoint Protection Manager。

管理員帳戶 1：

- 在**「一般」**標籤上，輸入下列資訊：
  使用者名稱：john
- **全名:** John Smith
- **電子郵件地址:** john@<*sampledomain*>.local
- 在**「存取權」**標籤上，按下**「系統管理員」**。
- 在**「驗證」**標籤上，按下**「目錄驗證」**。
  在**「目錄伺服器」**下拉式清單中，選取 <*sampledomain*> Active Directory。
  在**「帳戶名稱」**欄位中，輸入 john。
  按下**「檢查帳戶」**。
  系統管理員 john 就可以使用目錄驗證，登入 Symantec Endpoint Protection Manager。

管理員帳戶 2：

- 在**「一般」**標籤上，輸入下列資訊：
- **使用者名稱:** john
- **全名:** John Smith
- **電子郵件地址:** john@<*sampledomain*>.local
- 在**「存取權」**標籤上，按下**「系統管理員」**。
- 在**「驗證」**標籤上，按下**「目錄驗證」**。
  在**「目錄伺服器」**下拉式清單中，選取 <*sampledomain*> LDAP with User Name。
  在**「帳戶名稱」**欄位中，輸入 john。
  按下**「檢查帳戶」**。
  系統管理員 john 無法使用目錄驗證，登入 Symantec Endpoint Protection Manager。

管理員帳戶 3：

- 在**「一般」**標籤上，輸入下列資訊：
- **使用者名稱:** john
- **全名:** John Smith
- **電子郵件地址:** john@<*sampledomain*>.local
- 在**「存取權」**標籤上，按下**「系統管理員」**。
- 在**「驗證」**標籤上，按下**「目錄驗證」**。
  在**「目錄伺服器」**下拉式清單中，選取 <*sampledomain*> LDAP with User Name。
  在**「帳戶名稱」**欄位中，輸入 John Smith。
  按下**「檢查帳戶」**。
  系統管理員 john 可以使用目錄驗證，登入 Symantec Endpoint Protection Manager。

管理員帳戶 4 (用於匿名存取)：

- 在「**一般**」標籤上，輸入下列資訊：
- **使用者名稱:** `john`
- **全名:** `John Smith`
- **電子郵件地址:** `john@<sampledomain>.local`
- 在「**存取權**」標籤上，按下「**系統管理員**」。
- 在「**驗證**」標籤上，按下「**目錄驗證**」。
  在「**目錄伺服器**」下拉式清單中，選取 `<sampledomain> LDAP without User Name`。
  在「**帳戶名稱**」欄位中，輸入 `John Smith`。
  按下「**檢查帳戶**」。
  帳戶驗證失敗，但是系統管理員 `John Smith` 可以登入 Symantec Endpoint Protection Manager。

請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。

變更管理員帳戶或內嵌資料庫的密碼

變更管理員帳戶的密碼

如果密碼已忘記、遺失或遭受破壞，您需要變更您的帳戶或其他管理員帳戶的密碼。

變更密碼時適用下列規則：

- 系統管理員可以變更所有管理員的密碼。
- 網域管理員可以變更同一個網域中其他網域管理員和限制的管理員的密碼。
- 限制的管理員只能變更自己的密碼。

如果變更密碼是為了解決管理員帳戶鎖定問題，管理員仍必須等到鎖定期結束。

附註：密碼必須包含至少 8 個字元且少於 16 個字元。它必須包含至少一個小寫字母 [a-z]、一個大寫字母 [A-Z]、一個數字字元 [0-9]，以及一個特殊字元 ["/ \ [ ] : ; | = , + * ? < >]。

請參閱第 260 頁的「在嘗試太多次登入後解除鎖定管理員的帳戶」。

變更管理員帳戶的密碼

1. 在主控台中，按下「**管理員**」>「**管理員**」。
2. 在「**管理員**」下方，選取管理員帳戶，再按下「**變更密碼**」。
   按 `F1`，查看密碼限制。
3. 輸入您的密碼和管理員的新密碼。
4. 按下「**變更**」。

請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。

請參閱第 256 頁的「顯示「忘記了您的密碼?」連結，以便管理員可以重設遺失密碼」。

變更內嵌資料庫密碼

如果架構管理伺服器時選取內嵌式資料庫，輸入的預設管理員帳戶 admin 密碼也會成為資料庫密碼。如果您變更預設管理員的密碼，資料庫密碼並不會自動變更。自 14 起，透過重新執行「管理伺服器組態精靈」並重新架構 Symantec Endpoint Protection Manager，您可以變更資料庫密碼。

變更內嵌資料庫密碼

1. 在 Windows 的**「開始」**功能表上，瀏覽到 **Symantec Endpoint Protection Manager** > **「Symantec Endpoint Protection Manager 工具」**>**「管理伺服器組態精靈」**。
2. 按下**「重新架構管理伺服器」**，然後按**「下一步」**>**「下一步」**。

   請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。
3. 按下**「預設內嵌資料庫」**>**「變更資料庫管理員密碼」**，然後輸入新密碼。
4. 遵循每個面板的指示來完成架構

Symantec Endpoint Protection Manager 密碼遺失後重設

如果您有系統管理員帳戶，您可以重設自己的密碼並允許其他管理員重設他們自己的密碼。

要重設遺失的密碼，請確定啟用了以下項目：

- 管理員可以重設自己的密碼。
  請參閱第 256 頁的「顯示「忘記了您的密碼?」連結，以便管理員可以重設遺失密碼」。
- **「忘記了您的密碼?」**連結已設為出現在管理伺服器登入畫面上。依據預設，會出現此連結。
  請參閱第 259 頁的「在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊」。
- 必須架構郵件伺服器，以便郵件伺服器傳送通知。
  若要疑難排解 Symantec Endpoint Protection Manager 電子郵件失敗，請參閱在 Endpoint Protection Manager Console 中傳送測試電子郵件訊息失敗。
  請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。

將此方法用於透過使用 Symantec Management Server 驗證進行驗證，而不是透過 RSA SecurID 驗證或目錄驗證進行驗證的管理員帳戶。

附註：密碼必須包含至少 8 個字元且少於 16 個字元。它必須包含至少一個小寫字母 [a-z]、一個大寫字母 [A-Z]、一個數字字元 [0-9]，以及一個特殊字元 ["/ \ [ ] : ; | = , + * ? < >]。

請參閱第 243 頁的「選擇管理員帳戶的驗證方法」。

Symantec Endpoint Protection Manager 密碼遺失後重設

1. 在管理伺服器電腦上，按下**「開始」**>**「所有程式」**> **Symantec Endpoint Protection Manager** > **Symantec Endpoint Protection Manager**。

   依據預設，**「忘記了您的密碼?」**連結出現在管理伺服器登入畫面上。
2. 在**「登入」**畫面上，按下**「忘記了您的密碼?」**。
3. 在**「忘記了密碼」**對話方塊中，輸入要重設密碼的帳戶的使用者名稱。

   對於網域管理員和限制的管理員，輸入帳戶的網域名稱。如果未設定網域，請保留網域欄位空白。
4. 按下**「暫時密碼」**。

   管理員會收到包含用於啟用暫時密碼的連結的電子郵件。管理員每分鐘只能向管理主控台要求暫時密碼一次。由於安全原因，管理伺服器不會驗證輸入資訊。
5. 管理員必須在登入後立即變更暫時密碼。

若要驗證管理員是否順利重設密碼，請檢查管理員收到的電子郵件訊息。

請參閱第 254 頁的「變更管理員帳戶或內嵌資料庫的密碼」。

無法重設密碼時

如果您使用**「忘記了您的密碼?」**功能無法復原管理員密碼，Symantec 也無法協助復原您的密碼。您必須在不使用資料庫備份的情況下重新架構 Symantec Endpoint Protection Manager 和資料庫。此程序會覆寫先前的管理伺服器和資料庫設定，並可讓您重新建立新的密碼。因此，設定管理伺服器和稽核管理員帳戶資訊時正確架構電子郵件設定很重要。

請參閱第 652 頁的「還原資料庫」。

請參閱重新安裝或重新架構 Symantec Endpoint Protection Manager。

顯示「忘記了您的密碼?」連結，以便管理員可以重設遺失密碼

如果您有系統管理員帳戶，您可以讓其他管理員重設其忘記的密碼。啟用**「忘記了您的密碼?」**連結 (位於 Symantec Endpoint Protection Manager 登入畫面)，以便管理員可要求暫時密碼。

允許管理員重設忘記的密碼

1. 在主控台中，按下**「管理員」**。
2. 在**「管理員」**頁面中，按下**「伺服器」**。

3 在「**伺服器**」下方，選取本機站台。

您只能針對本機站台控制此設定。

4 按下「**編輯站台屬性**」。

5 在「**密碼**」標籤上，勾選「**允許管理員重設密碼**」。

6 按下「**確定**」。

請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。

請參閱第 259 頁的「在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊」。

使 Symantec Endpoint Protection Manager 登入密碼永久有效

如果您使用 Symantec Endpoint Protection Manager 驗證，則密碼的預設選項設定為在 60 天後到期。

如果是 12.1.5 及更新版本，您可以顯示選項，供管理員使用永久有效的密碼。此選項預設為停用以增加安全性，因此您必須先啟用它。啟用此選項後，選項會出現在管理員帳戶的「**驗證**」標籤上。

使 Symantec Endpoint Protection Manager 登入密碼永久有效

1 在主控台中，按下「**管理員**」。

2 在「**管理員**」頁面中，按下「**網域**」。

3 在「**網域**」下，選取允許管理員儲存登入認證的網域。

4 按下「**編輯網域屬性**」。

5 在「**密碼**」標籤上，按下「**允許管理員使用永不到期密碼**」。

6 按下「**確定**」。

7 按下「**管理員**」>「**管理員**」，然後開啟管理員帳戶。

8 在「**驗證**」標籤上，按下「**密碼永久有效**」，然後按下「**確定**」。

請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。

請參閱第 260 頁的「在嘗試太多次登入後解除鎖定管理員的帳戶」。

關於接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證

當您安裝 Symantec Endpoint Protection Manager 時，呈現於瀏覽器中的網頁自我簽署憑證會包含在安裝裡。當您第一次從遠端主控台存取這些網頁時，您必須接受自我簽署憑證，才能顯示網頁。

會為每位使用者單獨儲存憑證。每個管理員帳戶都必須為每個連線到管理伺服器的遠端位置接受憑證。

如需將安全憑證新增至網頁瀏覽器的指示，請參閱文章：如何安裝用於 Web 主控台存取的 Endpoint Protection Manager 憑證。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息

您可以建立和顯示所有管理員登入主控台之前會看到的自訂訊息。最主要的用途是向即將登入專屬電腦的管理員顯示法律聲明。

在管理員鍵入其使用者名稱和密碼並按下**「登入」**後，會在主控台中顯示此訊息。管理員閱讀訊息後，他們可以同意聲明的內容並按下**「確定」**，即可登入成為管理員。如果管理員按下**「取消」**，則會取消登入程序，而管理員會回到登入視窗。

如果管理員從連線至管理伺服器的獨立網頁瀏覽器執行報告功能，此訊息也會出現。

在管理員登入 Symantec Endpoint Protection Manager 主控台之前向其顯示訊息

1. 在主控台中，依序按下**「管理員」**和**「網域」**。
2. 選取要為其新增登入橫幅的網域。
3. 在**「工作」**下，按下**「編輯網域屬性」**。
4. 在**「登入橫幅」**標籤上，勾選**「當管理員登入 Symantec Endpoint Protection Manager 時，顯示法律聲明」**。
5. 輸入橫幅標題和文字。

   如需詳細資訊，按下**「說明」**。
6. 按下**「確定」**。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊

系統管理員可啟用**「記住我的使用者名稱」**和**「記住我的密碼」**核取方塊，使其出現在其他管理員帳戶的 Symantec Endpoint Protection Manager 登入畫面上。管理員的使用者名稱和密碼會預先填入登入畫面。

在登入畫面上顯示「記住我的使用者名稱」和「記住我的密碼」核取方塊

1. 在主控台中，按下**「管理員」**。
2. 在**「管理員」**頁面中，按下**「網域」**。
3. 在**「網域」**下，選取允許管理員儲存登入憑證的網域。
4. 按下**「編輯網域屬性」**。
5. 在**「密碼」**標籤上，勾選**「允許使用者在登入時儲存憑證」**。
6. 按下**「確定」**。

請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。

授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取

根據預設，會授予對所有主控台的存取。管理員可以從本機或遠端網路中的任何一台電腦登入主要主控台。

您可以透過拒絕對某些電腦的存取，保護管理主控台不進行遠端連線。

您最好授予或拒絕以下類型的使用者或電腦進行的存取：

- 您應該拒絕 Internet 上任何人進行存取。否則，主控台會面臨 Internet 攻擊的風險。
- 如果受限管理員使用非其管理之網路上的主控台，您應該拒絕他們存取。
- 您應該授予系統管理員和 IT 管理員存取權。
- 您應該授予實驗室電腦 (例如用於測試的電腦) 存取。

除了全域授予或拒絕存取之外，您也可以用 IP 位址指定例外。如果授予存取所有遠端主控台，管理伺服器會拒絕存取例外項目。相反地，如果您拒絕存取所有遠端主控台，那麼將會自動授予存取例外項目。當您建立例外時，指定的電腦必須具有靜態 IP 位址。您也可以指定子網路遮罩，針對電腦群組建立例外。例如，您可能想要在您管理的所有區域中授予存取。不過，您可能會想要拒絕位於公共區域之主控台的存取。

授予或拒絕遠端主控台的存取

1 在主控台中，按下**「管理員」**，再按下**「伺服器」**。

2 在**「伺服器」**下，選取您要變更遠端主控台存取權限的伺服器。

3 在**「工作」**下方，按下**「編輯伺服器屬性」**。

4 在**「一般」**標籤上，按下**「授予存取」**或**「拒絕存取」**。

5 如果您要指定電腦 IP 位址，將其設為此主控台存取權限的例外，請按下**「新增」**。

您新增的電腦成為例外項目。 如果您按下**「授予存取」**，您指定的電腦會被拒絕存取。 如果您按下**「拒絕存取」**，您指定的電腦會被授予存取。 您可以針對單一電腦或電腦群組建立例外。

6 在**「拒絕主控台存取」**對話方塊中，按下列其中一個選項：

- **單一電腦**
  針對單一電腦，輸入 IP 位址。
- **電腦群組**
  對於多台電腦，輸入群組的 IP 位址及子網路遮罩。

7 按下**「確定」**。

此時電腦會出現在例外清單中。會顯示每個 IP 位址與遮罩的權限狀態。

如果您將**「授予存取」**變更為**「拒絕存取」**，或將「拒絕存取」變更為「授予存取」，所有例外也會一併變更。如果您曾經建立拒絕存取的例外，此時會變更為允許存取。

8 按下**「編輯全部」**，變更顯示在例外清單上電腦的 IP 位址或主機名稱。

「IP 位址編輯器」隨即出現。**「IP 位址編輯器」**是一種文字編輯器，可讓您編輯 IP 位址和子網路遮罩。

9 按下**「確定」**。

10 完成新增例外至清單或完成編輯清單後，請按下**「確定」**。

請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

在嘗試太多次登入後解除鎖定管理員的帳戶

Symantec Endpoint Protection Manager 會在管理員嘗試登入失敗達一定次數後，鎖定管理員一段時間。 依預設，管理伺服器會在嘗試失敗 5 次之後鎖定管理員達 15 分鐘的時間。

您必須等指定的時間結束後才能解除鎖定管理員帳戶。 不過，您可以停用管理員帳戶的鎖定，即使此動作不會解除帳戶鎖定。 您也可以變更登入嘗試失敗次數和鎖定帳戶前允許的等待時間。 密碼變更不會重設或影響到鎖定時間間隔。

在 12.1.5 和更新版本中，為提高安全性，第一次鎖定之後，每額外鎖定 1 次都會將鎖定時間間隔加倍。 Symantec Endpoint Protection Manager 在成功登入後或第一次鎖定後的 24 小時之後，會恢復原始的鎖定時間間隔。 例如，如果原始鎖定時間間隔為 15 分鐘，第二次鎖定會觸發 30 分鐘的鎖定時間間隔。 第三次鎖定則會觸發 60 分鐘的鎖定時間間隔。 如果第一次鎖定發生於星期四的下午 2 點，那麼 24 小時的時間間隔會結束於星期五的下午 2 點，且 Symantec Endpoint Protection Manager 會將鎖定時間間隔重設為 15 分鐘。

解除鎖定嘗試太多次登入後的管理員帳戶

1. 在主控台中，按下**「管理員」**>**「管理員」**。
2. 在**「管理員」**下，選取遭到鎖定的管理員帳戶。
3. 在**「工作」**下，按下**「編輯管理員」**。
4. 在**「一般」**標籤上，取消勾選**「達到指定的登入失敗次數後鎖定帳戶」**。

請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。

請參閱第 254 頁的「變更管理員帳戶或內嵌資料庫的密碼」。

請參閱第 257 頁的「使 Symantec Endpoint Protection Manager 登入密碼永久有效」。

變更保持登入 Symantec Endpoint Protection Manager 主控台的逾時期間

為了協助保護 Symantec Endpoint Protection Manager，主控台會在一小時後要求您重新輸入使用者名稱和密碼。若要增加安全性，您可以減少必須再次登入管理主控台之前的逾時期間。

當您從管理主控台本機或透過遠端 Java 主控台登入，即適用此登入逾時期間。遠端 Web 主控台的登入逾時期間會基於您定義的最短逾時值。例如，您可以將**「站台屬性」**設定設為 60 分鐘，將 Apache 設定設為 30 分鐘，以及將瀏覽器設定設為 10 分鐘。那麼，主控台會在 10 分鐘之後逾時。

變更保持登入 Symantec Endpoint Protection Manager 本機或遠端 Java 主控台的逾時期間

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 按下**「本機站台」**或遠端站台，並且按下**「編輯站台屬性」**。
3. 在**「一般」**標籤上，按下**「主控台逾時」**下拉式清單，然後選取其中一個可用選項作為時間長度。
4. 按下**「確定」**。

變更 Apache Tomcat 中用於保持登入 Symantec Endpoint Protection Manager 遠端 Web 主控台的逾時期間

1 在執行 Symantec Endpoint Protection Manager 的伺服器上，於文字編輯器中開啟以下檔案：

```
Program Files\Symantec\Symantec Endpoint Protection
Manager\tomcat\etc\conf.properties
```

2 新增下列一行 (如果尚不存在)：

scm.web.timeout.minutes=*timeout_value*

值 *timeout_value* 為無活動的分鐘數，在此時間之後，主控台即會登出。最大值為 60。值 0 與完全不新增該行的效果相同。

如果出現這行，您可以變更逾時值。

3 儲存並關閉檔案。

4 為了讓變更生效，請開啟 Windows 服務 (servicess.msc)，並重新啟動 Symantec Endpoint Protection Manager 服務。

變更 Internet Explorer 中用於保持登入 Symantec Endpoint Protection Manager 遠端 Web 主控台的逾時期間

- 遵循 Microsoft 文章如何變更 Internet Explorer 中的預設 Keep-Alive 逾時值中的指示，變更登錄機碼 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings。

變更 Mozilla Firefox 中用於保持登入 Symantec Endpoint Protection Manager 遠端 Web 主控台的逾時期間

1 在網址列中輸入下列：

```
about:config
```

2 按下以認可警告。

3 搜尋下列行：

network.http.keep-alive.timeout

4 將值 (秒) 變更為您需要的值。預設值為 115。

附註：Google Chrome 沒有可針對網路逾時期間架構的設定。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

14

管理網域

本章包含以下主題：

關於網域

安裝管理伺服器時，Symantec Endpoint Protection Manager 主控台中有一個稱為 Default 的網域。 網域是從 Symantec Endpoint Protection Manager 基礎架構分離出的資料的邏輯分隔。網域是主控台中的結構性配置區，可用來編排群組、用戶端、電腦和政策的階層。 您可以設定額外的網域，以管理網路資源。

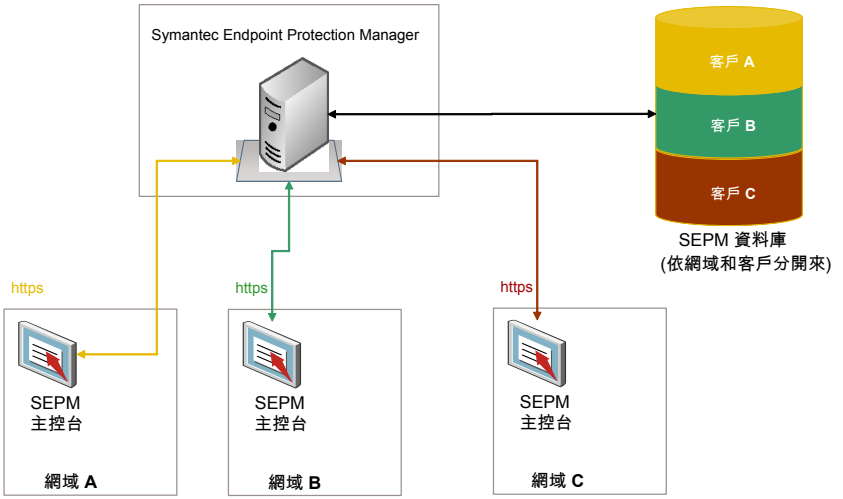
網域的主要目的在於，受管服務提供者可以建置一個可為多個客戶提供服務的 Symantec Endpoint Protection Manager 基礎架構。

附註：Symantec Endpoint Protection Manager 中的網域不等同於 Windows 網域或其他網路網域。

新增的每個網域都將共用相同的管理伺服器和資料庫，並提供其他主控台實例。各個網域的全部資料都會完全分隔。這種分隔可避免某個網域的管理員檢視其他網域的資料。您可以新增管理員帳戶，以便各個網域有各自的管理員。 這些管理員只能檢視及管理其自己的網域內容。

如果您的公司規模相當大，在許多地區都有營業處，您可能需要能夠集中檢視管理資訊。 您可以委派管理權限、實際分隔安全資料，或設定編排使用者、電腦和政策的較大彈性。如果您是受管服務提供者 (MSP)，可能需要管理多家獨立的公司，以及「Internet 服務供應商」。為滿足這些需求，您可以建立多個網域。例如，針對各個國家、地區或公司，您可以建立個別的網域。

圖 14-1 Symantec Endpoint Protection Manager 網域的概觀



新增網域時，網域中空無內容。 您必須將該網域設定為目前的網域。然後將管理員、群組、用戶端、電腦和政策新增至此網域。

您可以將政策從一個網域複製到另一個網域。若要在網域間複製政策，您可以從來源網域匯出政策，然後將此政策匯入目的地網域。

您也可以將用戶端從一個網域移動到另一個網域。若要在網域之間移動某用戶端，舊網域的管理員必須從用戶端群組中刪除該用戶端。然後就可以將用戶端上的「通訊設定」檔案取代為新網域中的檔案。

如果您不再需要某個網域，則可以將其停用。 當嘗試停用網域時，確定未將它設定為目前網域。

請參閱第 264 頁的「新增網域」。

請參閱第 239 頁的「管理管理員帳戶」。

請參閱第 265 頁的「切換至目前的網域」。

請參閱第 663 頁的「使用 SylinkDrop 工具還原用戶端伺服器通訊設定」。

新增網域

您可以建立網域來編排組織中群組、用戶端、電腦和政策的階層。 例如，您可能想新增網域來依部門組織使用者。

附註：您可以使用網域 ID 來進行災難復原。如果組織內的管理伺服器皆已故障，則您必須使用與舊伺服器相同的 ID 來重建管理伺服器。您可以從任何用戶端的 sylink.xml 檔案取得舊的網域 ID。

新增網域

1 在主控台中，按下**「管理員」**。

2 在**「管理員」**頁面中，按下**「網域」**。

3 在「工作」下，按下**「新增網域」**。

4 在「新增網域」對話方塊中，輸入網域名稱，並選擇性地輸入公司名稱和聯絡資訊。

5 如果您要新增網域 ID，請按下**「進階」**，然後在文字方塊中輸入值。

6 按下**「確定」**。

請參閱第 263 頁的「關於網域」。

切換至目前的網域

預設網域名為 **Default**，且設定為目前網域。 在 Symantec Endpoint Protection Manager 主控台中新增網域時，網域中空無內容。若要為新網域新增群組、用戶端、政策和管理員，必須首先將其設定為目前網域。 將網域指定為目前網域後，標題中的網域名稱後將顯示文字**「目前網域」**。如果您有多個網域，必須捲動**「網域」**清單以顯示目前網域是哪一個。

如果您以系統管理員的身分登入主控台，不論何者為目前網域，您都會看見全部的網域。然而，您只會看見目前網域中建立的管理員和限制的管理員。如果您以管理員或限制的管理員等身分登入主控台，只會看見您可存取的網域。

如果移除目前的網域，管理伺服器會將您登出。只能移除不是目前網域，且不是唯一網域的網域。

切換至目前的網域

1 在主控台中，按下**「管理員」**。

2 在**「管理員」**頁面中，按下**「網域」**。

3 在**「網域」**下，按下要設為目前網域的網域。

4 在**「工作」**下，按下**「管理網域」**。

5 在「管理員網域」對話方塊中，若要進行確認，按下**「是」**。

6 按下**「確定」**。

請參閱第 263 頁的「關於網域」。

請參閱第 264 頁的「新增網域」。

部分 4

使用安全政策管理防護

15

使用政策管理安全性

本章包含以下主題：

更新用戶端政策

如果您認為沒有最新的政策，可更新 Symantec Endpoint Protection 用戶端電腦上的政策。如果用戶端未收到更新，則可能是通訊出現問題。

檢查政策序號，以查證您的受管用戶端電腦是否可與管理伺服器通訊。

請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。

您只能手動更新用戶端電腦上的政策。如果政策設定阻止您開啟使用者介面或通知區域圖示，您可能無法手動更新政策。

請參閱第 221 頁的「防止和允許使用者變更用戶端的使用者介面」。

在 Symantec Endpoint Protection Manager 中，沒有任何指令可用於手動提示用戶端更新政策。用戶端會根據提取模式或推送模式的更新方法檢查政策更新。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

從 Windows 工作列更新用戶端上的用戶端政策

1. 在 Windows 工作列中，於通知區域中的 Symantec Endpoint Protection 圖示上按下滑鼠右鍵。
2. 按下**「更新政策」**。

從用戶端使用者介面更新用戶端政策

1. 在用戶端電腦中，按下**「說明」>「疑難排解」**。
2. 在**「疑難排解」**對話方塊的左欄中，按下**「管理」**。
3. 在**「管理」**面板中的**「政策設定檔」**下方，按下列其中一個選項：
   - 按下**「更新」**，直接從管理主控台更新政策。
   - 按下**「匯入」**，匯入具有從管理主控台匯出之政策的政策。按照提示來選取要匯入的政策檔案。

請參閱第 268 頁的「執行適用於所有政策的工作」。

執行適用於所有政策的工作

安全性政策定義防護技術如何保護電腦免受已知和不明威脅的侵擾。

您可以採用多種方法管理您的 Symantec Endpoint Protection 安全性政策。 例如，您可以自行建立安全性政策，然後依據特定需求加以自訂。您可以鎖定和解除鎖定某些設定，以便使用者無法在用戶端電腦上變更這些設定。

表 15-1　適用所有政策的工作

工作	敘述
新增政策	若不欲使用預設政策，可新增政策。 您可以新增共用政策或非共用政策。 **附註：**如果您在**「政策」**頁面中新增或編輯共用政策，還必須得將這些政策指派到群組或位置。 否則這些政策不會生效。 請參閱第 270 頁的「安全政策類型」。 請參閱第 278 頁的「關於共用和非共用政策」。 請參閱第 272 頁的「新增政策」。
鎖定和解除鎖定政策設定	您可以允許或防止用戶端使用者架構部分政策設定和用戶端使用者介面設定。 請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。
編輯政策	如果您希望變更現有政策中的設定，則可以對其進行編輯。 您可以透過修改電腦的安全性政策來提高或降低電腦的防護程度。 除非變更群組指派，否則不必重新指派經過修改的政策。 請參閱第 272 頁的「編輯政策」。
指派政策	若要使用政策，必須將政策指派給一個或多個群組或位置。 請參閱第 275 頁的「指派政策給群組或位置」。
測試政策	賽門鐵克建議您在生產環境中運用新政策之前，一律先測試新政策。
更新用戶端政策	可依據可用頻寬，架構用戶端使用推送模式或提取模式作為政策更新方法。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。
取代政策	可使用一個共用政策取代另一個共用政策。 您可以取代所有位置或某一位置的共用政策。 請參閱第 276 頁的「取代政策」。
複製和貼上政策	您可能想要複製目前的政策作為新政策的基礎使用，而非新增新政策。 您可以在**「政策」**頁面或**「用戶端」**頁面上的**「政策」**標籤上複製和貼上政策。 **附註：**還可以使用**「用戶端」**頁面上的**「政策」**標籤，複製群組中的所有政策，將其貼到其他群組中。 請參閱第 274 頁的「在「用戶端」頁面上複製並貼上政策」。 請參閱第 273 頁的「在「政策」頁面中複製和貼上政策」。

工作	敘述
將共用政策轉換為非共用政策	您可以複製共用政策的內容，然後從該內容建立非共用政策。 請參閱第 278 頁的「關於共用和非共用政策」。 您可以透過使用複本，變更某個位置中的共用政策內容，而不影響所有其他位置。 此複本會覆寫現有非共用政策。 當共用政策不再套用至所有群組或所有位置時，您可將此政策轉換為非共用政策。 完成轉換時，轉換後具有新名稱的政策會出現在「位置限定的政策與設定」下方。 請參閱第 278 頁的「將共用政策轉換為非共用政策」。
匯出和匯入政策	若要在不同站台或管理伺服器使用現有政策，可匯出該政策。 之後可以匯入此政策，並將其應用於群組或特定位置。 請參閱第 277 頁的「匯出和匯入個別 Endpoint Protection 政策」。
撤銷政策	如果刪除某政策，Symantec Endpoint Protection Manager 將從資料庫中移除該政策。如果您不想刪除某政策，但也不想再使用它，可以撤銷政策。 您可以撤銷**「病毒和間諜軟體防護政策」**和**「LiveUpdate 設定政策」**以外的任何類型的政策。 請參閱第 279 頁的「從群組或位置解除指派政策」。
刪除政策	如果政策已指派至一個或多個群組和位置，則您無法刪除政策，除非其從所有群組和位置取消指派該政策。您也可以將政策取代為另一個政策
檢查用戶端是否具有最新的政策	您可以檢查用戶端是否具有最新政策。 如果不是，您可以在用戶端上手動更新政策。 請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。 請參閱第 268 頁的「更新用戶端政策」。

安全政策類型

可以使用多種不同類型的安全性政策來管理網路安全性。多數類型的政策會在安裝期間自動建立。可以使用預設政策，也可以自訂政策以符合特定環境的需要。

請參閱第 268 頁的「執行適用於所有政策的工作」。

表 15-2 安全政策類型

政策類型	敘述
病毒和間諜軟體防護政策	**病毒和間諜軟體防護政策**提供下列防護: ■ 透過使用特徵，偵測、移除和修復病毒和安全性風險的負面影響。 ■ 透過使用「下載智慧型掃描」中的信譽資料，偵測使用者所嘗試下載檔案中的威脅。 ■ 透過使用 SONAR 啟發式技術和信譽資料，偵測顯示可疑行為的應用程式。 **病毒和間諜軟體防護政策**透過其 SONAR 技術尋找行為異常情況。 **附註：**「下載智慧型掃描」和 SONAR 技術僅可用於 Windows 用戶端。 請參閱第 357 頁的「在用戶端電腦上管理掃描」。
防火牆政策	**防火牆政策**提供下列防護: ■ 攔截未授權的使用者存取連線至 Internet 的電腦和網路。 ■ 偵測駭客攻擊。 ■ 清除不需要的網路流量來源。 **附註：**防火牆政策僅能套用於 Windows 用戶端。 請參閱第 288 頁的「管理防火牆防護」。
入侵預防政策	**入侵預防政策**自動偵測並攔截網路攻擊和瀏覽器上的攻擊，以及保護應用程式免受弱點攻擊。 請參閱第 325 頁的「管理入侵預防」。
LiveUpdate 政策	**LiveUpdate 內容政策**和 **LiveUpdate 設定政策**包含決定用戶端電腦如何以及何時從 LiveUpdate 下載內容更新的設定。可以定義用戶端所聯絡的電腦，以檢查更新和排程用戶端電腦檢查更新的時間和方法。 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。
應用程式與裝置控制	**應用程式與裝置控制政策**保護系統資源免受應用程式使用並管理可連線到電腦的週邊裝置。 請參閱第 433 頁的「設定應用程式控制」。 應用程式控制政策僅適用於 Windows 用戶端。裝置控制政策適用於 Windows 和 Mac 電腦。
主機完整性	**主機完整性政策**提供定義、強制執行和還原用戶端電腦的安全性的功能，以保護企業網路和資料的安全。使用此政策驗證存取網路的用戶端是否執行防毒軟體、修正程式和定義的其他應用程式準則。 請參閱第 524 頁的「設定主機完整性」。

政策類型	敘述
例外政策	**例外政策**提供從病毒和間諜軟體掃描偵測以及 SONAR 偵測中排除應用程式和程序的能力。 您還可以從應用程式控制中排除應用程式。 請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。
記憶體攻擊緩和	**「記憶體攻擊緩和政策」**會使用緩和技術 (例如 DLL 劫取、HeapSpray 緩和與 Java 侵入預防) 來阻止對軟體的弱點攻擊。 請參閱第 339 頁的「使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊」。

新增政策

Symantec Endpoint Protection Manager 針對各種類型的防護隨附有預設政策。如果您需要自訂政策，可以新增政策並加以編輯。您可以為各類型的政策建立多個版本。

賽門鐵克建議您在生產環境中使用新政策之前，一律先測試新政策。

新增政策

1. 在主控台中，按下**「政策」**。
2. 在**「政策」**頁面中，選取政策類型，再按下新增新政策的連結。
3. 修改政策設定以提升或降低防護。
4. 按下**「確定」**儲存政策。
5. 可選擇將新政策指派至群組。

   您可以在建立政策期間或建立政策之後，將新政策指派至群組。新政策將取代相同防護類型的目前指派政策。

   請參閱第 275 頁的「指派政策給群組或位置」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

編輯政策

您可以在**「用戶端」**頁面及**「政策」**頁面的**「政策」**標籤上編輯共用和非共用政策。

位置與群組可以共用相同的政策。您必須先完成編輯，才能指派共用政策。

請參閱第 275 頁的「指派政策給群組或位置」。

在「政策」頁面上編輯政策

1 在主控台中，按下**「政策」**。

2 在**「政策」**頁面的**「政策」**下，按下政策類型。

3 在**「<政策類型> 政策」**窗格中，按下要編輯的特定政策。

4 在**「工作」**下，按下**「編輯政策」**。

5 必要時，在**「<政策類型> 政策概述」**窗格中，編輯政策的名稱和敘述。

6 若要編輯政策，請針對政策按下任一個**「<政策類型> 政策」**頁面。

在「用戶端」頁面上編輯政策

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**頁面的**「用戶端」**下，選取要為其編輯政策的群組。

3 在**「政策」**標籤中，取消核取**「從父群組 <群組名稱> 繼承政策和設定」**。

您必須停用此群組的繼承。如果沒有取消核取繼承，就無法編輯政策。

4 在**「位置限定的政策與設定」**下，捲動尋找要編輯其中政策的位置名稱。

5 找出要編輯的位置限定政策。

6 在選取的政策右側，按下**「工作」**，然後按下**「編輯政策」**。

7 執行下列其中一項工作：

- 若要編輯非共用政策，請進行步驟 8。
- 若要編輯共用政策，請在**「編輯政策」**對話方塊中，按下**「編輯共用」**以編輯所有位置中的該政策。

8 對於要編輯的政策類型，您可以按下連結。

在「政策」頁面中複製和貼上政策

您可以在**「政策」**頁面中複製和貼上政策。例如，您可能想要稍微編輯政策設定以套用於其他群組。

在「政策」頁面中複製政策

1 在主控台中，按下**「政策」**。

2 在**「政策」**頁面的**「政策」**下方，按下要複製的政策類型。

3 在**「*政策類型*政策」**窗格中，按下要複製的特定政策。

4 在**「政策」**頁面的**「工作」**下，按下**「複製政策」**。

5 如果您不想再收到關於此程序的通知，請在「**複製政策**」對話方塊中，勾選「**不要再顯示此訊息**」。

若要重新顯示「**不要再顯示此訊息**」核取方塊，請按下「**管理**」>「**管理員**」，選取管理員帳戶，然後按下「**重設複製政策提醒**」。

6 按下「**確定**」。

在「政策」頁面中貼上政策

1 在主控台中，按下「**政策**」。

2 在「**政策**」頁面的「**政策**」下，按下要貼上的政策類型。

3 在「***政策類型*政策**」窗格中，按下要貼上的特定政策。

4 在「**政策**」頁面的「**工作**」下，按下「**貼上政策**」。

請參閱第 274 頁的「在「用戶端」頁面上複製並貼上政策」。

在「用戶端」頁面上複製並貼上政策

您可以複製並貼上政策而不必新增政策。您可以在「**用戶端**」頁面上複製共用或非共用政策。

請參閱第 268 頁的「執行適用於所有政策的工作」。

在「用戶端」頁面上複製政策

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面的「**用戶端**」下，選取要為其複製政策的群組。

3 在「**政策**」標籤的「**位置限定的政策與設定**」下，捲動尋找要複製其中政策的位置名稱。

4 找出您在該位置中要複製的特定政策。

5 在政策的右側，按下「**工作**」，然後按下「**複製**」。

6 按下「**確定**」。

在「用戶端」頁面上貼上政策

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面的「**用戶端**」下，選取要為其貼上政策的群組。

3 在「**政策**」標籤中，取消核取「**從父群組 <群組名稱> 繼承政策和設定**」。

您必須停用此群組的繼承。如果沒有取消核取繼承，就無法貼上政策。

4 在「**位置限定的政策與設定**」下，捲動尋找要貼上其中政策的位置名稱。

5 找出您在該位置中要貼上的特定政策。

6 在政策的右側，按下「**工作**」，然後按下「**貼上**」。

7 當畫面出現覆寫現有政策的提示時，按下「**是**」。

指派政策給群組或位置

您可以透過群組將政策指派到用戶端電腦。每一群組的每一防護類型任何時間皆必須指派一個且僅一個政策。通常，您可為執行不同平台的用戶端建立單獨的群組。如果將執行不同平台的用戶端置於同一群組，則每個用戶端平台會忽略未套用的任何設定。

未指派的政策不會下載到群組和位置中的用戶端電腦。如果您在新增政策時沒有指派政策，可以稍後再指派給群組和位置。您也可以重新指派政策給不同的群組或位置。

政策指派至電腦群組的情形如下：

- 初始安裝時，賽門鐵克預設的安全政策會指派至 **My Company** 父群組。
- **My Company** 父群組內的安全政策會自動指派至每一新增的子群組。依據預設，新建的子群組會從 **My Company** 繼承。
  新群組一律會繼承自其直屬父群組。 如果您建立子群組階層，那麼每一個群組都會從其直屬父群組繼承，而不是從頂層父群組繼承。
- 您可利用指派其他同類型政策的方式，取代群組內的政策。您可取代已指派至 **My Company** 父群組或任何子群組的政策。

這些圖示顯示了下列資訊：

表 15-3　　政策圖示

圖示	敘述
	未指派政策的群組。
	已指派政策的群組。文字為粗體。
	未指派政策的位置。
	已指派政策的位置。文字為粗體。
	繼承自父群組且未指派政策的位置。
	繼承自父群組且已指派政策的位置

指派政策給群組或位置

1　在主控台中，按下**「政策」**>*「政策類型」*。

2　在**「政策」**頁面上，選取政策，然後按下**「指派政策」**。

3 在「**指派政策**」對話方塊中，選取群組或位置，然後按下「**指派**」。

4 按下「**確定**」以確認。

請參閱第 279 頁的「從群組或位置解除指派政策」。

取代政策

您可能需要以其他共用政策取代某個共用政策。您可以在所有位置或為個別位置取代共用政策。

當您取代所有位置的政策時，管理伺服器只會針對有該政策的位置取代政策。例如，假設 Sales 群組在其四個位置的其中三個使用「業務」政策。如果要用「行銷」政策取代「業務」政策，就只有這三個位置會收到「行銷」政策。

您可能需要某一組用戶端使用相同的設定，不論各用戶端的位置在哪裡。在這種狀況下，您可以使用共用政策取代非共用政策。使用共用政策分別為每個位置取代非共用政策。

請參閱第 268 頁的「執行適用於所有政策的工作」。

取代所有位置的共用政策

1 在主控台中，按下「**政策**」。

2 在「**政策**」頁面的「**政策**」下方，按下要取代的政策類型。

3 在「**<政策類型> 政策**」窗格中，按下政策。

4 在「**政策**」頁面的「**工作**」下方，按下「**取代政策**」。

5 在「**取代 <政策類型> 政策**」對話方塊中的「**新 <政策類型> 政策**」清單方塊中，選取要取代舊政策的共用政策。

6 選取要取代現有政策的群組和位置。

7 按下「**取代**」。

8 當取代群組和位置政策的確認提示顯示時，按下「**是**」。

取代某個位置的共用政策或非共用政策

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面中的「**用戶端**」下，選取要為其取代政策的群組。

3 在「**政策**」標籤中，取消核取「**從父群組 <群組名稱> 繼承政策和設定**」。

您必須停用此群組的繼承。如果沒有取消核取繼承，就無法取代政策。

4 在「**位置限定的政策與設定**」下，捲動尋找包含政策的位置。

5 在要取代的政策旁邊，按下「**工作**」，然後按下「**取代政策**」。

6 在「**取代政策**」對話方塊中的「**新政策**」清單方塊內，選取取代政策。

7 按下「**確定**」。

匯出和匯入個別 Endpoint Protection 政策

可以匯出和匯入政策而不是重新建立政策。所有與政策關聯的設定都會自動匯出。

可能需要針對下列原因匯出政策：

- 從舊版管理伺服器更新為新版管理伺服器。需要使用先前自訂的政策更新新的管理伺服器。
- 需要匯出政策以在另一個網站中使用。

一次匯出和匯入一個政策。匯出檔案後，將它匯入並套用至群組，或只套用至位置。可以在**「用戶端」**頁面中為特定位置匯出共用或非共用政策。

請參閱第 268 頁的「執行適用於所有政策的工作」。

從「政策」頁面匯出單一政策

1 在主控台中，按下**「政策」**。

2 在**「政策」**頁面的**「政策」**下，按下要匯出的政策類型。

3 在**「*<政策類型>* 政策」**窗格中，按下要匯出的特定政策。

4 在**「政策」**頁面中的**「工作」**下，按下**「匯出政策」**。

5 在**「匯出政策」**對話方塊中，尋找要匯出政策檔案的資料夾，然後按下**「匯出」**。

從「用戶端」頁面匯出共用或非共用政策

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下，選取要針對其匯出政策的群組。

3 在**「政策」**標籤中，取消勾選**「從父群組 <群組名稱> 繼承政策和設定」**。

您必須停用此群組的繼承。如果沒有取消勾選繼承，就無法匯出政策。

4 在**「位置限定的政策與設定」**下，捲動尋找要匯出其中政策的位置名稱。

5 找出要匯出的位置限定政策。

6 在政策的右邊按下**「工作」**，然後按下**「匯出政策」**。

7 在**「匯出政策」**對話方塊中，瀏覽到您要將政策匯出至哪一個資料夾。

8 在**「匯出政策」**對話方塊中，按下**「匯出」**。

匯入單一政策

1 在主控台中，按下**「政策」**。

2 在**「政策」**頁面的**「政策」**下，按下您要匯入的政策類型。

3 在**「*<政策類型>* 政策」**窗格中，按下要匯入的政策。

4 在**「政策」**頁面的**「工作」**下方，按下**「匯入 <**政策類型**> 政策」**。

5 在**「匯入政策」**對話方塊中，瀏覽至要匯入的政策檔案，然後按下**「匯入」**。

關於共用和非共用政策

政策可以是共用政策或非共用政策。如果將政策套用於多個群組或位置，則該政策為共用政策。如果您建立共用政策，則可以在所有使用政策的群組和位置輕鬆編輯和取代政策。您可以在 My Company 群組層級或較低層級套用共用政策，而子群組能夠繼承政策。您可以擁有多個共用政策。

如果對於特定的群組或位置，需要一個特定政策，則可建立一個唯一政策。您可以將此唯一、非共用政策指派到一個特定群組或位置。在每個位置，每種政策類型僅能有一個政策。

例如，下面是一些可能的狀況：

- 財務部門中的一個使用者群組在辦公室和在家裡時，需要使用不同的位置連線到企業網路。對於該群組，您可能需要將具有各自的規則集和設定的不同防火牆政策套用於每個位置。
- 您的遠端使用者通常會使用 DSL 及 ISDN，因此他們可能需要 VPN 連線。其他遠端使用者需要使用撥號來連線至企業網路。但是，銷售及行銷群組還需要使用無線連線。針對這些群組連接至企業網路時所處的位置，每個群組可能需要有自己的防火牆政策。
- 對於在大多數員工工作站上安裝的非驗證應用程式，您需要實作限制性政策以保護企業網路免受攻擊。您的 IT 群組可能需要存取其他應用程式。因此相較於一般員工，IT 群組的安全性政策限制可能要少些。在這種狀況下，您可以為 IT 群組建立不同的防火牆政策。

您通常會在**「政策」**頁面的**「政策」**標籤上新增群組和位置共用的任何政策。不過，如果增加的政策不是群組之間共用的政策，而只套用到特定位置，請在**「用戶端」**頁面中新增。如果決定要在**「用戶端」**頁面中新增政策，可以使用下列任何方法增加新政策：

- 新增政策。
  請參閱第 272 頁的「新增政策」。
- 複製現有政策以此為基礎建立新政策。
  請參閱第 273 頁的「在「政策」頁面中複製和貼上政策」。
  請參閱第 274 頁的「在「用戶端」頁面上複製並貼上政策」。
- 匯入以前從其他站台匯出的政策。
  請參閱第 277 頁的「匯出和匯入個別 Endpoint Protection 政策」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

請參閱第 278 頁的「將共用政策轉換為非共用政策」。

將共用政策轉換為非共用政策

您可以複製共用政策的內容，然後從該內容建立非共用政策。您可以透過使用複本，來變更某個位置中的共用政策內容，而不影響所有其他位置。複本會覆寫現有的共用政策。

完成轉換時，轉換後具有新名稱的政策會出現在**「位置限定的政策與設定」**下方。

請參閱第 278 頁的「關於共用和非共用政策」。

請參閱第 273 頁的「在「政策」頁面中複製和貼上政策」。

將共用政策轉換為非共用政策

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**頁面的**「用戶端」**下，選取您要為其轉換政策的群組。
3. 在與上一步驟所選群組關聯的窗格中，按下**「政策」**。
4. 在**「政策」**標籤中，取消核取**「從父群組 <群組名稱> 繼承政策和設定」**。

   您必須停用此群組的繼承。如果沒有取消核取繼承，就無法取代政策。
5. 在**「位置限定的政策與設定」**下，捲動尋找位置名稱以及要轉換的特定政策。
6. 在特定政策旁，按下**「工作」**，然後按下**「轉換為非共用政策」**。
7. 在**「概述」**對話方塊中，編輯政策的名稱與敘述。
8. 根據需要，修改其他政策設定。
9. 按下**「確定」**。

請參閱第 268 頁的「執行適用於所有政策的工作」。

從群組或位置解除指派政策

如果要永久刪除某個政策或儲存政策以便日後使用，則可能需要從群組或位置解除指派該政策。

例如，某個特定群組可能在您採用新政策後發生問題。如果您想將政策保留在資料庫中，則可以將政策撤銷而不是刪除。撤銷政策時，政策會自動從您將政策指定至的群組和位置中撤銷。使用政策的位置數量會顯示在**「政策」**頁面的**「<政策類型> 政策」**窗格中。

附註：刪除政策前，必須從所有群組和位置撤銷政策或取代政策。

您可以從某個位置或群組中的**「政策」**頁內撤銷下列政策以外的所有政策：

- **病毒和間諜軟體防護**
- **LiveUpdate 設定**

僅能以其他**「病毒和間諜軟體防護」政策**或 **LiveUpdate 政策**來取代他們。

請參閱第 276 頁的「取代政策」。

請參閱第 275 頁的「指派政策給群組或位置」。

在「政策」頁面中解除指派共用政策

1. 在主控台中，按下**「政策」**。
2. 在**「政策」**頁面的**「政策」**下，按下您要撤銷的政策類型。

3 在「**<政策類型> 政策**」窗格中，按下要撤銷的特定政策。

4 在「**政策**」頁面的「**工作**」下，按下「**撤銷政策**」。

5 在「**撤銷政策**」對話方塊中，勾選您要從其中撤銷政策的群組和位置。

6 按下「**撤銷**」。

7 當自群組和位置撤銷政策的確認提示顯示時，按下「**是**」。

在「用戶端」頁面中解除共用或非共用政策

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」頁面的「**用戶端**」下，選取您要為其撤銷政策的群組。

3 在「**政策**」標籤中，取消核取「**從父群組 <群組名稱> 繼承政策和設定**」。

您必須停用此群組的繼承。如果沒有取消核取繼承，就無法撤銷政策。

4 在「**位置限定的政策與設定**」下，捲動尋找您要為其撤銷政策的位置名稱。

5 找出要從該位置撤銷的政策。

6 按下「**工作**」，然後按下「**撤銷政策**」。

7 在「**撤銷政策**」對話方塊中，按下「**是**」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

防止使用者在用戶端電腦上停用防護

以 Symantec Endpoint Protection Manager 管理員身分，透過設定使用者控制等級或鎖定政策選項，防止使用者停用用戶端電腦上的防護。例如，防火牆政策使用控制等級，而病毒和間諜軟體防護政策則使用鎖定。

賽門鐵克建議您始終防止使用者停用防護。

- 什麼是使用者控制等級？
- 變更使用者控制等級
- 鎖定和解除鎖定政策設定
- 防止使用者停用特定防護技術
- 從 Symantec Endpoint Protection Manager 更新用戶端政策

什麼是使用者控制等級？

使用使用者控制等級來提供對特定功能的用戶端使用者控制。使用者控制等級也會決定用戶端使用者介面完全不顯示項目、顯示部分功能集或顯示完整的使用者介面。

表 15-4 使用者控制等級

使用者控制等級	敘述
伺服器控制	授予使用者最低的用戶端控制權。透過伺服器控制，使用者可以對解除鎖定的設定進行變更，但這些設定會在下次活動訊號時被覆寫。
用戶端控制	授予使用者最高的用戶端控制權。用戶端控制允許使用者架構設定。用戶端修改的設定優先於伺服器設定。套用新政策時不會覆寫這些設定，除非這些設定在新政策中鎖定。 用戶端控制對於在遠端位置或家中工作的員工很有用。 **附註：**使用者必須位於 Windows 管理員群組，才能在**「用戶端控制」**模式或**「混合控制」**模式下變更任何設定。
混合控制	授予使用者用戶端的混合控制權。透過將此選項設定為**「伺服器控制」**或**「用戶端控制」**，可以決定您要讓使用者架構哪些選項。對於處於用戶端控制下的這些項目，使用者會保留對設定的控制。對於處於伺服器控制下的這些項目，會保留對設定的控制。

對於 Windows 用戶端，您可以架構所有選項。對於 Mac 用戶端，伺服器控制和用戶端控制中只有通知區域圖示和部分 IPS 選項可用。

當伺服器套用隔離所政策時，在**「用戶端控制」**或**「混合控制」**中執行的用戶端會切換成**「伺服器控制」**。

請參閱第 221 頁的「防止和允許使用者變更用戶端的使用者介面」。

變更使用者控制等級

部分受管設定具有相依性。例如，使用者可能有權限架構防火牆規則，但無法存取用戶端使用者介面。由於使用者無法存取**「架構防火牆規則」**對話方塊，也就無法建立規則。

變更使用者控制等級

1. 在主控台中，按下**「用戶端」**。
2. 在**「檢視用戶端」**下方選取群組後，再按下**「政策」**標籤。
3. 在**「位置限定的政策與設定」**下，再到要修改的位置下，展開**「位置限定的設定」**。
4. 在**「用戶端使用者介面控制設定」**旁，按下**「工作」>「編輯設定」**。
5. 在**「用戶端使用者介面控制設定」**對話方塊中，執行下列其中一個選項：
   - 按下**「伺服器控制」**，再按下**「自訂」**。
     架構任何設定，然後按下**「確定」**。
   - 按下**「用戶端控制」**。
   - 按下**「混合控制」**，再按下**「自訂」**。
     架構任何設定，然後按下**「確定」**。
6. 按下**「確定」**。

請參閱第 319 頁的「架構混合控制的防火牆設定」。

鎖定和解除鎖定政策設定

您可以鎖定和解除鎖定某些政策設定。使用者無法變更已鎖定的設定。可鎖定的設定旁會顯示掛鎖圖示。您可以鎖定和解除鎖定病毒和間諜軟體防護設定、竄改防護設定、傳送設定和入侵預防設定。

防止使用者停用特定防護技術

如果您將用戶端設定為**「混合控制」**或**「伺服器控制」**，但未鎖定選項，則使用者可變更設定。這些變更會保留在原位，直到 Symantec Endpoint Protection Manager 出現下次活動訊號。鎖定各種政策中的政策選項可確保使用者無法對設定進行任何變更，即使處於**「用戶端控制」**也是如此。

附註：無論**「位置限定的設定」**組態為何，非管理員的 Windows 使用者群組均無法變更 Symantec Endpoint Protection 用戶端使用者介面中的設定。即使在您設定這些選項之後，Windows 10 管理員仍可透過通知區域圖示停用產品。但是，他們無法透過用戶端使用者介面停用個別防護技術。

附註：如果您不想針對所有群組變更政策，請在要進行變更的群組上停用政策繼承。如果編輯共用政策，即使政策繼承已停用，編輯後的政策也會套用至已套用共用政策的每個群組。

防止使用者停用防火牆或應用程式與裝置控制

1. 在主控台中，按下**「用戶端」**。
2. 按下要限制的用戶端群組，然後按下**「政策」**標籤。
3. 展開**「位置限定的設定」**。
4. 在**「用戶端使用者介面控制設定」**旁，按下**「工作」>「編輯設定」**。
5. 按下**「伺服器控制」**或**「混合控制」**，然後按下**「自訂」**。
6. 在**「用戶端使用者介面設定」**對話方塊 (伺服器控制) 或窗格 (混合控制) 上，取消勾選**「允許下列使用者啟用和停用防火牆」**和**「允許使用者啟用和停用應用程式裝置控制」**。
7. 按下**「確定」**，然後再按下**「確定」**。

防止使用者停用入侵預防

1. 在主控台中，按下**「用戶端」**。
2. 按下要限制的用戶端群組，然後按下政策的**「政策」**標籤。
3. 展開**「位置限定的政策」**。
4. 在**「入侵預防政策」**旁，按下**「工作」>「編輯政策」**。

5 按下「**入侵預防**」，然後按下「**啟用網路入侵預防**」和「**啟用瀏覽器入侵預防**」旁的鎖定，以鎖定這些功能。

6 按下「**確定**」。

防止使用者停用病毒和間諜軟體防護

1 在主控台中，按下「**用戶端**」。

2 按下要限制的用戶端群組，然後按下「**政策**」標籤。

3 展開「**位置限定的政策**」。

4 在「**病毒和間諜軟體防護政策**」旁，按下「**工作**」>「**編輯政策**」。

5 在「**Windows 設定**」下方，鎖定以下功能：

- 按下「**自動防護**」，然後按下「**啟用自動防護**」旁的鎖定。
- 按下「**下載防護**」，然後按下「**啟用下載鑑識以根據檔案信譽偵測下載檔案中的潛在風險**」旁的鎖定。
- 按下 **SONAR**，然後按下「**啟用 SONAR**」旁的鎖定。
- 按下「**提早啟動防惡意軟體驅動程式**」，然後按下「**啟用賽門鐵克提早啟動防惡意軟體**」旁的鎖定。
- 按下「**Microsoft Outlook 自動防護**」，然後按下「**啟用 Microsoft Outlook 自動防護**」旁的鎖。
- 對於低於 14.2 RU1 的版本，按下「**Internet 電子郵件自動防護**」，然後按下「**啟用 Internet 電子郵件自動防護**」旁的鎖。
- 對於低於 14.2 RU1 的版本，按下「**Lotus Notes 自動防護**」，然後按下「**啟用 Lotus Notes 自動防護**」旁的鎖。
- 按下「**全域掃描選項**」，然後按下「**針對以下項目啟用 Insight**」和「**啟用 Bloodhound 啟發式病毒偵測**」旁的鎖定。

6 按下「**確定**」。

防止使用者停用記憶體攻擊緩和 (自 14.0.1 起)

1 在主控台中，按下「**用戶端**」。

2 按下要限制的用戶端群組，然後按下政策的「**政策**」標籤。

3 展開「**位置限定的設定**」。

4 在「**記憶體攻擊緩和**」旁，按下「**工作**」>「**編輯政策**」。

5 按下「**記憶體攻擊緩和**」，然後按下「**啟用記憶體攻擊緩和**」旁的鎖定。

6 按下「**確定**」。

從 Symantec Endpoint Protection Manager 更新用戶端政策

進行這些變更後，群組中的用戶端會根據群組的通訊設定接收更新的政策。如果群組處於推送模式，Symantec Endpoint Protection Manager 會提示用戶端花幾秒的時間登入。如果群組處於提取模式，用戶端會在下次排程的活動訊號時登入。

如果您希望它們在下次活動訊號之前實現，可提示用戶端登入並更新其政策。您也可以從 Symantec Endpoint Protection 用戶端更新政策。

請參閱第 268 頁的「更新用戶端政策」。

一旦用戶端更新政策，當您在 Symantec Endpoint Protection 通知區域圖示上按下滑鼠右鍵時，「**停用 Symantec Endpoint Protection**」會顯示為灰色。

監控在用戶端電腦執行的應用程式與服務

Windows 用戶端會監控並收集每台電腦上執行的應用程式和服務的相關資訊。 您可以架構用戶端將資訊收集於清單中，然後將清單傳送至管理伺服器。 應用程式及其特性的清單稱為探索到的應用程式。

您可以使用此資訊，找出使用者執行的應用程式。 您也可以視需要使用下列有關應用程式資訊的項目：

- 防火牆政策
- 應用程式與裝置控制政策
- SONAR 技術
- 主機完整性政策
- 網路應用程式監控
- 檔案指紋清單

附註：Mac 和 Linux 用戶端不會監控在這些電腦上執行的應用程式和服務。

您可以執行數個工作來設定並使用探索到的應用程式。

表 15-5　監控應用程式的步驟

步驟	敘述
啟用探索到的應用程式	架構管理伺服器後即可收集用戶端電腦執行的應用程式相關資訊。 請參閱第 285 頁的「收集有關用戶端電腦執行的應用程式資訊」。

步驟	敘述
搜尋應用程式	您可以使用查詢工具搜尋用戶端電腦執行的應用程式清單。 搜尋準則可以應用程式或電腦為基礎。 例如，您可以找出各個用戶端電腦使用的 Internet Explorer 版本。 請參閱第 286 頁的「搜尋有關電腦執行的應用程式資訊」。 您可以儲存應用程式的搜尋結果，供日後檢視。

附註：在某些國家/地區，當地法令可能不允許在某些狀況下使用探索到的應用程式工具，例如，當員工從家中使用公司手提式電腦登入公司網路時，從手提式電腦取得應用程式使用資訊。 在您使用此工具之前，請確定當地法令允許您的用途。 如果不允許，請按照指示停用工具。

收集有關用戶端電腦執行的應用程式資訊

您可以針對某個群組或位置啟用探索到的應用程式。 然後，用戶端會保持追蹤所執行的每個應用程式，並將該資料傳送到管理伺服器。

附註：Mac 和 Linux 用戶端不會監控在這些電腦上執行的應用程式和服務。

群組或位置中的每個用戶端執行應用程式時，您可以設定將通知傳送至您的電子郵件地址。

請參閱第 577 頁的「設定管理員通知」。

附註：您只能修改不是從父群組繼承政策和設定之子群組的設定。

將探索到的應用程式清單傳送至某一群組的管理伺服器

1. 在主控台中，按下**「用戶端」**。
2. 在**「檢視用戶端」**下，選取一個群組。
3. 在**「政策」**標籤上，按下**「通訊設定」**。
4. 在**「用於 *group name* 的通訊設定」**對話方塊中，確定已勾選**「探索在用戶端電腦執行的應用程式」**。
5. 按下**「確定」**。

傳送探索到的應用程式至某一位置的管理伺服器

1. 在主控台中，按下**「用戶端」**。
2. 在**「檢視用戶端」**下，選取一個群組。
3. 在**「位置限定的政策與設定」**下，選取位置，然後展開**「位置限定的設定」**。

4 在「**通訊設定**」右邊，按下「**工作**」，然後取消核取「**使用群組通訊設定**」。

勾選此設定能讓您建立一個位置設定，而不是群組設定。

5 按下「**工作**」，然後按下「**編輯設定**」。

6 在「**<位置名稱>的通訊設定**」對話方塊中，勾選「**探索在用戶端電腦執行的應用程式**」。

7 按下「**確定**」。

請參閱第 284 頁的「監控在用戶端電腦執行的應用程式與服務」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

搜尋有關電腦執行的應用程式資訊

當管理伺服器收到來自用戶端的應用程式清單之後，您可以執行查詢以尋找有關這些應用程式的詳細資料。例如，您可以尋找所有使用未經授權應用程式的用戶端電腦。然後您可以建立防火牆規則，來攔截用戶端電腦上的應用程式。或者，您可能會想要升級所有用戶端電腦，以使用最新版的 Microsoft Word。您可以使用來自任何政策類型的「**搜尋應用程式**」工作。

附註：Mac 用戶端不會監控在 Mac 電腦上執行的應用程式和服務。

您可以使用下列方式搜尋應用程式：

- 根據應用程式。
  您可以將搜尋範圍限制為特定應用程式或應用程式詳細資料，例如名稱、檔案指紋、路徑、大小、版本或最後修改時間。
- 根據用戶端或用戶端電腦。
  您可以搜尋特定使用者或特定用戶端電腦執行的應用程式。例如，您可以根據電腦的 IP 位址進行搜尋。

您也可以直接在防火牆政策內搜尋要新增到防火牆規則的應用程式名稱。

請參閱第 301 頁的「定義應用程式的相關資訊」。

附註：啟用可記錄用戶端執行之各種應用程式的功能前，不會收集「**搜尋**」方塊中的資訊。您可以移至每個群組或位置的「**用戶端**」頁面的「**通訊設定**」對話方塊，來啟用此功能。

搜尋有關電腦執行的應用程式資訊

1 在主控台中，按下「**政策**」。

2 在「**政策**」頁面的「**工作**」下方，按下「**搜尋應用程式**」。

3 在「**搜尋應用程式**」對話方塊的「**搜尋應用程式於**」欄位右側，按下「**瀏覽**」。

4 在**「選取群組或位置」**對話方塊中，選取您要檢視應用程式的用戶端群組，然後按下**「確定」**。

您一次只能指定一個群組。

5 請確定勾選**「搜尋子群組」**。

6 執行下列其中一項動作：

- 若要根據使用者或電腦資訊進行搜尋，請按下**「依據用戶端/電腦資訊」**。
- 若要根據應用程式進行搜尋，請按下**「依據應用程式」**。

7 按下**「搜尋欄位」**下的空白儲存格，然後從清單中選取搜尋條件。

「搜尋欄位」儲存格會顯示所選選項的條件。如需這些條件的詳細資料，請按下**「說明」**。

8 按下「比較運算子」下的空白儲存格，然後選取其中一個運算子。

9 按下「值」下的空白儲存格，然後選取或輸入值。

「值」儲存格可能會從下拉式清單提供格式或值，視您在「搜尋欄位」儲存格中選取的條件而定。

10 若要加入其他搜尋條件，請按下第二列，然後在「搜尋欄位」、「比較運算子」和「值」儲存格中輸入資訊。

如果您輸入多列的搜尋條件，則查詢會嘗試符合所有條件。

11 按下**「搜尋」**。

12 在「查詢結果」表格中，執行下列任一動作：

- 按下捲動箭頭，可檢視更多列和欄。
- 按下**「上一頁」**和**「下一頁」**，可查看資訊的其他畫面。
- 選取某列，然後按下**「檢視詳細資料」**，可查看有關應用程式的其他資訊。

除非您將結果匯出至檔案，否則不會儲存結果。

13 若要移除查詢結果，請按下**「清除全部」**。

14 按下**「關閉」**。

請參閱第 284 頁的「監控在用戶端電腦執行的應用程式與服務」。

請參閱第 268 頁的「執行適用於所有政策的工作」。

16

管理防火牆防護

本章包含以下主題：

管理防火牆防護

防火牆允許您在防火牆政策中指定的進出網路流量。Symantec Endpoint Protection 防火牆政策包含規則與防護設定，大部分可由您啟用或停用，以及架構。

表 16-1　管理防火牆防護的選擇性工作

工作	敘述
讀取防火牆防護的相關資訊	在架構防火牆防護之前，您應當先熟悉一下防火牆。 請參閱第 289 頁的「防火牆的運作方式」。 請參閱第 290 頁的「關於 Symantec Endpoint Protection 防火牆」。

工作	敘述
建立防火牆政策	Symantec Endpoint Protection 與預設的防火牆政策一起安裝。您可以修改預設政策，也可以建立新政策。 您必須先建立政策，然後才能為該政策架構防火牆規則和防火牆防護設定。 請參閱第 291 頁的「建立防火牆政策」。
建立及自訂防火牆規則	防火牆規則是控制防火牆保護用戶端電腦免受惡意攻擊的方式的政策元件。 預設防火牆政策包含預設防火牆規則。建立新政策後，Symantec Endpoint Protection 將提供預設防火牆規則。但是，您可以修改預設規則，也可以建立新規則。 請參閱第 295 頁的「新增防火牆規則」。 請參閱第 311 頁的「自訂防火牆規則」。
啟用防火牆防護設定	在防火牆完成特定作業後，控制權就會移交給數個元件。每個元件都是設計來執行不同類型的封包分析。 請參閱第 320 頁的「為網路服務啟用通訊而非新增規則」。 請參閱第 321 頁的「自動攔截連線至攻擊電腦」。 請參閱第 323 頁的「防止對電腦的外部隱藏攻擊」。 請參閱第 323 頁的「停用 Windows 防火牆」。 請參閱第 531 頁的「透過架構點對點驗證攔截遠端電腦」。
監控防火牆防護	定期監控電腦上的防火牆防護狀態。 請參閱第 539 頁的「監控端點防護」。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

請參閱第 319 頁的「架構混合控制的防火牆設定」。

防火牆的運作方式

防火牆執行下列所有工作：

- 防止任何未獲授權的使用者存取組織中連線到 Internet 的電腦和網路
- 監控您的電腦與 Internet 上其他電腦之間的通訊
- 建立防護措施，允許或攔截他人企圖存取您電腦上的資訊
- 警告您來自其他電腦的連線嘗試
- 警告您電腦上的應用程式嘗試連線到其他電腦

防火牆檢視 Internet 上載送的資料封包。封包是不連續的資料單位，屬於兩台電腦間資訊流的一部分。封包會在目的地重組起來，成為不中斷的資料流。

套件包含顯示下列關於資料的資訊：

- 來源電腦
- 指定收件者
- 封包資料的處理方式
- 接收封包的通訊埠
  通訊埠是一種通道，會將來自 Internet 上的資料流分隔開來。 電腦上執行的應用程式會接聽通訊埠。 應用程式會接受傳送到通訊埠的資料。

網路攻擊即是利用易受攻擊的應用程式中的弱點。 攻擊者會利用這些弱點，將包含惡意程式碼的封包傳送到通訊埠。 當易受攻擊的應用程式接聽通訊埠時，惡意程式碼就能讓攻擊者存取電腦。

請參閱第 290 頁的「關於 Symantec Endpoint Protection 防火牆」。

請參閱第 288 頁的「管理防火牆防護」。

關於 Symantec Endpoint Protection 防火牆

Symantec Endpoint Protection 防火牆會使用防火牆政策和規則來允許或攔截網路流量。 Symantec Endpoint Protection 包含預設的防火牆政策，提供辦公室環境所需的預設防火牆規則和防火牆設定。辦公室環境通常受到企業防火牆、邊界封包篩選器或防毒伺服器的保護。因此辦公室環境比起使用有限邊界保護的大多數家用環境，通常要更安全。

防火牆規則可控制用戶端如何保護用戶端電腦，不受惡意入埠流量及惡意離埠流量的攻擊。防火牆自動根據這些規則檢查所有入埠及離埠的封包。然後，防火牆根據規則中指定的資訊允許或攔截封包。當一台電腦嘗試與另一台電腦連線時，防火牆會將連線類型與其防火牆規則清單進行比較。防火牆也會對所有網路流量使用狀態式檢測。

當您首次安裝主控台時，它會自動將預設防火牆政策新增至每個群組。

每當您新增位置時，主控台會自動將防火牆政策複製到預設位置。

您可以決定使用者與用戶端互動的程度，即允許或禁止其架構防火牆規則和防火牆設定。只有在用戶端將新的網路連線和可能的問題通知使用者時，使用者才能與用戶端互動。您也可以為他們授予對使用者介面的完全存取權。

您可以使用預設防火牆設定安裝用戶端。在大多數情況下，您無須變更設定。不過，如果您對網路有深入的瞭解，可以對用戶端防火牆做許多變更，自行調整用戶端電腦'的防護功能。

自 14.2 版起，Mac 用戶端僅提供適用於受管用戶端的防火牆。僅當管理員已允許用戶端控制時，使用者才能啟用或停用防火牆。由於它會在不同於 Mac 作業系統防火牆的網路層運作，因此可以同時啟用和並行執行。

請參閱第 291 頁的「關於 Mac 用戶端的防火牆設定」。

請參閱第 288 頁的「管理防火牆防護」。

請參閱第 289 頁的「防火牆的運作方式」。

請參閱第 300 頁的「防火牆如何使用狀態式檢測」。

請參閱第 270 頁的「安全政策類型」。

關於 Mac 用戶端的防火牆設定

包含在適用於 Mac 的 Symantec Endpoint Protection 用戶端中的防火牆設定如下：

- 防火牆智慧型規則
- 自訂防火牆規則

只有 Symantec Endpoint Protection Manager 管理員能架構這些設定。防火牆僅適用於受管用戶端。

表 16-2　　防火牆設定

設定類型	說明
防火牆智慧型規則	防火牆智慧型規則提供防護來防止常見的攻擊類型。這些規則也會在 Mac 對特定的通訊協定提出初始要求時，允許該通訊協定上的流量。 防護設定包括： ■ 通訊埠掃描偵測 ■ 服務阻斷偵測 ■ 防 MAC 詐騙 ■ 自動攔截攻擊者的 IP 位址 流量通訊協定包括： ■ 智慧型 DHCP ■ 智慧型 DNS 適用於 Mac 的 Symantec Endpoint Protection 防火牆未與作業系統的內建防火牆整合，而是會並行執行。作業系統防火牆會在應用層進行檢查，而 Symantec Endpoint Protection 防火牆則在較低層級 (網路和傳輸) 進行檢查。 適用於 Mac 的 Symantec Endpoint Protection 防火牆不提供點對點攔截規則，但是您可以透過自訂防火牆規則建立部分這類規則。
自訂防火牆規則	自訂防火牆規則可讓管理員建立涉及各種網路流量屬性的規則。

請參閱第 288 頁的「管理防火牆防護」。

建立防火牆政策

Symantec Endpoint Protection 包含預設的防火牆政策，提供辦公室環境所需的預設防火牆規則和預設防火牆設定。辦公室環境通常受到企業防火牆、邊界封包篩選器或防毒伺服器的保護。因此辦公室環境比起使用有限邊界保護的大多數家用環境，通常要更安全。

當您首次安裝主控台時，它會自動將預設防火牆政策加入每個群組。

附註：變更預設防火牆政策的名稱可能會導致升級未更新政策。這一點同樣適用於預設防火牆政策中的預設規則。

每當您新增位置時，主控台會自動將防火牆政策複製到預設位置。如果預設的防護並不適合，您可以自訂每個位置的防火牆政策，例如主站台或客戶站台。如果您不想使用預設防火牆政策，可以進行編輯或以其他共用政策加以取代。

表 16-3 說明可執行以架構新防火牆政策的工作。您首先必須增加防火牆政策，但之後其餘的工作是選擇性的，您可以按任何順序完成這些工作。

表 16-3 如何建立防火牆政策

工作	敘述
新增防火牆規則	防火牆規則是政策元件，會控制防火牆防護用戶端電腦不受惡意連入流量和應用程式侵襲的方式。防火牆會自動根據這些規則檢查所有連入封包及連出封包。防火牆會根據規則中指定的資訊允許或攔截封包。您可以修改預設規則、建立新的規則或停用預設規則。 建立新的防火牆政策時，Symantec Endpoint Protection 會提供預設啟用的預設防火牆規則。 請參閱第 295 頁的「新增防火牆規則」。
啟用和自訂告知使用者所存取的應用程式已受到攔截的通知	您可以向使用者傳送已攔截其要存取的應用程式的通知。 依預設會停用這些設定。 請參閱第 304 頁的「通知使用者已攔截存取應用程式」。
啟用自動防火牆規則	您可以啟用自動允許特定網路服務之間進行通訊的選項。使用這些選項，就不需建立明確允許這些服務的規則。您也可以啟用流量設定，偵測和攔截透過 NetBIOS 與 Token Ring 進行通訊的流量。 依預設，只會啟用流量通訊協定。 請參閱第 320 頁的「為網路服務啟用通訊而非新增規則」。 如果 Symantec Endpoint Protection 用戶端偵測到網路攻擊，會自動攔截連線以保護用戶端電腦的安全。用戶端會啟動主動回應，此功能會自動攔截特定期間內所有進出攻擊電腦的通訊。單一位置會攔截攻擊電腦的 IP 位址。 此選項預設為停用。 請參閱第 321 頁的「自動攔截連線至攻擊電腦」。

工作	敘述
架構防護和隱藏設定	您可啟用設定，偵測並記錄可能在用戶端上進行的攻擊，並攔截詐騙行動。您可啟用防止外部攻擊偵測用戶端相關資訊的設定。 請參閱第 323 頁的「防止對電腦的外部隱藏攻擊」。 依預設會停用所有防護選項和隱藏選項。
將 Symantec Endpoint Protection 防火牆與 Windows 防火牆整合	您可以指定 Symantec Endpoint Protection 停用 Windows 防火牆的條件。解除安裝 Symantec Endpoint Protection 後，Symantec Endpoint Protection 會將 Windows 防火牆設定還原為安裝 Symantec Endpoint Protection 之前的狀態。 預設設定為僅停用 Windows 防火牆一次，並停用 Windows 防火牆停用訊息。 請參閱第 323 頁的「停用 Windows 防火牆」。
架構點對點驗證	您可以使用點對點驗證，允許遠端用戶端電腦 (對等者) 連線至同一企業網路內的其他用戶端電腦 (驗證者)。驗證者會暫時攔截遠端電腦的入埠 TCP 和 UDP 流量，直到遠端電腦通過主機完整性檢查。 此選項預設為停用。 請參閱第 531 頁的「透過架構點對點驗證攔截遠端電腦」。

啟用防火牆防護時，政策會允許所有入埠 IP 網路流量和所有離埠 IP 網路流量，但以下情況例外：

- 預設的防火牆防護會攔截與所有遠端系統的入埠與離埠 IPv6 流量。

  附註：IPv6 是用於網際網路的網路層通訊協定。如果您在執行 Microsoft Vista 的電腦上安裝用戶端，則**「規則」**清單會包含攔截 IPv6 乙太網路通訊協定類型的數種預設規則。如果移除這些預設規則，就必須建立攔截 IPv6 的規則。

- 預設的防火牆防護會限制一些經常用於進行攻擊之通訊協定 (例如 Windows 檔案共用) 的入埠連線。
  允許內部網路連線，但會攔截外部網路。

請參閱第 288 頁的「管理防火牆防護」。

請參閱第 235 頁的「針對遠端用戶端之防火牆政策設定的最佳實務準則」。

管理防火牆規則

防火牆規則會控制防火牆如何防護您的電腦不受惡意的連入流量和應用程式侵襲。防火牆會針對您啟用的規則，檢查所有連入和連出封包。它會根據您在防火牆規則中指定的條件，允許或攔截封包。

Symantec Endpoint Protection 會與包含預設規則的預設防火牆政策一併安裝。建立新的防火牆政策時，Symantec Endpoint Protection 會提供預設防火牆規則。如果您的管理員允許，或者您的用戶端未受管理，則可以修改任何預設規則，或建立新的防火牆規則。

政策中必須至少有一個規則。不過，您可以視需要使用任意數量的規則。您可以視需要啟用或停用規則。例如，您可能需要停用某個規則以執行疑難排解，並在完成後再次啟用該規則。

表 16-4 說明管理防火牆規則所需瞭解的相關內容。

表 16-4 管理防火牆規則

工作	敘述
瞭解防火牆規則如何運作以及構成防火牆規則的內容	在您修改防火牆規則之前，應該先瞭解下列關於防火牆規則如何運作的資訊： ■ 用戶端使用者控制等級以及使用者與防火牆規則的互動，兩者之間的關係。伺服器規則和用戶端規則之間的關係。請參閱第 296 頁的「關於防火牆伺服器規則和用戶端規則」。 ■ 如何排序規則，以確保先評估限制最嚴格的規則，最後評估最一般的規則 請參閱第 297 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。 ■ 從父群組繼承規則的含義，以及如何處理繼承的規則 請參閱第 298 頁的「關於繼承的防火牆規則」。 ■ 用戶端使用狀態式檢測，可保持追蹤網路連線的狀態 請參閱第 300 頁的「防火牆如何使用狀態式檢測」。 ■ 組成防火牆規則的防火牆元件 當您瞭解這些觸發條件以及如何能充分加以善用後，就可以自訂防火牆規則來保護您的用戶端和伺服器。 請參閱第 301 頁的「關於防火牆規則應用程式觸發條件」。 請參閱第 305 頁的「關於防火牆規則主機觸發條件」。 請參閱第 308 頁的「關於防火牆規則網路服務觸發條件」。 請參閱第 309 頁的「關於防火牆規則網路配接卡觸發條件」。
新增防火牆規則	您可以執行下列工作來管理防火牆規則： ■ 使用幾種方法，透過主控台新增防火牆規則 有一種方法可讓您增加具有預設設定的空白規則。另一種方法則會提供精靈，在建立新規則的過程中給您指導。 請參閱第 295 頁的「新增防火牆規則」。 ■ 藉由變更任何防火牆規則準則來自訂規則 ■ 從其他防火牆政策匯出和匯入防火牆規則 請參閱第 310 頁的「匯入和匯出防火牆規則」。 ■ 複製並貼上防火牆規則 您可以複製與要建立之規則類似的現有規則，以節省建立新防火牆規則的時間。然後，您可以修改複製的規則以配合您的需要。

工作	敘述
自訂防火牆規則	建立新規則後 (或者，如果您要自訂預設規則)，您可以修改任何防火牆規則條件。 請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 288 頁的「管理防火牆防護」。

新增防火牆規則

您可以使用下列任一種方法建立新的防火牆規則：

空白的規則
: 空白規則會允許所有流量。
請參閱第 295 頁的「新增新的空白防火牆規則」。

新增防火牆規則精靈
: 如果您使用**「新增防火牆規則」**精靈新增規則，請務必架構該規則。此精靈不會架構具有多個準則的新規則。
請參閱第 296 頁的「使用精靈新增防火牆規則」。

您應該盡可能在規則中同時指定入埠和離埠流量。您無須建立 HTTP 等流量的入埠規則。Symantec Endpoint Protection 用戶端會針對 TCP 流量使用狀態式檢測。因此，不需要規則來篩選用戶端啟始的傳回流量。

當您建立新的防火牆規則時，它會自動啟用。如果您要允許存取特定的電腦或應用程式，可以停用某項防火牆規則。 所有繼承政策都會停用該規則。

若為共用政策，則所有位置也都會停用該規則；若為位置特定政策，則只有一個位置會停用該規則。

附註：規則必須啟用，防火牆才能處理這些規則。

新增新的空白防火牆規則

1. 在主控台中，開啟防火牆政策。
2. 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。
3. 在**「規則」**標籤的**「規則」**清單下，按下**「新增空白規則」**。
4. 或者，您也可以視需要變更防火牆規則準則。
5. 架構完此規則後，按下**「確定」**。

使用精靈新增防火牆規則

1 在主控台中，開啟防火牆政策。

2 在「**防火牆政策**」頁面的「**Windows 設定**」或「**Mac 設定**」下方，按下「**規則**」。

在「**規則**」標籤的「**規則**」清單下，按下「**新增規則**」。

3 在每個畫面上填寫選項，然後按「**下一步**」。

4 按下「**完成**」。

或者，您也可以視需要變更防火牆規則準則。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 300 頁的「防火牆如何使用狀態式檢測」。

關於防火牆伺服器規則和用戶端規則

規則可分為伺服器規則或用戶端規則。伺服器規則是您在 Symantec Endpoint Protection Manager 建立並下載至 Symantec Endpoint Protection 用戶端的規則。用戶端規則是使用者在用戶端上建立的規則。

Mac 用戶端上的所有規則都是伺服器規則。Mac 使用者沒有為 Mac 用戶端建立用戶端規則的選項。

表 16-5說明以下兩者之間的關係，用戶端使用者控制等級以及使用者與防火牆規則的互動。

表 16-5 使用者控制等級和規則狀態

使用者控制等級	使用者互動
伺服器控制	Windows 用戶端接收到伺服器規則，但使用者無法檢視這些規則。使用者無法建立用戶端規則。 Mac 用戶端不允許使用者啟用或停用防火牆。
混合控制	Windows 用戶端接收到伺服器規則。使用者可以建立用戶端規則，這些規則會與伺服器規則以及用戶端安全設定合併。 Mac 用戶端允許或不允許使用者啟用或停用防火牆。此取決於精細設定設定為伺服器控制或用戶端控制。
用戶端控制	用戶端不接收伺服器規則。使用者可以建立用戶端規則。Symantec Endpoint Protection Manager 管理員無法檢視用戶端規則。 Mac 用戶端允許使用者啟用或停用防火牆。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

表 16-6 列出防火牆對伺服器規則、用戶端規則和用戶端設定的處理順序。

表 16-6 伺服器規則和用戶端規則的處理優先順序

優先順序	規則類型或設定
第一	高優先順序的伺服器規則 (「**規則**」清單中藍線以上的規則)
第二	用戶端規則
第三	低優先順序的伺服器規則 (「**規則**」清單中藍線以下的規則) 在用戶端，藍線以下的伺服器規則會在用戶端規則之後處理。
第四	用戶端安全設定
第五	用戶端應用程式專用的設定

在用戶端，使用者可以修改用戶端規則或安全設定，但使用者無法修改伺服器規則。

警告：如果用戶端為混合控制，使用者可以建立允許所有流量的用戶端規則。此規則會覆寫藍線以下所有的伺服器規則。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 300 頁的「變更防火牆規則的順序」。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

關於防火牆規則、防火牆設定和入侵預防處理順序

防火牆規則會在規則清單中，從最高到最低優先順序，依序排列。如果第一項規則未指定如何處理封包，防火牆就會檢查第二項規則。這項程序會持續進行，直到防火牆找到符合的規則為止。防火牆找到符合的規則後，就會採取該規則指定的動作，而不會再檢查優先順序較低的後續規則。例如，若第一項規則指定攔截所有流量，而下一項規則允許所有流量，則用戶端會攔截所有流量。

您可以根據限制的嚴格性將規則排序。先評估限制最嚴格的規則，最後評估最普通的規則。例如，攔截流量的規則應該排在規則清單前幾位，清單中優先順序較低的規則可能會允許流量。

規則清單中有條藍色分隔線。在下列情況中，分隔線會設定各項規則的優先順序：

- 子群組繼承父群組的規則。
- Windows 用戶端設定為混合控制。防火牆同時處理伺服器規則和用戶端規則。

表 16-7 顯示防火牆處理規則、防火牆設定和入侵預防設定的順序。

表 16-7 處理順序

優先順序	設定
第一	自訂 IPS 特徵
第二	入侵預防設定、流量設定及隱藏設定
第三	內建規則
第四	防火牆規則
第五	通訊埠掃描檢查
第六	透過 LiveUpdate 下載的 IPS 特徵

請參閱第 300 頁的「變更防火牆規則的順序」。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 289 頁的「防火牆的運作方式」。

請參閱第 328 頁的「入侵預防的運作方式」。

關於繼承的防火牆規則

子群組的政策可以僅繼承父群組中啟用的防火牆規則。當您已繼承規則時，可以停用這些規則，但無法加以修改。當新規則新增至父群組的政策時，新規則會自動新增至繼承政策。

繼承的規則顯示在**「規則」**清單中時，會加上斜體 (14.x 版) 或紫色 (12.1.x 版) 陰影。在藍字那行上面，繼承的規則會新增到您以 Symantec Endpoint Protection Manager 管理員身分所建立的規則上面。在藍字那行下面，繼承的規則會新增到您所建立的規則下面。

防火牆政策也會繼承預設規則，因此子群組的防火牆政策可能會有兩組的預設規則。您可能會想要刪除其中一組預設規則。

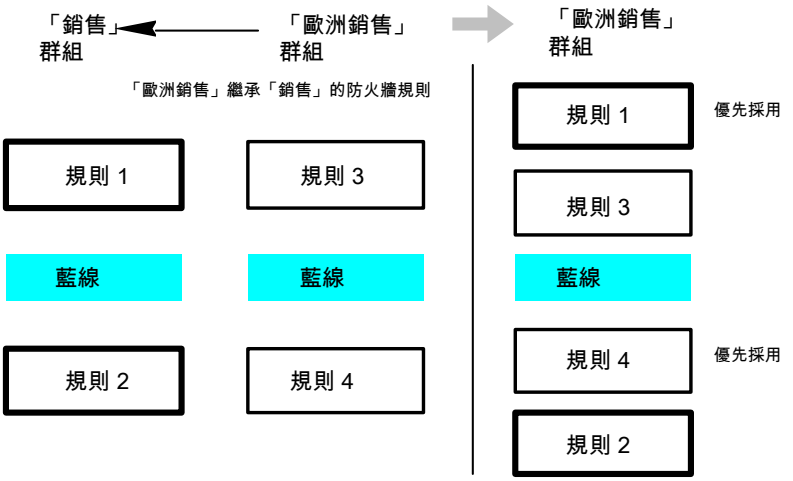
若要移除繼承的規則，請移除繼承，而不是刪除這些規則。您必須移除所有繼承的規則，而不是選取的規則。

防火牆處理**「規則」**清單中繼承的防火牆規則，其方式如下：

在藍色分隔線之上	政策繼承的規則優先順序高於您建立的規則。
在藍色分隔線之下	您建立的規則優先順序高於政策繼承的規則。

圖 16-1 顯示當子群組從父系群組繼承規則時，**「規則」**清單如何排列規則順序。此例中，「銷售」群組是父群組。「歐洲銷售」群組從「銷售」群組繼承。

圖 16-1 防火牆規則互相繼承方式的範例



請參閱第 293 頁的「管理防火牆規則」。

請參閱第 299 頁的「新增繼承自父群組的防火牆規則」。

新增繼承自父群組的防火牆規則

您可以藉由從父群組繼承規則，將防火牆規則新增至防火牆政策。若要從父群組繼承規則，子群組的政策必須不是共用政策。

附註：如果群組的所有政策都繼承自父群組，則無法使用此選項。

新增繼承自父群組的防火牆規則

1 在主控台中，開啟防火牆政策。

2 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。

3 在**「規則」**標籤上，勾選**「從父群組繼承防火牆規則」**。

若要移除繼承的規則，請取消勾選**「從父群組繼承防火牆規則」**。

4 按下**「確定」**。

請參閱第 272 頁的「編輯政策」。

請參閱第 298 頁的「關於繼承的防火牆規則」。

請參閱第 293 頁的「管理防火牆規則」。

變更防火牆規則的順序

防火牆會由上而下處理防火牆規則清單。您可以變更防火牆規則的順序，以決定防火牆處理防火牆規則的方式。

如果 Symantec Endpoint Protection 用戶端使用位置切換，則當您變更防火牆規則順序時，該變更只會影響目前位置的順序。

附註：為加強防護效果，請將最嚴格的規則放在最前面，最寬鬆的規則放在最後面。

請參閱第 297 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。

變更防火牆規則的順序

1. 在主控台中，開啟某個防火牆政策。
2. 在**「防火牆政策」**頁面上，按下**「規則」**，再選取要移動的規則。
3. 執行下列其中一項工作：
   - 若要將所選規則調整到上一則規則之前處理，請按下**「上移」**。
   - 若要將所選規則調整到下一則規則之後處理，請按下**「下移」**。
4. 按下**「確定」**。

請參閱第 272 頁的「編輯政策」。

請參閱第 293 頁的「管理防火牆規則」。

防火牆如何使用狀態式檢測

防火牆防護會使用狀態式檢測追蹤目前連線。狀態式檢測可追蹤來源及目的 IP 位址、通訊埠、應用程式以及其他連線資訊。 用戶端檢查防火牆規則之前，會先根據連線資訊決定流量。

例如，如果防火牆規則允許電腦連線至 Web 伺服器，防火牆便會記錄連線資訊。 當伺服器回覆時，防火牆預測會產生從 Web 伺服器到電腦的回應。 便會允許 Web 伺服器流量傳送到發起流量的電腦，而不會檢查規則資料庫。 在防火牆將連線記錄之前，規則必須允許最初的離埠流量。

使用狀態式檢測就不必再建立新規則。 對於單向起始的流量，您無須建立允許雙向流量的規則。 單向起始的用戶端流量包括 Telnet (通訊埠 23)、HTTP (通訊埠 80) 及 HTTPS (通訊埠 443)。 用戶端電腦會發起此離埠流量，您可以為這些通訊協定建立允許離埠流量的規則。 狀態式檢測會自動允許回應出埠流量的傳回流量。由於防火牆在本質上是狀態式的，因此您只需建立起始連線的規則，無需建立特定封包的特性。所有屬於允許連線的封包隱含允許作為同一連線不可缺少的部分。

狀態式檢測支援指引 TCP 流量的所有規則。

狀態式檢測不支援篩選 ICMP 流量的規則。 對於 ICMP 流量，您必須建立允許雙向流量的規則。 例如，若要讓用戶端使用 Ping 指令並接收回覆，您必須建立允許雙向 ICMP 流量的規則。

您可以定期清除維護連線資訊的狀態表。 例如，當防火牆政策更新已處理或 Symantec Endpoint Protection 服務已重新啟動時，便會清除它。

請參閱第 289 頁的「防火牆的運作方式」。

請參閱第 293 頁的「管理防火牆規則」。

關於防火牆規則應用程式觸發條件

如果應用程式是您在允許流量的規則中定義的唯一觸發條件，則防火牆會允許該應用程式執行任何網路作業。應用程式才是發揮作用的值，而不是應用程式執行的網路作業。例如，假設您允許 Internet Explorer，而且未定義其他任何觸發條件。則使用者可以存取使用 HTTP、HTTPS、FTP、Gopher 及網頁瀏覽器所支援其他任何通訊協定的遠端站台。您可以定義其他觸發條件，說明允許進行通訊的特定網路通訊協定和主機。

以應用程式為基礎的規則可能不太容易進行疑難排解，因為應用程式可能使用有多種通訊協定。例如，如果防火牆先處理允許 Internet Explorer 的規則，再處理攔截 FTP 的規則，使用者仍可以與 FTP 通訊。使用者可以在瀏覽器輸入使用 FTP 的 URL，例如 ftp://ftp.symantec.com。

例如，假設您允許 Internet Explorer，而且未定義其他任何觸發條件。則電腦使用者可以存取使用 HTTP、HTTPS、FTP、Gopher，以及網頁瀏覽器所支援之其他通訊協定的遠端站台。您可以定義其他觸發條件，描述允許進行通訊的網路通訊協定和主機。

請不要使用應用程式規則來控制網路層級的流量。例如，如果使用者使用其他網頁瀏覽器，攔截或限制使用 Internet Explorer 的規則就沒有作用。其他網頁瀏覽器所產生的流量還是會與 Internet Explorer 規則以外的所有其他規則比對。規則架構為攔截傳送和接收流量的應用程式時，以應用程式為基礎的規則才比較適用。

請參閱第 301 頁的「定義應用程式的相關資訊」。

請參閱第 304 頁的「通知使用者已攔截存取應用程式」。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 303 頁的「攔截可能受到攻擊的網路應用程式」。

定義應用程式的相關資訊

您可以定義用戶端執行的應用程式的相關資訊，並將此資訊納入防火牆規則中。

您可以使用下列方式定義應用程式：

- 手動輸入資訊。
  請參閱第 302 頁的「手動定義應用程式的相關資訊」。
- 在探索到的應用程式清單中搜尋應用程式。

探索到的應用程式清單中的應用程式是您網路中用戶端電腦執行的應用程式。
請參閱第 302 頁的「從探索到的應用程式清單搜尋應用程式」。

手動定義應用程式的相關資訊

1 在主控台中，開啟某個防火牆政策。

2 在**「防火牆政策」**頁面的**「Windows 設定」**下方，按下**「規則」**。

3 在**「規則」**標籤的**「規則」**清單中，用滑鼠右鍵按下要變更規則的**「應用程式」**欄位，再按下**「編輯」**。

4 在**「應用程式清單」**對話方塊中，按下**「新增」**。

5 在**「新增應用程式」**對話方塊中，輸入下列一或多個欄位：

- 檔案名稱，可包含檔案路徑
- 檔案敘述
  此欄位僅作為顯示之用。無法作為比對條件使用。
- 檔案大小 (位元組)
- 應用程式上次變更的日期
- 檔案指紋

附註：必須啟用「網路應用程式監控」才能依檔案大小、上次修改日期或檔案指紋定義防火牆規則。如果停用「網路應用程式監控」，規則處理會忽略**「檔案名稱」**以外的所有欄位。

---

6 按下**「確定」**新增應用程式條件。

7 按下**「確定」**儲存應用程式清單。

從探索到的應用程式清單搜尋應用程式

1 在**「防火牆政策」**頁面上，按下**「規則」**。

2 在**「規則」**標籤選取規則，用滑鼠右鍵按下**「應用程式」**欄位，再按下**「編輯」**。

3 在**「應用程式清單」**對話方塊中，按下**「新增自」**。

4 在**「搜尋應用程式」**對話方塊中搜尋應用程式。

5 在**「查詢結果」**表下，若要新增應用程式到**「應用程式」**清單，請選取應用程式，按**「新增」**，再按**「確定」**。

6 按下**「關閉」**。

7 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 272 頁的「編輯政策」。

請參閱第 301 頁的「關於防火牆規則應用程式觸發條件」。

攔截可能受到攻擊的網路應用程式

網路應用程式監控會將應用程式的行為記錄在安全日誌中。如果應用程式的內容修改太過頻繁，應用程式可能是受到特洛伊木馬程式攻擊，用戶端電腦就處於不安全的狀態。如果應用程式的內容修改並非經常性，則可能已安裝修正程式，而用戶端電腦處於安全狀態。您可以使用這些資訊建立防火牆規則來允許或攔截應用程式。

您可以架構用戶端偵測和監控用戶端電腦上執行的任何網路應用程式。網路應用程式會傳送和接收流量。用戶端會偵測應用程式的內容是否變更。

如果您懷疑應用程式受到了特洛伊木馬程式攻擊，可以使用網路應用程式監控架構用戶端攔截應用程式。您也可以架構用戶端詢問使用者是允許還是攔截應用程式。

應用程式內容變更的原因如下：

- 應用程式受到特洛伊木馬程式攻擊。
- 應用程式已更新為新版本或使用更新程式進行了更新。

您可以將應用程式新增到清單，設定用戶端不監控它們。您可以將認為不會受到特洛伊木馬程式攻擊，但經常會有自動修正程式更新的應用程式排除在監控之外。

您也可以將詢問使用者允許或攔截網路應用程式的通知數減至最少。

攔截可能受到攻擊的網路應用程式

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下方選取群組後，再按下**「政策」**。
3. 在**「政策」**標籤的**「與位置無關的政策與設定」**下方，按下**「網路應用程式監控」**。
4. 在**「用於 <*群組名稱*> 的網路應用程式監視」**對話方塊中，按下**「啟用網路應用程式監控」**。
5. 在**「偵測到應用程式變更時」**下拉式清單中，選取防火牆要對用戶端上執行的應用程式採取的動作：

詢問	詢問使用者是允許還是攔截應用程式。
攔截流量	攔截應用程式使其無法執行。
允許並記錄日誌	允許應用程式執行，並將資訊記錄在安全日誌中。 防火牆只會對修改過的應用程式採取此動作。

6. 如果選取**「詢問」**，請按下**「其他文字」**。
7. 在**「其他文字」**對話方塊中，鍵入要出現在標準訊息下方的文字，再按下**「確定」**。

8 若要將應用程式排除在監控之外，請在**「未受監控的應用程式清單」**下方，執行下列其中一個工作：

手動定義應用程式	按下**「新增」**，填寫一個或多個欄位，然後按下**「確定」**。
從已知的應用程式清單定義應用程式	按下**「新增自」**。 探索到的應用程式清單會監控網路和非網路應用程式。您只能從探索到的應用程式清單選取網路應用程式。將應用程式加入到**「未受監控的應用程式清單」**之後，您可以啟用、停用、編輯或刪除它們。

9 勾選應用程式旁邊的方塊可以啟用應用程式；取消選中此方塊可停用應用程式。

10 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 304 頁的「通知使用者已攔截存取應用程式」。

請參閱第 301 頁的「關於防火牆規則應用程式觸發條件」。

請參閱第 286 頁的「搜尋有關電腦執行的應用程式資訊」。

請參閱第 285 頁的「收集有關用戶端電腦執行的應用程式資訊」。

通知使用者已攔截存取應用程式

您可以向使用者傳送已攔截其要存取的應用程式的通知。此通知會顯示在使用者電腦上。

附註：啟用太多通知不僅會使使用者感到不知所措，還會向這些使用者傳送警示。啟用通知時請務必小心。

通知使用者已攔截存取應用程式

1 在主控台中，開啟防火牆政策。

2 在**「防火牆政策」**頁面上，按下**「規則」**。

3 在**「通知」**標籤上，勾選**「用戶端攔截應用程式時在電腦上顯示通知」**，並選擇性地新增自訂訊息。

4 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 333 頁的「針對入侵預防和記憶體攻擊緩和架構用戶端通知」。

請參閱第 577 頁的「設定管理員通知」。

關於防火牆規則主機觸發條件

定義主機觸發條件時，您須指定位於所述網路連線兩端的主機。

一般表示主機之間關係的方式，是將主機稱為網路連線的來源或目的。

您可以使用下列其中一種方式定義主機關係：

來源和目的	主機是來源還是目的取決於流量的方向。有時候可能本機用戶端電腦是來源，而有時候則可能遠端電腦是來源。 來源與目的關係較常用於網路型防火牆。
本機及遠端	本地主機一定是本機用戶端電腦，而遠端主機則一定是位於網路其他位置的遠端電腦。這種主機關係的表示方式與流量方向無關。 本機與遠端關係較常用於主機型防火牆，而且比較容易查看流量。

您可以定義多個來源主機和多個目的主機。

圖 16-2 以流量方向來說明來源和目的的關係。

圖 16-2　　來源與目的主機之間的關係

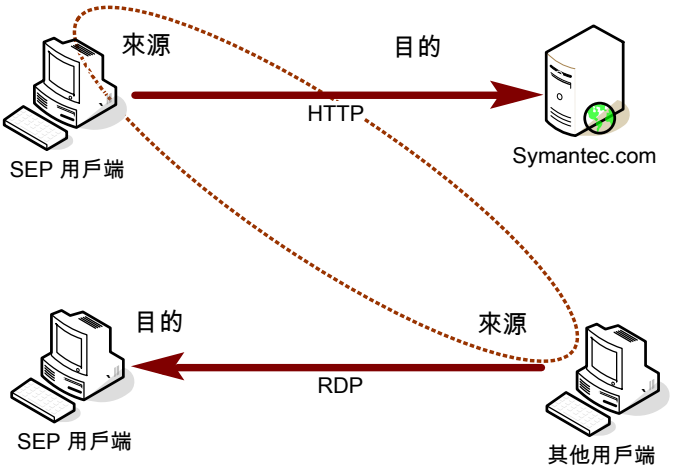
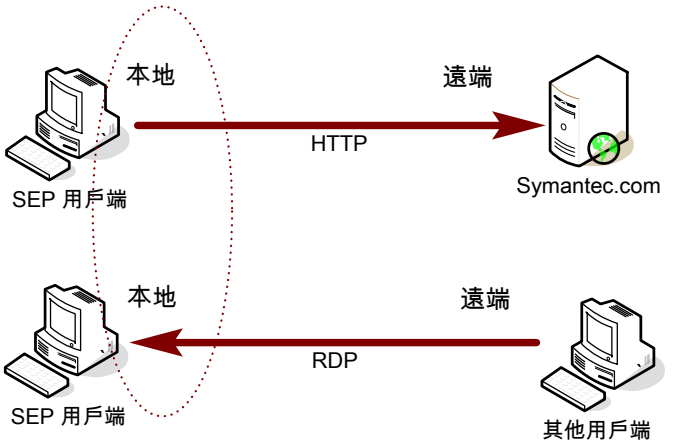


圖 16-3以流量方向說明本地主機與遠端主機的關係。

圖 16-3 本機與遠端主機之間的關係



關係可使用下列陳述類型評估：

在連線 (來源和目的之間) 任一端定義的主機	OR 陳述式
選取的主機	AND 陳述式

例如，假設有個規則定義了單一本地主機和多個遠端主機。當防火牆檢查封包時，本地主機必須符合相關的 IP 位址。不過，位址的另一端則可符合任何遠端主機。例如，您可以定義規則以允許本地主機和 Symantec.com、Yahoo.com 或 Google.com 之間的 HTTP 通訊。單一規則與三個規則相同。

請參閱第 306 頁的「新增主機群組」。

請參閱第 313 頁的「攔截來往於特定伺服器的流量」。

請參閱第 293 頁的「管理防火牆規則」。

新增主機群組

主機群組是 DNS 網域名稱、DNS 主機名稱、IP 位址、IP 範圍、MAC 位址或子網路的集合，在同一個名稱之下組成一個群組。主機群組的目的是為了不必重複輸入主機位址和名稱。例如，您可以將多個 IP 位址一次一個新增到防火牆規則中。或者，可以將多個 IP 位址新增到一個主機群組，然後將群組新增到防火牆規則。

當您加入主機群組時，必須說明群組的使用位置。如果您稍後決定刪除主機群組，必須先從參照此群組的所有防火牆規則中移除主機群組。

新增主機群組時，主機群組會出現在**「主機」**清單最下方。您可以從防火牆規則的**「主機」**欄位中存取**「主機」**清單。

新增主機群組

1 在主控台中，按下**「政策」**。

2 展開**「政策元件」**，然後按下**「主機群組」**。

3 在**「工作」**下，按下**「新增主機群組」**。

4 在 **「主機群組」**對話方塊中輸入名稱，再按下**「新增」**。

5 在**「主機」**對話方塊中，按下**「類型」**下拉式清單，再選取主機。

6 輸入每種主機類型的適當資訊。

7 按下**「確定」**。

8 視需要新增其他主機。

9 按下**「確定」**。

請參閱第 305 頁的「關於防火牆規則主機觸發條件」。

定義根據位置的 DNS 查詢

可以定義您要在特定位置執行 DNS 查詢的頻率。此功能可讓您架構一個比其他位置會更頻繁查詢 DNS 伺服器的位置。

例如，假設您有一個政策，會攔截公司網路外部的所有流量 (VPN 流量除外)。並且，假設出差中的使用者必須從旅館網路透過 VPN 存取您的網路。您可以為使用 DNS 解析的 VPN 連線建立政策。Symantec Endpoint Protection 會持續每 5 秒傳送一次 DNS 查詢，直到它切換至此位置為止。這樣，您的使用者即可更快速地存取您的網路。

注意：當您將此設定架構為很低的值時，請格外謹慎。 例如，如果所有系統每 5 秒存取一次伺服器，則可能會使 DNS 伺服器的效能降低。

定義根據位置的 DNS 查詢

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下方，選取此功能要套用的群組。

3 在**「工作」**下方，按下**「管理位置」**。

4 確定勾選**「DNS 查詢迴圈於」**。

5 按下時間設定和增量，並根據需要進行修改。

您可以設定以秒、分鐘或小時為單位的值。

預設值是 30 分鐘。

6 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 305 頁的「關於防火牆規則主機觸發條件」。

關於防火牆規則網路服務觸發條件

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。網路服務會使用一或多個通訊協定或通訊埠，藉此傳送特定類型的流量。例如，HTTP 服務會透過 TCP 通訊協定使用通訊埠 80 和 443。您可以建立允許或攔截網路服務的防火牆規則。網路服務觸發條件會根據所述的網路流量，識別產生作用的一項或多項網路通訊協定。

定義 TCP 型或 UDP 型服務觸發時，您可以指明所描述網路連線兩端的通訊埠。一般將通訊埠稱為網路連線的來源或目的。

請參閱第 308 頁的「新增網路服務至預設網路服務清單」。

請參閱第 316 頁的「允許用戶端瀏覽網路中的檔案和印表機」。

請參閱第 293 頁的「管理防火牆規則」。

新增網路服務至預設網路服務清單

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。您可以建立允許或攔截網路服務的防火牆規則。

使用網路服務清單，就無須在建立攔截或允許網路服務的防火牆規則時還要重複輸入通訊協定和通訊埠。建立防火牆規則時，您可以從預設的常用網路服務清單中選取網路服務。您也可以將網路服務新增到預設清單。不過，您需要瞭解服務所使用的通訊協定類型和通訊埠。

附註：IPv4 和 IPv6 是兩種用於網際網路的網路層通訊協定。如果您在執行 Windows Vista 的電腦上安裝用戶端，則**「規則」**清單會包含攔截 IPv6 乙太網路通訊協定類型的數種預設規則。如果移除這些預設規則，就必須建立攔截 IPv6 的規則。

附註：您可以透過防火牆規則新增自訂網路服務。不過，該網路服務不會加入預設清單。您無法從任何其他規則存取自訂網路服務。

新增網路服務至預設網路服務清單

1. 在主控台中，按下**「政策」**。
2. 展開**「政策元件」**，然後按下**「網路服務」**。
3. 在**「工作」**下，按下**「新增網路服務」**。
4. 在**「網路服務」**對話方塊中，鍵入服務的名稱，再按下**「新增」**。
5. 從**「通訊協定」**下拉式清單選取通訊協定。

   其他選項會根據您所選的通訊協定變更。
6. 輸入適當欄位，然後按下**「確定」**。

7 視需要新增一或多個其他通訊協定。

8 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 308 頁的「關於防火牆規則網路服務觸發條件」。

請參閱第 315 頁的「控制網路電腦是否可以共用郵件、檔案和列印」。

請參閱第 316 頁的「允許用戶端瀏覽網路中的檔案和印表機」。

關於防火牆規則網路配接卡觸發條件

您可以定義防火牆規則，攔截或允許通過 (傳輸或接收) 網路配接卡到的流量。

當您定義特定類型的配接卡時，請將配接卡的使用方式列入考量。例如，如果規則允許乙太網路配接卡的離埠 HTTP 流量，則已安裝的所有同類型配接卡都會允許 HTTP 通過。唯一的例外是同時指定了本地主機位址。用戶端電腦可能會使用多 NIC 的伺服器和工作站來橋接兩個以上的網路區段。若要控制特定配接卡的相關流量，就必須使用每個區段的位址配置，而不是配接卡本身。

網路配接卡清單可讓使用者無須為防火牆規則重新輸入配接卡類型。建立防火牆規則時，您可以從常用網路配接卡的預設清單選取網路配接卡。您也可以將網路配接器新增到預設清單。

您可以從防火牆政策和規則之間共用的預設清單選取網路配接器。**「政策元件」**清單的預設清單包含最常見的配接卡。

附註：您可以透過防火牆規則新增自訂網路配接卡。但是，該網路配接卡不會加入預設清單。您無法從任何其他規則存取自訂網路配接卡。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 309 頁的「將自訂網路配接卡新增到網路配接卡清單」。

請參閱第 318 頁的「控制通過網路配接卡的流量」。

將自訂網路配接卡新增到網路配接卡清單

您可以對每個網路配接卡分別套用不同的防火牆規則。例如，您可能會想要在辦公室攔截經由 VPN 的流量，但不會想在家裡這麼做。

您可以從所有防火牆政策和規則共用的預設清單選取網路配接卡。**「政策元件」**清單的預設清單包含最常見的配接卡。使用預設清單，您就無須為每個建立的規則重新輸入每個網路配接卡。

使用網路配接卡清單，就無須為防火牆規則重新輸入配接卡。建立防火牆規則時，您可以從預設的常用網路配接卡清單中選取網路配接卡。您也可以將網路配接卡新增到預設清單。

附註：您可以透過防火牆規則新增自訂網路配接卡。但是，該網路配接卡不會加入預設清單。您無法從任何其他規則存取自訂網路配接卡。

將自訂網路配接卡新增到網路配接卡清單

1. 在主控台中，按下**「政策」>「政策元件」>「網路配接卡」**。
2. 在**「工作」**下，按下**「新增網路配接卡」**。
3. 在**「網路配接卡」**對話方塊中，按下**「配接卡類型」**下拉式清單，再選取配接卡。
4. 在**「配接卡名稱」**欄位中，選擇性地輸入敘述。
5. 在**「配接卡識別」**文字方塊中，輸入配接卡品牌名稱，須區分大小寫。

   若要找出配接卡的品牌名稱，可開啟用戶端的指令行，並輸入下列文字：

   ```
   ipconfig/all
   ```
6. 按下**「確定」**。

請參閱第 293 頁的「管理防火牆規則」。

請參閱第 309 頁的「關於防火牆規則網路配接卡觸發條件」。

請參閱第 318 頁的「控制通過網路配接卡的流量」。

匯入和匯出防火牆規則

您可以從其他防火牆政策匯出和匯入防火牆規則與設定，如此就不須重新建立這些規則與設定。例如，您可將某個政策的部分規則集匯入至另一個政策。若要匯入規則，您必須先將規則匯出至 .dat 檔案，並有該檔案的存取權。

規則會以其在父政策所列的順序新增，以藍線為準。您可以稍後變更其處理順序。

匯出防火牆規則

1. 在主控台中，開啟防火牆政策。
2. 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。
3. 在**「規則」**清單中，選取要匯出的規則並按下滑鼠右鍵，再按下**「匯出」**。
4. 在**「匯出政策」**對話方塊中，找出目錄來儲存 .dat 檔案，然後輸入檔案名稱，再按下**「匯出」**。

匯入防火牆規則

1. 在主控台中，開啟防火牆政策。
2. 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。
3. 用滑鼠右鍵按下「規則」清單，再按下**「匯入」**。
4. 在**「匯入政策」**對話方塊中，找出包含想要匯入防火牆規則的 .dat 檔案，再按下**「匯入」**。

5 在「**輸入**」對話方塊中，輸入政策的新名稱，再按下「**確定**」。

6 按下「**確定**」。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 297 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。

自訂防火牆規則

建立新的防火牆政策時，該政策會包括多個預設規則。您可以根據需要修改一個或多個規則元件。

防火牆規則的元件如下：

動作

動作參數會指定防火牆成功比對到規則時所採取的動作。如果有規則符合並被選取來回應接收的封包，則防火牆會執行全部動作。防火牆可以允許或攔截封包，也可以記錄或不記錄封包。如果防火牆允許流量通過，則會讓規則指定的流量存取網路。如果防火牆攔截流量，則會攔截規則指定的流量，不讓流量存取網路。

動作如下：

- 允許
  防火牆允許網路連線。
- 攔截
  防火牆攔截網路連線。

附註：Mac 用戶端防火牆會監控封包，但不會記錄封包。

觸發條件

當防火牆評估規則時，全部觸發條件都必須為真，才會出現完全符合的狀況。對於目前封包而言，如果其中有任一個觸發條件不是真，防火牆即不會套用規則。您可以結合各項觸發條件的定義，形成更複雜的規則，例如根據特定目的位址，識別特定通訊協定。

觸發條件如下：

- 應用程式
  如果應用程式是您在允許流量規則中定義的唯一觸發條件，防火牆將允許此應用程式執行任何網路作業。應用程式才是發揮作用的值，而不是應用程式執行的網路作業。您可以定義其他觸發條件，描述允許進行通訊的特定網路通訊協定和主機。
  請參閱第 301 頁的「關於防火牆規則應用程式觸發條件」。
- 主機
  在定義主機觸發條件時，您可以指定位於所述網路連線兩端的主機。
  一般表示主機之間關係的方式，是將主機稱為網路連線的來源或目標。
  請參閱第 305 頁的「關於防火牆規則主機觸發條件」。
- 網路服務
  網路服務觸發條件會識別對所述流量而言非常重要的一個或多個網路通訊協定。
  本機主機電腦一定擁有本機通訊埠，而遠端電腦一定擁有遠端通訊埠。這項通訊埠關係的說明與流量方向無關。
  請參閱第 308 頁的「關於防火牆規則網路服務觸發條件」。
- 網路配接卡
  如果您定義網路配接卡觸發條件，規則只會與使用指定配接卡類型傳輸或接收的流量有關。您可以指定任何配接卡，也可以指定目前與用戶端電腦關聯的配接卡。
  請參閱第 309 頁的「關於防火牆規則網路配接卡觸發條件」。

條件

規則條件包含規則排程和螢幕保護程式狀態。

條件參數不會描述網路連線的任何內容。條件參數會決定規則的作用中狀態。您可以定義排程或識別螢幕保護程式的狀態，決定將規則視為作用中或非作用中的狀況。條件參數是選用項目，如果未經定義，則不會有任何作用。防火牆不會評估非作用中的規則。

通知

「日誌」設定用於指定流量事件符合針對這項規則設定的條件時，伺服器是建立日誌項目還是傳送電子郵件。

「嚴重性」設定用於指定違規的嚴重性等級。

自訂防火牆規則

1 在主控台中，開啟防火牆政策。

2 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。

3 在**「規則」**標籤的**「規則」**清單中，在**「已啟用」**欄位中，確定已勾選此方塊啟用此規則；取消勾選此方塊將停用此規則。

Symantec Endpoint Protection 僅處理您啟用的規則。根據預設，會啟用所有規則。

4 連按兩下**「名稱」**欄位，然後鍵入防火牆規則的唯一名稱。

5 在「**動作**」欄位上按下滑鼠右鍵，選取在觸發規則時 Symantec Endpoint Protection 要執行的動作。

6 在「**應用程式**」欄位中，定義應用程式。

請參閱第 301 頁的「定義應用程式的相關資訊」。

7 在「**主機**」欄位中，指定主機觸發條件。

請參閱第 313 頁的「攔截來往於特定伺服器的流量」。

8 除指定主機觸發條件外，您還可以指定允許存取本機子網路的流量。

請參閱第 314 頁的「僅允許本機子網路的特定流量」。

9 在「**服務**」欄位中，指定網路服務觸發條件。

請參閱第 315 頁的「控制網路電腦是否可以共用郵件、檔案和列印」。

10 在「**日誌**」欄位中，指定在違反此防火牆規則時，您希望 Symantec Endpoint Protection 傳送電子郵件給您的時間。

請參閱第 318 頁的「設定違反防火牆規則通知」。

11 在「**嚴重性**」欄位上按下滑鼠右鍵，並選取違規的嚴重性等級。

12 在「**配接卡**」欄中，指定規則的配接卡觸發條件。

請參閱第 318 頁的「控制通過網路配接卡的流量」。

13 在「**時間**」欄中，指定此規則處於使用中狀態的時段。

14 在「**螢幕保護程式**」欄位上按下滑鼠右鍵，並指定用戶端電腦的螢幕保護程式必須處於哪一種狀態時，規則才會啟用。

「**建立於**」欄位無法編輯。如果共用政策，則會顯示「共用」一詞。如果未共用政策，此欄位將顯示指派了此非共用政策的群組的名稱。

15 在「**說明**」欄位上按下滑鼠右鍵，按下「**編輯**」，輸入規則的說明(可選)，然後按下「**確定**」。

16 架構完此規則後，按下「**確定**」。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 293 頁的「管理防火牆規則」。

攔截來往於特定伺服器的流量

若要攔截來往於特定伺服器的流量，請以 IP 位址攔截流量，而不要以網域名稱或主機名稱來攔截流量。否則，使用者還是可以存取與主機名稱對等的 IP 位址。

攔截來往於特定伺服器的流量

1 在主控台中，開啟防火牆政策。

2 在「**防火牆政策**」頁面上，按下「**規則**」。

3 在「**規則**」標籤的「**規則**」清單中，選取要編輯的規則，在「**主機**」欄位按下滑鼠右鍵，然後按下「**編輯**」。

4 在「**主機清單**」對話方塊中，執行下列其中一個動作：

- 按下「**來源/目的**」。
- 按下「**本機/遠端**」。

5 執行下列其中一項工作：

從「**類型**」下拉式清單中選取主機類型	執行下列所有工作： ■ 在「**來源及目的**」或「**本機及遠端**」表中，按下「**新增**」。 ■ 在「**主機**」對話方塊中，從「**類型**」下拉式清單中選取主機類型，然後輸入各主機類型的相應資訊。 ■ 按下「**確定**」。 您建立的主機將自動啟用。
選取主機群組	在「**主機清單**」對話方塊中，執行下列其中一個動作： ■ 按下「**來源/目的**」。 ■ 按下「**本機/遠端**」。 然後在「**主機清單**」對話方塊中，對要新增到此規則的任何主機群組勾選「**已啟用**」欄中的方塊。

6 視需要新增其他主機。

7 按下「**確定**」回到「**規則**」清單。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 306 頁的「新增主機群組」。

僅允許本機子網路的特定流量

您可以建立防火牆規則，來僅允許本機子網路的特定流量。此防火牆規則會永遠套用至本機子網路 IP 位址，而不管該位址為何。因此，即使您變更本機子網路 IP 位址，您也從不必為新位址修改此規則。

例如，您可以建立此規則以僅允許本機子網路通訊埠 80 的流量，而不管本機子網路 IP 位址為何。

僅允許本機子網路的特定流量

1 在主控台中，開啟防火牆政策。

2 在「**防火牆政策**」頁面的「**Windows 設定**」或「**Mac 設定**」下方，按下「**規則**」。

3 在「**規則**」標籤的「**防火牆規則**」表格中，尋找您要編輯的規則。

4 連按兩下您要建立本機子網路流量條件之規則的**「主機」**欄。

5 在此規則套用的主機類型 (「本機」或「遠端」) 下，按下**「新增」**。

6 按下**「地址類型」**下拉式清單並選取下列其中一項：

- Windows：**本機子網路**
- Mac：**子網路**

7 按下**「確定」**，然後再次按下**「確定」**關閉**「主機清單」**對話方塊。

請參閱第 311 頁的「自訂防火牆規則」。

控制網路電腦是否可以共用郵件、檔案和列印

網路服務可讓網路電腦傳送和接收郵件、共用檔案以及列印。您可以建立允許或攔截網路服務的防火牆規則。

您可以透過防火牆規則新增自訂網路服務。不過，該網路服務不會加入預設清單。您無法從任何其他規則存取自訂服務。

控制網路電腦是否可以共用郵件、檔案和列印

1 在主控台中，開啟防火牆政策。

2 在**「防火牆政策」**頁面的**「Windows 設定」**或**「Mac 設定」**下方，按下**「規則」**。

3 在**「規則」**標籤的**「規則」**清單中，選取要編輯的規則，在**「服務」**欄位按下滑鼠右鍵，然後按下**「編輯」**。

4 在**「服務清單」**對話方塊中，對要觸發規則的每項服務，勾選其旁邊的方塊。

5 若只要為選取的規則新增其他服務，請按下**「新增」**。

6 在**「通訊協定」**對話方塊中，從**「通訊協定」**下拉式清單選取通訊協定。

7 填入適當的欄位。

8 按下**「確定」**。

9 按下**「確定」**。

10 按下**「確定」**。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 308 頁的「關於防火牆規則網路服務觸發條件」。

請參閱第 308 頁的「新增網路服務至預設網路服務清單」。

允許用戶端瀏覽網路中的檔案和印表機

您可以讓用戶端在區域網路上提供其檔案共用，或瀏覽區域網路上的共用檔案和印表機。為防止網路型攻擊，您可能不需要啟用網路檔案和印表機共用。

您可以新增防火牆規則來啟用網路檔案和列印共用。防火牆規則允許存取通訊埠來瀏覽和共用檔案及印表機。您可以先建立一個防火牆規則，讓用戶端可以提供其檔案共用。接著再建立第二個防火牆規則，讓用戶端可以瀏覽其他檔案和印表機。

根據您為用戶端指定的控制類型，此設定會以不同方式執行，如下所示：

用戶端控制或混合控制	Windows 用戶端上的使用者可以在「防網路和主機刺探利用」中架構這些設定，以自動啟用設定。 Mac 用戶端上的使用者只能啟用或停用防火牆。
混合控制	指定這種類型流量的伺服器防火牆規則可以在 Windows 上覆寫這些設定。 在 Mac 上，所有防火牆規則均為伺服器防火牆規則。
伺服器控制	這些設定在用戶端上無法使用。

允許 Windows 用戶端瀏覽網路中的檔案和印表機

1. 在主控台中，開啟防火牆政策。
2. 在**「防火牆政策」**頁面的**「Windows 設定」**下方，按下**「規則」**。
3. 在**「規則」**標籤的**「規則」**清單中，選取要編輯的規則，在**「服務」**欄位按下滑鼠右鍵，然後按下**「編輯」**。
4. 在**「服務清單」**對話方塊中，按下**「新增」**。
5. 在**「通訊協定」**對話方塊的**「通訊協定」**下拉式清單中，按下 **TCP**，再按下**「本機/遠端」**。
6. 執行下列其中一項工作：

允許用戶端瀏覽網路中的檔案和印表機	在**「遠端通訊埠」**下拉式清單中，輸入 **88, 135, 139, 445**。
讓其他電腦瀏覽用戶端上的檔案	在**「本機通訊埠」**下拉式清單中，輸入 **88, 135, 139, 445**。

7. 按下**「確定」**。
8. 在**「服務清單」**對話方塊中，按下**「新增」**。
9. 在**「通訊協定」**對話方塊的**「通訊協定」**下拉式清單中，按下 **UDP**。

10 執行下列其中一項工作：

允許用戶端瀏覽網路中的檔案和印表機	在「**本機通訊埠**」下拉式清單中，輸入 **137, 138**。 在「**遠端通訊埠**」下拉式清單中，輸入 **88**。
讓其他電腦瀏覽用戶端上的檔案	在「**本機通訊埠**」下拉式清單中，輸入 **88, 137, 138**。

11 按下「**確定**」。

12 在「**服務清單**」對話方塊中，確保兩項服務均啟用，然後按下「**確定**」。

13 在「**規則**」標籤上，確保將「**動作**」欄位設定為「**允許**」。

14 架構完此政策後，按下「**確定**」。

允許 Mac 用戶端瀏覽網路中的檔案和印表機

1 在主控台中，開啟防火牆政策。

2 在「**防火牆政策**」頁面的「**Mac 設定**」下方，按下「**規則**」。

3 在「**規則**」標籤的「**規則**」清單中，選取要編輯的規則，在「**服務**」欄位按下滑鼠右鍵，然後按下「**編輯**」。

4 在「**服務清單**」對話方塊中，按下「**新增**」。

5 在「**通訊協定**」對話方塊的「**通訊協定**」下拉式清單中，按下 **TCP**，再按下「**本機/遠端**」。

6 若要讓其他電腦能夠瀏覽用戶端上的檔案，請在「**本機通訊埠**」下拉式清單中輸入 **139** 和 **445**。

預設會啟用從 Mac 瀏覽網路的外寄要求。

7 按下「**確定**」。

8 在「**服務清單**」對話方塊中，確保新服務已啟用，然後按下「**確定**」。

9 在「**規則**」標籤上，確保將「**動作**」欄位設定為「**允許**」。

10 架構完此政策後，按下「**確定**」。

可透過 Bonjour 服務在 Mac 上執行印表機搜尋，該服務預設為開啟。您不需要架構 Bonjour 服務的自訂規則。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

設定違反防火牆規則通知

您可以架構 Symantec Endpoint Protection 在每次防火牆偵測到違反規則、攻擊或事件時，寄發電子郵件訊息給您。例如，您可能想在用戶端攔截來自某個特定 IP 位址的流量時收到通知。

為防火牆違規設定通知

1. 在主控台中，開啟防火牆政策。
2. 在「**防火牆政策**」頁面的「**Windows 設定**」或「**Mac 設定**」下方，按下「**規則**」。
3. 在「**規則**」標籤中選取規則，然後在「**日誌**」欄位上按下滑鼠右鍵，再執行下列其中一或多項工作：

觸發防火牆規則時傳送電子郵件訊息	勾選「**傳送電子郵件警示**」。
觸發防火牆規則時產生日誌事件	若為 Windows 規則，同時勾選「**寫入至流量日誌**」和「**寫入至封包日誌**」。 若為 Mac 規則，請勾選「**寫入至流量日誌**」。

4. 架構完此政策後，按下「**確定**」。
5. 架構安全警示。
6. 架構郵件伺服器。
7. 按下「**確定**」。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 577 頁的「設定管理員通知」。

控制通過網路配接卡的流量

如果您定義了網路配接卡觸發條件，則規則只會與指定配接卡轉送或接收的流量有關。

您可以透過防火牆規則新增自訂網路配接卡。不過，該配接卡不會加入共用清單。您無法從任何其他規則存取自訂配接卡。

控制通過網路配接卡的流量

1. 在主控台中，開啟防火牆政策。
2. 在「**防火牆政策**」頁面的「**Windows 設定**」下方，按下「**規則**」。
3. 在「**規則**」標籤的「**規則**」清單中，選取要編輯的規則，在「**配接卡**」欄按下滑鼠右鍵，然後按下「**更多配接卡**」。

4 在「**網路配接卡**」對話方塊中，執行下列其中一個動作：

觸發任何配接卡的規則 (即使未列出)	按下「**套用規則到所有配接卡**」，然後跳至步驟 7。
觸發選取配接卡的規則	按下「**套用規則到下列配接卡**」。 然後，對要觸發規則的每個配接卡勾選其旁邊的方塊。

5 若要只為選取的規則新增自訂配接卡，請執行下列工作：

- 按下「**新增**」。
- 在「**網路配接卡**」對話方塊中，選取配接卡類型，然後在「**配接卡識別**」文字欄位中輸入配接卡的品牌名稱。

6 按下「**確定**」。

7 按下「**確定**」。

8 按下「**確定**」。

請參閱第 295 頁的「新增防火牆規則」。

請參閱第 311 頁的「自訂防火牆規則」。

請參閱第 309 頁的「關於防火牆規則網路配接卡觸發條件」。

架構混合控制的防火牆設定

您可以架構用戶端，讓使用者不能控制、完全控制或有限控制其可架構的防火牆設定。

在 Mac 防火牆中，無論用戶端使用者介面設定為何，使用者都無法建立防火牆規則或變更設定。選項未曾顯示在用戶端使用者介面中。

伺服器控制	在 Windows 中，使用者無法建立任何防火牆規則或啟用防火牆設定。 在 Mac 中，使用者無法啟用或停用防火牆。
用戶端控制	在 Windows 中，使用者可以建立防火牆規則和啟用所有防火牆設定。 在 Mac 中，使用者可以啟用和停用防火牆。
混合控制	在 Windows 中，使用者可以建立防火牆規則。您可以決定使用者能夠啟用哪些防火牆設定。 在 Mac 中，您可以決定使用者是否可以啟用或停用防火牆。

架構混合控制的防火牆設定

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」下，選取具有您要修改之使用者控制層級的群組。

3 在「**政策**」標籤的「**位置限定的政策與設定**」下，展開某位置下方的「**位置限定的設定**」。

4 在「**用戶端使用者介面控制設定**」的右側，按下「**工作**」>「**編輯設定**」。

5 在「**控制模式設定**」對話方塊中，按下「**混合控制**」，然後按下「**自訂**」。

6 在「**用戶端/伺服器控制設定**」標籤的「**防火牆政策**」類別下，執行下列其中一項工作：

- 若要讓使用者可以架構用戶端設定，請按下「**用戶端**」。
- 若要架構用戶端設定，請按下「**伺服器**」。

7 按下「**確定**」。

8 按下「**確定**」。

9 針對您要設為「**伺服器**」的每個防火牆設定，在防火牆政策中啟用或停用該設定。

請參閱第 288 頁的「管理防火牆防護」。

請參閱第 320 頁的「為網路服務啟用通訊而非新增規則」。

為網路服務啟用通訊而非新增規則

您可以啟用自動允許特定網路服務之間進行通訊的選項，這樣您就不必定義明確允許這些服務的規則。您也可以啟用流量設定，偵測和攔截透過 NetBIOS 與 Token Ring 進行通訊的流量。

您可允許已架構使用 DHCP、DNS 和 WINS 流量的網路連線進行離埠要求和入埠回應。

這些過濾會允許 DHCP、DNS 或 WINS 用戶端接收來自伺服器的 IP 位址。此外，也可防護用戶端在下列情況下不受來自網路的攻擊：

如果用戶端傳送要求至伺服器	用戶端會等待五秒後再允許入埠回應。
如果用戶端沒有傳送要求至伺服器	所有過濾均不允許封包。

啟用這些選項時，Symantec Endpoint Protection 會在有要求發出時允許封包；它不會攔截封包。您必須建立防火牆規則來攔截封包。

附註：若要在混合控制中架構這些設定，您還必須在「**用戶端使用者介面混合控制設定**」對話方塊中啟用這些設定。

為網路服務啟用通訊而非新增規則

1 在主控台中，開啟某個防火牆政策。

2 在「**防火牆政策**」頁面的「**Windows 設定**」或「**Mac 設定**」下方，按下「**內建規則**」。

3 勾選要啟用的選項。

4 按下「**確定**」。

5 如果系統顯示提示，請將政策指派至某個位置。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 272 頁的「編輯政策」。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

自動攔截連線至攻擊電腦

如果 Symantec Endpoint Protection 用戶端偵測到網路攻擊，會自動攔截連線以保護用戶端電腦的安全。用戶端會啟動主動回應，此功能會自動攔截特定期間內所有進出攻擊電腦的通訊。單一位置會攔截攻擊電腦的 IP 位址。

攻擊者的 IP 位址會記錄在「安全日誌」中。您可以取消特定 IP 位址或取消全部的主動回應來取消攔擊攻擊。

如果您將用戶端設定為混合控制，則可以指定用戶端上是否提供該設定供使用者啟用。如果未提供該設定，就必須在「**用戶端使用者介面混合控制設定**」對話方塊中啟用它。

更新的 IPS 特徵、更新的服務阻斷特徵、通訊埠掃描以及 MAC 詐騙也會觸發主動回應。

自動攔截連線至攻擊電腦

1 在主控台中，開啟防火牆政策。

2 在「**防火牆政策**」頁面的左窗格中，按下列其中一個選項：

- 在「**Windows 設定**」下方：「**防護與隱藏**」
- 在「**Mac 設定**」下方：「**防護**」

3 在「**防護設定**」下方，勾選「**自動攔截攻擊者的 IP 位址**」。

4 在「**攔截 IP 位址的秒數...秒**」文字方塊中，指定攔截可能攻擊者的秒數。

您可以輸入 1 到 999,999 的值。

5 按下「**確定**」。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 319 頁的「架構混合控制的防火牆設定」。

請參閱第 272 頁的「編輯政策」。

偵測潛在的攻擊和詐騙嘗試

您可以啟用各種設定讓 Symantec Endpoint Protection 偵測和記錄用戶端上的潛在攻擊並攔截詐騙嘗試。這些選項全部預設為停用。

您可以啟用的設定如下：

啟用通訊埠掃描偵測	啟用此設定時，Symantec Endpoint Protection 會監控任何安全規則攔截的所有連入封包。如果規則短時間內在不同通訊埠上攔截幾個不同的封包，Symantec Endpoint Protection 會建立安全日誌項目。 通訊埠掃描偵測不會攔截任何封包。您必須建立安全政策，以便在執行通訊埠掃描時攔截流量。
啟用服務阻斷偵測	服務阻斷偵測是一種入侵偵測。啟用此設定時，用戶端會在偵測到已知特徵的模式時攔截流量，不論埠號或使用的 Internet 通訊協定類型為何。
啟用防 MAC 詐騙	啟用此設定時，如果對該特定主機提出要求，則 Symantec Endpoint Protection 會允許下列連入流量和連出流量： ■ 位址解析通訊協定 (ARP) (IPv4) ■ 芳鄰搜尋通訊協定 (NDP) (IPv6) 系統會攔截所有其他非預期的流量，並在安全日誌中產生項目。

附註：若要在混合控制中架構這些設定，您還必須在**「用戶端使用者介面混合控制設定」**對話方塊中啟用這些設定。

偵測潛在的攻擊和詐騙嘗試

1 在主控台中，開啟某個防火牆政策。

2 在**「防火牆政策」**頁面上，按下列其中一項：
   - 在**「Windows 設定」**下方：**「防護與隱藏」**
   - 在**「Mac 設定」**下方：**「防護」**

3 在**「防護設定」**下，勾選您要啟用的任何選項。

4 按下**「確定」**。

5 如果系統顯示提示，請將政策指派至某個位置。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

請參閱第 272 頁的「編輯政策」。

防止對電腦的外部隱藏攻擊

您可啟用防止外部攻擊偵測用戶端相關資訊的設定。這些設定預設為停用。

附註：若要在混合控制中架構這些設定，您還必須在**「用戶端使用者介面混合控制設定」**對話方塊中啟用這些設定。

附註：這些隱藏設定不適用於 Mac 防火牆。

防止對電腦的外部隱藏攻擊

1. 在主控台中，開啟某個防火牆政策。
2. 在**「防火牆政策」**頁面中，按下**「防護與隱藏」**。
3. 在**「隱藏設定」**下，勾選您要啟用的任何選項。
4. 按下**「確定」**。
5. 如果系統顯示提示，請將政策指派至某個位置。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

請參閱第 272 頁的「編輯政策」。

停用 Windows 防火牆

您可以指定 Symantec Endpoint Protection 停用 Windows 防火牆的條件。發生下列情況時，Symantec Endpoint Protection 會將 Windows 防火牆設定還原為安裝 Symantec Endpoint Protection 之前的狀態：

- Symantec Endpoint Protection 已移除。
- Symantec Endpoint Protection 防火牆已停用。

附註：Symantec Endpoint Protection 不會修改任何現有的 Windows 防火牆政策規則或排除項目。

一般而言，如果停用 Windows 防火牆，Windows 使用者會在其電腦重新啟動時收到通知。依據預設，Symantec Endpoint Protection 會停用此通知，以避免在停用 Windows 防火牆時向使用者傳送警示。然而如有需要，可以啟用通知。

停用 Windows 防火牆

1 在主控台中，按下「**政策**」。

2 在「**政策**」之下按「**防火牆**」。

3 執行下列其中一項工作：

- 建立新的防火牆政策。
- 在「**防火牆政策**」清單中，連按兩下要修改的防火牆政策。

4 在「**防火牆政策**」下方，按下「**Windows 整合**」。

5 在「**停用 Windows 防火牆**」下拉式清單中，指定您希望何時停用 Windows 防火牆。

預設設定為「**僅停用一次**」。

如需關於選項的詳細資訊，請按下「**說明**」。

6 在「**Windows 防火牆停用訊息**」下拉式清單中，指定您是否希望在啟動時停用會說明已停用防火牆的 Windows 訊息。

預設設定為「**停用**」，表示使用者不會在電腦啟動時收到說明已停用 Windows 防火牆的訊息。

7 按下「**確定**」。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 270 頁的「安全政策類型」。

17

管理入侵預防和作業系統強化

本章包含以下主題：

管理入侵預防

預設入侵預防設定可保護用戶端電腦免受各種威脅的侵害。 您可以變更網路的預設設定。

如果您在伺服器上執行 Symantec Endpoint Protection，則入侵預防可能會影響伺服器資源或應變時間。如需詳細資訊，請參閱：

在 Windows Servers 上端點防護的最佳實務準則

附註：Linux 用戶端不支援入侵預防。

表 17-1 管理入侵預防

工作	敘述
瞭解入侵預防	瞭解入侵預防如何偵測和攔截網路及瀏覽器攻擊。 請參閱第 328 頁的「入侵預防的運作方式」。 請參閱第 329 頁的「關於賽門鐵克 IPS 特徵」。
啟用入侵預防	為確保用戶端電腦安全，您應該讓入侵預防保持啟用狀態。 ■ 網路入侵預防 ■ 瀏覽器入侵預防 (僅限 Windows 電腦) 您也可以將瀏覽器入侵預防架構為只記錄偵測但不攔截它們。 您應該暫時使用此組態，因為它會降低用戶端的安全性設定檔。 例如，只有當您對用戶端上遭攔截的流量進行疑難排解時，您才會架構只記錄模式。 在檢閱攻擊日誌以識別及排除攔截流量的特徵之後，請停用只記錄模式。 請參閱第 330 頁的「啟用網路入侵預防或瀏覽器入侵預防」。 請參閱第 331 頁的「為 IPS 特徵建立例外」。 在群組或用戶端上執行**「啟用網路威脅防護」**指令時，您也可以啟用這兩種類型的入侵預防以及防火牆。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

工作	敘述
建立例外以變更賽門鐵克網路入侵預防特徵的預設行為	您可能希望建立例外，以變更預設賽門鐵克網路入侵預防特徵的預設行為。依據預設，某些特徵會攔截流量，某些特徵會允許流量。 **附註：**您無法變更瀏覽器入侵預防特徵的行為。 基於下列原因，您可能希望變更某些網路特徵的預設行為： ■ 減少用戶端電腦上的資源消耗。 例如，您可能希望減少攔截流量的特徵數目。但是，請確定攻擊特徵不會造成任何威脅後，再排除攔截該特徵。 ■ 允許賽門鐵克預設攔截的某些網路特徵。 例如，當無害網路活動與攻擊特徵相符時，您可能希望建立例外以降低誤報。如果您確定網路活動是安全的，則可以建立例外。 ■ 攔截賽門鐵克允許的某些特徵。 例如，賽門鐵克包含點對點應用程式的特徵，並且預設允許通訊。您可以建立例外來攔截流量。 ■ 使用稽核特徵來監控某些類型的流量 (僅限 Windows) 稽核特徵對於某些流量類型 (例如來自即時訊息應用程式的流量) 的預設動作為**「不記錄」**。您可以建立例外以記錄流量，以便您可以檢視日誌並在您的網路中監控此流量。然後，可以使用該例外來攔截流量、建立防火牆規則來攔截流量，或是略過流量。 您也可以針對流量建立應用程式規則。 請參閱第 331 頁的「為 IPS 特徵建立例外」。 您可以使用應用程式控制來防止使用者在其電腦上執行點對點應用程式。 請參閱第 438 頁的「將自訂規則新增至應用程式控制」。 如果您希望攔截傳送和接收點對點流量的通訊埠，請使用「防火牆」政策。 請參閱第 291 頁的「建立防火牆政策」。
建立例外以忽略用戶端電腦上的瀏覽器特徵 (僅限 Windows 用戶端)	您可以建立例外，在 Windows 電腦上將瀏覽器特徵排除在瀏覽器入侵預防範圍之外。 如果瀏覽器入侵預防會導致網路中的瀏覽器發生問題，不妨忽略瀏覽器特徵。 請參閱第 331 頁的「為 IPS 特徵建立例外」。
將特定電腦排除在網路入侵預防掃描範圍以外	您可能希望將某些電腦排除在網路入侵預防範圍以外。例如，內部網路某些電腦的用途可能設定為測試之用。您可能希望 Symantec Endpoint Protection 忽略進出這些電腦的流量。 排除電腦時，還會將其排除在服務阻斷防護和防火牆提供的通訊埠掃描防護範圍以外。 請參閱第 332 頁的「設定排除的電腦清單」。

工作	敘述
架構入侵預防通知	依據預設，用戶端電腦會顯示有關入侵嘗試的訊息。您可以自訂這個訊息。 請參閱第 333 頁的「針對入侵預防和記憶體攻擊緩和架構用戶端通知」。
建立自訂入侵預防特徵 (僅限 Windows)	您可以撰寫自己的入侵預防特徵以識別特定威脅。撰寫自己的特徵時，您可以降低此特徵導致誤報的可能性。 例如，您可能希望使用自訂入侵預防特徵來攔截和記錄網站。 請參閱第 334 頁的「管理自訂入侵預防特徵」。 您必須安裝並啟用防火牆，才能使用自訂 IPS 特徵。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。
監控入侵預防	定期檢查您網路中的用戶端電腦是否啟用了入侵預防。 請參閱第 539 頁的「監控端點防護」。

入侵預防的運作方式

入侵預防和防火牆是網路威脅防護的一部分。自 14 版起，「網路威脅防護」和「記憶體攻擊緩和」是防網路和主機侵入的一部分。

入侵預防會自動偵測和攔截網路攻擊。在 Windows 電腦上，入侵預防還會偵測和攔截對於受支援瀏覽器的瀏覽器攻擊。入侵預防是繼防火牆之後用於保護用戶端電腦的另一層防護。入侵預防有時亦稱為入侵預防系統 (IPS)。

入侵預防會截取網路層中的資料。它使用特徵掃描封包或封包串流。透過尋找與網路攻擊或瀏覽器攻擊對應的模式，入侵預防可以個別掃描各個封包。入侵預防會偵測作業系統元件和應用層的攻擊。

表 17-2 入侵預防的類型

類型	敘述
網路入侵預防	網路入侵預防使用特徵來識別用戶端電腦上的攻擊。對於已知攻擊，入侵預防會自動捨棄與特徵符合的封包。 您也可以在 Symantec Endpoint Protection Manager 中建立自訂網路特徵。您無法直接在用戶端上建立自訂特徵，但可以在用戶端上匯入自訂特徵。自訂特徵僅支援在 Windows 電腦上使用。 請參閱第 329 頁的「關於賽門鐵克 IPS 特徵」。

類型	敘述
瀏覽器入侵預防 (僅限 Windows)	瀏覽器入侵預防會監控 Internet Explorer 和 Firefox 上的攻擊。所有其他瀏覽器均不支援瀏覽器入侵預防。 Firefox 可能會停用 Symantec Endpoint Protection 外掛程式，但可以重新開啟它。 此類型的入侵預防使用攻擊特徵和啟發式技術來識別瀏覽器上的攻擊。 對於某些瀏覽器攻擊，入侵預防會要求用戶端終止瀏覽器。用戶端電腦上會顯示通知。 如需瀏覽器入侵預防所保護瀏覽器的最新資訊，請參閱：支援瀏覽器入侵預防的瀏覽器版本。

請參閱第 325 頁的「管理入侵預防」。

關於賽門鐵克 IPS 特徵

根據預設，會在用戶端上安裝賽門鐵克入侵預防特徵。

入侵預防使用賽門鐵克特徵來監控各個封包或封包串流。對於封包串流，入侵預防能記住以前封包的型樣或部分型樣清單。然後，會將此資訊應用於後續的封包檢查。

賽門鐵克特徵包括網路入侵預防的特徵，這些特徵已下載至用戶端作為 LiveUpdate 內容的一部分。對於 Mac 電腦，存在一些內建到軟體的其他網路入侵預防特徵。

在 Windows 電腦上，LiveUpdate 內容還包括瀏覽器入侵預防的特徵。

網路入侵預防特徵

網路特徵會比對可導致應用程式當機或利用用戶端電腦上作業系統漏洞的攻擊型樣。

您可以變更賽門鐵克網路特徵攔截或允許通訊。您還可以變更 Symantec Endpoint Protection 是否應在安全日誌中記錄根據特徵的偵測。

瀏覽器入侵預防特徵 (僅限 Windows)

瀏覽器特徵會比對支援瀏覽器上的攻擊型樣 (例如，可導致瀏覽器當機的程序檔)。

您無法自訂瀏覽器特徵的動作或日誌設定，但可以排除瀏覽器特徵。

您可以將瀏覽器入侵預防架構為記錄瀏覽器偵測但不攔截它們。此動作可協助您識別可能需要排除的那些瀏覽器特徵。在建立特徵排除之後，請停用只記錄模式。

賽門鐵克安全機制應變中心團隊提供攻擊特徵。根據預設，會在用戶端上安裝入侵預防引擎和相應的特徵集。特徵是您在用戶端上更新的部分內容。

您可以在下列賽門鐵克網站頁面上檢視有關 IPS 特徵的資訊：

攻擊特徵

如需適用於 Mac 用戶端的內建 IPS 特徵的相關資訊，請參閱下列文章：

Symantec Endpoint Protection IPS for Mac 的內建特徵

請參閱第 331 頁的「為 IPS 特徵建立例外」。

請參閱第 325 頁的「管理入侵預防」。

關於自訂 IPS 特徵

您可以建立自己的 IPS 網路特徵。 這些特徵以封包為基礎。

與賽門鐵克特徵不同的是，自訂特徵只會掃描單一封包酬載。但是，自訂特徵可偵測到 TCP/IP 堆疊中速度比賽門鐵克特徵快的攻擊。

封包式特徵會檢查單一封包是否符合規則。規則根據各種準則 (如通訊埠、通訊協定、來源或目的 IP、TCP 旗標號碼或應用程式) 而制定。例如，自訂特徵可監控收到的資訊封包中是否有 GET / cgi-bin/phf? 中的字串 phf，該字串表示 CGI 程式攻擊。每個封包都要經過評估，看是否具有該特定型樣。 如果流量的封包符合規則，則用戶端會允許或攔截該封包。

您可以指定 Symantec Endpoint Protection 是否在封包日誌中記錄根據自訂特徵的偵測。

附註：您必須安裝並啟用防火牆，才能使用自訂 IPS 特徵。

僅 Windows 電腦支援自訂特徵。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

啟用網路入侵預防或瀏覽器入侵預防

入侵預防預設為啟用。通常您不應停用任一類型的入侵預防。

您可以對瀏覽器入侵預防啟用只記錄模式，以記錄它在未影響用戶端使用者的情況下所攔截的流量。您可以隨後使用 Symantec Endpoint Protection Manager 中的**「防網路和主機侵入」**攻擊日誌，在**「入侵預防」**政策中建立例外，以忽略特定的瀏覽器特徵。然後，您會停用只記錄模式。

附註：若要在混合控制中架構這些設定，您還必須在**「用戶端使用者介面混合控制設定」**對話方塊中啟用這些設定。

啟用網路入侵預防或瀏覽器入侵預防

1. 在主控台中，開啟某個入侵預防政策。
2. 在政策頁面上，按下**「入侵預防」**。
3. 確定勾選下列選項：
   - **啟用網路入侵預防**

您還可以從網路入侵預防中排除特定電腦。
請參閱第 332 頁的「設定排除的電腦清單」。

- **啟用 Windows 瀏覽器入侵預防**

4 按下**「確定」**。

請參閱第 331 頁的「為 IPS 特徵建立例外」。

請參閱第 325 頁的「管理入侵預防」。

請參閱第 319 頁的「架構混合控制的防火牆設定」。

為 IPS 特徵建立例外

您可以使用例外變更賽門鐵克 IPS 特徵的行為。

對於 Windows 和 Mac 電腦，您可以變更 IPS 辨識網路特徵時用戶端所採取的動作。您也可以變更用戶端是否將事件記錄至「安全日誌」。

對於 Windows 電腦，您無法變更賽門鐵克瀏覽器特徵的行為；與網路特徵不同，瀏覽器特徵不允許自訂動作和記錄設定。然而，您可以為瀏覽器特徵建立例外，以便用戶端忽略該特徵。

附註：當您新增瀏覽器特徵例外時，Symantec Endpoint Protection Manager 會將該特徵包含到例外清單中，並自動將動作設定為**「允許」**，將日誌設定設為**「不記錄」**。您無法自訂動作或日誌設定。

請參閱第 325 頁的「管理入侵預防」。

附註：若要變更您建立或匯入之自訂 IPS 特徵，您可以直接編輯該特徵。僅 Windows 電腦支援自訂特徵。

建立 IPS 特徵例外

1 在主控台中，開啟某個入侵預防政策。

2 在**「Windows 設定」**或**「Mac 設定」**下，按下**「例外」**，然後按下**「新增」**。

附註：特徵清單會以管理主控台下載的最新 LiveUpdate 內容填入。對於 Windows 電腦，如果管理伺服器尚未下載內容，則此清單顯示為空白。對於 Mac 電腦，此清單一律至少包含內建特徵，這些特徵已自動安裝在 Mac 用戶端上。

---

3 在**「新增入侵預防例外」**對話方塊中，執行下列動作以過濾特徵：

- (僅限 Windows) 若只要顯示特定類別的特徵，請從**「顯示類別」**下拉式清單中選取選項。如果您選取**「瀏覽器防護」**，特徵動作選項會自動變更為**「允許」**和**「不記錄」**。

- (Windows 和 Mac) 若要顯示按特定嚴重性分類的特徵，請從**「顯示嚴重性」**下拉式清單中選取選項。

4 選取一個或多個特徵。

若要為所有特徵設定相同行為，請按下**「全選」**。

5 按**「下一步」**。

6 在**「特徵動作」**對話方塊中，設定下列選項，然後按下**「確定」**。

- 將**「動作」**設定為**「攔截」**或**「允許」**。
- 將**「記錄」**設定為**「記錄流量」**或**「不記錄流量」**。

附註：這些選項只適用於網路特徵。如果是瀏覽器特徵，請按下**「確定」**。

如果您要將特徵的行為轉化成原始行為，請在**「例外」**清單中選取此特徵，然後按下**「刪除」**。

7 按下**「確定」**儲存政策變更。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

設定排除的電腦清單

僅網路入侵預防支援排除的主機。

您可以設定電腦清單，針對這些電腦，用戶端不會比對攻擊特徵，或是檢查是否有通訊埠掃描或受到阻絕服務攻擊。網路入侵預防和點對點驗證允許來自排除的主機清單中主機的任何來源流量。不過，網路入侵預防和點對點驗證會繼續評估送往清單中主機的任何目的地流量。此清單會套用至入埠和離埠流量，但僅適用於流量的來源。此清單也僅適用於遠端 IP 位址。

例如，您可能還要排除一些電腦，允許 Internet 服務供應商掃描您網路中的通訊埠，以確保遵從其服務合約。或者，您可以將內部網路的某些電腦設為測試用途。

附註：您也可以設定電腦清單，在 IPS 特徵未偵測到攻擊時允許這些電腦的所有入埠流量和離埠流量。在此情況下，您可以建立允許所有主機的防火牆規則。

設定排除的電腦清單

1 在主控台中，開啟某個入侵預防政策。

2 在政策頁面上，按下**「入侵預防」**。

3 勾選**「啟用排除的主機」**(若尚未勾選)，再按下**「排除的主機」**。

4 在「**排除的主機**」對話方塊中，勾選您要從網路入侵防護中排除的所有主機群組旁邊的「**已啟用**」。

請參閱第 313 頁的「擱截來往於特定伺服器的流量」。

5 若要新增您要排除的主機，請按下「**新增**」。

6 在「**主機**」對話方塊的下拉式清單中，選取下列其中一種主機類型：

- IP 位址
- IP 位址範圍
- 子網路

7 針對所選取的主機類型，輸入與其關聯的適當資訊。

若需這些選項的詳細資訊，請按下「**說明**」。

8 按下「**確定**」。

9 重複 5 和 8，以新增更多裝置和電腦到排除的電腦清單。

10 若要編輯或刪除任何排除的主機，請選取某一列，再按下「**編輯**」或「**刪除**」。

11 按下「**確定**」。

12 架構完此政策後，按下「**確定**」。

針對入侵預防和記憶體攻擊緩和架構用戶端通知

根據預設，當用戶端偵測到入侵防護事件和記憶體攻擊緩和時，用戶端電腦上會顯示通知。這些通知啟用時，通知會顯示標準訊息。針對 IPS 通知，您可以在標準訊息中加入自訂的文字。

針對入侵預防和記憶體攻擊緩和架構用戶端通知

1 在主控台中，按下「**用戶端**」，然後在「**用戶端**」下方選取群組。

2 在「**政策**」標籤的「**位置限定的政策與設定**」下，展開某位置下方的「**位置限定的設定**」。

3 在「**用戶端使用者介面控制設定**」的右側，按下「**工作**」，然後再按「**編輯設定**」。

4 在「***<群組名稱>***的**用戶端使用者介面控制設定**」對話方塊中，按下「**伺服器控制**」或「**混合控制**」。

5 在「**混合控制**」或「**伺服器控制**」旁，按下「**自訂**」。

如果您按下「**混合控制**」，在「**用戶端/伺服器控制設定**」標籤的「**顯示/隱藏入侵防護通知**」旁，按下「**伺服器**」。然後按下「**用戶端使用者介面設定**」標籤。

6 在「**用戶端使用者介面設定**」對話方塊或標籤中，按下「**顯示入侵預防和記憶體攻擊緩和通知**」。

7 若要在通知出現時啟用音效，請按下「**通知使用者時使用音效**」。

8 按下「**確定**」。

9 按下「**確定**」。

請參閱第 325 頁的「管理入侵預防」。

請參閱第 339 頁的「使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊」。

請參閱第 577 頁的「設定管理員通知」。

管理自訂入侵預防特徵

您可以自行撰寫網路入侵預防特徵，來識別特定入侵，並減少特徵導致誤報的可能性。您在自訂特徵加入的資訊愈多，特徵就愈有效。

警告：在制訂入侵預防特徵之前，您應該熟悉 TCP、UDP 或 ICMP 通訊協定。 格式不正確的特徵可能會損毀自訂特徵庫及用戶端的完整性。

附註：您必須安裝並啟用防火牆，才能使用自訂 IPS 特徵。請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

表 17-3 管理自訂入侵預防特徵

工作	敘述
建立含有特徵群組的自訂特徵庫	若要包含自訂特徵，必須建立自訂特徵庫。建立自訂特徵庫時，可以使用特徵群組，以便更輕鬆地管理特徵。必須將至少一個特徵群組新增至自訂特徵庫，才能新增特徵。 請參閱第 330 頁的「關於自訂 IPS 特徵」。 請參閱第 335 頁的「建立自訂 IPS 特徵庫」。
將自訂 IPS 特徵新增至自訂特徵庫	您可以將自訂 IPS 特徵新增至自訂特徵庫中的特徵群組。 請參閱第 336 頁的「將特徵新增至自訂 IPS 特徵庫」。
將特徵庫指派給用戶端群組	您可以將自訂特徵庫指派給用戶端群組而不是某個位置。 請參閱第 339 頁的「指派多個自訂 IPS 程式庫至群組」。

工作	敘述
變更特徵的順序	入侵預防會使用第一個規則比對。 Symantec Endpoint Protection 會按特徵在特徵清單中列出的順序檢查特徵。 例如，如果您新增一個特徵群組來攔截目的通訊埠 80 的雙向 TCP 流量，可以新增以下特徵： ■ 攔截通訊埠 80 的所有流量。 ■ 允許通訊埠 80 的所有流量。 如果「攔截所有流量」特徵列出在前面，「允許所有流量」特徵永遠不會套用。如果「允許所有流量」特徵列出在前面，「攔截所有流量」特徵永遠不會套用，且會永遠允許所有 HTTP 流量。 **附註：**防火牆規則會優先於入侵預防特徵。 請參閱第 337 頁的「變更自訂 IPS 特徵的順序」。
複製並貼上特徵	您可以在群組之間和特徵庫之間複製和貼上特徵。
定義特徵的變數	新增自訂特徵時，可以使用變數來代表特徵中的可變資料。如果資料變更，您可以編輯變數，無須編輯整個特徵庫中的特徵。 請參閱第 338 頁的「定義自訂 IPS 特徵的變數」。
測試自訂特徵	您應該測試自訂入侵預防特徵以確保它們可以正常運作。 請參閱第 339 頁的「測試自訂 IPS 特徵」。

建立自訂 IPS 特徵庫

您可以建立自訂 IPS 特徵庫以包含您的自訂 IPS 特徵。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

建立自訂 IPS 特徵庫

1. 在主控台中的**「政策」**頁面上，在**「政策」**下按下**「入侵預防」**。
2. 按下**「自訂入侵預防」**標籤。
3. 在**「工作」**下，按下**「新增自訂入侵預防特徵」**。
4. 在**「自訂入侵預防特徵」**對話方塊中，鍵入特徵庫的名稱和 (選擇性) 敘述。

   NetBIOS Group 是特徵群組範例，其中有一個特徵範例。您可以編輯現有群組或新增群組。
5. 若要增加新群組，請在**「特徵」**標籤的**「特徵群組」**清單下，按下**「新增」**。

6 在「**入侵預防特徵群組**」對話方塊中，鍵入群組名稱和(選擇性)敘述，然後按下「**確定**」。

群組預設為啟用。如果啟用特徵群組，該群組內的所有特徵會自動啟用。若要保留群組供參考但要停用它，請取消勾選「**啟用這個群組**」。

7 新增自訂特徵。

請參閱第 336 頁的「將特徵新增至自訂 IPS 特徵庫」。

將特徵新增至自訂 IPS 特徵庫

您可以將自訂入侵預防特徵新增至新的或現有自訂 IPS 特徵庫。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

新增自訂特徵

1 建立自訂 IPS 特徵庫。

請參閱第 335 頁的「建立自訂 IPS 特徵庫」。

2 在「**特徵**」標籤的「**此群組的特徵**」下，按下「**新增**」。

3 在「**新增特徵**」對話方塊中，鍵入特徵的名稱和 (選擇性) 敘述。

4 在「**嚴重性**」下拉式清單中，選取嚴重性等級。

符合特徵條件的事件將會記錄為此嚴重性等級。

5 在「**方向**」下拉式清單中，指定要特徵檢查的流量方向。

6 在「**內容**」欄位中，鍵入特徵的語法。

例如，某些常見通訊協定的特徵使用下列語法：

HTTP
```
rule tcp, dest=(80,443), saddr=$LOCALHOST,
msg="MP3 GET in HTTP detected",
regexpcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*"
```

FTP
```
rule tcp, dest=(21), tcp_flag&ack, saddr=$LOCALHOST,
msg="MP3 GET in FTP detected",
regexpcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"
```

如需語法的詳細資訊，可以按下「**說明**」。

7 如果您要應用程式觸發特徵，請按下「**新增**」。

8 在「**新增應用程式**」對話方塊中，鍵入應用程式的檔案名稱和 (選擇性) 敘述。

例如，若要新增應用程式 Internet Explorer，請將檔案名稱鍵入為 **iexplore** 或 **iexplore.exe**。如果不指定檔案名稱，任何應用程式都可以觸發特徵。

9 按下「**確定**」。

新增的應用程式預設為啟用。如果要停用應用程式稍後再啟用，請取消勾選「**已啟用**」欄的核取方塊。

10 在「**動作**」群組方塊中，選取特徵偵測到事件時用戶端要採取的動作：

攔截	識別並攔截事件或攻擊，並且記錄在安全日誌中
允許	識別並允許事件或攻擊，並且記錄在安全日誌中

11 若要將事件或攻擊記錄在封包日誌中，請勾選「**寫入至封包日誌**」。

12 按下「**確定**」。

新增的特徵預設為啟用。如果要停用特徵稍後再啟用，請取消勾選「**已啟用**」欄的核取方塊。

13 您可以新增其他特徵。完成之後，按下「**確定**」。

14 如果系統提示您，請指派自訂 IPS 特徵給群組。

您也可以將多個自訂 IPS 程式庫指派給群組。

請參閱第 339 頁的「指派多個自訂 IPS 程式庫至群組」。

變更自訂 IPS 特徵的順序

自訂特徵的IPS引擎會按照特徵清單中的特徵列示順序來檢查特徵。每個封包只會觸發一個特徵。當入埠或離埠流量封包有符合的特徵時，IPS 引擎就會停止檢查其他特徵。如此，IPS 引擎才能以正確的順序執行特徵。您可以在特徵清單中變更特徵的順序。如果有多個相符的特徵，請將優先順序較高的特徵移至頂端。

例如，如果您新增一個特徵群組來攔截目的通訊埠 80 的雙向TCP 流量，可以新增以下特徵：

- 攔截通訊埠 80 的所有流量。
- 允許通訊埠 80 的所有流量。

如果「攔截所有流量」特徵列出在前面，「允許所有流量」特徵永遠不會套用。如果「允許所有流量」特徵列出在前面，「攔截所有流量」特徵永遠不會套用，且會永遠允許所有HTTP流量。

附註：防火牆規則會優先於入侵預防特徵。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

變更自訂 IPS 特徵的順序

1 開啟自訂 IPS 特徵庫。

2 在「**特徵**」標籤的「**此群組的特徵**」表格中，選取要移動的特徵，然後執行下列其中一個動作：

- 若要先處理此特徵再處理其上面的特徵，請按下「**上移**」。
- 若要在處理此特徵前先處理其下面的特徵，請按下「**下移**」。

3 架構完此特徵庫後，請按下「**確定**」。

定義自訂 IPS 特徵的變數

新增自訂 IPS 特徵時，可以使用變數來代表特徵中的可變資料。如果資料變更，您可以編輯變數，無須編輯整個特徵庫中的特徵。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

您必須先定義特徵的變數，然後才能使用。自訂特徵庫中所定義的變數，可以用於該特徵庫中的任何特徵。

建立內容時，您可以複製並貼上現有範例變數，然後繼續編輯。

定義自訂 IPS 特徵的變數

1 建立自訂 IPS 特徵庫。

2 在「**自訂入侵預防特徵**」對話方塊中，按下「**變數**」標籤。

3 按下「**新增**」。

4 在「**新增變數**」對話方塊中，鍵入變數的名稱和選擇性敘述。

5 新增變數值的內容字串，最多 255 個字元。

輸入變數內容字串時，應遵從的語法與輸入特徵內容值使用的語法相同。

6 按下「**確定**」。

變數新增至表格後，您就可以將該變數用於此自訂特徵庫中的任何特徵。

在自訂 IPS 特徵中使用變數

1 在「**特徵**」標籤上，新增或編輯特徵。

2 在「**新增特徵**」或「**編輯特徵**」對話方塊中，於「**內容**」欄位鍵入變數名稱，前面加上貨幣符號 ($)。

例如，若要建立名為 HTTP 的變數，用來指定 HTTP 連接埠，請鍵入：

$HTTP

3 按下「**確定**」。

4 架構完此特徵庫後，請按下「**確定**」。

指派多個自訂 IPS 程式庫至群組

建立自訂 IPS 特徵庫之後，您可將它指派給群組而非個別位置。您可以稍後再將更多的自訂 IPS 程式庫指派給群組。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

指派多個自訂 IPS 特徵庫至群組

1. 在主控台中，按下「**用戶端**」。
2. 在「**用戶端**」下方，選取要將自訂特徵指派到的群組。
3. 在「**政策**」標籤的「**與位置無關的政策與設定**」下方，按下「**自訂入侵預防**」。
4. 在「**用於 <群組名稱> 的自訂入侵預防**」對話方塊中，針對要指派至該群組的每個自訂 IPS 程式庫，勾選「**已啟用**」欄中的核取方塊。
5. 按下「**確定**」。

測試自訂 IPS 特徵

在建立自訂 IPS 特徵後，應測試它們以確保可正常發揮作用。

表 17-4　　測試自訂 IPS 特徵

步驟	敘述
步驟 1：確保用戶端使用目前政策	用戶端下次收到政策時，會套用新的自訂特徵。 請參閱第 268 頁的「更新用戶端政策」。
步驟 2：測試用戶端上的特徵內容	應該測試您要在用戶端電腦上攔截的流量。 例如，如果您的自訂 IPS 特徵應攔截 MP3 檔案，則嘗試將某些 MP3 檔案下載到用戶端電腦。如果在多次嘗試後，下載未執行或逾時，則表示自訂 IPS 特徵成功。 可以按下「說明」，瞭解有關可在自訂 IPS 特徵中使用的語法詳細資訊。
步驟 3：檢視 Symantec Endpoint Protection Manager 中攔截的事件	可以在防網路和主機刺探利用攻擊日誌中檢視事件。在自訂 IPS 特徵中指定的訊息會出現在此日誌中 請參閱第 539 頁的「監控端點防護」。

請參閱第 334 頁的「管理自訂入侵預防特徵」。

使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊

- 記憶體攻擊緩和如何保護應用程式？

- 侵入防護的類型
- 記憶體攻擊緩和需求
- 修正和防止誤報
- 尋找記憶體攻擊緩和事件的日誌和報告
- 稽核已終止應用程式的防護
- 停用記憶體攻擊緩和
- 向安全機制應變中心報告誤報

記憶體攻擊緩和如何保護應用程式？

從 14 版開始，Symantec Endpoint Protection 包含記憶體攻擊緩和，其使用多種緩和技術來阻止對軟體中弱點的攻擊。例如，當用戶端使用者執行 Internet Explorer 之類應用程式時，侵入可能改為啟動包含惡意程式碼的其他應用程式。

為了阻止侵入，記憶體攻擊緩和會將 DLL 插入至受保護的應用程式。在記憶體攻擊緩和偵測到侵入嘗試之後，它會攔截侵入或終止侵入所威脅的應用程式。Symantec Endpoint Protection 會對用戶端電腦上的使用者顯示有關偵測的通知，並且在用戶端的安全日誌中記錄事件。

例如，用戶端使用者可能會看見以下通知：

```
Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite
detected. Symantec Endpoint Protection will terminate <application name>
application
```

記憶體攻擊緩和會繼續攔截侵入或終止應用程式，直到用戶端電腦執行已修正弱點的軟體版本為止。

附註：在 14 MPx 中，「記憶體攻擊緩和」稱為「防一般攻擊程式」。

使用防一般攻擊程式

侵入防護的類型

記憶體攻擊緩和使用多種類型的緩和技術來處理侵入，端視該類型的應用程式最適合的技術為何。例如，StackPvt 和 RopHeap 技術會攔截攻擊 Internet Explorer 的侵入。

Symantec Endpoint Protection 記憶體攻擊緩和技術

附註： 如果您已在電腦上啟用 Microsoft App-V 功能，記憶體攻擊緩和不會保護 App-V 所保護的 Microsoft Office 程序。

記憶體攻擊緩和需求

只有在已安裝入侵預防的情況下，才能使用記憶體攻擊緩和。記憶體攻擊緩和有自己的一組獨立特徵，這些特徵會隨入侵預防定義檔一起下載。不過，您可以獨立地啟用或停用入侵預防和記憶體攻擊緩和。

附註：從 14.0.1 開始，記憶體攻擊緩和有專屬的政策。在 14 MPx 版中，它屬於入侵預防政策的一部分。如果您停用**「總覽」**標籤上的入侵預防政策，就會停用記憶體攻擊緩和。

請參閱第 330 頁的「啟用網路入侵預防或瀏覽器入侵預防」。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

此外，您必須至少執行 LiveUpdate 一次，應用程式清單才會出現在記憶體攻擊緩和政策中。根據預設，出現在政策中的所有應用程式均啟用防護。

請參閱第 162 頁的「確認 Symantec Endpoint Protection Manager 具有最新內容」。

修正和防止誤報

記憶體攻擊緩和偶爾會意外終止用戶端電腦上的應用程式。如果您判斷應用程式的行為是合法並且未被侵入，偵測即為誤報。針對誤報，您應該停用防護，直到賽門鐵克安全機制應變中心變更記憶體攻擊緩和的行為為止。

表 17-5 顯示處理誤報偵測的步驟。

表 17-5 尋找和修正誤報的步驟

工作	
步驟 1：找出用戶端電腦上非預期終止的應用程式。	您可以使用下列方式找出用戶端電腦上終止的應用程式： ■ 用戶端電腦上的使用者通知您某個應用程式未執行。 ■ 開啟記憶體攻擊緩和日誌或報告，其中列出哪項緩和技術終止了用戶端電腦上的應用程式。 **附註：**由於侵入的本質，有時緩和技術不會產生日誌。 尋找記憶體攻擊緩和事件的日誌和報告

工作	
步驟 2：停用防護並稽核終止應用程式的技術。	先將防護停用在最低層級，使得其他處理程序保持受到保護。請勿關閉記憶體攻擊緩和，以允許應用程式執行，直到您已嘗試所有其他方法為止。 在以下每個子工作之後，前往步驟 3。 **1** 首先，稽核緩和技術所終止的特定應用程式的防護。 例如，如果 Mozilla Firefox 已終止，您會停用 SEHOP 技術或 HeapSpray 技術。由於侵入的本質，有時緩和技術不會建立日誌事件，因此，您無法確定哪項緩和技術終止了應用程式。在此情況下，您應該停用保護該應用程式的每項技術，一次一項，直到您找出造成終止的技術為何。 **2** 稽核單一緩和技術保護的所有應用程式的防護。 **3** 稽核所有應用程式的防護，而不論技術為何。此選項類似於停用記憶體攻擊緩和，除了管理伺服器會為偵測收集日誌事件。使用此選項來檢查舊版 14 MPx 用戶端上的誤報。 稽核已終止應用程式的防護
步驟 3：更新用戶端電腦上的政策並重新執行應用程式。	■ 如果應用程式正確執行，該緩和技術的偵測即為誤報。 ■ 如果應用程式未以您預期的方式執行，該偵測即為檢出。 ■ 如果應用程式仍終止，請在層級限制的層級上稽核。例如，稽核不同的緩和技術或技術保護的所有應用程式。 請參閱第 268 頁的「更新用戶端政策」。
步驟 4：報告誤報並為檢出重新啟用防護。	針對誤報偵測： **1** 通知賽門鐵克安全機制應變中心該偵測為誤報。 向安全機制應變中心報告誤報 報告可疑的錯誤的偵測 (誤報) **2** 透過將每項技術的動作設定為**「否」**，針對終止的應用程式保持停用防護。 **3** 在安全機制應變解決問題之後，透過將技術的動作變更為**「是」**重新啟用防護。 針對檢出偵測： **1** 透過將該緩和技術規則的動作變更回**「是」**重新啟用防護。 **2** 檢查是否有受感染應用程式的修補版本或較新的發行版可修正目前的弱點。安裝修補的應用程式之後，在用戶端電腦上重新執行該應用程式，以查看記憶體攻擊緩和是否仍會終止該應用程式。

尋找記憶體攻擊緩和事件的日誌和報告

您必須檢視日誌並執行快速報告，以尋找記憶體攻擊緩和終止的應用程式。

尋找記憶體攻擊緩和事件的日誌和報告

◆ 在主控台中，執行下列其中一個動作：

- 針對日誌，按下**「監視器」**>**「日誌」**>**「防網路和主機刺探利用」**日誌類型 >**「記憶體攻擊緩和」**日誌內容 >**「檢視日誌」**。
  尋找**「記憶體攻擊緩和已攔截事件」**事件類型。**「事件類型」**欄會列出緩和技術，而**「動作」**欄則列出**「應用程式名稱」**欄中的應用程式是否已遭攔截。例如，下列日誌事件表示 Stack Pivot 攻擊：

  ```
  Attack: Return Oriented Programming Changes Stack Pointer
  ```

- 針對快速報告，按下**「報告」**>**「快速報告」**>**「防網路和主機刺探利用」**報告類型 >**「記憶體攻擊緩和偵測」**報告 >**「建立報告」**。
  尋找攔截的記憶體攻擊緩和偵測。

稽核已終止應用程式的防護

對誤報進行測試時，請變更記憶體攻擊緩和行為，使其可稽核偵測，但也讓應用程式執行。不過，記憶體攻擊緩和不會保護應用程式。

稽核已終止應用程式的防護

1. 在主控台中，按下**「政策」**>**「記憶體攻擊緩和」**>**「記憶體攻擊緩和」**。
2. 在**「緩和技術」**標籤上，於**「選擇緩和技術」**旁，選取終止應用程式的技術，例如**StackPvt**。
3. 在**「受保護」**欄下方，選取終止的應用程式，然後將**「預設值 (是)」**變更為**「只記錄」**。
   在驗證該偵測真的是誤報之後，將動作變更為**「否」**。**「只記錄」**和**「否」**兩者會允許可能的侵入，但也會讓應用程式執行。
   部分應用程式有會攔截侵入的多項緩和技術，因此請個別對每項技術執行此步驟。
4. (選擇性) 執行下列其中一個步驟，然後按下**「確定」**：
   - 如果您不確定哪項技術終止了應用程式，請按下**「為此技術的所有應用程式選擇防護動作」**。此選項會覆寫每項技術的設定。
   - 如果您同時具有 14.0.1 用戶端和舊版 14 MPx 用戶端，而您只想要測試 14.0.1 用戶端，請按下**「將所有技術的防護動作設為只記錄」**。
5. (選擇性)如果要測試應用程式而不論技術為何，請在**「應用程式規則」**標籤上，於**「受保護」**欄中，取消勾選終止的應用程式，然後按下**「確定」**。
   針對舊版 14 MPx 用戶端，您僅可以使用此選項。升級至 14.0.1 版用戶端之後，重新啟用防護並執行較精細的調整。開啟**「電腦狀態」**日誌來尋找哪個用戶端執行哪個產品版本。

在步驟 3 到 5 之後，在用戶端電腦上執行應用程式。查看記憶體攻擊緩和日誌以驗證應用程式是否仍執行。

停用記憶體攻擊緩和

因此，您可能會因為下列原因想要停用記憶體攻擊緩和：

- 您還找不出哪項緩和技術終止了用戶端上執行的應用程式。在此情況下，請通知賽門鐵克安全機制應變中心。賽門鐵克建議您在完成疑難排解之後立即重新啟用記憶體攻擊緩和。
- 您不想要防範軟體弱點。

停用記憶體攻擊緩和

1 在主控台中，按下**「政策」>「記憶體攻擊緩和」**。

2 取消勾選**「啟用記憶體攻擊緩和」**。

3 按下**「確定」**。

向安全機制應變中心報告誤報

如果您懷疑 MEM 偵測為誤報，請聯絡安全機制應變中心以解決問題。安全機制應變中心需要使用您提供的資訊重現誤報。

將誤報相關資訊提交至安全機制應變中心

1 在 Symantec Endpoint Protection Manager 中，請確保已啟用 Symantec Insight。Insight 預設為啟用。

請參閱第 411 頁的「自訂下載鑑識設定」。

2 在用戶端電腦上下載並執行 SymDiag 工具。

下載 SymDiag 以偵測賽門鐵克產品問題

3 在 SymDiag 工具的**「首頁」**上，按下**「收集支援資料」**，並針對**「除錯記錄」>「進階」**選項，將**「WPP 除錯」>「追蹤層級」**設為**「詳細資訊」**。

在 SymDiag 中針對 Symantec Endpoint Protection 用戶端使用進階除錯記錄選項

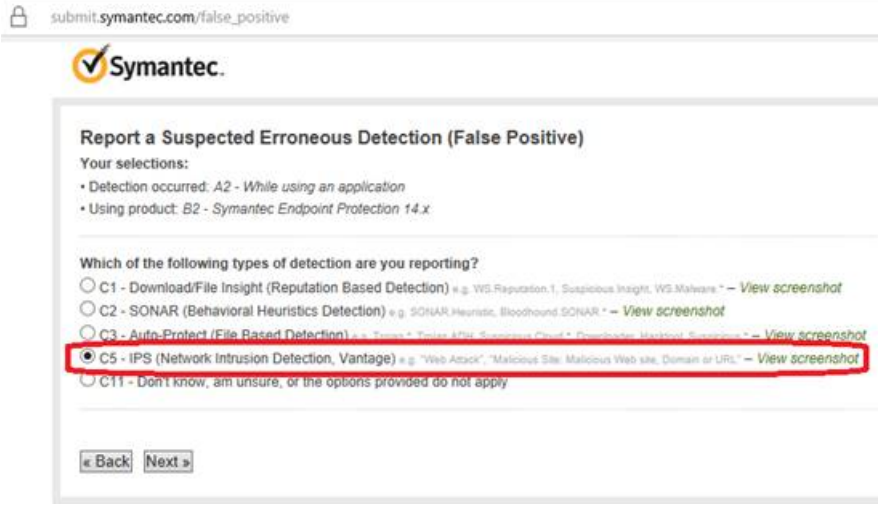
4 重現誤報偵測。

5 日誌收集完成後，透過開啟一個新案例或使用此新資訊更新現有案例，將 `.sdbz` 檔案提交至技術支援。

為技術支援案例提供資料的方法

6 將偵測到的應用程式提交至誤報入口網站，並執行下列工作：

- 選擇偵測發生的時間，選擇 **B2 Symantec Endpoint Protection 14.x** 產品，然後按下 **C5 - IPS** 事件。



- 在提交附註中，提供步驟 5 中的技術支援案例編號、觸發 MEM 偵測的應用程式，以及有關應用程式版本號碼的詳細資料。
  例如，您可能會新增：「"Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe"，vlc.exe 的版本為 2.2.0-git-20131212-0038。這不是最新的可用版本，卻是我們的組織需要使用的版本。」
  塞門鐵克行家秘訣：成功提交！

7 在用戶端電腦上，壓縮位於以下位置的提交資料夾的複本：
`%PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK`。

將此資料夾提交至技術支援，並通知他們您在步驟 6 中開啟的誤報提交的追蹤號碼。技術支援可確保所有必要的日誌和材料完整保留且與誤報調查相關聯。

18

管理病毒和間諜軟體防護

本章包含以下主題：

- 阻止和處理病毒和間諜軟體對用戶端電腦的攻擊
- 移除病毒和安全風險
- 使用 Symantec Endpoint Protection 移除與防範勒索軟體
- Windows 用戶端如何從雲端接收定義檔
- 在用戶端電腦上管理掃描
- 設定在 Windows 電腦上執行的排程掃描
- 設定在 Mac 電腦上執行的排程掃描
- 設定在 Linux 電腦上執行的排程掃描
- 在用戶端電腦上執行隨選掃描
- 調整掃描以改善電腦效能
- 調整掃描以增強對用戶端電腦的防護
- 管理「下載鑑識」偵測
- Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策
- Symantec Endpoint Protection 如何使用進階機器學習？
- Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？
- 管理 Windows 用戶端的隔離所
- 管理顯示在用戶端電腦上的病毒和間諜軟體通知
- 關於出現在 Windows 8 用戶端上的彈出式通知

- 啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知
- 管理提早啟動防惡意軟體 (ELAM) 偵測
- 調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項
- 架構站台使用私用 Insight 伺服器進行信譽查詢
- 將用戶端群組架構為使用私用伺服器進行信譽查詢和提交

阻止和處理病毒和間諜軟體對用戶端電腦的攻擊

您可以遵循一些重要準則來阻止和處理病毒和間諜軟體對用戶端電腦的攻擊。

表 18-1 保護電腦免受病毒和間諜軟體攻擊

工作	敘述
確定電腦已安裝 Symantec Endpoint Protection	網路中的所有電腦和所有伺服器應該已安裝 Symantec Endpoint Protection。確定 Symantec Endpoint Protection 執行正常。 請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。
使定義檔保持最新	確定用戶端電腦已安裝最新的定義檔。 您可以在**「用戶端」**標籤上檢查定義檔日期。您可執行指令以更新過期的定義檔。 您還可以執行電腦狀態報告以檢查最新的定義檔日期。 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。
執行定期掃描	根據預設，「自動防護」和 SONAR 在用戶端電腦上執行。預設排程作用中掃描也會在用戶端電腦上執行。 您可以根據需求執行掃描。您可以自訂掃描設定。 請參閱第 374 頁的「在用戶端電腦上執行隨選掃描」。 您可能希望建立和自訂排程掃描。 一般而言，您最好每週執行一次完整排程掃描，並且每天執行一次作用中掃描。根據預設，Symantec Endpoint Protection 會產生在下午 12:30 執行的作用中掃描。在非受管電腦上，Symantec Endpoint Protection 還包含已停用的預設開機掃描。 請確定網路中的電腦每天執行一次作用中掃描。如果懷疑網路中有非作用中威脅，您最好排程每週或每月執行一次完整掃描。 完整掃描會消耗更多的電腦資源，而且可能會影響電腦效能。 請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。 請參閱第 373 頁的「設定在 Mac 電腦上執行的排程掃描」。 請參閱第 374 頁的「設定在 Linux 電腦上執行的排程掃描」。

工作	敘述
讓用戶端立即上傳重大事件	請確定用戶端 (僅限 Windows) 可以略過活動訊號間隔並立即將重大事件傳送至管理伺服器。重大事件包括任何發現的風險 (cookie 除外) 及任何入侵事件。您可以在**「用戶端」>「政策」>「通訊設定」**中找到該選項。此選項預設為啟用。 當將相關通知的調節器期間設定為**「無」**時，管理員通知會立即警示您。 請參閱第 577 頁的「設定管理員通知」。 **附註：**只有 12.1.4 和更新版本的用戶端可以立即傳送重大事件。舊版用戶端只能按照活動訊號間隔傳送事件。
檢查或修改掃描設定以提昇防護	根據預設，病毒和間諜軟體掃描會偵測、移除和修復病毒和安全風險的負面影響。 預設掃描設定可在最佳化用戶端電腦效能的同時，仍然提供高階的防護。但是，您可以提高防護等級。 例如，您可能希望提升 Bloodhound 啟發式防護。 您可能還希望啟用對網路磁碟機的掃描。 請參閱第 378 頁的「調整掃描以增強對用戶端電腦的防護」。
允許用戶端將有關偵測的資訊傳送給賽門鐵克	用戶端可將有關偵測的資訊傳送給賽門鐵克。所傳送的資訊有助於賽門鐵克處理威脅。 請參閱第418頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。
執行入侵預防	賽門鐵克建議您在用戶端電腦上執行入侵預防以及病毒和間諜軟體防護。 請參閱第 325 頁的「管理入侵預防」。
根據需要對感染進行矯正	執行掃描後，用戶端電腦可能仍然存在感染。例如，新威脅可能沒有特徵，或者 Symantec Endpoint Protection 無法完全移除該威脅。在某些情況下，用戶端電腦需要重新啟動，以便 Symantec Endpoint Protection 完成清除程序。 請參閱第 348 頁的「移除病毒和安全風險」。

移除病毒和安全風險

作為對電腦上的病毒和間諜軟體攻擊進行處理的一部分，您可對風險進行矯正。

您可以使用主控台中的報告和監控功能來確定哪些電腦已受感染，並檢視矯正結果。

表 18-2 移除病毒和安全風險

步驟	敘述
步驟 1：辨識受感染和有風險的電腦	您可以從 Symantec Endpoint Protection Manager 取得有關受感染和有風險的電腦的資訊。 在首頁上，檢查「病毒和風險活動摘要」中「新感染」和「仍受感染」的計數。 「新感染」的計數為「仍受感染」的計數的子集。 「新感染」的計數顯示您在摘要中指定的間隔期間受感染和有風險的電腦的數目。 **附註：**沒有將未矯正的 SONAR 偵測計為「仍受感染」。 它們在摘要中為「可疑」計數的一部分。 如果後續掃描將電腦偵測為受感染，則這些電腦會被視為仍受感染。 例如，排程掃描可能會部分清除某個檔案。「自動防護」隨後會將該檔案偵測為風險。 當新定義檔到達時或一旦用戶端電腦閒置，就會重新掃描被視為「仍受感染」的檔案。 請參閱第 350 頁的「識別受感染及有風險的電腦」。
步驟 2：更新定義檔和重新掃描	您應確保用戶端使用最新的定義檔。 對於在 Windows 電腦上執行的舊版用戶端，還應確保排程和隨選掃描使用「智慧型掃描查詢」功能。自 14 版起，排程和隨選掃描始終使用智慧型掃描查詢。 您可在「受感染和處於風險的電腦」報告中檢查定義檔日期。 可從「風險日誌」中執行「更新內容並掃描」指令。 如果首頁上的「病毒和風險活動摘要」顯示「仍受感染」和「新感染」計數為零，則已經清除了所有風險。 請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。
步驟 3：檢查掃描動作和重新掃描	可將掃描架構為略過風險。 您可能希望編輯病毒和間諜軟體防護政策並變更針對風險類別的動作。 下次掃描執行時，Symantec Endpoint Protection 會套用新動作。 您可在**「動作」**標籤上針對特定掃描類型 (管理員定義或隨選掃描，或自動防護) 設定動作。 您還可以針對「下載鑑識」和 SONAR 變更偵測動作。 請參閱第 351 頁的「檢查掃描動作及重新掃描識別出的電腦」。
步驟 4：重新啟動電腦以完成矯正作業 (如有必要)	電腦由於需要重新啟動，才能完成病毒或安全風險的矯正作業，故而可能仍處於風險之中或受感染。 您可以檢視「風險日誌」，以確定是否有任何電腦需要重新啟動。 您可從電腦狀態日誌執行指令以重新啟動電腦。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

步驟	敘述
步驟 5：調查和清除殘留的風險	如果仍殘留有任何風險，您應做進一步的調查。 您也可以檢視「賽門鐵克安全機制應變中心」網頁，取得病毒和安全風險的最新資訊。 http://www.symantec.com/zh/tw/security_response/index.jsp 在用戶端電腦上，您還可以從掃描結果對話方塊中存取「安全機制應變中心」網站。 您也可以從 Symantec Endpoint Protection Manager 執行 Power Eraser 以分析和矯正困難的永久性威脅。 Power Eraser 是一項應在一台電腦上執行的主動分析，而只有當電腦不穩定或嚴重感染時，才應在少量電腦上執行。 請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。 賽門鐵克技術支援還會提供 Threat Expert 工具，該工具可快速提供對威脅的詳細分析。 您還可以執行載入點分析工具，該工具可幫助您對問題進行疑難排解。 請直接在用戶端電腦上執行這些工具。 請參閱第 656 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。
步驟 6：檢查電腦狀態日誌	檢視電腦狀態日誌，以確保已矯正風險或已將風險從用戶端電腦中移除。 請參閱第 563 頁的「檢視日誌」。

如需詳細資訊，請參閱 網路上的病毒移除和疑難排解。

請參閱第 347 頁的「阻止和處理病毒和間諜軟體對用戶端電腦的攻擊」。

請參閱第 539 頁的「監控端點防護」。

識別受感染及有風險的電腦

您可以使用 Symantec Endpoint Protection Manager 首頁和風險報告來識別受感染及有風險的電腦。

識別受感染的電腦

1 在主控台中，按下**「首頁」**並檢視「病毒和風險活動摘要」。

如果您是系統管理員，就會看到站台中「新感染」和「仍受感染」的電腦數。如果您是網域管理員，可看到網域中「新感染」和「仍受感染」的電腦數。

「仍受感染」是「新感染」的子集合，「仍受感染」的數目會隨著您刪除網路中的風險而降低。如果後續掃描將電腦報告為「受感染」，則電腦仍會處於受感染狀態。例如，Symantec Endpoint Protection 可能只能部分清除電腦中的風險，因此「自動防護」仍會偵測到該風險。

2 在主控台中，按下**「報告」**。

3 在**「報告類型」**清單方塊中，按下**「風險」**。

4 在**「選取報告」**清單方塊中，按下**「受感染和處於風險的電腦」**。

5 按下**「建立報告」**，然後留意顯示的受感染及有風險的電腦清單。

請參閱第 348 頁的「移除病毒和安全風險」。

檢查掃描動作及重新掃描識別出的電腦

如果您的任何電腦已受感染以及有感染風險，則應找出這些電腦仍處於感染和風險狀態的原因。檢查針對受感染和有風險電腦上每個風險所採取的動作。架構及採取的動作有可能是「略過」。如果動作是「略過」，您應該清除電腦中的風險、將電腦從網路中移除，或接受風險。若是 Windows 用戶端，您可能想要編輯「病毒和間諜軟體防護」政策並變更掃描動作。

請參閱第 348 頁的「移除病毒和安全風險」。

識別需要變更的動作及重新掃描識別出的電腦

1 在主控台中，按下**「監視器」**。

2 在**「日誌」**標籤中，選取「風險日誌」，然後按下**「檢視日誌」**。

從「風險日誌事件」欄中，您可以查看發生的事件以及採取的動作。從「風險名稱」欄中，您可以查看仍在作用中風險的名稱。從「網域群組使用者」欄中，您可以查看電腦屬於哪一個群組。

如果用戶端因為掃描採取**「略過」**動作而存在風險，您可能需要變更群組的病毒和間諜軟體防護政策。在**「電腦」**欄中，您可以查看仍處於風險之中的電腦名稱。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

如果您的政策架構為使用推送模式，則在下次活動訊號時，該政策就會被推送至群組中的用戶端。

請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。

3 按**「上一步」**。

4 在**「日誌」**標籤中，選取「電腦狀態日誌」，然後按下**「檢視日誌」**。

5 如果您變更了動作並推送了新政策，請選取需要使用新設定重新掃描的電腦。

6 在「**指令**」清單方塊中，選取「**掃描**」，然後按下「**開始**」以重新掃描電腦。

您可以從「**指令狀態**」標籤，監控「掃描」指令的狀態。

使用 Symantec Endpoint Protection 移除與防範勒索軟體

Petya 勒索軟體

WannaCry 勒索軟體

何謂勒索軟體？

勒索軟體是一種惡意軟體類別，會破壞文件並使文件無法使用，但電腦使用者仍可存取電腦。勒索軟體攻擊者會迫使受害者透過明確註明的付款方式支付贖金，然後才會讓受害者能存取其資料。不過，無法使用移除工具將勒索軟體解密。

勒索鎖定程式是一種相關類型的惡意軟體，會透過鎖定使用者的電腦，使得使用者無法存取其裝置或資料。受害者會收到訊息，該訊息看起來是來自當地的執法單位，要求受害者支付「罰款」，才能避免被捕並解除鎖定其電腦。

如何移除勒索軟體

CryptoLocker 是一種勒索軟體變體，惡意軟體通常藉此對使用者的檔案進行加密，並且經常會刪除原始檔案。攻擊者會要求贖金，才會對檔案解密。不只是本機電腦上的檔案會遭到損壞，任何此電腦具有寫入存取權限的共用或連接網路磁碟機上的檔案也會遭殃。

組織必須回應日益增加的勒索軟體威脅

別支付贖金：對抗新安全威脅的勒索軟體

賽門鐵克安全威脅集合：勒索軟體一年 3400 萬美元業務

預防勒索軟體的 5 個步驟

強化環境以抵禦勒索軟體

若要避免勒索軟體感染，請遵循下列步驟：

1. **定期備份電腦和伺服器。**

   定期備份用戶端電腦和伺服器上的檔案。您可以在電腦離線時備份檔案，或是使用網路電腦和伺服器無法寫入的系統。如果您沒有專用的備份軟體，也可以將重要檔案複製到抽取式媒體。然後退出並拔掉抽取式媒體；不要讓抽取式媒體持續插著。

2. **用密碼和存取控制限制保護對應網路磁碟機，來鎖定這些磁碟機。**

   對網路磁碟機上的檔案，使用唯讀存取權，除非絕對需要擁有這些檔案的寫入存取權。限制使用者權限可限制威脅可以加密哪些檔案。

3. **從 Symantec Endpoint Protection Manager 部署並啟用以下防護功能：**

   - **IPS**
     IPS 會攔截光靠傳統病毒定義檔無法阻止的某些威脅。IPS 是最佳防禦工具，可以防止從 Internet 不知不覺地下載軟體時所發生的　渡式下載。攻擊者通常使用侵入套件，透過　渡式下載進行 CryptoLocker 之類的網頁式攻擊。
     請參閱第 330 頁的「啟用網路入侵預防或瀏覽器入侵預防」。
   - **SONAR**
     SONAR 的行為式防護功能是另一個防禦惡意軟體的重要功能。SONAR 可防止 CryptoLocker 之類的勒索軟體變體的雙重可執行檔名稱執行。
     在「病毒和間諜軟體防護」政策中，按下 **SONAR** > **「啟用 SONAR」**。
   - **下載鑑識**
     在**「病毒和間諜軟體 - 高安全性」**政策中修改下載鑑識，以隔離賽門鐵克客戶群尚未證明為安全的檔案。
     請參閱第 354 頁的「利用下載鑑識防止勒索軟體攻擊」。

   使用內建的 Windows 工具復原被勒索鎖定的檔案

4. **下載適用於 Web 應用程式架構的最新修正程式，以及網頁瀏覽器外掛程式。**

   攻擊侵入套件無法進行　渡式下載，除非有較舊版的外掛程式 (如 Flash) 可以利用。根據歷史事實，攻擊是透過網路釣魚和網頁瀏覽器來進行的。最近，更多攻擊是透過易受攻擊的 Web 應用程式來進行 (如 JBOSS、WordPress 和 Joomla)。

5. **請使用電子郵件安全性產品，來安全處理電子郵件。**

   CryptoLocker 通常透過含有惡意附件的垃圾郵件來散播。利用專用的郵件安全性產品或服務來掃描入埠電子郵件是否含有威脅，對於確保勒索軟體和其他惡意軟體遠離您的組織非常重要。如需重要的指示和建議，請參閱：

   支援觀點：W97M.Downloader 作戰計劃

如何移除勒索軟體

目前沒有勒索軟體移除工具或 CryptoLocker 移除工具。萬一您的用戶端電腦感染到勒索軟體，且您的資料遭到加密，請遵循以下步驟：

1. **不要支付贖金。**

   如果您支付贖金：

   - 這不能保證攻擊者會提供解除鎖定電腦或解密檔案的方法。
   - 攻擊者會使用贖金來資助對其他使用者的其他攻擊。

2. **在勒索軟體可以攻擊受感染電腦可以存取的網路磁碟機之前，先將受感染的電腦隔離。**
3. **使用 Symantec Endpoint Protection Manager 更新病毒定義檔，並掃描用戶端電腦。**

新的定義檔可以偵測並修正勒索軟體。只要用戶端受管理並且連線至 Symantec Endpoint Protection Manager，Symantec Endpoint Protection Manager 便會自動將病毒定義檔下載到用戶端。

在 Symantec Endpoint Protection Manager 中，按下**「用戶端」**，在群組上按下滑鼠右鍵，然後按下**「對群組執行指令」>「更新內容和掃描」**。

4. **從已知良好的備份還原損壞的檔案。**

   至於其他安全性產品，Symantec Endpoint Protection 無法對勒索鎖定程式已破壞的檔案進行解密。

5. **將惡意軟體提交至賽門鐵克安全機制應變中心。**

   如果您可以識別惡意的電子郵件或可執行檔，請將其傳送至賽門鐵克安全機制應變中心。這些樣本可以讓賽門鐵克建立新特徵，以及改進防禦勒索軟體的功能。

   塞門鐵克行家秘訣：成功提交！

如需詳細資訊

- 對於重大的勒索軟體資安事端，請洽詢塞門鐵克全球資安事端回應小組。他們可以協助驗證您是否遭受攻擊，並能協助您決定後續步驟。請參閱：
  塞門鐵克資安事端回應中心協助因應勒索軟體的 10 個方式
  如需立即協助解決資安事端：
  電子郵件：incidentresponse@symantec.com
  資安事端回應熱線： (855) 378-0073
- 有關勒索軟體威脅的其他資訊

利用下載鑑識防止勒索軟體攻擊

若要防止勒索軟體變體，請架構「下載鑑識」隔離賽門鐵克客戶群已知為惡意的檔案，或是尚未證明為惡意的檔案。

請參閱第 352 頁的「使用 Symantec Endpoint Protection 移除與防範勒索軟體」。

利用下載鑑識防止勒索軟體攻擊

1 在主控台中，開啟**「病毒和間諜軟體防護政策 - 高安全性」**並按**「下載防護」**。

2 在**「下載鑑識」**標籤上，確定勾選**「啟用下載鑑識以根據檔案信譽偵測下載檔案中的潛在風險」**。

3 檢查以下預設選項：

- **具有 *5* 個或更少使用者的檔案**
- **在 *2* 或更少天內的使用者已知檔案**

低的預設值會迫使用戶端將尚未由超過五個使用者向賽門鐵克報告的任何檔案，或是將不足 2 天的任何檔案視為未證明的檔案。如果未證明的檔案符合這些準則，「下載鑑識」會將這些檔案偵測為惡意檔案。

4 請確定勾選**「自動信任從信任的 Internet 或內部網路網站下載的任何檔案」**。

5 在**「動作」**標籤的**「惡意檔案」**下，使第一個動作保持為**「隔離風險」**，第二個動作則保持為**「略過」**。

6 在**「未證明的檔案」**下方，按下**「隔離風險」**。

7 按下**「確定」**。

Windows 用戶端如何從雲端接收定義檔

從 14 版開始，Symantec Endpoint Protection 標準和內嵌/VDI 用戶端利用雲端中的定義檔提供即時防護。舊版提供了一些具有各種功能的雲端防護，例如下載鑑識。現在，所有病毒和間諜軟體功能使用雲端來評估檔案。雲端內容包括整組病毒和間諜軟體定義檔，以及賽門鐵克具有的有關檔案和潛在威脅的最新資訊。

附註：僅 Windows 用戶端支援 Intelligent Threat Cloud Service。

用戶端支援啟用雲端的內容

啟用雲端的內容包括提供充分防護的一組減小大小的定義檔。當用戶端需要新的定義檔時，用戶端會下載或查詢在雲端的定義檔，以取得更好的效能和速度。

從 14 開始，標準用戶端和內嵌式/VDI 用戶端支援啟用雲端的內容。

請參閱第 99 頁的「如何選擇用戶端安裝類型」。

所有掃描會自動使用雲端查詢

雲端查詢包括查詢 Symantec Insight 的檔案信譽資訊以及雲端中的定義檔檢查。

- 排程和隨選掃描會自動執行雲端查詢。
- 自動防護還會自動執行雲端查詢。現在，自動防護在使用者模式而非核心模式下執行，可減少記憶體使用量，並提供更好的效能。

除了定義檔在磁碟上佔用較少的使用量，Intelligent Threat Cloud Service 還可減少 15% 的掃描時間。

附註：12.1.x 智慧型掃描查詢功能針對舊版用戶端上入口網站檔案的排程和隨選掃描提供檔案信譽查詢。此選項包含單獨的敏感程度。在 14.0.x 版中，12.1.x 用戶端使用針對下載鑑識設定的敏感程度，您只能啟用或停用智慧型掃描查詢。

用戶端會自動將檔案信譽查詢的相關資訊傳送至賽門鐵克。

請參閱第 420 頁的「管理用戶端傳送給賽門鐵克的匿名或非匿名資料」。

雲端查詢如何在網路中運作

Symantec Endpoint Protection 會將雲端查詢直接傳送至雲端。

附註：如果您使用 EDR 伺服器，信譽查詢將在到達雲端之前透過 EDR 伺服器路由。

請參閱第 397 頁的「將用戶端群組架構為使用私用伺服器進行信譽查詢和提交」。

如果您要使用代理伺服器，可在用戶端的瀏覽器「網際網路選項」中指定 HTTPS 代理。或者，您可以使用 Symantec Endpoint Protection Manager 主控台在**「政策」>「外部通訊」**中為用戶端指定 HTTPS 代理。

請參閱第 422 頁的「指定用於用戶端傳送資訊和其他外部通訊的代理伺服器」。

Intelligent Threat Cloud Service 用戶端所使用的頻寬量與 14 之前的用戶端幾乎相同，這些用戶端僅使用具有特定功能的信譽查詢，如下載鑑識。

Symantec Endpoint Protection Manager 如何向您警示雲端查詢錯誤

如果用戶端嘗試雲端查詢 3 天但未成功，則 Symantec Endpoint Protection Manager 預設會將電子郵件通知傳送給系統管理員。也可以在**「監視器」>「日誌」>「系統日誌」>「用戶端活動」**中檢視警示。通知條件類型為**「檔案信譽偵測」**。

請參閱第 563 頁的「檢視日誌」。

請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。

什麼是入口網站檔案？

當下載鑑識檢查使用者從支援入口網站下載的檔案時，會將該檔案標示為入口網站檔案。排程和隨選掃描、自動防護和下載鑑識使用為下載鑑識設定的敏感程度評估入口網站檔案的信譽。

附註：必須啟用下載鑑識，將檔案標示為入口網站檔案。

支援的入口網站包含 Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Google Chrome、Windows Live Messenger 和 Yahoo Messenger。入口網站清單 (或自動防護入口網站清單) 是 LiveUpdate 下載到管理伺服器或用戶端的病毒和間諜軟體防護內容的一部分。

掃描和下載鑑識一律使用賽門鐵克設定的預設內部敏感程度來評估非入口網站檔案。內部預設值僅偵測大多數惡意檔案。

請參閱第 380 頁的「管理「下載鑑識」偵測」。

雲端查詢動作範例

Intelligent Threat Cloud Service 保護用戶端的方式範例：

- 用戶端使用者執行 Internet Explorer 並嘗試下載檔案。下載鑑識使用雲端中的 Symantec Insight 提供之敏感程度和信譽資訊，判斷檔案是否無害。
- 下載鑑識判斷檔案的信譽是否可接受，允許下載檔案，並將該檔案標示為入口網站檔案。
- 之後，賽門鐵克從其廣泛的 Global Intelligence Network 取得有關檔案的詳細資訊。賽門鐵克判斷該檔案可能有害，並更新 Insight 信譽資料庫。賽門鐵克可能會在雲端的定義檔中提供檔案的最新特徵。
- 如果使用者開啟檔案或執行掃描，自動防護或掃描會從雲端取得有關檔案的最新資訊。透過最新檔案信譽和下載鑑識敏感程度或透過最新檔案特徵，自動防護或掃描現在可以偵測檔案為具有潛在惡意。

必要設定和建議設定

依據預設，Symantec Endpoint Protection 會使用雲端。如果您停用其中任何選項，便會限制或停用雲端防護。

- 自動防護
  必須啟用「自動防護」。「自動防護」預設為啟用。
- 下載鑑識
  必須啟用「下載鑑識」，以便它可以檢查檔案下載，並將檔案下載標示為入口網站檔案以供日後掃描。如果您停用「下載鑑識」，所有檔案下載都將視為非入口網站檔案。掃描僅偵測大多數惡意的非入口網站檔案。
  請參閱第 380 頁的「管理「下載鑑識」偵測」。
- 智慧型掃描查詢
  必須啟用「智慧型掃描查詢」。智慧型掃描查詢選項可控制信譽查詢以及雲端定義查詢。此選項預設為啟用。

  警告：如果停用「智慧型掃描查詢」，雲端防護將會完全停用。

- 產品使用狀況和用戶端傳送
  賽門鐵克建議允許伺服器和用戶端與賽門鐵克共用資訊。與賽門鐵克共用的資料可提升偵測功能的效能。可能會攻擊您電腦的潛在惡意軟體的相關資訊可協助改善安全性領域並加快解決威脅的速度。賽門鐵克會竭盡所能讓資料匿名，以防止傳輸個人識別資訊。
  請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

請參閱第 682 頁的「針對 Windows 用戶端 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能相依性」。

在用戶端電腦上管理掃描

某些掃描會預設執行，但您可能希望變更設定或設定自己的排程掃描。您還可以自訂掃描，並變更這些掃描在您的用戶端電腦上提供的防護程度。

從 14 版開始，掃描會存取在雲端設定的完整定義檔。

請參閱第 355 頁的「Windows 用戶端如何從雲端接收定義檔」。

表 18-3 在用戶端電腦上修改掃描

工作	敘述
檢視掃描類型和預設設定	檢查您的掃描設定。您可以檢視預設值，然後決定是否要進行變更。 請參閱第 359 頁的「關於掃描和即時防護的類型」。 請參閱第 367 頁的「關於預設的病毒和間諜軟體防護政策掃描設定」。
建立排程掃描和執行隨選掃描	您可以使用排程掃描與隨選掃描，增強自動防護所提供的防護。自動防護會在您讀寫檔案時，提供防護。排程掃描與隨選掃描則可以掃描用戶端電腦儲存的所有檔案。也可以防護用戶端電腦的記憶體、載入點，及其他重要位置。 排程掃描設定可以儲存為範本。架構多個政策時，使用掃描範本可節省時間。您可使用存為範本的任何掃描，做為不同政策中新掃描的基礎。 **附註：**對於受管理用戶端，Symantec Endpoint Protection 提供預設排程掃描，掃描用戶端電腦中所有的檔案、資料夾及位置。 請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。 請參閱第 373 頁的「設定在 Mac 電腦上執行的排程掃描」。 請參閱第 374 頁的「設定在 Linux 電腦上執行的排程掃描」。 請參閱第 374 頁的「在用戶端電腦上執行隨選掃描」。
為您的環境自訂掃描設定	您可以自訂「自動防護」設定及管理員定義掃描中的選項。您可能希望變更掃描設定以處理偵測誤報、最佳化電腦或掃描效能，或變更掃描動作或通知。 對於排程掃描，您還可以針對未執行掃描、隨機化掃描及是否要掃描網路磁碟機來設定選項。 請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。 請參閱第 401 頁的「自訂在 Mac 電腦上執行的病毒和間諜軟體掃描」。 請參閱第 401 頁的「自訂在 Linux 電腦上執行的病毒和間諜軟體掃描」。
調整掃描以提高用戶端電腦效能	根據預設，Symantec Endpoint Protection 會在提供高安全性等級的同時，將對用戶端電腦效能的影響降至最低。但是，您可以變更某些設定，進一步最佳化電腦效能。最佳化在虛擬環境中很重要。 **附註：**透過調整設定來最佳化用戶端電腦效能，或許會降低用戶端電腦的一些安全性。 請參閱第 375 頁的「調整掃描以改善電腦效能」。

工作	敘述
調整掃描以提高對用戶端電腦的防護	預設掃描設定可在最佳化用戶端電腦效能的同時，仍然提供高階的防護。但是，您可以提高防護等級。 請參閱第 378 頁的「調整掃描以增強對用戶端電腦的防護」。
管理下載鑑識偵測	「下載智慧型掃描」會檢查使用者嘗試透過網頁瀏覽器、文字訊息用戶端及其他入口網站下載的檔案。「下載智慧型掃描」使用來自「賽門鐵克智慧型掃描」的信譽資訊進行檔案相關決策。 請參閱第 380 頁的「管理「下載鑑識」偵測」。
管理 SONAR	SONAR 屬於用戶端電腦上「主動型威脅防護」的一部分。但是，SONAR 設定是「病毒和間諜軟體防護」政策的一部分。 請參閱第 425 頁的「管理 SONAR」。
架構掃描的例外	您可以為已知是安全的檔案和應用程式建立例外。 Symantec Endpoint Protection 還會自動排除某些檔案和資料夾。 請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。 請參閱第 365 頁的「關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾」。
管理隔離所中的檔案	您可以監控和刪除用戶端電腦上已隔離的檔案。 還可以指定隔離所的設定。 請參閱第 387 頁的「管理 Windows 用戶端的隔離所」。
允許用戶端將有關偵測的資訊傳送給賽門鐵克	根據預設，用戶端會將有關偵測的資訊傳送給賽門鐵克。您可以關閉遞送或選擇用戶端遞送的資訊類型。 賽門鐵克建議您始終允許用戶端傳送資訊。此資訊有助於賽門鐵克處理威脅。 請參閱第418頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。
管理顯示在用戶端電腦上的病毒和間諜軟體通知	您可以決定是否要在用戶端電腦上顯示病毒和間諜軟體事件的通知。 請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

關於掃描和即時防護的類型

Symantec Endpoint Protection 包含不同類型的掃描和即時防護，用於偵測不同類型的病毒、威脅和風險。

附註：從 14 版開始，掃描會存取在雲端設定的完整定義檔。

請參閱第 355 頁的「Windows 用戶端如何從雲端接收定義檔」。

預設情況下，Symantec Endpoint Protection 會在每天中午 12:30 執行作用中掃描。Symantec Endpoint Protection 還會在新定義檔到達用戶端電腦時執行作用中掃描。 在非受管電腦上，Symantec Endpoint Protection 還包含已停用的預設開機掃描。

附註：當用戶端電腦關機或處於休眠或睡眠模式時，電腦可能會錯過排程的掃描。 當電腦開機或喚醒時，預設會在指定的間隔時間內重試掃描。 如果間隔時間已經結束，Symantec Endpoint Protection 則不會執行掃描，而會等到下次的排程時間再執行。 您可以修改錯過排程掃描的設定。

請確定網路中的電腦每天執行一次作用中掃描。 如果懷疑網路中有非作用中威脅，您最好排程每週或每月執行一次完整掃描。 完整掃描會消耗更多的電腦資源，而且可能會影響電腦效能。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

表 18-4 掃描類型

掃描類型	敘述
自動防護	「自動防護」會持續檢查寫入電腦或從電腦讀取的檔案和電子郵件資料。「自動防護」會自動處理或清除偵測到的病毒和安全風險。 Mac 用戶端和 Linux 用戶端僅支援對檔案系統的「自動防護」。 從 14 版開始，在連線至雲端的標準和內嵌式/VDI 用戶端上，自動防護會自動查詢雲端的最新定義檔。 請參閱第 404 頁的「自訂 Linux 用戶端的自動防護」。
下載智慧型掃描 (僅限 Windows 用戶端)	「下載智慧型掃描」會透過以下方法提升「自動防護」掃描的安全性：當使用者嘗試從瀏覽器及其他入口網站下載檔案時檢查這些檔案。 它會使用來自「賽門鐵克智慧型掃描」的信譽資訊來允許或攔截下載嘗試。 「下載智慧型掃描」包含在「自動防護」中，因此需要啟用「自動防護」。 請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。

掃描類型	敘述
管理員定義掃描	管理員定義的掃描會透過檢查用戶端電腦上的全部檔案和程序來偵測病毒及安全風險。 管理員定義的掃描還可檢查記憶體及載入點。 可用的管理員定義的掃描類型如下： ■ 排程掃描 排程掃描會於指定時間在用戶端電腦上執行。任何排程時間相同的掃描都會按順序執行。若於排程掃描期間電腦為關閉、休眠或睡眠狀態，除非電腦已架構為重試錯過的掃描，否則不會執行此掃描。 當電腦啟動或喚醒時，Symantec Endpoint Protection 會重試掃描，直到掃描開始或重試間隔到期為止。 您可以針對 Windows 用戶端排程作用中掃描、完整掃描或自訂掃描。 您只能對 Mac 用戶端或 Linux 用戶端排程自訂掃描。 排程掃描設定可以儲存為範本。 您可使用另存為範本的任何掃描作為不同掃描的基礎。架構多個政策時，使用掃描範本可節省時間。根據預設，政策中會包含排程掃描範本。預設排程掃描會掃描所有的檔案和目錄。 ■ 開機掃描和觸發掃描 開機掃描於使用者登入電腦時執行。觸發掃描於新的病毒定義檔下載至電腦時執行。 **附註：**開機掃描和觸發掃描僅可用於 Windows 用戶端。 ■ 隨選掃描 隨選掃描是指，您在 Symantec Endpoint Protection Manager 中選取掃描指令時立即執行的掃描。 您可以從**「用戶端」**標籤或日誌中選取該指令。 如果 Windows 適用的 Symantec Endpoint Protection 用戶端偵測到大量的病毒、間諜軟體或高風險威脅，則進入主動掃描模式。 掃描將重新啟動並使用智慧型掃描查詢。 請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。 請參閱第 373 頁的「設定在 Mac 電腦上執行的排程掃描」。
SONAR (僅限 Windows 用戶端)	SONAR 針對零時差攻擊提供即時防護。 SONAR 甚至可以在傳統的特徵型定義檔偵測到威脅之前，阻止進攻。 SONAR 使用啟發式和檔案信譽資料做出有關應用程式或檔案的決策。 與主動型威脅掃描相同，SONAR 也會偵測鍵盤記錄程式、間諜軟體以及任何其他可能具有惡意或具有潛在惡意的應用程式。 請參閱第 424 頁的「關於 SONAR」。
提早啟動防惡意軟體 (ELAM) (僅限 Windows 用戶端)	與 Windows 提早啟動惡意軟體防護驅動程式搭配使用。僅自 Windows 8 和 Windows Server 2012 起受支援。 提早啟動防惡意軟體會在網路中的電腦啟動時，以及第三方驅動程式初始化之前，為電腦提供防護。 請參閱第 393 頁的「管理提早啟動防惡意軟體 (ELAM) 偵測」。

關於自動防護的類型

自動防護會掃描檔案及某些類型的電子郵件和電子郵件附件。

預設會啟用所有類型的自動防護。如果您使用伺服器型電子郵件掃描解決方案，例如Symantec Mail Security，就可能不需要啟用電子郵件自動防護。

Mac 用戶端和 Linux 用戶端不支援電子郵件自動防護掃描。

表 18-5　　自動防護的類型

自動防護的類型	敘述
自動防護	從用戶端電腦讀取檔案或將檔案寫入用戶端電腦時，進行連續掃描。 預設會為檔案系統啟用自動防護。自動防護在電腦啟動時載入。此項防護將檢測所有檔案中是否存在病毒及安全風險，並攔截安全風險的安裝。可選擇掃描檔案副檔名、掃描遠端電腦上的檔案，以及掃描磁片上的開機病毒。可選擇先備份檔案，再嘗試修復檔案、終止程序及停止服務。 您可以架構「自動防護」只掃描選取的副檔名。當自動防護掃描選取的副檔名時，即使病毒變更了檔案的副檔名，自動防護也能判斷檔案的類型。 對於不執行電子郵件自動防護的那些用戶端，啟用自動防護後，用戶端電腦仍會受到保護。大多數電子郵件應用程式會在使用者啟動電子郵件附件時，將附件儲存到暫存資料夾。「自動防護」會在檔案寫入暫存資料夾時掃描檔案，並偵測是否存在任何病毒或安全性風險。如果使用者嘗試將受感染的附件儲存到本機磁碟機或網路磁碟機，「自動防護」也會偵測病毒。
Microsoft Outlook 自動防護 (僅限 Windows)	下載內送的Microsoft Outlook 電子郵件附件，並在使用者閱讀訊息並開啟附件時，掃描是否存在病毒和安全風險。 Microsoft Outlook 自動防護支援 Microsoft Outlook 98 到 Outlook 2013 的 MAPI 或 Internet 通訊協定。Microsoft Outlook 自動防護支援 32 位元和 64 位元系統。 在安裝期間，如果套件中已納入「Microsoft Outlook 自動防護」，且電腦上已經安裝 Microsoft Outlook，則 Symantec Endpoint Protection 會安裝此防護。 如果使用者透過慢速連線下載大型附件，會影響電子郵件效能。如果您確定文件是安全的，則可以建立例外。 請參閱第 475 頁的「從掃描中排除檔案或資料夾」。 **附註：**請不要在 Microsoft Exchange Server 上安裝 Microsoft Outlook 自動防護。您應改為安裝 Symantec Mail Security for Microsoft Exchange。

自動防護的類型	敘述
Internet 電子郵件自動防護 (僅限 Windows) 此功能僅適用於低於 14.2 RU1 的用戶端版本。	掃描入埠 Internet 電子郵件內文和電子郵件附件是否存在病毒和安全風險；此外，也執行離埠電子郵件啟發式掃描。 依據預設，「Internet 電子郵件自動防護」支援透過 POP3 與 SMTP 連線的加密密碼及電子郵件。「Internet 電子郵件自動防護」支援 32 位元或 64 位元系統。如果您使用 POP3 或 SMTP 搭配安全通訊端層 (SSL)，則用戶端會偵測安全連線，但不會掃描加密的郵件。 **附註：**基於效能考量，伺服器作業系統不支援 POP3 的「Internet 電子郵件自動防護」。 電子郵件掃描不支援 IMAP、AOL 或 HTTP 式的電子郵件，例如 Hotmail 或 Yahoo!Mail.
Lotus Notes 自動防護 (僅限 Windows) 此功能僅適用於低於 14.2 RU1 的用戶端版本。	掃描內送的 Lotus Notes 電子郵件附件是否存在病毒和安全風險。 Lotus Notes 自動防護支援 Lotus Notes 7.x 或更新版本。 在安裝期間，如果套件中已納入「Lotus Notes 自動防護」，且電腦上已經安裝 Lotus Notes，則 Symantec Endpoint Protection 會安裝該防護。

請參閱第 359 頁的「關於掃描和即時防護的類型」。

請參閱第 405 頁的「為 Windows 電腦上的電子郵件掃描自訂自動防護」。

關於病毒和安全風險

Symantec Endpoint Protection 可以掃描病毒和安全風險。病毒和安全風險可透過電子郵件訊息或即時通訊程式感染。通常使用者會因為接受軟體程式的「使用者授權許可協議」，而在不知情的狀況下載風險。

許多病毒和安全風險都以偷渡式下載安裝到電腦。這類下載通常發生於使用者瀏覽惡意網站或受感染的網站時，而應用程式的下載程式會透過電腦上的合法漏洞進行安裝。

您可以變更 Symantec Endpoint Protection 在偵測到病毒或安全風險時要執行的動作。對於 Windows 用戶端，安全風險類別是動態的，會隨時間變化，因為賽門鐵克會收集有關風險的資訊。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

您可以在「賽門鐵克安全機制應變中心」網站上檢視有關特定病毒和安全風險的資訊。

表 18-6 病毒和安全風險

風險	說明
病毒	執行時將本身附加在其他電腦程式或檔案的程式或檔案。當受感染的程式執行時，附加的病毒程式會啟動，並將自己附加到其他程式和檔案中。 病毒類別中包含下列威脅類型： ■ 惡意 Internet Bot 在 Internet 上執行自動化工作的程式。Bot 可用來自動化對電腦的攻擊，或從網站收集資訊。 ■ 病蟲 複製時不會感染其他程式的程式。有些病蟲透過在磁碟間自我複製來進行傳播，而另外一些病蟲在記憶體中進行複製，從而降低電腦效能。 ■ 特洛伊木馬程式 將自己隱藏在諸如遊戲或公用程式之類的無害程式中的程式。 ■ 混合型威脅 將病毒、病蟲、特洛伊木馬程式和程式碼與伺服器和 Internet 弱點混合，以便起始、傳送和散佈攻擊的威脅。混合型威脅利用多種方法和技術迅速傳播，並導致大範圍的破壞。 ■ Rootkit 藏匿在電腦作業系統中的程式。
廣告程式	提供任何廣告內容的程式。
Cookie	Web 伺服器出於識別電腦或使用者的目的傳送給網頁瀏覽器的訊息。
撥接工具	這類程式通常會利用電腦，在沒有使用者許可或不知情的狀況下，透過 Internet 撥號到 900 號碼或是 FTP 網站。通常，撥接這些號碼，會產生費用。
駭客工具	駭客所使用的程式，可以未經授權存取使用者的電腦。例如，有一種駭客工具叫做按鍵記錄器，它可以追蹤與記錄個別的按鍵，並傳回這個資訊給駭客。然後駭客就可以執行通訊埠掃描或是漏洞掃描。駭客工具也可以用來建立病毒。
惡作劇程式	這種程式企圖以幽默或嚇人的方式，來改變或中斷電腦的作業。例如，玩笑程式會在使用者試圖刪除項目時，使資源回收筒遠離滑鼠。
誤導應用程式	故意誤報電腦安全性狀態的應用程式。這些應用程式通常偽裝成安全性通知，告知必須移除的任何假病毒感染。
家長防護網程式	監控或限制電腦使用的程式。這些程式在執行時不會被偵測到，並且通常會將監控資訊傳輸到其他電腦。
遠端存取程式	這種程式允許由其他電腦透過 Internet 存取，因此它們可以得到資訊，或是攻擊或改變使用者的電腦。
安全評定工具	用於收集資訊以便取得對電腦的未經授權的存取的程式。
間諜軟體	是一種單機的程式，可以秘密地監控系統活動，並偵測密碼以及其他機密的資訊，再將它轉遞回另一台電腦。

風險	說明
追蹤軟體	單機或附加的應用程式，可追蹤使用者在 Internet 上的路徑，並將資訊傳送到控制者或駭客系統。

關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾

當 Symantec Endpoint Protection 偵測到特定第三方應用程式和某些 Symantec 產品存在時，它會自動為這些檔案和資料夾建立排除項目。用戶端會從所有掃描中排除這些檔案和資料夾。

附註：用戶端不會將系統暫存資料夾排除在掃描範圍外，因為這樣做會產生明顯的電腦安全弱點。

若要提高掃描效能或減少誤報偵測，您可以將檔案或資料夾例外新增到「例外」政策以排除檔案。您也可以指定要包含在特定掃描中的副檔名或資料夾。

警告：從掃描中排除的檔案或資料夾不會受到保護，因此可能受到病毒和安全風險的威脅。

您可以檢視用戶端自動建立的排除項目。

請查看 Windows 登錄的以下位置：

- 在 32 位元電腦上，檢視 HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions。
- 在 64 位元電腦上，檢視 HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions。

警告：請勿直接編輯此登錄機碼。

表 18-7 檔案與資料夾排除

檔案	敘述
Microsoft Exchange	用戶端軟體會為下列版本的 Microsoft Exchange Server 自動建立檔案和資料夾的掃描排除項目： ■ Exchange 5.5 ■ Exchange 6.0 ■ Exchange 2000 ■ Exchange 2003 ■ Exchange 2007 ■ Exchange 2007 SP1 ■ Exchange 2010 ■ Exchange 2013 ■ Exchange 2016 對於 Exchange 2007，請參閱使用者文件，瞭解防毒軟體的相容性。在少數情況下，可能需要為某些 Exchange 2007 資料夾手動建立掃描排除項目。例如，在叢集的環境中，您可能需要建立一些排除項目。 用戶端軟體會定期檢查 Microsoft Exchange 檔案和資料夾位置是否有變更。如果您在已安裝用戶端軟體的電腦上安裝 Microsoft Exchange，則用戶端檢查變更狀況時，會建立排除項目。用戶端會排除相應的檔案和資料夾；如果單一檔案移出排除的資料夾，該檔案仍然會在排除範圍內。 如需詳細資訊，請參閱文章防止 Symantec Endpoint Protection 掃描 Microsoft Exchange 2007 目錄結構。
Microsoft Forefront	用戶端會自動為以下 Microsoft Forefront 產品建立檔案和資料夾排除項目： ■ Forefront Server Security for Exchange ■ Forefront Server Security for SharePoint ■ Forefront Threat Management Gateway 檢查 Microsoft 網站中建議排除項目的清單。 另請參閱文章：為 Microsoft Forefront 架構 Symantec Endpoint Protection 排除項目。
Active Directory 網域控制器	用戶端會自動為 Active Directory 網域控制器資料庫、日誌和工作檔案建立檔案和資料夾排除項目。用戶端會監控安裝在用戶端電腦上的應用程式。如果軟體偵測到用戶端電腦上有 Active Directory，便會自動建立排除項目。
賽門鐵克產品	在偵測到某些賽門鐵克產品時，用戶端會自動建立適當的檔案和資料夾掃描排除項目。 用戶端會為下列賽門鐵克產品建立排除項目： ■ Symantec Mail Security 4.0、4.5、4.6、5.0、6.0 for Microsoft Exchange ■ Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange ■ Norton AntiVirus 2.x for Microsoft Exchange ■ Symantec Endpoint Protection Manager 內嵌資料庫和日誌

檔案	敘述
Veritas 產品	在偵測到某些 Veritas 產品時，用戶端會自動建立適當的檔案和資料夾掃描排除項目。 ■ Veritas Backup Exec ■ Veritas NetBackup ■ Veritas System Recovery
選取的副檔名和 Microsoft 資料夾	對於各種類型的管理員定義掃描或自動防護，您可以按照副檔名選取要包含的檔案。對於管理員定義掃描，您也可以按照資料夾選取要包含的檔案。例如，您可以指定排程掃描只掃描某些副檔名，而「自動防護」掃描所有副檔名。 對於執行檔和 Microsoft Office 檔案，即使病毒變更檔案的副檔名，自動防護也可以確定檔案的類型。 Symantec Endpoint Protection 預設會掃描所有的副檔名和資料夾。您取消選取的任何副檔名或資料夾，都會從該特定掃描中排除。 Symantec 不建議您從掃描中排除任何副檔名。然而，如果您決定按副檔名排除檔案和任何 Microsoft 資料夾，則應考慮網路所需的防護程度。您還應考慮用戶端電腦完成掃描所需的時間和資源量。 **附註：**您從檔案系統「自動防護」掃描中排除的任何副檔名，也會從「下載鑑識」中排除。 如果您正在執行「下載鑑識」，則應將常用程式和文件的副檔名包含在要掃描的副檔名清單中。您也應務必掃描 .msi 檔案。
檔案與資料夾排除	您可使用例外政策，為您希望 Symantec Endpoint Protection 從所有病毒和間諜軟體掃描中排除的檔案或資料夾建立例外。 **附註：**預設情況下，用戶端電腦上的使用者也可以建立檔案和資料夾例外。 例如，您可能需要為電子郵件應用程式收件匣建立檔案排除項目。 如果在隨選掃描或排程掃描過程中，用戶端在收件匣檔案中偵測到病毒，則用戶端會隔離整個收件匣。您也可以建立例外以排除收件匣檔案。然而，如果用戶端在使用者開啟電子郵件時偵測到病毒，則用戶端仍會隔離或刪除該郵件。
受信任檔案	病毒和間諜軟體掃描使用 Insight，它可讓掃描略過受信任檔案。您可以為要略過的檔案選擇信任層級，也可以停用該選項。如果您停用該選項，可能會增加掃描時間。 自動防護也可以略過由受信任程序 (例如 Windows 搜尋) 存取的檔案。

請參閱第 475 頁的「從掃描中排除檔案或資料夾」。

關於預設的病毒和間諜軟體防護政策掃描設定

Symantec Endpoint Protection Manager 包含三種預設政策。

- 病毒和間諜軟體防護平衡政策
- 病毒和間諜軟體防護高安全性政策

高安全性政策是所有預先架構的政策中最嚴格的。您必須注意，它可能會影響其他應用程式的效能。

- 病毒和間諜軟體防護高效能政策
  與高安全性政策相比，高效能政策可提供更佳的效能，但不提供相同的防護措施。該政策主要依靠「自動防護」來掃描具有所選取檔案副檔名的檔案，以偵測威脅。

基本病毒和間諜軟體防護政策完善地兼顧了安全性與效能。

表 18-8 病毒和間諜軟體防護平衡政策掃描設定

設定	敘述
檔案系統的自動防護	已啟用 「下載鑑識」惡意檔案靈敏度設定為等級 5。 「下載鑑識」對於未證明的檔案採取的動作為**「忽略」**。 「自動防護」包含下列設定： ■ 對所有檔案進行病毒和安全風險掃描。 ■ 攔截安裝安全風險。 ■ 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 ■ 隔離有安全風險的檔案。記錄無法隔離的檔案。 ■ 檢查所有磁片是否有開機病毒。記錄開機病毒。 ■ 通知電腦使用者病毒和安全風險的相關資訊。
電子郵件的自動防護	已啟用 其他類型的「自動防護」包含下列設定： ■ 掃描所有檔案，其中包括壓縮檔內的檔案。 ■ 清除受病毒感染的檔案。隔離無法清除的檔案。 ■ 隔離有安全風險的檔案。記錄無法隔離的檔案。 ■ 將有關偵測到的病毒和安全風險的訊息傳送給電腦使用者。
SONAR	已啟用 ■ 高風險的啟發式偵測已被隔離 ■ 記錄任何低風險的啟發式偵測 ■ 主動模式已停用 ■ **「偵測到時顯示警示」**已啟用 ■ 系統變更偵測動作設定為「忽略」。 ■ 可疑行為偵測會攔截高風險威脅並忽略低風險威脅。

設定	敘述
管理員定義掃描	排程掃描包含下列預設設定： ■ 每天下午 12:30 執行一次作用中掃描。該掃描為隨機進行。 ■ 掃描所有檔案和資料夾，包括壓縮檔內的檔案。 ■ 掃描記憶體、常見感染位置，以及已知的病毒和安全風險位置。 ■ 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 ■ 隔離有安全風險的檔案。記錄無法隔離的檔案。 ■ 在三天內重試未執行的掃描。 隨選掃描政策提供了下列防護： ■ 掃描所有檔案和資料夾，包括壓縮檔內的檔案。 ■ 掃描記憶體及常見的感染位置。 ■ 清除受病毒感染的檔案。先備份檔案再修復。隔離無法清除的檔案。 ■ 隔離有安全風險的檔案。記錄無法隔離的檔案。

預設的病毒和間諜軟體高安全性政策提供高階安全性，並且包含病毒和間諜軟體防護政策中的許多設定。此政策要求執行更多的掃描。

表 18-9 病毒和間諜軟體防護高安全性政策設定

設定	敘述
檔案系統和電子郵件的自動防護	與病毒和間諜軟體防護平衡政策相同 「自動防護」還會檢查遠端電腦上的檔案。
SONAR	與病毒和間諜軟體防護平衡政策相同，但有下列差異： ■ 攔截任何系統變更事件。
全域設定	Bloodhound 設定為「主動」。 **附註：**「主動」選項可能會產生更多的誤報結果。僅建議進階使用者使用此選項。

預設的病毒和間諜軟體防護高效能政策提供高階效能。該政策包含病毒和間諜軟體防護政策中的許多設定。此政策提供的安全性低一些。

表 18-10 病毒和間諜軟體防護高效能政策設定

設定	敘述
檔案系統的自動防護	與病毒和間諜軟體防護平衡政策相同，但有下列差異： ■ 「下載鑑識」惡意檔案靈敏度設定為等級 1。

設定	敘述
Microsoft Outlook 自動防護 Internet 電子郵件自動防護* Lotus Notes 自動防護* * 僅適用於低於 14.2 RU1 的用戶端版本	已停用
SONAR	與病毒和間諜軟體防護平衡政策相同，但有下列差異： ■ 忽略任何系統變更事件。 ■ 忽略任何行為政策強制執行事件。
管理員定義掃描	與病毒和間諜軟體防護平衡政策相同。

Symantec Endpoint Protection 處理病毒和安全性風險偵測結果的方式

Symantec Endpoint Protection 會使用預設動作處理對病毒和安全性風險的偵測結果。您可以變更部分預設值。

表 18-11 Symantec Endpoint Protection 處理病毒和安全風險偵測結果的方式

偵測結果	說明
病毒	依預設，Symantec Endpoint Protection 用戶端會先嘗試清除感染病毒的檔案。 如果用戶端軟體無法清除檔案，就會執行下列動作： ■ 將檔案移動至受感染電腦上的隔離所 ■ 拒絕對檔案的任何存取動作 ■ 記錄事件
安全風險	依預設，用戶端會將任何受到安全性風險感染的檔案移至受感染電腦上的隔離所。用戶端也會嘗試移除或修復風險的副作用。 如果安全風險無法被隔離和修復，則第二個動作將記錄風險。 依預設，隔離所包含用戶端所有已執行動作的記錄。您可以使電腦回到用戶端嘗試移除和修復作業之前所存在的狀態。

會將 SONAR 執行的偵測視為可疑事件。您可以在 SONAR 組態中，為這些偵測結果架構動作。

請參閱第 425 頁的「管理 SONAR」。

對於 Windows 用戶端和 Linux 用戶端，您可以為 Symantec Endpoint Protection 指派在發現風險時要採取的第一個與第二個動作。您可以為病毒和安全性風險架構不同的動作。您可以針對排程掃描、隨選掃描或自動防護掃描使用不同的動作。

附註：有風險的 Cookie 一律刪除，除非您指定想要記錄 Cookie。您只能針對 Cookie 指定一個動作：**「刪除」**或**「略過 (只記錄)」**。

附註：在 Windows 用戶端上，安全風險偵測類型清單是動態的，會隨著賽門鐵克發現新的類別而有所改變。當新的定義檔到達時，會將新的類別下載到主控台或用戶端電腦。

對於 Mac 用戶端，您可以指定 Symantec Endpoint Protection 是否要修復其發現的受感染檔案。也可以指定 Symantec Endpoint Protection 是否要將無法修復的受感染檔案移至隔離所。您可以針對排程掃描、隨選掃描或自動防護掃描使用不同的動作。

請參閱第 387 頁的「管理 Windows 用戶端的隔離所」。

Symantec Endpoint Protection 如何在 Windows 8 電腦上處理偵測

Symantec Endpoint Protection 會同時保護 Windows 8 樣式使用者介面以及 Windows 8 桌面。不過，與 Windows 8 樣式應用程式和檔案相關的偵測動作運作方式與其他偵測動作的運作方式不同。

在 Windows 8 樣式使用者介面上裝載的應用程式，會在與作業系統中的其他程序隔開的配置區內實作。Symantec Endpoint Protection 不會清除也不會隔離影響 Windows 8 樣式應用程式或檔案的任何偵測。對於牽涉到這些應用程式和檔案的所有偵測，Symantec Endpoint Protection 只會刪除或記錄偵測。

對於與 Windows 8 樣式應用程式和檔案不相關的任何偵測，Symantec Endpoint Protection 可以隔離並修復偵測，並且如同它通常在任何其他 Windows 作業系統上一樣進行操作。

在「病毒和間諜軟體防護」政策中設定動作時，以及執行報告時，您應該注意其差異。

請參閱第 392 頁的「關於出現在 Windows 8 用戶端上的彈出式通知」。

請參閱第 370 頁的「Symantec Endpoint Protection 處理病毒和安全性風險偵測結果的方式」。

設定在 Windows 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。

附註：Windows 設定包含的一些選項不適用於在其他作業系統上執行的用戶端。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。

請參閱第 478 頁的「從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名」。

當您為安全網路中的 Windows 電腦設定排程掃描時，請考慮下列重點：

多個同時掃描會接續執行	如果您在同一台電腦上排程執行多重掃描，且掃描的開始時間都相同，則掃描會接續執行。一個掃描作業完成後，再開始另一個。例如，您可能在電腦上排定三種不同的掃描於下午 1:00 執行。每種掃描會掃描不同的磁碟機。一個掃描掃描磁碟機 C，另一個掃描磁碟機 D，第三個掃描磁碟機 E。在這個範例中，較好的解決方式是，建立一個排程掃描，來掃描磁碟機 C、D 和 E。
錯過的排程掃描可能不會執行	如果您的電腦由於某種原因錯過排程掃描，Symantec Endpoint Protection 預設會嘗試執行掃描，直到啟動為止，或直到指定時間間隔到期為止。如果 Symantec Endpoint Protection 無法在重試間隔內啟動錯過的掃描，就不會再執行該掃描。
排程掃描時間可能偏離	如果最後一次執行的掃描由於掃描持續時間或錯過排程掃描設定而發生在不同的時間，Symantec Endpoint Protection 可能不會使用排程的時間。例如，您可以將每週掃描架構為在每星期日午夜執行且重試間隔為一天。如果電腦錯過掃描，並在星期一上午 6 點時啟動，則掃描會在上午 6 點執行。而下次掃描會在距離星期一上午 6 點的一週後執行，而不是在下一個星期日午夜執行。 如果您並未在星期二早上 6 點 (晚了兩天，且超過重試間隔) 之前重新啟動電腦，Symantec Endpoint Protection 就不會重試掃描。它會等到下一個星期日的午夜再嘗試執行掃描。 不論是何種情況，如果您隨機設定掃描開始時間，您可能會變更掃描的最後一次執行時間。

若需此程序中所用選項的詳細資訊，您可以按下「說明」。

設定在 Windows 電腦上執行的排程掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在**「Windows 設定」**下方，按下**「管理員定義掃描」**。
3. 在**「掃描」**標籤的**「已排程的掃描」**下方，按下**「新增」**。
4. 在**「新增排程掃描」**對話方塊中，按下**「建立新的排程掃描」**。
5. 按下**「確定」**。
6. 在**「新增排程掃描」**對話方塊的**「掃描詳細資料」**標籤中，輸入此排程掃描的名稱和說明。
7. 按下**「作用中掃描」**、**「完整掃描」**或**「自訂掃描」**。
8. 如果您選取**「自訂」**，就可以在**「掃描」**下指定要掃描的資料夾。

9 在「**檔案類型**」下方，按下「**掃描所有檔案**」或「**只掃描選取的副檔名**」。

附註：除非您停用「**進階掃描選項**」下的「**掃描壓縮檔內的檔案**」選項，或為配置區副檔名建立特定例外，否則排程掃描一律會掃描配置區檔案。

10 在「**勾選以下項目以加強掃描**」下，勾選或取消勾選「**記憶體**」、「**常見威染位置**」或「**已知病毒和安全風險位置**」。

11 在「**排程**」標籤的「**掃描排程**」下方，設定應該執行掃描的頻率和時間。

「**錯過掃描排程**」下的重試設定，會根據您選取「**每日**」、「**每週**」或「**每月**」自動變更。

12 在「**錯過掃描排程**」下，您可以停用相應選項，以執行錯過的掃描，也可以變更重試時間間隔。

您也可以指定掃描暫停之前的最長掃描持續時間。您也可以隨機產生掃描開始時間。

13 若要將此掃描儲存為範本，請勾選「**另存複本為排程掃描範本**」。

14 按下「**確定**」。

設定在 Mac 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

請參閱第 407 頁的「為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描」。

附註：Mac 設定並未包含執行於 Windows 之用戶端適用的所有選項。

設定在 Mac 電腦上執行的排程掃描

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Mac 設定**」下方，按下「**管理員定義掃描**」。

3 在「**掃描**」標籤的「**已排程的掃描**」下方，按下「**新增**」。

4 在「**新增排程掃描**」對話方塊中，按下「**建立新的排程掃描**」，然後按下「**確定**」。

5 在「**新增排程掃描**」對話方塊的「**掃描詳細資料**」標籤中，鍵入掃描的名稱和敘述。

6 在「**掃描磁碟機和資料夾**」下，指定要掃描的項目。

7 在「**排程**」標籤的「**掃描排程**」下，設定應該執行掃描的頻率和時間。

8 若要將此掃描儲存為範本，請勾選「**另存複本為排程掃描範本**」。

9 按下「**確定**」。

設定在 Linux 電腦上執行的排程掃描

您可以在設定病毒和間諜軟體防護政策時架構排程掃描。

設定在 Linux 電腦上執行的排程掃描

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在「**Linux 設定**」下，按下「**管理員定義掃描**」。
3. 在「**掃描**」標籤的「**已排程的掃描**」下，按下「**新增**」。
4. 在「**新增排程掃描**」對話方塊中，按下「**新增排程掃描**」。
5. 在「**新增排程掃描**」對話方塊的「**掃描詳細資料**」標籤中，鍵入此排程掃描的名稱和敘述。
6. 在「**資料夾類型**」下，按下「**掃描所有資料夾**」，或指定要掃描的資料夾。
7. 在「**檔案類型**」下，按下「**掃描所有檔案**」或「**只掃描選取的副檔名**」。

附註：除非您停用「**掃描壓縮檔內的檔案**」選項，或為配置區副檔名建立特定例外，否則排程掃描一律會掃描配置區檔案。

---

8. 在「**其他選項**」下，勾選或取消勾選「**掃描安全風險**」。
9. 在「**排程**」標籤的「**掃描排程**」下方，設定應該執行掃描的頻率和時間。

   「**錯過掃描排程**」下的重試設定，會根據您選取「**每日**」、「**每週**」或「**每月**」自動變更。
10. 在「**錯過掃描排程**」下，您可以停用相應選項，以執行錯過的掃描，也可以變更重試時間間隔。
11. 若要將此掃描儲存為範本，請勾選「**另存複本為排程掃描範本**」。
12. 按下「**確定**」。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

在用戶端電腦上執行隨選掃描

您可以從管理主控台遠端為用戶端電腦執行手動或隨選掃描。 您的策略可能包括執行隨選掃描，以防止和處理用戶端電腦上的病毒和間諜軟體攻擊。

依預設，作用中掃描會在您更新定義檔之後自動執行。 您可以將隨選掃描架構為完整掃描或自訂掃描，然後執行該隨選掃描，進行更廣泛的掃描。

隨選掃描的設定很類似排程掃描的設定。

對於 Windows 用戶端電腦，您可以執行作用中掃描、完整掃描或自訂隨選掃描。對於 Mac 和 Linux 用戶端電腦，您只能執行自訂隨選掃描。

自訂掃描會使用病毒和間諜軟體防護政策中為隨選掃描架構的設定。

附註：如果您在執行隨選掃描的用戶端電腦上發出重新啟動的指令，掃描會停止，且用戶端電腦將重新啟動。 掃描並不會重新啟動。

您可以從電腦狀態日誌或從主控台中的**「用戶端」**標籤執行隨選掃描。

您可以從「電腦狀態」日誌，取消所有正在進行的掃描以及放入所選用戶端佇列中的掃描。如果您確認了指令，表格會重新整理，然後您會看見取消的指令新增到指令狀態表格中。

在用戶端電腦上執行隨選掃描

1. 在主控台中，按下**「用戶端」**。
2. 在**「用戶端」**下，在要掃描的群組或用戶端上按下滑鼠右鍵。
3. 執行下列其中一項動作：
   - 按下**「對群組執行指令」>「掃描」**。
   - 按下**「對電腦執行指令」>「掃描」**。

   按下**「更新內容和掃描」**以更新定義檔，然後一步執行掃描。
4. 對於 Windows 用戶端，請選取**「作用中掃描」**、**「完整掃描」**或**「自訂掃描」**，然後按下**「確定」**。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

請參閱第 347 頁的「阻止和處理病毒和間諜軟體對用戶端電腦的攻擊」。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

請參閱第 215 頁的「什麼是可對用戶端電腦執行的指令？」。

調整掃描以改善電腦效能

依據預設，系統會執行病毒和間諜軟體掃描，以將對用戶端電腦資源的影響降至最低。您可以變更某些掃描設定，以進一步最佳化效能。 此處建議的多項工作，對於在虛擬機器 (VM) 上的訪客作業系統中執行 Symantec Endpoint Protection 的環境裡非常有用。

表 18-12 調整掃描以改善 Windows 電腦的電腦效能

工作	敘述
修改排程和隨選掃描的調整和壓縮檔選項	您可以調整排程和隨選掃描的下列選項： ■ 變更調整選項 您可以將掃描調整變更為**「最佳應用程式效能」**。當您利用此設定架構掃描時，掃描可以啟動，但僅會在用戶端電腦閒置時執行。 如果將作用中掃描架構為在收到新定義檔時執行，當使用者正在使用電腦時，掃描可能長達 15 分鐘無法執行。 ■ 變更要掃描壓縮檔的層數 預設層數為 3。您可以將層數變更為 1 或 2，以縮短掃描時間。 請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。
使用可繼續的掃描	對於網路中具有大型磁碟區的電腦，可將排程掃描架構為可繼續的掃描。 掃描持續時間選項會提供執行掃描的指定期間。如果掃描在指定持續時間結束前未完成，則該掃描會在下個排程掃描期間繼續。該掃描會在其停止的地方繼續，直到完成整個磁碟區的掃描為止。通常，您可以使用伺服器上的掃描持續時間選項。 **附註：**如果您懷疑電腦受到感染，請勿使用可繼續的掃描。您應執行會掃描整個電腦的完整掃描。如果掃描可在指定時間間隔之前完成，也不應使用可繼續的掃描。 請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。
調整自動防護設定	您可以針對檔案系統的自動防護掃描，調整一些可能改善用戶端電腦效能的設定。 您可以設定下列選項： ■ **檔案快取** 請確保檔案快取處於啟用狀態 (預設為啟用)。啟用檔案快取時，「自動防護」會記住其掃描的未感染檔案，不會重新掃描。 ■ **網路設定** 如果遠端電腦的自動防護掃描已啟用，則務必啟用**「只在執行檔案時」**。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。
允許所有掃描略過受信任檔案	病毒和間諜軟體掃描包含稱為「智慧型掃描」的選項，該選項會略過受信任的檔案。 預設會啟用「智慧型掃描」選項。您可以變更掃描略過之檔案類型的信任層級： ■ **賽門鐵克和社群信任的檔案** 此層級會略過賽門鐵克和賽門鐵克社群信任的檔案。 ■ **賽門鐵克信任的檔案** 此層級僅會略過賽門鐵克信任的檔案。 請參閱第 410 頁的「修改 Windows 用戶端的全域掃描設定」。

工作	敘述
隨機設定排程掃描	在部署了多部虛擬機器 (VM) 的虛擬環境中，同時進行掃描會造成資源問題。例如，單一伺服器可執行 100 部或更多的 VM。在這些 VM 上同時進行掃描，會耗盡伺服器上的資源。 您可以隨機設定掃描，以限制對伺服器的影響。 請參閱第 409 頁的「隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能」。
在虛擬環境中使用共用智慧型掃描快取	使用共用智慧型掃描快取就無需重新掃描 Symantec Endpoint Protection 已確認未感染病毒的檔案。您可以使用共用智慧型掃描快取在用戶端電腦上進行排程和手動掃描。共用智慧型掃描快取是安裝在伺服器或虛擬環境中的個別應用程式。 請參閱第 587 頁的「啟用網路型共用智慧型掃描快取」。
停用提早啟動防惡意軟體(ELAM)偵測	Symantec Endpoint Protection ELAM 會與 Windows ELAM 搭配，共同提供對惡意啟動驅動程式的防護。 請參閱第 393 頁的「管理提早啟動防惡意軟體 (ELAM) 偵測」。

表 18-13 調整掃描以改善 Mac 電腦的電腦效能

工作	敘述
啟用閒置狀態掃描	適用於在 Mac 電腦上執行之用戶端的排程掃描。 此選項會將排程掃描架構為僅在電腦處於閒置狀態時執行。 請參閱第 407 頁的「為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描」。
修改壓縮檔設定	適用於自動防護和隨選掃描。 您可以啟用或停用該選項，但無法指定要掃描的壓縮檔層數。 請參閱第 403 頁的「自訂 Mac 用戶端的自動防護」。

表 18-14 調整掃描以改善 Linux 電腦的電腦效能

工作	敘述
依資料夾類型掃描	預設為掃描所有資料夾類型。您可以指定任一資料夾：**Root**、**Home**、**Bin**、**Usr**、**Etc** 和 **Opt**。如果您知道某個資料夾是安全的，可以在清單中將其取消勾選。
依檔案類型掃描	預設為掃描所有檔案。如果您知道某種特定副檔名是安全的，可以在清單中將其取消勾選。
掃描壓縮檔內的檔案	您可以在壓縮檔內展開最多三層目錄結構。您可以將層數變更為 1 或 2，以縮短掃描時間。

工作	敘述
掃描安全風險	可讓您選擇是否掃描安全風險。安全風險可透過 LiveUpdate 進行更新。掃描安全風險會讓掃描速度變慢，但會提升安全性。預設為掃描安全風險。若要改善電腦效能，請取消勾選此選項。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

調整掃描以增強對用戶端電腦的防護

預設情況下，Symantec Endpoint Protection 可提供高層級的安全防護。您可以進一步增強這道防護。

在 Windows 電腦上執行的用戶端與在 Mac 和 Linux 電腦上執行的用戶端的設定不同。

附註：如果您增強對用戶端電腦的防護，則可能會影響電腦的效能。

表 18-15　調整掃描以增強對 Windows 電腦的防護

工作	敘述
鎖定掃描設定	預設情況下，某些設定處於鎖定狀態；您也可以鎖定其他設定，這樣使用者就無法變更其電腦上的防護。
修改管理員定義掃描的設定	您應該檢查或修改下列選項： ■ 掃描效能 將掃描調整設定為**「最佳掃描效能」**。不過，此設定可能會影響用戶端電腦的效能。即使在電腦不是處於閒置狀態時，掃描也會執行。 ■ 排程掃描持續時間 預設情況下，排程掃描會執行直到指定的時間間隔到期為止，然後在用戶端電腦閒置時繼續執行。您可以將掃描持續時間設定為**「到掃描完成」**。 ■ 在 12.1.6.x 和舊版用戶端上使用智慧型掃描查詢 智慧型掃描查詢會使用來自雲端的最新定義檔集以及智慧型掃描信譽資料庫中的資訊進行掃描，並做出與從支援的入口網站下載之檔案相關的決策。 在 12.1.6.x 和舊版中，您可以架構智慧型掃描查詢靈敏度，以及啟用或停用智慧型掃描查詢。自 14 版起，您只能啟用或停用 12.1.6.x 用戶端的智慧型掃描查詢。 **警告：**請確定已啟用智慧型掃描查詢。如果停用智慧型掃描查詢，雲端防護將會完全停用。在 14 中，排程掃描和隨選掃描永遠使用雲端來評估入口網站檔案。自動防護也使用雲端來評估入口網站檔案。 請參閱第406頁的「為在Windows電腦上執行的用戶端自訂管理員定義的掃描」。 請參閱第 355 頁的「Windows 用戶端如何從雲端接收定義檔」。

工作	敘述
指定更嚴格的掃描偵測動作	為偵測指定「**隔離**」、「**刪除**」或「**終止**」動作。 **附註：**對安全風險偵測使用「**刪除**」或「**終止**」動作時，請小心。這些動作可能會導致一些合法應用程式喪失功能。 請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。
提高 Bloodhound 防護的層級	Bloodhound 會找到並隔離檔案的邏輯區域以偵測類似病毒的行為。您可以將偵測層級從「**自動**」變更為「**主動**」來增強對電腦的防護。不過，「**主動**」設定可能會產生更多的誤報結果。 請參閱第 410 頁的「修改 Windows 用戶端的全域掃描設定」。
調整自動防護設定	您可以變更下列選項： ■ **檔案快取** 您可以停用檔案快取，以便讓「自動防護」重新掃描無毒檔案。 ■ **網路設定** 預設情況下，網路磁碟機上的檔案只有在處於執行狀態時才會進行掃描。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。

表 18-16　調整掃描以增強對 Mac 和 Linux 電腦的防護

工作	敘述
修改掃描的壓縮檔選項	預設設定是掃描壓縮檔中 3 層深的檔案。若要增強防護，請保留 3 層深，或變更為 3 (若為較深的層級)。 請參閱第 407 頁的「為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描」。 請參閱第 408 頁的「為在 Linux 電腦上執行的用戶端自訂管理員定義掃描」。
鎖定自動防護設定	預設情況下，某些設定處於鎖定狀態；您也可以鎖定其他設定，這樣使用者就無法變更其電腦上的防護。在 Mac 用戶端和 Linux 用戶端上，您可以按下「**啟用自動防護**」，然後按下鎖定圖示來鎖定設定。 請參閱第 403 頁的「自訂 Mac 用戶端的自動防護」。 請參閱第 404 頁的「自訂 Linux 用戶端的自動防護」。
指定更嚴格的掃描偵測動作	針對偵測指定「**隔離**」或「**刪除**」(僅限 Linux) 動作。 **附註：**對安全風險偵測使用「**刪除**」動作時，請小心。這些動作可能會導致一些合法應用程式喪失功能。 請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

管理「下載鑑識」偵測

「自動防護」包含一項名為「下載鑑識」的功能，該功能可檢查使用者試圖透過網頁瀏覽器、文字訊息用戶端以及其他入口網站下載的檔案。

支援的入口網站包含 Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Google Chrome、Windows Live Messenger 和 Yahoo Messenger。

「下載鑑識」根據有關檔案信譽的相關證據，決定下載的檔案是否存在風險。 只有 Windows 電腦上執行的用戶端支援「下載鑑識」。

附註：如果您針對用戶端電腦上的電子郵件安裝「自動防護」，則「自動防護」也會掃描使用者以電子郵件附件形式收到的檔案。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

表 18-17 管理「下載鑑識」偵測

工作	敘述
瞭解「下載鑑識」如何使用信譽資料做出關於檔案的決策	「下載鑑識」只會使用信譽資訊進行有關下載檔案的決策。 它不會使用特徵或啟發式技術進行決策。 如果「下載鑑識」允許檔案，則「自動防護」或 SONAR 將在使用者開啟或執行該檔案時掃描該檔案。 請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。
檢視下載風險分佈報告以檢視「下載鑑識」偵測	您可以使用下載風險分佈報告，檢視「下載鑑識」在您的用戶端電腦上偵測到的檔案。 您可以依照 URL、Web 網域或應用程式排序報告。 您也可以查看使用者是否已選擇允許某個偵測到的檔案。 **附註：**「下載鑑識」偵測的風險詳細資料只顯示嘗試下載的第一個入口網站應用程式。 例如，使用者可以使用 Internet Explorer 嘗試下載「下載鑑識」偵測的檔案。 如果使用者接著使用 Firefox 嘗試下載該檔案，則風險詳細資料會將 Internet Explorer 顯示為入口網站。 顯示在報告中的使用者允許檔案可能表示偵測誤報。 您也可以指定在使用者允許進行任何新下載時，接收電子郵件通知。 請參閱第 577 頁的「設定管理員通知」。 使用者可以透過回應顯示的偵測通知允許下載檔案。 Symantec Endpoint Protection Manager 會產生並透過電子郵件傳送每週報告，其中包括提供給管理員的報告。 您必須在安裝過程中為管理員指定電子郵件地址，或在管理員屬性中架構。 您也可以從主控台的**「報告」**標籤中產生報告。 請參閱第 559 頁的「執行和自訂快速報告」。

工作	敘述
為特定檔案或 Web 網域建立例外	您可以為使用者下載的應用程式建立例外。 您也可以為您認為受信任的特定 Web 網域建立例外。 請參閱第 479 頁的「指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式」。 請參閱第 480 頁的「從 Windows 用戶端上的掃描中排除信任的 Web 網域」。 **附註：**如果用戶端電腦使用帶驗證功能的代理，您必須為 Symantec URL 指定信任的 Web 網域例外。透過使用例外，可以讓用戶端電腦與 Symantec Insight 及其他重要的賽門鐵克網站進行通訊。 如需建議例外的相關資訊，請參閱下列文章： ■ 如何測試 Insight 與賽門鐵克授權伺服器的連線 ■ 允許 Symantec Endpoint Protection 連線到賽門鐵克信譽與授權伺服器所需排除的代理伺服器 依據預設，「下載鑑識」不會檢查使用者從信任的 Internet 或內部網路網站下載的任何檔案。您可以在 Windows **「控制台」>「網際網路選項」>「安全性」**標籤上，架構信任的網站和信任的本機內部網路網站。 如果已啟用**「自動信任從內部網路網站下載的任何檔案」**選項，則 Symantec Endpoint Protection 會允許使用者從任何清單中的網站下載的任何檔案。 Symantec Endpoint Protection 會在使用者登入時及每四個小時檢查「網際網路選項」信任網站清單的更新。 **附註：**「下載鑑識」只辨識明確架構的信任網站。 允許使用萬用字元，但不支援無法路由的 IP 位址範圍。例如，「下載鑑識」不會將 10.*.*.* 識別為信任網站。此外，「下載鑑識」不支援由**「網際網路選項」>「安全性」>「自動偵測內部網路」**選項搜尋到的網站。
確定已啟用智慧型掃描查詢	「下載鑑識」需要使用來自 Symantec Insight 的信譽資料進行關於檔案的決策。如果您停用「智慧型掃描查詢」，則「下載鑑識」會執行，但只會偵測信譽最差的檔案。 依據預設，「智慧型掃描查詢」已啟用。 請參閱第 411 頁的「自訂下載鑑識設定」。

工作	敘述
自訂下載鑑識設定	您可能因以下原因需要自訂「下載鑑識」設定： ■ 增加或減少「下載鑑識」偵測的數目。 您可以調整惡意檔案靈敏度滑動軸，以增加或減少偵測數目。 敏感程度愈低，「下載鑑識」偵測到的惡意檔案愈少，偵測到的未證明的檔案愈多。 誤報偵測也愈少。 敏感程度愈高，「下載鑑識」偵測到的惡意檔案愈多，偵測到的未證明的檔案愈少。 誤報偵測也愈多。 ■ 變更偵測到惡意檔案或未證明的檔案時採取的動作。 您可以變更「下載鑑識」處理惡意檔案或未證明檔案的方式。 指定的動作不僅會影響偵測結果，也會影響使用者是否可與偵測結果進行互動。 例如，您可將針對未證明檔案採取的動作變更為**「忽略」**。 然後，「下載鑑識」會一律允許未證明的檔案，而不會向使用者發出警示。 ■ 針對「下載鑑識」偵測結果向使用者發出警示。 當啟用通知時，惡意檔案靈敏度的設定會影響使用者收到的通知數量。 如果您提高靈敏度，則會增加使用者通知的數目，因為偵測的總數會增加。 您可以關閉通知，讓使用者在「下載鑑識」進行偵測時無法進行動作。 如果您將通知保持啟用狀態，則可將針對未證明檔案進行的動作設為**「忽略」**，一律允許這些偵測，且不通知使用者。 不論通知設定為何，當「下載鑑識」偵測到未證明的檔案且動作為**「提示」**時，使用者就可以允許或攔截檔案。 如果使用者允許該檔案，則該檔案會自動執行。 當啟用通知且「下載鑑識」隔離某個檔案時，使用者可以復原隔離動作並允許使用檔案。 **附註：**如果使用者允許使用隔離的檔案，則此檔案不會自動執行。 使用者可以從 Temporary Internet Files 資料夾執行此檔案。通常，資料夾位置為下列其中之一： ■ Windows 8 及更新版本：*Drive*:\Users*username*\AppData\Local\Microsoft\Windows\INetCache ■ Windows Vista/7：*Drive*:\Users*username*\AppData\Local\Microsoft\Windows\Temporary Internet Files ■ Windows XP (針對舊版 12.1.x 用戶端)：*Drive*:\Documents and Settings*username*\Local Settings\Temporary Internet Files 請參閱第 411 頁的「自訂下載鑑識設定」。
允許用戶端將有關信譽偵測的資訊傳送給賽門鐵克	依據預設，用戶端會將有關信譽偵測的資訊傳送給賽門鐵克。 賽門鐵克建議您為信譽偵測啟用傳送功能。 此資訊有助於賽門鐵克處理威脅。 請參閱第 420 頁的「管理用戶端傳送給賽門鐵克的匿名或非匿名資料」。

Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策

賽門鐵克會從其全球數百萬使用者的社群及 Global Intelligence Network 收集有關檔案的資訊。收集的資訊可透過 Symantec Insight 供雲端中的賽門鐵克產品使用。Symantec Insight 可提供檔案信譽資料庫以及最新的病毒和間諜軟體定義檔。

賽門鐵克產品會利用 Insight 保護用戶端電腦，使其免受新威脅、目標威脅和變種威脅的危害。該資料有時也稱為雲端資料，因為它並非置於用戶端電腦。Symantec Endpoint Protection 必須要求或查詢 Insight 以取得資訊。查詢稱為信譽查詢、雲端查詢或智慧型掃描查詢。

Insight 信譽分級

Symantec Insight 可判斷每個檔案的風險等級或安全性分級。分級亦稱為檔案的信譽。

Insight 可透過檢查檔案的下列特性及其內容，判斷檔案的安全性等級：

- 檔案來源
- 檔案新舊程度
- 檔案在社群中的常用程度
- 其他安全性衡量標準，例如檔案可能與惡意軟體關聯的程度

智慧型掃描查詢

Symantec Endpoint Protection 中的掃描功能會利用智慧型掃描來進行檔案和應用程式的相關決策。 病毒和間諜軟體防護包含一項名為「下載智慧型掃描」的功能。 下載鑑識需要信譽資訊來進行偵測。SONAR 也會使用信譽資訊進行偵測。

您可以在**「用戶端」**標籤上變更智慧型掃描查詢設定。移至**「政策」>「設定」>「外部通訊」>「用戶端傳送資訊」**。

從 14 開始，在標準和內嵌式/VDI 用戶端上，智慧型掃描查詢選項還會允許自動防護與排程掃描和手動掃描查詢檔案信譽資訊以及雲端中的定義檔。賽門鐵克建議您將此選項保持啟用。

警告：下載鑑識、SONAR 以及病毒和間諜軟體掃描會使用智慧型掃描查詢來偵測威脅。賽門鐵克建議您始終允許智慧型掃描查詢。停用查詢會停用「下載鑑識」，並影響SONAR啟發式掃描以及病毒和間諜軟體掃描的功能。

請參閱第 682 頁的「針對 Windows 用戶端 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能相依性」。

檔案信譽傳送

依據預設，用戶端電腦會將信譽偵測的相關資訊傳送到賽門鐵克安全機制應變中心進行分析。此資訊有助於調整智慧型掃描的信譽資料庫以及雲端中的最新定義檔。傳送資訊的用戶端愈多，信譽資料庫就會變得愈有用。

賽門鐵克建議您持續為信譽偵測啟用用戶端傳送資訊功能。

請參閱第 380 頁的「管理「下載鑑識」偵測」。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

請參閱第 396 頁的「架構站台使用私用 Insight 伺服器進行信譽查詢」。

Symantec Endpoint Protection 如何使用進階機器學習？

進階機器學習如何運作？

進階機器學習 (AML) 引擎會透過學習程序判斷檔案是良好還是無效檔案。賽門鐵克安全機制應變中心會訓練該引擎來辨識惡意屬性，以及定義 AML 引擎用來進行偵測的規則。賽門鐵克會在實驗室環境中使用下列程序訓練和測試 AML 引擎：

- LiveUpdate 會下載 AML 模型至用戶端，並執行數日。
- AML 引擎會學習用戶端執行的應用程式，並使用用戶端的遙測資料侵入。每個用戶端電腦均屬於會將模型的相關資訊傳回賽門鐵克的 Global Intelligence Network 的一部分。
- 賽門鐵克會根據賽門鐵克從用戶端的遙測資料所探索的資訊來調整 AML 模型。
- 賽門鐵克會修改 AML 模型來攔截侵入通常攻擊的應用程式。

AML 屬於靜態資料掃描程式 (SDS) 引擎的一部分。SDS 引擎包括模擬器、Intelligent Threat Cloud Service (ITCS) 和 CoreDef-3 定義檔引擎。

Symantec Endpoint Protection 在下載鑑識、SONAR 以及病毒和間諜軟體掃描中使用進階機器學習，這些均使用智慧型掃描查詢來偵測威脅。

AML 如何與雲端搭配運作？

賽門鐵克利用 Intelligent Threat Cloud Service (ITCS) 來確認 AML 在用戶端電腦上進行的偵測正確。有時在 AML 向 ITCS 查詢之後，可能會撤銷原判。雖然 AML 引擎不需要 Symantec Insight，但此回饋會使賽門鐵克能夠訓練 AML 演算法，以減少誤報和增加檢出。當電腦在線上時，Symantec Endpoint Protection 可以阻止平均 99% 的威脅。

請參閱第 355 頁的「Windows 用戶端如何從雲端接收定義檔」。

請參閱第 386 頁的「Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？」。

如何架構 AML？

您無法架構進階機器學習。依據預設，LiveUpdate 會下載 AML 定義檔。不過，您需要確定已啟用以下技術。

表 18-18 確保 AML 保護用戶端電腦的步驟

工作	敘述
步驟 1：確定已啟用雲端查詢可用性	AML 對 Symantec Insight 進行的查詢稱為信譽查詢、雲端查詢或智慧型掃描查詢。如果智慧型掃描查詢已啟用，針對 SONAR 和病毒與間諜軟體掃描的 AML 偵測會具有較少的誤報。 若要驗證已啟用智慧型掃描查詢，請參閱： 請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。 此外，請確定已啟用用戶端傳送資訊。此資訊有助於賽門鐵克衡量和改善偵測技術的有效性。 請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。
步驟 2：確定已啟用 Bloodhound 偵測	將 Bloodhound 偵測層級設定為自動或主動。 請參閱第 410 頁的「修改 Windows 用戶端的全域掃描設定」。 當 AML 引擎遇到某些高度風險檔案時，用戶端會自動進入更主動的掃描。 進入主動掃描模式時： ■ 隨即會重新啟動掃描。 ■ 用戶端上會出現以下通知： `Running an aggressive scan that uses Insight lookups to clean your computer.` 在主動模式中，您可能需要進一步管理誤報。
步驟 3：確定 LiveUpdate 下載高密集度定義檔 (14.0.1) (選擇性)	LiveUpdate 一律會下載 AML 內容。 自 14.0.1 起，LiveUpdate 會下載更主動的定義檔集，可搭配您自雲端取得的低頻寬政策使用。您可以停用 AML 內容，使其不再透過 LiveUpdate 下載。 從 LiveUpdate 至 Symantec Endpoint Protection Manager： 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。 從 Symantec Endpoint Protection Manager 至 Windows 用戶端： 請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。 請參閱第 163 頁的「關於 LiveUpdate 下載的內容類型」。

工作	敘述
步驟 4：處理誤報	使用「例外」政策管理誤報。 請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。 請參閱第 427 頁的「處理和避免 SONAR 偵測誤報」。 當 Symantec Endpoint Protection 刪除您認為是安全的檔案時的最佳實務準則

疑難排解進階機器學習

進階機器學習偵測的日誌和報告與其他 SDS 引擎相同。若要查看具有最新威脅的報告，請針對**「網路中偵測到的新風險」**執行風險報告。

自 14.0.1 起，您可以針對 AML 偵測執行排程報告。在**「報告」**頁面上，按下**「排程報告」**>**「新增」**>**「電腦狀態」**>**「進階機器學習 (靜態) 內容派送」**。Symantec Endpoint Protection Manager 網域必須在雲端主控台中註冊，才能顯示此報告。

請參閱第 561 頁的「如何執行排程報告」。

請參閱第 563 頁的「檢視日誌」。

Symantec Endpoint Protection 中的模擬器如何偵測和清理惡意軟體？

Symantec Endpoint Protection 14 推出了功能強大的新模擬器，來防範來自自訂封包程式惡意軟體的攻擊。針對自動防護和病毒掃描，這個模擬器可將掃描效能和有效性較舊版至少提升 10%。此防躲避技術可解決包裝的惡意軟體迷惑技術，並能偵測自訂封包程式中隱藏的惡意軟體。

什麼是自訂封包程式？

許多惡意軟體程式利用「封包程式」，或是用來壓縮和加密檔案進行傳輸的軟體程式。然後，當這些檔案到達使用者的電腦時，即會在記憶體中執行。

雖然封包程式本身並非惡意軟體，但攻擊者會使用它們來隱藏惡意軟體並混淆程式碼的實際意圖。一旦將惡意軟體解除封包，它會執行並啟動其惡意酬載，經常會略過防火牆、閘道和惡意軟體防護。攻擊者已從使用商業封包程式 (例如 UPX、PECompact、ASProtect 和 Themida) 轉變為建立自訂封包程式。自訂封包程式使用專屬的演算法來略過標準的偵測技術。

許多新出現的自訂封包程式為變種。它們使用防偵測策略，其中程式碼本身經常變更，但惡意軟體的目的和功能仍保持不變。自訂封包程式也使用聰明的方式來將程式碼插入目標程序並變更其執行流程，經常能擺脫解除封包程式常式。它們當中的一部分為運算密集型，會呼叫特殊 API 使得難以解除封裝。

自訂封包程式變得愈來愈老練，可隱藏攻擊，發現時多半為時已晚。

Symantec Endpoint Protection 模擬器如何防範自訂封包程式?

Symantec Endpoint Protection 中的高速模擬器會欺騙惡意軟體，讓其認為它是在一般電腦上執行。模擬器實則會在用戶端電腦上的輕量虛擬沙箱中將自訂封裝檔案解除封裝並觸發。然後，惡意軟體會將其酬載開啟至滿載，造成威脅在遏制的環境中顯現。包含了防毒引擎和啟發式引擎的靜態資料掃描程式會對該酬載採取行動。沙箱是暫時的，會在處理完威脅之後消失。

模擬器需要模擬作業系統、API 和處理器指示的複雜技術。它會同時管理虛擬記憶體並執行各種啟發式和偵測技術來檢查酬載。對乾淨的檔案平均需要 3.5 毫秒，而對惡意軟體則需要 300 毫秒，大約是用戶端使用者在桌面上按下檔案所需的相同時間。模擬器可以快速偵測威脅，對效能和產能的影響程度最低，因此用戶端使用者不會被中斷。此外，模擬器會使用最低的磁碟空間量和虛擬環境中最多 16 MB 的記憶體。

模擬器可以與其他防護技術搭配使用，其中包括進階機器學習、記憶體攻擊緩和、行為監控和信譽分析。有時會有多個引擎加入，協同回應以預防、偵測和矯正攻擊。

模擬器不使用 Internet。不過，根據模擬器從自訂封包程式解壓縮的惡意軟體，靜態資料掃描程式內的引擎可能需要 Internet。

請參閱第 384 頁的「Symantec Endpoint Protection 如何使用進階機器學習？」。

如何架構模擬器？

模擬器內建在 Symantec Endpoint Protection 軟體中，因此您不需要架構它。賽門鐵克會定期新增或變更模擬器內容以取得新威脅，並每季發行內容更新至模擬器引擎。依據預設，LiveUpdate 會自動下載此內容與病毒和間諜軟體定義檔。

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

Symantec Endpoint Protection Manager 不會包括模擬器所進行偵測的個別日誌。您可以改為在風險日誌和掃描日誌中尋找任何偵測。

請參閱第 563 頁的「檢視日誌」。

管理 Windows 用戶端的隔離所

當病毒和間諜軟體掃描或 SONAR 掃描偵測到威脅時，Symantec Endpoint Protection 會將受感染檔案放置在用戶端電腦的本機隔離所。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

表 18-19　　管理隔離所

工作	敘述
監控隔離所中的檔案	您應該定期檢查隔離的檔案，以避免累積大量檔案。當網路上出現新病毒疫情 (爆發) 時，檢查隔離的檔案。 請將發生不明感染的檔案保留在隔離所。當用戶端收到新的定義檔時，它會重新掃描隔離所中的項目，且可能會刪除或修復檔案。

工作	敘述
刪除隔離所中的檔案	如果有保留檔案備份，或已從受信任的來源取得檔案複本，則可以刪除隔離的檔案。 您可以在受感染的電腦上直接刪除隔離的檔案，或使用 Symantec Endpoint Protection 主控台中的「風險日誌」進行刪除。 請參閱第 390 頁的「使用風險日誌刪除用戶端電腦中隔離的檔案」。
架構當新的定義檔到達時，Symantec Endpoint Protection 應重新掃描隔離所中項目的方式	依據預設，當新的定義檔到達時，Symantec Endpoint Protection 會重新掃描隔離所中的項目。它會自動以無訊息模式修復與還原項目。您通常應保留預設的設定，但可以根據需要變更重新掃描動作。 請參閱第 389 頁的「架構 Windows 用戶端處理隔離項目的方式」。
管理隔離檔案的儲存	依據預設，隔離所會將備份、修復和隔離的檔案儲存在預設資料夾中。它會在 30 天後自動刪除檔案。 您可以使用下列方式管理隔離項目儲存： ■ 指定用以儲存隔離檔案的本機資料夾。 您可以使用預設資料夾或選擇的資料夾。 請參閱第 388 頁的「指定本機隔離所資料夾」。 ■ 請指定自動刪除檔案的時間。 隔離所會在指定的天數後自動刪除檔案。您也可以架構隔離所在儲存檔案的資料夾達到指定大小時刪除檔案。您可以分別為修復、備份和隔離的檔案架構設定。 請參閱第 389 頁的「指定自動刪除修復、備份和隔離檔案的時間」。
收集隔離項目的相關資訊	您可以架構用戶端，將受感染或可疑檔案和相關副作用轉送至 Central Quarantine Server，以進行進一步的分析。您可以使用此資訊，調整其偵測和修復。 您可以將隔離所中以特徵為基礎的偵測，從本機隔離所轉送至現有 Central Quarantine Server。本機隔離所中的信譽偵測無法傳送至 Central Quarantine Server。 請參閱第 389 頁的「架構 Windows 用戶端處理隔離項目的方式」。

指定本機隔離所資料夾

如果您不想使用預設的隔離所資料夾儲存用戶端電腦上的隔離檔案，則可以另外指定一個本機資料夾。您可以使用路徑擴展，方法是在輸入路徑時使用百分比符號。例如，您可以輸入 %COMMON_APPDATA%。如此便不允許使用相對路徑。

請參閱第 387 頁的「管理 Windows 用戶端的隔離所」。

指定本機隔離所資料夾

1 在「**病毒和間諜軟體防護政策**」頁面的「**Windows 設定**」下，按下「**隔離**」。

2 在「**一般**」標籤上的「**本機隔離所選項**」下方，按下「**指定隔離所資料夾**」。

3 在文字方塊中，輸入用戶端電腦上的本機資料夾名稱。您可以使用路徑擴展，方法是在輸入路徑時使用百分比符號。例如，您可以輸入 %COMMON_APPDATA%，但不允許相對路徑。

4 按下**「確定」**。

指定自動刪除修復、備份和隔離檔案的時間

Symantec Endpoint Protection 會自動刪除超過指定天數的修復、備份和隔離的檔案。您也可以架構隔離所，使其在儲存檔案的資料夾達到特定大小時刪除檔案。

您可以使用其中一個設定，也可以同時使用兩者。如果您兩種類型的限制都設定了，則會先清除所有比您設定的時間舊的檔案。如果資料夾的大小仍超過您所設定的大小限制，則會從最舊的檔案逐一進行刪除。系統會持續刪除檔案，直到資料夾大小低於指定限制為止。

請參閱第 387 頁的「管理 Windows 用戶端的隔離所」。

指定自動刪除修復、備份和隔離檔案的時間

1 在主控台中，開啟「病毒和間諜軟體防護」政策，然後在**「Windows 設定」**下方，按下**「隔離」**。

2 在**「清理」**標籤上，勾選或取消勾選啟用或停用它們的選項，然後架構時間間隔和大小上限。

3 按下**「確定」**。

架構 Windows 用戶端處理隔離項目的方式

您可以架構新定義檔到達 Symantec Endpoint Protection 用戶端電腦時應採取的動作。根據預設，用戶端會重新掃描隔離所的項目，並自動以無訊息方式修復和還原項目。如果您已在隔離所中建立某個檔案或應用程式的例外，則 Symantec Endpoint Protection 會在新的定義檔到達後還原該檔案。

此外，您可以架構用戶端將隔離項目自動傳送至中央隔離所伺服器。您可以使用此中央儲存庫來新增在您的環境中偵測到的威脅範本。您可以使用該資訊來設定「紅隊」攻擊以加強您的安全性。

附註：14 版不包含隔離所伺服器及隔離所主控台。您可以透過舊版中的安裝光碟安裝這些工具。

請參閱第 387 頁的「管理 Windows 用戶端的隔離所」。

請參閱第 348 頁的「移除病毒和安全風險」。

架構 Windows 用戶端處理隔離項目的方式

1. 在主控台中，開啟「病毒和間諜軟體防護」政策，按下**「隔離」**。
2. 在**「一般」**標籤的**「當新的病毒定義檔到達時」**下方，按下以下其中一個選項。
3. 若要將隔離的項目傳送至中央隔離所伺服器，請勾選**「允許用戶端電腦自動傳送已隔離的項目至隔離所伺服器」**，並指定伺服器名稱和埠號。
4. 按下**「確定」**。

使用風險日誌刪除用戶端電腦中隔離的檔案

您可以使用 Symantec Endpoint Protection Manager 主控台中的「風險日誌」刪除用戶端電腦中隔離的檔案。您需要從日誌中，為想要刪除的任何隔離檔案執行**「從隔離所刪除」**指令。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

如果 Symantec Endpoint Protection 偵測到壓縮檔案中的風險，壓縮檔案會整個遭到隔離。然而，「風險日誌」包含壓縮檔案中每個檔案的單獨項目。為成功刪除壓縮檔中的所有風險，您必須選取壓縮檔中的所有檔案。

使用風險日誌刪除用戶端電腦上隔離所內的檔案

1. 按下**「監視器」**。
2. 在**「日誌」**標籤的**「日誌類型」**清單方塊中，選取**「風險」**日誌，然後按下**「檢視日誌」**。
3. 執行下列其中一項動作：
   - 在日誌中選取一個檔案被隔離的項目。
   - 選取壓縮檔案中所有的檔案項目。
     您必須讓壓縮檔案中的所有項目顯示於日誌檢視中。您可以使用**「其他設定」**下的**「限制」**選項，增加檢視的項目數。
4. 從**「動作」**清單方塊，選取**「從隔離所刪除」**。
5. 按下**「開始」**。
6. 在顯示的對話方塊中，按下**「刪除」**。
7. 在顯示的確認對話方塊中，按下**「確定」**。

管理顯示在用戶端電腦上的病毒和間諜軟體通知

您可以決定是否要在用戶端電腦上顯示病毒和間諜軟體事件的通知。您可以自訂有關偵測結果的訊息。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

表 18-20 管理顯示在用戶端電腦上的病毒和間諜軟體通知的工作

工作	敘述
自訂掃描偵測訊息	對於 Windows 和 Linux 用戶端電腦，您可以為以下掃描類型架構偵測訊息： ■ 所有自動防護類型 ■ 排程掃描和隨選掃描 對於排程掃描，您可以為每個掃描架構個別的訊息。 **附註：**如果某個程序持續將相同的安全性風險下載到用戶端電腦，則經過三次偵測之後，自動防護會自動停止傳送通知。自動防護也會停止記錄事件。不過，在某些情況下，自動防護不會停止傳送通知和記錄事件。當偵測對應的動作為**「略過(只記錄)」**時，自動防護會繼續傳送通知和記錄事件。 對於 Mac 用戶端電腦，您可以架構套用至所有排程掃描、隨選掃描和自動防護偵測的偵測訊息。這些通知訊息會出現在 macOS 通知中心。無法為 Mac 自訂訊息。 請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。 請參閱第 407 頁的「為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描」。 請參閱第 408 頁的「為在 Linux 電腦上執行的用戶端自訂管理員定義掃描」。
變更關於下載鑑識偵測的使用者通知設定	僅適用於 Windows 用戶端電腦。 您可以變更使用者收到的「下載鑑識」偵測相關通知。 請參閱第 380 頁的「管理「下載鑑識」偵測」。
變更關於 SONAR 偵測的使用者通知設定	僅適用於 Windows 用戶端電腦。 您可以變更使用者收到的 SONAR 偵測相關通知。 請參閱第 425 頁的「管理 SONAR」。
選擇是否顯示自動防護結果對話方塊	僅適用於 Windows 用戶端電腦。 僅適用於檔案系統的自動防護。 請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。
設定自動防護電子郵件通知	僅適用於 Windows 用戶端電腦。 當自動防護電子郵件掃描發現風險時，自動防護可傳送電子郵件通知，向電子郵件寄件者及您指定的任何其他電子郵件地址發出警示。您也可以在電子郵件中插入警告。 對於 Internet 電子郵件自動防護，您也可以指定當自動防護掃描電子郵件時，顯示有關掃描進度的通知。「Internet 電子郵件自動防護」僅適用於低於 14.2 RU1 的用戶端版本。 請參閱第 405 頁的「為 Windows 電腦上的電子郵件掃描自訂自動防護」。

工作	敘述
允許使用者查看掃描進度及啟動或停止掃描	僅適用於 Windows 用戶端電腦。 您可以架構是否顯示掃描進度對話方塊。您可以架構是否允許使用者暫停或延遲掃描。 如果您允許使用者檢視掃描進度，用戶端使用者介面的主頁上會顯示掃描進度對話方塊連結。另外也會顯示重新排程下一個排程掃描的連結。 請參閱第414頁的「允許使用者在Windows電腦上檢視掃描進度並與掃描互動」。
架構警告、錯誤和提示	僅適用於 Windows 用戶端電腦。 您可以啟用或停用幾種顯示在用戶端電腦上有關病毒和間諜軟體防護事件的警示類型。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。
啟用或停用 Windows 8 樣式使用者介面上的彈出式通知	適用於 Windows 8 上執行的用戶端。 您可以啟用或停用出現在 Windows 8 樣式使用者介面中，用於偵測和其他重要事件的彈出式通知。 請參閱第 393 頁的「啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知」。

關於出現在 Windows 8 用戶端上的彈出式通知

在 Windows 8 電腦上，用於惡意軟體偵測及其他重要 Symantec Endpoint Protection 事件的彈出式通知會出現在 Windows 8 樣式使用者介面和 Windows 8 桌面上。不論使用者目前檢視的是哪一個介面，通知都會警示使用者 Windows 8 樣式使用者介面或 Windows 8 桌面上發生的事件。

您可以在用戶端電腦上啟用或停用彈出式通知。

附註：Windows 8 組態也包含顯示或隱藏通知的設定。只有在將 Windows 8 架構為顯示 Symantec Endpoint Protection 彈出式通知時，才會出現這些通知。在 Windows 8 樣式使用者介面上，**「設定」**窗格或**「變更電腦設定」**選項可讓您顯示或隱藏應用程式通知。如需詳細資訊，請參閱 Windows 8 使用者說明文件。

如果使用者在 Windows 8 樣式使用者介面上按下某個通知，則 Windows 8 桌面便會出現。如果使用者按下 Windows 8 桌面上的通知，通知將會消失。針對惡意軟體或安全風險偵測，使用者可以在 Windows 8 桌面上，於**「偵測結果」**對話方塊中檢視偵測相關資訊。

當 Symantec Endpoint Protection 通知 Windows 8 偵測到影響 Windows 8 樣式應用程式的惡意軟體或安全風險時，在應用程式磚上會出現一個警示圖示。當使用者按下這個磚時，Windows 應用程式商店便會出現，讓使用者可以重新下載該應用程式。

請參閱第 393 頁的「啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知」。

請參閱第 371 頁的「Symantec Endpoint Protection 如何在 Windows 8 電腦上處理偵測」。

啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 彈出式通知

依據預設，彈出式通知會出現在 Windows 8 樣式使用者介面與 Windows 8 桌面上，用於惡意軟體偵測及其他重要 Symantec Endpoint Protection 事件。

使用者可以檢視 Windows 桌面，以查看產生通知之事件的詳細資料。使用者可能需要採取動作，例如重新下載應用程式。不過，在某些情況下，您可能想要向使用者隱藏這些彈出式通知。您可以在 Symantec Endpoint Protection 架構中啟用或停用此類型的通知。

附註：Windows 8 架構也包含顯示或隱藏通知的設定。只有在將 Windows 8 架構為顯示 Symantec Endpoint Protection 通知時，才會出現這些通知。在 Windows 8 樣式使用者介面上，**「設定」**窗格或**「變更電腦設定」**選項可讓您顯示或隱藏應用程式通知。如需詳細資訊，請參閱 Windows 8 使用者說明文件。

啟用或停用 Windows 8 用戶端上顯示的 Symantec Endpoint Protection 通知

1. 在主控台的**「用戶端」**標籤中，於**「政策」**標籤的**「位置限定的設定」**下方，按下**「用戶端使用者介面控制設定」**旁的**「伺服器控制」**。
2. 在**「伺服器控制」**旁，按下**「自訂」**。
3. 在**「用戶端使用者介面設定」**對話方塊中，勾選或取消勾選**「一般」**下的**「啟用 Windows Toast 通知」**。
4. 按下**「確定」**。

請參閱第 392 頁的「關於出現在 Windows 8 用戶端上的彈出式通知」。

管理提早啟動防惡意軟體 (ELAM) 偵測

提早啟動防惡意軟體 (ELAM) 會在電腦啟動時，以及第三方驅動程式初始化之前，為您網路中的電腦提供防護。可以當作驅動程式或 Rootkit 載入的惡意軟體，可能會在作業系統完全載入且 Symantec Endpoint Protection 啟動前攻擊系統。Rootkit 有時候可能會躲避病毒和間諜軟體掃描。提早啟動防惡意軟體會在系統啟動時偵測這些 Rootkit 和惡意驅動程式。

附註：僅 Microsoft Windows 8 或更新版本和 Windows Server 2012 或更新版本支援 ELAM。

Symantec Endpoint Protection 提供的 ELAM 驅動程式可搭配 Windows ELAM 驅動程式使用，以提供防護。您必須啟用 Windows ELAM 驅動程式，Symantec ELAM 驅動程式才會有作用。

您可以使用 Windows 群組原則編輯器檢視及修改 Windows ELAM 設定。如需詳細資訊，請參閱 Windows 說明文件。

表 18-21 管理 ELAM 偵測

工作	敘述
檢視用戶端電腦的 ELAM 狀態	您可以在「電腦狀態」日誌中檢視 Symantec Endpoint Protection ELAM 是否已啟用。 請參閱第 563 頁的「檢視日誌」。
檢視 ELAM 偵測	您可以在「風險日誌」中檢視提早啟動防惡意軟體偵測。 當 Symantec Endpoint Protection ELAM 架構為報告偵測到 Windows 未知的惡意驅動程式或惡意的重要驅動程式時，Symantec Endpoint Protection 會將偵測結果記錄為**「只記錄」**。依預設，Windows ELAM 允許載入未知的驅動程式。 請參閱第 563 頁的「檢視日誌」。
啟用或停用 ELAM	您可能需要停用 Symantec Endpoint Protection ELAM，以協助改善電腦效能。 請參閱第 395 頁的「調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項」。 請參閱第 375 頁的「調整掃描以改善電腦效能」。
如果您得到誤報，請調整 ELAM 偵測設定	Symantec Endpoint Protection ELAM 設定提供的選項可將惡意驅動程式或惡意的重要驅動程式視為不明。惡意的重要驅動程式就是被識別為惡意軟體但卻是啟動電腦所必需的驅動程式。如果得到可攔截重要驅動程式的誤報偵測，您可以選取覆寫選項。如果您攔截重要驅動程式，您可能會使用戶端電腦無法啟動。 **附註：**ELAM 不支援個別驅動程式的特定例外。覆寫選項可全域套用到 ELAM 偵測。 請參閱第 395 頁的「調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項」。

工作	敘述
對 Symantec Endpoint Protection 無法矯正的 ELAM 偵測執行 Power Eraser	在某些情況下，ELAM 偵測需要 Power Eraser。在這類情況下，日誌中會顯示一則訊息，建議您執行 Power Eraser。您可以從主控台執行 Power Eraser。Power Eraser 也是賽門鐵克說明工具的一部分。您應在 Rootkit 模式下執行 Power Eraser。 請參閱第 678 頁的「從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析」。 請參閱第 656 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。

調整 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 選項

Symantec Endpoint Protection 提供的 ELAM 驅動程式會搭配 Microsoft ELAM 驅動程式使用，以便在電腦啟動時，為您網路中的電腦提供防護。自 Microsoft Windows 8 和 Windows Server 2012 起，支援這些設定。

Symantec Endpoint Protection ELAM 驅動程式是一種特殊類型的驅動程式，該驅動程式會先初始化並檢測其他啟動驅動程式是否包含惡意程式碼。當驅動程式偵測到啟動驅動程式時，它會判斷該驅動程式是良好、惡意還是未知。Symantec Endpoint Protection 驅動程式接著將資訊傳遞給 Windows，以決定允許還是攔截偵測到的驅動程式。

您無法為個別的 ELAM 偵測建立例外；但是，您可以建立全域例外，將所有的惡意驅動程式記錄為未知。依預設，允許載入未知的驅動程式。

對於需要矯正的某些 ELAM 偵測，您可能需要執行 Power Eraser。Power Eraser 是賽門鐵克說明工具的一部分。

附註：「自動防護」會掃描載入的所有驅動程式。

調整 Symantec Endpoint Protection ELAM 選項

1. 在 Symantec Endpoint Protection Manager 主控台的**「政策」**標籤上，開啟「病毒和間諜軟體防護」政策。
2. 在**「防護技術」**下，選取**「提早啟動防惡意軟體驅動程式」**。
3. 勾選或取消勾選**「啟用賽門鐵克提早啟動防惡意軟體」**。

   您必須啟用 Windows ELAM 驅動程式，才能啟用這個選項。您可以使用 Windows 群組原則編輯器或登錄檔編輯器來檢視及修改 Windows ELAM 設定。如需詳細資訊，請參閱 Windows 說明文件。

4 如果您要僅記錄偵測，請在「**偵測設定**」下，選取「**將偵測記錄為不明，以便 Windows 允許載入驅動程式**」。

5 按下「**確定**」。

請參閱第 393 頁的「管理提早啟動防惡意軟體 (ELAM) 偵測」。

請參閱第 656 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。

架構站台使用私用 Insight 伺服器進行信譽查詢

如果您已購買並安裝 Symantec Insight for Private Clouds，則私用 Insight 伺服器設定可讓您將用戶端信譽查詢指向內部網路伺服器。 Symantec Insight for Private Clouds 通常安裝在缺乏網際網路連線的網路中。 私用 Insight 伺服器會儲存賽門鐵克智慧型掃描之信譽資料庫的複本。 Symantec Endpoint Protection 信譽查詢由私用 Insight 伺服器處理，而不是由 Symantec Insight 伺服器進行處理。

私用伺服器會透過加密的安全連線來下載 Symantec Insight 資料。 您可以手動更新 Insight 資料，也可以使用第三方工具來自動檢查更新及下載資料。 您所使用的更新方法，取決於您的網路，以及執行 Symantec Insight for Private Clouds 所在伺服器的類型。

當您使用私用 Insight 伺服器時，賽門鐵克既不會接收也不會傳送任何有關檔案信譽的查詢。

架構站台使用私用 Insight 伺服器進行信譽查詢

1 在主控台的「**管理員**」頁面上，選取「**伺服器**」。

2 選取站台，然後在「**工作**」下，選取「**編輯站台屬性**」。

3 在「**私用 Insight 伺服器**」標籤上，確認已勾選「**啟用私用 Insight 伺服器**」。

您還必須輸入「**名稱**」、「**伺服器 URL**」和「**埠號**」。

附註：如果您將現有伺服器 URL 變更為無效的 URL，用戶端會使用先前有效的私用 Insight 伺服器 URL。 如果您先前從未架構過伺服器 URL，而現在輸入的 URL 無效，用戶端會使用預設的 Symantec Insight 伺服器。

在下次活動訊號出現時，您的用戶端會開始使用指定的私用伺服器來進行信譽查詢。

請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。

請參閱第 397 頁的「將用戶端群組架構為使用私用伺服器進行信譽查詢和提交」。

將用戶端群組架構為使用私用伺服器進行信譽查詢和提交

您可以將用戶端信譽查詢 (智慧型掃描查詢) 從群組導向至私用內部網路伺服器。私用伺服器可以是 Symantec Endpoint Detection and Response 硬體裝置或是您購買並在您的網路中分開安裝的 Symantec Insight for Private Clouds 伺服器。

以下是用於群組的私用伺服器選項：

- Symantec Endpoint Detection and Response
  Symantec EDR 伺服器會收集用戶端偵測的相關資料並提供蒐證分析。當您使用 Symantec EDR 伺服器時，Symantec Endpoint Protection 會將所有信用查詢 (查詢) 和大部分的用戶端傳送資訊類型傳送到 Symantec EDR。然後，Symantec EDR 將查詢或傳送資訊傳送至賽門鐵克。請注意，Symantec EDR 會接收防毒、SONAR 和 IPS 傳送資訊，但是它不會接收檔案信譽傳送資訊。Symantec Endpoint Protection 一律將檔案信譽傳送資訊直接傳送至賽門鐵克。
- Symantec Insight for Private Clouds
  此選項會將信譽查詢從群組中的用戶端重新導向至私用 Insight 伺服器。 私用 Insight 伺服器會儲存賽門鐵克的智慧型掃描信譽資料庫的複本。 私用 Insight 伺服器會處理信譽查詢，而不是由 Symantec Insight 伺服器進行處理。 當您使用私用 Insight 伺服器時，用戶端會繼續將關於偵測的傳送傳送至賽門鐵克。 您通常會在暗網中使用私用 Insight 伺服器，暗網是指與 Internet 中斷連線的網路。在該情況下，賽門鐵克無法接收任何用戶端傳送。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

您也可以將私用伺服器架構複製到其他用戶端群組。

您可以指定多台私用伺服器以負載平衡網路流量。 您也可以指定多組伺服器來管理容錯移轉。

當您選擇啟用 EDR 伺服器時，EDR 連線狀態會顯示在用戶端使用者介面以及管理主控台日誌和報告中。若要與 EDR 伺服器通訊，Symantec Endpoint Protection 用戶端必須至少執行病毒和間諜軟體防護。

附註：如果您對群組啟用私用伺服器，當指定的私用伺服器無法使用時，這些群組中的 12.1.5 及更早版本用戶端將無法使用賽門鐵克伺服器。 12.1.5 及更早版本用戶端無法使用優先順序清單，必須架構為使用單一伺服器。

將用戶端群組架構為使用私用伺服器

1. 在主控台中，移至**「用戶端」**，然後選取應使用私用伺服器清單的群組。
2. 在**「政策」**標籤上，按下**「外部通訊設定」**。
3. 在**「私人雲端」**標籤上，按下**「啟用私用伺服器以管理我的資料」**。

4 根據您使用的伺服器類型而定，按下**「使用 Advanced Threat Protection 伺服器進行智慧型掃描查詢和傳送」**或**「使用私用 Insight 伺服器進行智慧型掃描查詢」**。

您不應該在優先順序清單中混合伺服器類型。

5 如果您希望用戶端使用賽門鐵克伺服器進行信譽查詢以及用戶端防毒和SONAR傳送，請按下**「當私用伺服器不可用時，使用賽門鐵克伺服器」**。

用戶端一律將檔案信譽傳送傳送至賽門鐵克。

6 在**「私用伺服器」**下方，按下**「新增」>「新伺服器」**。

7 在**「新增私用伺服器」**對話方塊中，選取通訊協定，然後輸入 URL 的主機名稱。

8 指定伺服器的通訊埠編號。

9 若要將此伺服器指定為 12.1.5 及更早版本用戶端使用的單一伺服器，請按下**「將此伺服器用作適用於 12.1.5 及更早版本用戶端的私用 Insight 伺服器」**。 12.1.5 及更早版本用戶端無法使用伺服器清單，因此您必須指定這些舊版用戶端應使用哪一部伺服器。

10 若要新增優先順序群組，請按下**「新增」>「新群組」**。

11 若要將設定套用至其他用戶端群組，請按下**「複製設定」**。 選取群組和位置，然後按下**「確定」**。

19

自訂掃描

本章包含以下主題：

自訂在 Windows 電腦上執行的病毒和間諜軟體掃描

您可以為 Windows 電腦上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以自訂自動防護的選項。

表 19-1 自訂 Windows 電腦上的病毒和間諜軟體掃描

工作	敘述
自訂「自動防護」設定	您可以採用多種方法自訂「自動防護」，包括進行下列設定的架構： ■ 「自動防護」掃描的檔案類型 ■ 「自動防護」進行偵測時所採取的動作 ■ 「自動防護」偵測的使用者通知 您還可以針對檔案系統的「自動防護」掃描，啟用**「掃描結果」**對話方塊。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。 請參閱第 405 頁的「為 Windows 電腦上的電子郵件掃描自訂自動防護」。
自訂管理員定義的掃描	您可以為排程掃描和隨選掃描自訂以下類型的選項。 ■ 壓縮檔 ■ 調整選項 ■ 進階排程選項 ■ 有關偵測的使用者通知 請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。 您也可以自訂掃描動作。
調整 ELAM 設定	如果您認為 ELAM 影響電腦的效能，可能會想要啟用或停用 Symantec Endpoint Protection 提早啟動防惡意軟體 (ELAM) 偵測。或者，如果出現太多誤報 ELAM 偵測結果，您也可以覆寫預設偵測設定。 請參閱第 393 頁的「管理提早啟動防惡意軟體 (ELAM) 偵測」。
調整「下載鑑識」設定	您可能需要調整惡意檔案靈敏度，以增加或減少偵測的數目。您也可以修改偵測的動作和偵測的使用者通知。 請參閱第 411 頁的「自訂下載鑑識設定」。
自訂掃描動作	您可以變更 Symantec Endpoint Protection 進行偵測時採取的動作。 請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。
自訂全域掃描設定	您可能需要自訂全域掃描設定，以增加或減少用戶端電腦上的防護程度。 請參閱第 410 頁的「修改 Windows 用戶端的全域掃描設定」。

工作	敘述
自訂「病毒和間諜軟體防護」的其他選項	您可以指定用戶端傳送至 Symantec Endpoint Protection Manager 的風險事件類型。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

自訂在 Mac 電腦上執行的病毒和間諜軟體掃描

您可以為 Mac 電腦上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以自訂自動防護的選項。

表 19-2 自訂 Mac 電腦上的病毒和間諜軟體掃描

工作	敘述
自訂自動防護	您可以為 Mac 電腦上執行的用戶端自訂「自動防護」設定。 請參閱第 403 頁的「自訂 Mac 用戶端的自動防護」。
自訂管理員定義的掃描	您可以自訂一般設定和通知，以及掃描優先順序。 您也可以啟用在定義檔過時的情況下警示使用者的警告。 請參閱第 407 頁的「為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描」。

自訂在 Linux 電腦上執行的病毒和間諜軟體掃描

您可以為 Linux 電腦上執行的管理員定義掃描 (排程掃描和隨選掃描) 自訂選項。您也可以為「自動防護」自訂選項。

表 19-3 自訂 Linux 電腦上的病毒和間諜軟體掃描

工作	敘述
自訂「自動防護」設定	您可以採用多種方法自訂「自動防護」，包括進行下列設定的架構： ■ 「自動防護」掃描的檔案類型 ■ 「自動防護」進行偵測時所採取的動作 ■ 「自動防護」偵測的使用者通知 您還可以針對檔案系統的「自動防護」掃描，啟用或停用**「掃描結果」**對話方塊。 請參閱第 404 頁的「自訂 Linux 用戶端的自動防護」。

工作	敘述
自訂管理員定義的掃描	您可以為排程掃描和隨選掃描自訂以下類型的選項。 ■ 檔案和資料夾類型 ■ 壓縮檔 ■ 安全風險 ■ 排程選項 ■ 使用者通知 您也可以自訂掃描動作。
自訂掃描動作	您可以變更 Symantec Endpoint Protection 進行偵測時採取的動作。 請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。
自訂「病毒和間諜軟體防護」的其他選項	您可以指定用戶端傳送至 Symantec Endpoint Protection Manager 的風險事件類型。 請參閱第 411 頁的「在 Linux 電腦上修改日誌處理設定」。

自訂 Windows 用戶端的自動防護

您可能需要自訂 Windows 用戶端的自動防護設定。

架構 Windows 用戶端的自動防護

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在**「Windows 設定」**下，在**「防護技術」**下，按下**「自動防護」**。

3 在**「掃描詳細資料」**標籤上，確保已勾選**「啟用自動防護」**。

警告：如果您停用「自動防護」，即使下載鑑識已啟用，仍將無法運作。

4 在**「掃描中」**的**「檔案類型」**下方，選取下列其中一個選項：

- **掃描所有檔案**
  此選項是預設值，也是最安全的選項。
- **只掃描選取的副檔名**
  您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。

5 在**「其他選項」**下，勾選或取消勾選**「掃描安全風險」**。

6 按下**「進階掃描與監控」**，變更用於觸發自動防護掃描之動作的選項，以及自動防護處理磁片掃描的方式。

7 按下**「確定」**。

8 在「**網路設定**」下，勾選或取消勾選「**掃描遠端電腦上的檔案**」，以啟用或停用網路檔案的自動防護掃描。

依預設，自動防護只會在執行檔案時掃描遠端電腦上的檔案。

您可能需要停用網路掃描，以改善掃描和電腦效能。

9 當啟用了遠端電腦上的檔案掃描時，請按下「**網路設定**」以修改網路掃描選項。

10 在「**網路設定**」對話方塊中，執行下列任何動作：

- 啟用或停用「自動防護」信任執行「自動防護」之遠端電腦上的檔案。
- 架構「自動防護」掃描的網路快取選項。

11 按下「**確定**」。

12 在「**動作**」標籤上，設定任一選項。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

您也可以為自動防護設定矯正選項。

13 在「**通知**」標籤上，設定任何通知選項。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

14 在「**進階**」標籤上，設定下列任何選項：

- **開機和關機**
- **重新載入選項**

15 在「**其他選項**」下，按下「**檔案快取**」或「**風險追蹤程式**」。

16 架構檔案快取或風險追蹤程式設定，然後按下「**確定**」。

17 架構完此政策後，按下「**確定**」。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

自訂 Mac 用戶端的自動防護

您可能需要為在 Mac 電腦上執行的用戶端自訂自動防護設定。

自訂 Mac 用戶端的自動防護

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Mac 設定**」下，在「**防護技術**」下，按下「**檔案系統自動防護**」。

3 在「**掃描詳細資料**」標籤的上方，按下鎖定圖示以鎖定或解除鎖定所有設定。

4 勾選或取消勾選下列任何選項：

- **啟用檔案系統自動防護**
- **自動修復受感染的檔案**
- **隔離無法修復的檔案**
- **掃描壓縮檔**

5 在「**一般掃描詳細資料**」下，指定「自動防護」掃描的檔案。

附註：若要從掃描中排除檔案，您必須選取「**掃描除指定資料夾外的所有位置**」，然後增加例外政策以指定要排除的檔案。

請參閱第 475 頁的「從掃描中排除檔案或資料夾」。

---

6 在「**掃描掛載磁碟詳細資料**」下，勾選或取消勾選任何可用選項。

7 在「**通知**」標籤上，設定任一通知選項，然後按下「**確定**」。

請參閱第 401 頁的「自訂在 Mac 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

自訂 Linux 用戶端的自動防護

您可能需要為在 Linux 電腦上執行的用戶端自訂自動防護設定。

自訂 Linux 用戶端的自動防護

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Linux 設定**」下方的「**防護技術**」下，按下「**自動防護**」。

3 在「**掃描詳細資料**」標籤上，勾選或取消勾選「**啟用自動防護**」。

4 在「**掃描中**」的「**檔案類型**」下，按下列其中一個選項：

- **掃描所有檔案**
  此選項是預設值，也是最安全的選項。
- **只掃描選取的副檔名**
  您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。

5 在「**其他選項**」下，勾選或取消勾選「**掃描安全風險**」。

6 按下「**進階掃描與監控**」，變更用於觸發自動防護掃描之動作的選項，以及自動防護處理壓縮檔掃描的方式。

7 按下「**確定**」。

8 在「**網路設定**」下，勾選或取消勾選「**掃描遠端電腦上的檔案**」，以啟用或停用網路檔案的自動防護掃描。

依預設，自動防護只會在執行檔案時掃描遠端電腦上的檔案。

您可能需要停用網路掃描，以改善掃描和電腦效能。

9 在「**動作**」標籤上，設定任一選項。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

您也可以為自動防護設定矯正選項。

10 在「**通知**」標籤上，設定任何通知選項。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

11 在「**進階**」標籤上，勾選或取消勾選「**啟用快取**」。設定快取大小，或接受預設值。

12 按下「**確定**」。

請參閱第 401 頁的「自訂在 Linux 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

為 Windows 電腦上的電子郵件掃描自訂自動防護

您可以為 Windows 電腦上的電子郵件掃描自訂自動防護。

為 Windows 電腦上的電子郵件掃描自訂自動防護

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Windows 設定**」下方，選取下列其中一個選項：

- **Microsoft Outlook 自動防護**
- **Internet 電子郵件自動防護***
- **Lotus Notes 自動防護***

* 僅適用於低於 14.2 RU1 的用戶端版本。

3 在「**掃描詳細資料**」標籤上，勾選或取消勾選「**啟用 Internet 電子郵件自動防護**」。

4 在「**掃描中**」的「**檔案類型**」下方，選取下列其中一個選項：

- **掃描所有檔案**
  此選項是預設值，也是最安全的選項。
- **只掃描選取的副檔名**
  您可以選取此選項以改善掃描效能，然而，這樣可能會降低對電腦的防護。

5 勾選或取消勾選「**掃描壓縮檔內的檔案**」。

6 在「**動作**」標籤上，設定任一選項。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

7 在「**通知**」標籤上的「**通知**」下，勾選或取消勾選「**在受感染的電腦上顯示通知訊息**」。您也可以自訂這個訊息。

8 在「**電子郵件通知**」下，勾選或取消勾選下列任何選項：

- **插入警告至電子郵件訊息**
- **傳送電子郵件給寄件者**
- **傳送電子郵件給其他人**

您可以自訂訊息文字，並加上一項警告。對於 Internet 電子郵件自動防護，您也必須指定郵件伺服器。

9 (僅) 對於 Internet 電子郵件自動防護，在「**進階**」標籤上的「**加密連線**」下，啟用或停用加密的 POP3 或 SMTP 連線。

10 在「**大量郵件病蟲啟發式掃描**」下方，勾選或取消勾選「**離埠病蟲啟發式掃描**」。

11 架構完此政策後，按下「**確定**」。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描

您可能需要為在 Windows 電腦上執行的用戶端自訂排程掃描或隨選掃描。您可以設定壓縮檔的掃描選項，並最佳化對電腦的掃描或掃描效能。

為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Windows 設定**」下方，按下「**管理員定義掃描**」。

3 執行下列其中一項動作：

- 在「**排程掃描**」下，選取要自訂的排程掃描，或建立新的排程掃描。
- 在「**管理員隨選掃描**」下，按下「**編輯**」。

4 在「**掃描詳細資料**」標籤上，選取「**進階掃描選項**」：

- 在「**壓縮檔**」標籤上，您可以減少要掃描的壓縮檔的層數。如果減少層數，則有可能會提高用戶端電腦的效能。
- 在「**調整**」標籤上，變更最佳用戶端電腦效能或最佳掃描效能的調整層級。

按下「**確定**」，以儲存變更。

5 在「**掃描詳細資料**」標籤上，可以僅針對舊版 12.1.x 用戶端啟用或停用智慧型掃描查詢。

6 僅針對排程掃描，在「**排程**」標籤上，設定下列任何選項：

- **掃描持續時間**
  您可以設定掃描在暫停並等待用戶端電腦閒置多長時間後開始執行。您也可以隨機產生掃描開始時間。
- **錯過掃描排程**
  您可以為錯過的掃描指定重試時間間隔。

7 在「**動作**」標籤上，變更任何偵測動作。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

8 在「**通知**」標籤上，啟用或停用掃描執行偵測時在用戶端電腦上顯示的通知。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

9 按下「**確定**」。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。

為在 Mac 電腦上執行的用戶端自訂管理員定義的掃描

您可以分別自訂排程掃描和隨選掃描。其中有部分選項不同。

自訂在 Mac 電腦執行的排程掃描

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Mac 設定**」下方，選擇「**管理員定義掃描**」。

3 在「**排程掃描**」下，選取要自訂的排程掃描，或建立新的排程掃描。

若需新掃描，可以手動建立新掃描，或者從範本建立排程掃描。

4 在「**掃描詳細資料**」標籤的「**掃描磁碟機和資料夾**」下，選取您要掃描的項目。

5 您也可以啟用或停用閒置狀態掃描。啟用此選項可改善電腦效能，停用此選項則可改善掃描效能。

6 按下「**確定**」。

編輯此政策中包含的任何其他掃描的掃描詳細資料。

7 在「**通知**」標籤上，啟用或停用與掃描偵測相關的通知訊息。此設定會套用到您在此政策中包含的所有排程掃描。

8 在「**一般設定**」標籤上，設定下列任何選項：

- **掃描選項**
- **動作**
- **警示**

這些選項會套用到您在此政策中包含的所有排程掃描。

9 按下「**確定**」。

自訂在 Mac 電腦上執行的隨選掃描

1 在「病毒和間諜軟體防護政策」頁面的「**Mac 設定**」下，選取「**管理員定義掃描**」。

2 在「**管理員隨選掃描**」下，按下「**編輯**」。

3 在「**掃描詳細資料**」標籤的「**掃描磁碟機和資料夾**」下，選取您要掃描的項目。

您也可以為掃描偵測指定動作，並啟用或停用壓縮檔的掃描。

4 在「**通知**」標籤上，啟用或停用偵測的通知。

您也可以指定顯示在用戶端上的訊息。

5 按下「**確定**」。

請參閱第 401 頁的「自訂在 Mac 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 373 頁的「設定在 Mac 電腦上執行的排程掃描」。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

為在 Linux 電腦上執行的用戶端自訂管理員定義掃描

您可能需要為在 Linux 電腦上執行的用戶端自訂排程掃描或隨選掃描。您可以設定壓縮檔的掃描選項，並最佳化對電腦的掃描或掃描效能。

為在 Linux 電腦上執行的用戶端自訂管理員定義掃描

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Linux 設定**」下，按下「**管理員定義掃描**」。

3 執行下列其中一項動作：

- 在「**排程掃描**」下，選取要自訂的排程掃描，或建立新的排程掃描。
- 在「**管理員隨選掃描**」下，按下「**編輯**」。

4 在「**掃描詳細資料**」標籤上，勾選「**掃描所有資料夾**」，或指定您要掃描的特定資料夾。

5 按下「**掃描所有檔案**」或「**只掃描選取的副檔名**」，並指定您要掃描的副檔名。

6 如果選擇了「**掃描壓縮檔內的檔案**」，您可以減少要掃描的壓縮檔的層數。如果減少層數，則有可能會提高用戶端電腦的效能。

7 勾選或取消勾選「**掃描安全風險**」。

8 僅針對排程掃描，在「**排程**」標籤上，設定下列任何選項：

- **掃描排程**
  您可以設定掃描的執行頻率：每日、每週或每月。
- **錯過掃描排程**
  您可以為錯過的掃描指定重試時間間隔。

9 在「**動作**」標籤上，變更任何偵測動作。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

10 在「**通知**」標籤上，啟用或停用掃描執行偵測時在用戶端電腦上顯示的通知。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

11 按下「**確定**」。

請參閱第 401 頁的「自訂在 Linux 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 374 頁的「設定在 Linux 電腦上執行的排程掃描」。

請參閱第 412 頁的「變更 Symantec Endpoint Protection 進行偵測時採取的動作」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

隨機設定掃描以在 Windows 用戶端上的虛擬環境中改善電腦效能

您可以隨機設定排程掃描，以改善 Windows 用戶端電腦的效能。隨機設定在虛擬化環境中很重要。

例如，您可以將掃描排程在晚上 8:00 執行。如果您選取 4 小時的時間間隔，則用戶端電腦上的掃描會於晚上 8:00 至凌晨 12:00 之間的某個隨機時間開始。

隨機設定掃描以在虛擬化環境中改善電腦效能

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Windows 設定**」下方，按下「**管理員定義掃描**」。

3 建立新的排程掃描，或選取要編輯的現有排程掃描。

4 在「**新增排程掃描**」或「**編輯排程掃描**」對話方塊中，按下「**排程**」標籤。

5 在「**掃描排程**」下，選取掃描應執行的頻率。

6 在「**掃描持續時間**」下，勾選「**最多掃描**」並選取小時數。小時數會控制隨機設定掃描的時間間隔。

7 確認啟用了「**在此期間隨機設定掃描開始時間 (建議在 VM 中)**」。

8 按下「**確定**」。

9 確認將政策套用到包含執行虛擬機器之電腦的群組。

請參閱第 375 頁的「調整掃描以改善電腦效能」。

請參閱第 371 頁的「設定在 Windows 電腦上執行的排程掃描」。

修改 Windows 用戶端的全域掃描設定

您可為在 Windows 用戶端電腦上執行的掃描自訂全域設定。您可能需要修改這些選項，以增進用戶端電腦的安全性。

附註：如果修改這些選項以增進對用戶端電腦的防護，可能會影響用戶端電腦的效能。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

修改 Windows 用戶端的全域掃描設定

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Windows 設定**」下方，按下「**全域掃描選項**」。

3 架構以下任何選項：

Insight	智慧型掃描可讓掃描略過賽門鐵克信任為良好 (安全性較高) 或社群信任為良好 (安全性較低) 的檔案。
Bloodhound	Bloodhound 會隔離並找出檔案的邏輯區域，來偵測出大多數未知病毒。然後 Bloodhound 會分析疑似病毒行為的程式邏輯。您可以指定偵測的靈敏度等級。
對應網路磁碟機的密碼	指定用戶端在掃描網路磁碟機時是否提示使用者輸入密碼。

4 按下「**確定**」。

在 Windows 電腦上修改日誌處理及通知設定

每項病毒和間諜軟體防護政策包含的選項，都可以套用到 Windows 用戶端電腦上執行的所有病毒和間諜軟體掃描。

您可以設定下列選項：

- 指定預設的 URL，讓 Symantec Endpoint Protection 在修復變更了瀏覽器首頁的安全風險時使用該網址。

- 指定風險日誌處理選項。
- 定義檔過期或遺失時警告使用者。
- 將虛擬影像排除在自動防護或管理員定義掃描的範圍之外。

在 Windows 電腦上修改日誌處理及通知設定

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Windows 設定**」下方，按下「**其他**」。

指定 **Internet 瀏覽器防護**的選項。

3 在「**日誌處理**」標籤上，設定事件過濾、日誌存留和日誌彙總的選項。

4 在「**通知**」標籤上，架構全域通知。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

5 按下「**確定**」。

請參閱第 390 頁的「管理顯示在用戶端電腦上的病毒和間諜軟體通知」。

在 Linux 電腦上修改日誌處理設定

每項病毒和間諜軟體防護政策包含的日誌處理設定，都可以套用到 Linux 用戶端電腦上執行的所有病毒和間諜軟體掃描。

Linux 電腦上的日誌處理設定

1 在主控台中，開啟「病毒和間諜軟體防護」政策。

2 在「**Linux 設定**」下方，按下「**其他**」。

3 在「**日誌處理**」標籤上，設定事件過濾、日誌存留和日誌彙總的選項。

請參閱第 563 頁的「檢視日誌」。

自訂下載鑑識設定

您可能需要自訂「下載鑑識」設定，以降低用戶端電腦上的偵測誤報率。您可以變更「下載鑑識」對於描述惡意檔案特徵的檔案信譽資料的敏感程度。您也可以變更「下載鑑識」進行偵測時顯示在用戶端電腦上的通知。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 380 頁的「管理「下載鑑識」偵測」。

自訂下載鑑識設定

1. 在主控台中，開啟「病毒和間諜軟體防護」政策，然後選擇**「下載防護」**。
2. 在**「下載鑑識」**標籤上，確定勾選**「啟用下載鑑識以根據檔案信譽偵測下載檔案中的潛在風險」**。

   如果停用「自動防護」，則即使「下載鑑識」已啟用，也無法運作。
3. 將惡意檔案靈敏度的滑桿移至適當層級。

   如果設定為更高等級，則「下載鑑識」會將較多的檔案偵測為惡意檔案，並將較少的檔案偵測為未證明的檔案。不過，設定等級愈高，傳回的誤報就越多。
4. 您可以勾選下列選項，用作檢查未證明檔案的附加條件：
   - **使用者數量不超過 *x* 個的檔案**
   - **使用者已知不超過 天的檔案**

   如果未證明的檔案符合這些準則，「下載鑑識」會將這些檔案偵測為惡意檔案。
5. 請確定勾選**「自動信任從信任的 Internet 或內部網路網站下載的任何檔案」**。
6. 在**「動作」**標籤的**「惡意檔案」**下方，指定第一個動作和第二個動作。
7. 在**「未證明的檔案」**下，指定動作。
8. 在**「通知」**標籤上，指定當「下載鑑識」進行偵測時，是否在用戶端電腦上顯示訊息。

   您也可以自訂當使用者允許「下載鑑識」偵測到的檔案時，顯示之警告訊息的文字。
9. 按下**「確定」**。

變更 Symantec Endpoint Protection 進行偵測時採取的動作

您可以架構掃描進行偵測時應採取的一或多個動作。每個掃描均有本身的動作集，例如「清除」、「隔離」、「刪除」或「略過 (只記錄)」。

在 Windows 用戶端和 Linux 用戶端上，每個偵測類別均可架構第一個和第二個動作；以便於在第一個動作無法進行時，能進行第二個動作。

依預設，Symantec Endpoint Protection 會嘗試清除感染病毒的檔案。如果 Symantec Endpoint Protection 無法清除檔案，則會執行下列動作：

- 將檔案移至受感染電腦上的隔離所，並拒絕對該檔案的任何存取。
- 記錄事件。

依預設，Symantec Endpoint Protection 會將任何受到安全性風險感染的檔案移至隔離所。

如果您將動作設定為只記錄，則依預設當使用者建立或儲存受感染的檔案時，Symantec Endpoint Protection 會刪除這些檔案。

在 Windows 電腦上，您也可以為檔案系統的管理員掃描、隨選掃描和自動防護掃描架構矯正動作。

您可以鎖定動作，讓使用者無法在使用此政策的用戶端電腦上變更動作。

警告：對於安全風險，請小心使用刪除動作。在某些情形下，刪除安全風險會導致應用程式無法運作。如果您架構用戶端刪除受到安全風險影響的檔案，將無法還原檔案。

若要備份受到安全風險影響的檔案，請改用隔離動作。

變更當 Symantec Endpoint Protection 在 Windows 或 Linux 用戶端上進行偵測時採取的動作

1. 在「病毒和間諜軟體防護政策」中的**「Windows 設定」**或**「Linux 設定」**下，選取掃描 (任何自動防護掃描、管理員掃描或隨選掃描)。
2. 在**「動作」**標籤的**「偵測」**下方，選取惡意軟體或安全風險類型。

   依據預設，每個子類別都會自動架構為使用為整個類別所設定的動作。

   附註：在 Windows 用戶端上，類別會隨著賽門鐵克取得有關風險的新資訊而隨時動態變更。

   ---

3. 若要僅針對子類別架構動作，請執行下列其中一項動作：
   - 勾選**「覆寫針對惡意軟體架構的動作」**，然後僅針對該子類別設定動作。

     附註：一個類別下方可能有單一子類別，視賽門鐵克目前對風險進行分類的方式而定。例如，在**「惡意軟體」**下方，可能有名為「病毒」的單一子類別。

   - 勾選**「覆寫針對安全風險架構的動作」**，然後僅針對該子類別設定動作。
4. 在**「動作目的」**下方，選取用戶端軟體在偵測到該病毒或安全風險類別時，所要採取的第一個與第二個動作。

   對於安全風險，請小心使用刪除動作。在某些情形下，刪除安全風險會導致應用程式無法運作。
5. 針對每個您想設定動作的 (病毒與安全風險) 類別重複上述步驟 。
6. 架構完此政策後，按下**「確定」**。

變更當 Symantec Endpoint Protection 在 Mac 用戶端上進行偵測時採取的動作

1. 在「病毒和間諜軟體防護」政策中的**「Mac 設定」**下方，選取**「管理員定義掃描」**。
2. 執行下列其中一項動作：
   - 對於排程掃描，請選取**「一般設定」**標籤。

- 對於隨選掃描，請在**「掃描」**標籤上的**「管理員隨選掃描」**下方，按下**「編輯」**。

3 在**「動作」**下方，選取以下任何一個選項：

- **自動修復受感染的檔案**
- **隔離無法修復的檔案**

4 對於隨選掃描，請按下**「確定」**。

5 架構完此政策後，按下**「確定」**。

請參閱第 400 頁的「自訂在 Windows 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 401 頁的「自訂在 Mac 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 401 頁的「自訂在 Linux 電腦上執行的病毒和間諜軟體掃描」。

請參閱第 380 頁的「管理「下載鑑識」偵測」。

請參閱第 425 頁的「管理 SONAR」。

請參閱第 351 頁的「檢查掃描動作及重新掃描識別出的電腦」。

請參閱第 348 頁的「移除病毒和安全風險」。

允許使用者在 Windows 電腦上檢視掃描進度並與掃描互動

您可以架構是否在 Windows 用戶端電腦上顯示掃描進度對話方塊。如果您允許此對話方塊顯示在用戶端電腦上，使用者就能暫停或延後管理員定義掃描。

當您允許使用者檢視掃描進度時，用戶端使用者介面的主要頁面會出現連結，以顯示目前執行的掃描的掃描進度。另外也會顯示重新排程下一個排程掃描的連結。

當您允許使用者檢視掃描進度時，用戶端使用者介面的主頁會顯示下列選項：

- 掃描執行時，將顯示**「*<掃描>* 進行中」**訊息連結。
  使用者可以按下此連結來顯示掃描進度。
- 另外也會顯示重新排程下一個排程掃描的連結。

您可以允許使用者完全停止掃描。您也可以架構使用者如何暫停或延後掃描的選項。

您可以允許使用者執行下列掃描動作：

暫停	使用者暫停掃描時，「掃描結果」對話方塊仍保持開啟，等候使用者繼續或放棄掃描。如果電腦關機，暫停的掃描就無法繼續執行。
延緩	使用者延緩排程掃描時，可以選擇將掃描延緩一小時或三小時。您可以架構延緩的次數。使用者延緩掃描後，「掃描結果」對話方塊就會關閉；它會在延緩期間結束後再次出現，並繼續掃描。

停止	使用者停止掃描時，掃描通常會立即停止。如果使用者停止掃描的同時，用戶端軟體正在掃描壓縮檔，則掃描不會馬上停止。在這種情況下，在壓縮檔一掃描完畢後就會停止掃描。停止的掃描則不會重新啟動。

暫停的掃描在經過一段指定的時間間隔後會自動重新啟動。

附註：使用者可以停止 Power Eraser 分析，但無法暫停或延緩該分析。

若需程序中使用選項的詳細資訊，您可以按下「敘述」。

允許使用者在 Windows 電腦上檢視掃描進度並與掃描互動

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在**「Windows 設定」**下方，按下**「管理員定義掃描」**。
3. 在**「進階」**標籤的**「掃描進度選項」**下，按下**「顯示掃描進度」**或**「顯示偵測到風險時的掃描進度」**。
4. 若要在掃描完成後自動關閉掃描進度指標，請勾選**「完成時關閉掃描進度視窗」**。
5. 勾選**「允許使用者停止掃描」**。
6. 按下**「暫停選項」**。
7. 在**「掃描暫停選項」**對話方塊中，執行下列任一動作：
   - 若要限制使用者可以暫停掃描的時間，請勾選**「限制掃描暫停的時間」**，然後輸入分鐘數。範圍是 3 至 180。
   - 若要限制使用者可以延後 (或延緩) 掃描的次數，請在**「延緩的次數上限」**方塊中，輸入 1 至 8 之間的數字。
   - 根據預設，使用者可將掃描動作延後一個小時。若要變更此限制為 3 小時，請勾選**「允許使用者延緩掃描 3 小時」**。
8. 按下**「確定」**。

請參閱第 357 頁的「在用戶端電腦上管理掃描」。

架構 Windows 資訊安全中心通知以搭配 Symantec Endpoint Protection 用戶端使用

您可以使用「病毒和間諜軟體防護」政策，在執行 Windows XP Service Pack 3 的用戶端電腦上架構「Windows 資訊安全中心」設定。

請參閱第 406 頁的「為在 Windows 電腦上執行的用戶端自訂管理員定義的掃描」。

附註：您可以在僅執行 Windows XP SP3 的用戶端電腦上架構所有 Windows 資訊安全中心選項。您僅可以在 Windows Vista 與 Windows 7 及更新版本上架構**「定義檔過期時，顯示 Windows 資訊安全中心訊息」**選項。

表 19-4　架構 Windows 資訊安全中心如何搭配用戶端使用的選項

選項	敘述	使用時機
停用 Windows 資訊安全中心	可讓您在用戶端電腦上永久或暫時停用「Windows 資訊安全中心」。 可用選項： ■ 從不。「Windows 資訊安全中心」永遠會在用戶端電腦上啟用。 ■ 一次。只會停用「Windows 資訊安全中心」一次。如果使用者啟用此選項，就不會再次停用「Windows 資訊安全中心」。 ■ 永遠。「Windows 資訊安全中心」會在用戶端電腦上永久停用。如果使用者啟用此選項，就會立即停用「Windows 資訊安全中心」。 ■ 還原。如果「病毒和間諜軟體防護」政策先前已停用「Windows 資訊安全中心」，就會將該程式啟用。	如果您不希望用戶端使用者收到「Windows 資訊安全中心」所提供的安全性警示，可永久停用該程式。用戶端使用者仍會收到 Symantec Endpoint Protection 警示。 如果您希望用戶端使用者收到「Windows 資訊安全中心」所提供的安全性警示，可永久啟用該程式。您可以將「Windows 資訊安全中心」設為顯示 Symantec Endpoint Protection 警示。
顯示 Windows 資訊安全中心內的防毒警示	讓您從 Symantec Endpoint Protection 用戶端設定防毒警示，以便在 Windows 通知區域中顯示警示。	如果您希望使用者在其電腦的 Windows 通知區域中收到 Symantec Endpoint Protection 警示以及其他安全性警示，請啟用此設定。
定義檔過期時，顯示 Windows 資訊安全中心訊息	讓您設定天數，「Windows 資訊安全中心」會在超過該天數後將定義檔視為過期。依據預設，「Windows 資訊安全中心」會在 30 天後傳送此訊息。	如果您希望「Windows 資訊安全中心」通知用戶端使用者定義檔過期的頻率，比預設時間 (30 天) 更為頻繁，請設定此選項。 **附註：**在用戶端電腦上，Symantec Endpoint Protection 會每隔 15 分鐘檢查一次，比較過期時間、定義檔的日期與目前日期。由於定義經常會自動更新，因此通常不會有過期狀態報告給「Windows 資訊安全中心」。如果您手動更新定義檔，可能需要等 15 分鐘才會在「Windows 資訊安全中心」看到正確的狀態。

架構「Windows 資訊安全中心」以搭配 Symantec Endpoint Protection 用戶端使用

1. 在主控台中，開啟「病毒和間諜軟體防護」政策。
2. 在**「Windows 設定」**下方，按下**「其他」**。
3. 在**「其他」**標籤上，指定 Windows 資訊安全中心的選項。
4. 按下**「確定」**。

20

管理管理伺服器和用戶端傳送給賽門鐵克的資訊

本章包含以下主題：

- 瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性
- 管理用戶端傳送給賽門鐵克的匿名或非匿名資料
- Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響
- 指定用於用戶端傳送資訊和其他外部通訊的代理伺服器

瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性

依據預設，Symantec Endpoint Protection 用戶端和 Symantec Endpoint Protection Manager 會向賽門鐵克提交某些類型的匿名資訊。用戶端也可以向賽門鐵克傳送非匿名資料以進行自訂分析。您可以控制自己的用戶端或 Symantec Endpoint Protection Manager 是否傳送資訊。

伺服器資料和用戶端傳送資訊對於改善網路安全都極為重要。

何謂伺服器資料收集？

何謂匿名用戶端提交？

何謂非匿名用戶端提交？

隱私權考量

頻寬使用量考量

何謂伺服器資料收集？

伺服器資料是可協助賽門鐵克衡量和改善偵測技術效能之資訊的一部分。

Symantec Endpoint Protection Manager 會向賽門鐵克提交下列類型的匿名資訊：

- 授權資訊，其中包括名稱、版本、語言及授權權利資料
- Symantec Endpoint Protection 防護功能的使用情況
- Symantec Endpoint Protection 組態的相關資訊。資訊包括作業系統資訊、伺服器硬體和軟體組態、CPU 大小、記憶體大小，以及已安裝套件的軟體版本和功能

您可以在安裝期間變更伺服器傳送資訊設定，也可以在主控台中變更伺服器**「站台屬性」>「資料收集」**標籤上的設定。

附註：賽門鐵克始終建議您保持伺服器資料收集為啟用狀態。

何謂匿名用戶端提交？

Symantec Endpoint Protection 用戶端會自動向賽門鐵克安全機制應變中心提交有關偵測、網路及組態的匿名資訊。賽門鐵克使用這些匿名資訊來應付新的威脅與不斷變化的威脅，以及改善產品效能。匿名資料不會直接用於識別特定使用者。

用戶端傳送的偵測資訊包括防毒偵測、入侵預防、SONAR 及檔案信譽偵測相關資訊。

附註：Mac 用戶端傳送資訊不包括 SONAR 或檔案信譽傳送資訊。Linux 用戶端不支援任何用戶端傳送。

用戶端傳送給賽門鐵克的匿名資訊可為您提供下列好處：

- 增強網路安全性
- 最佳化產品效能

不過，在某些情況下，您可能想要阻止用戶端傳送某些資訊。例如，您的公司政策可能不允許用戶端電腦向外部實體傳送任何網路資訊。您可以停用單一類型的傳送 (例如網路資訊的傳送)，而非停用所有類型的用戶端傳送資訊。

附註：賽門鐵克建議您始終保持用戶端傳送資訊為啟用狀態。停用傳送可能會妨礙對組織中獨佔使用之應用程式誤報偵測的快速解析。如果沒有組織中惡意軟體的相關資訊，產品和賽門鐵克對威脅的回應可能需要更長時間。

請參閱第 420 頁的「管理用戶端傳送給賽門鐵克的匿名或非匿名資料」。

請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。

請參閱第 383 頁的"檔案信譽傳送"。

何謂非匿名用戶端提交？

您可以選擇向賽門鐵克提交非匿名用戶端資訊。這種類型的資訊有利於進一步瞭解安全性挑戰，可協助賽門鐵克提供建議的自訂解決方案。

- 您應該只有在參與賽門鐵克贊助的計畫 (可提供自訂分析) 時，才使用此選項。
- 此選項預設為停用。

請參閱第 420 頁的「管理用戶端傳送給賽門鐵克的匿名或非匿名資料」。

隱私權考量

賽門鐵克會竭盡所能匿名化用戶端提交資料。

- 僅會傳送可疑的可執行檔。
- 將使用者名稱從路徑名稱中移除。
- 電腦和企業均由唯一的匿名化值識別。
- IP 位址在用於識別地理位置後即會捨棄。

如需隱私權的詳細資訊，請參閱下列文件：

隱私權聲明

頻寬使用量考量

Symantec Endpoint Protection 會最大限度降低用戶端傳送資訊對網路頻寬的影響。

您可以檢查用戶端活動日誌，來檢視用戶端電腦所傳送的資訊類型，以及監控頻寬使用量。

請參閱第 421 頁的「Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響」。

請參閱第 563 頁的「檢視日誌」。

管理用戶端傳送給賽門鐵克的匿名或非匿名資料

Symantec Endpoint Protection 可以透過將偵測相關資訊提交給賽門鐵克，為電腦提供保護。賽門鐵克會使用該資訊來應付新的與不斷變化的威脅。您傳送的任何資料都有助於賽門鐵克提高回應威脅以及為電腦自訂防護的能力。賽門鐵克建議您選擇傳送盡可能多的偵測資訊。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

用戶端電腦會匿名提交偵測相關資訊。您可以指定用戶端提交哪些類型的偵測資訊。Symantec 遙測收集的資料可能包括不可直接識別的匿名元素。Symantec 既不需要也不會設法使用遙測資料來識別任何個別使用者。

附註：Mac 用戶端傳送資訊不包括 SONAR 或檔案信譽傳送資訊。Linux 用戶端不支援任何用戶端傳送。

變更用戶端傳送資訊設定

1. 在主控台中，選取**「用戶端」**，然後按下**「政策」**標籤。
2. 在**「設定」**窗格中，按下**「外部通訊設定」**。
3. 選取**「用戶端傳送資訊」**標籤。
4. 啟用或停用**「將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報」**選項。
5. 如果想要啟用或停用特定傳送類型 (例如檔案信譽)，請選取**「更多選項」**。
6. 如果您參與了賽門鐵克贊助的自訂分析計畫，請選取**「將可識別用戶端的資料傳送給賽門鐵克進行自訂分析」**。

   警告：此選項會將非匿名資訊傳送給賽門鐵克。只有在您參與賽門鐵克贊助的計畫並且想要與賽門鐵克共用可識別用戶端的資料時，才使用此選項。

7. 選取**「確定」**。

附註：在 Mac 用戶端上，您也可以停用 IPS 連線偵測傳送。請參閱下列文章：

如何在 Symantec Endpoint Protection for Mac 用戶端上停用 IPS 資料傳送

Symantec Endpoint Protection 如何最大限度降低用戶端傳送資訊對網路頻寬的影響

Symantec Endpoint Protection 會調節用戶端電腦傳送，將對您網路的影響降至最低。Symantec Endpoint Protection 會以下列方式調節傳送：

- 用戶端電腦只會在電腦閒置時傳送範例。閒置傳送有助於在整個網路中隨機設定傳送流量。
- 用戶端電腦只會傳送唯一檔案的範例。如果賽門鐵克已經看見此檔案，用戶端電腦就不會傳送資訊。
- Symantec Endpoint Protection 會使用傳送控制資料 (SCD) 檔案。賽門鐵克會發布 SCD 檔案，並將其包含在 LiveUpdate 套件中。每個賽門鐵克產品都有各自的 SCD 檔案。

SCD 檔案會控制下列設定：

- 一天之中用戶端可傳送的次數
- 用戶端軟體重試傳送時等候的時間長度
- 傳送失敗後重試的次數
- 「賽門鐵克安全機制應變中心」擷取傳送內容的 IP 位址

如果 SCD 檔案過時，則用戶端會停止傳送。如果用戶端電腦已有 7 天未擷取 LiveUpdate，則賽門鐵克會認為該 SCD 檔案過時。 用戶端會在 14 天後停止傳送。

如果用戶端停止傳送，則用戶端軟體不會收集傳送資訊，也不會在稍後傳送它。用戶端再次開始傳送時，只會傳送在傳送重新開始之後發生的事件資訊。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

指定用於用戶端傳送資訊和其他外部通訊的代理伺服器

您可以架構 Symantec Endpoint Protection Manager 使用代理伺服器傳送資訊，以及進行 Windows 用戶端使用的其他外部通訊。

附註：如果用戶端電腦使用需驗證的代理，您可能需要在代理伺服器組態中為 Symantec URL 指定例外。透過使用例外，可以讓用戶端電腦與 Symantec Insight 及其他重要的賽門鐵克網站進行通訊。

如果您使用下列代理組態選項，則需要在代理伺服器設定中包含 Symantec URL 的例外：

- 您使用需驗證的代理伺服器。
- 您要在 Symantec Endpoint Protection Manager 的**「外部通訊」對話方塊**中選取**「使用用戶端瀏覽器指定的 Proxy 伺服器」**選項。
- 您要在瀏覽器的「網際網路選項」中使用自動偵測或自動設定。

如果您不使用自動偵測或自動設定，就不需要在代理伺服器設定中為 Symantec URL 指定例外。您應該在**「外部通訊」**對話方塊中選取**「使用自訂 Proxy 設定」**，然後指定驗證設定。

指定用於用戶端傳送資訊和其他外部通訊的代理伺服器

1. 在主控台的**「用戶端」**頁面上，選取群組並按下**「政策」**。
2. 在**「設定」**或**「位置限定的設定」**下方，按下**「外部通訊」**。
3. 在**「Proxy 伺服器 (Windows)」**標籤的**「HTTPS Proxy 架構」**下方，選取**「使用自訂 Proxy 設定」**。
4. 輸入用戶端使用之代理伺服器的相關資訊。如需這些選項的詳細資訊，請參閱線上說明。
5. 按下**「確定」**。

如需建議例外的相關資訊，請參閱下列文章：

- 如何測試 Insight 與賽門鐵克授權伺服器的連線
- 允許 Symantec Endpoint Protection 連線到賽門鐵克信譽與授權伺服器所需排除的代理伺服器

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

21

管理 SONAR 和竄改防護

本章包含以下主題：

關於 SONAR

SONAR 是可偵測執行於電腦的潛在惡意應用程式的即時防護。 SONAR 提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測威脅，從而解決威脅。

SONAR 使用啟發式技術及信譽資料來偵測新出現和不明威脅。SONAR 可為您的用戶端電腦提供額外的防護等級，並能與您現有的病毒和間諜軟體防護、入侵預防、記憶體攻擊緩和以及防火牆防護相輔相成

SONAR 使用啟發式系統偵測新出現的威脅，該系統會運用賽門鐵克的線上智慧型網路，並且對用戶端電腦進行主動型本機監視。 SONAR 也會偵測您應監視的用戶端電腦上的變更或行為。

附註：「自動防護」也會使用稱為 Bloodhound 的啟發式掃描來偵測檔案中是否有可疑行為。

SONAR 會將一些程式碼插入以 Windows 使用者模式執行的應用程式中，以監控這些應用程式是否有可疑的活動。在某些情況下，插入程式碼可能會影響應用程式效能，或導致執行應用程式時出現問題。 您可以建立例外，將檔案、資料夾或應用程式排除在這類監控的範圍之外。

SONAR 不會偵測應用程式類型，但會偵測程序的行為模式。 SONAR 只會在應用程式有惡意行為時才會採取動作，不論應用程式類型為何。 例如，如果某個特洛伊木馬程式或按鍵記錄器沒有惡意行為，則 SONAR 不會加以偵測。

SONAR 會偵測以下項目：

啟發式威脅	SONAR 會使用啟發式技術判斷不明檔案是否有可疑行為，以及可能會產生較高風險或較低風險。 它也會使用信譽資料，判斷威脅會產生較高風險或較低風險。
系統變更	SONAR 會偵測嘗試修改用戶端電腦上之 DNS 設定或主機檔案的應用程式或檔案。
呈現不良行為的受信任應用程式	某些沒有問題的受信任檔案可能會伴隨可疑行為。 SONAR 會將這些檔案偵測為可疑行為事件。 例如，常見的文件共用應用程式可能會建立可執行檔。

如果您停用自動防護，會限制 SONAR 偵測高風險和低風險檔案的能力。 如果您停用智慧型掃描查詢 (信譽查詢)，則也會限制 SONAR 的偵測功能。

附註：SONAR 不會將程式碼插入執行 Symantec Endpoint Protection 12.1.2 之前版本的電腦上的應用程式中。如果您使用 Symantec Endpoint Protection Manager 12.1.2 或更新版本來管理用戶端，這些舊版用戶端上會忽略「例外」政策中的 SONAR 檔案例外。如果使用舊版 Symantec Endpoint Protection Manager 來管理用戶端，舊版政策不支援 Symantec Endpoint Protection 12.1.2 用戶端的 SONAR 檔案例外。 不過，您可以在舊版政策中建立**「要監控的應用程式」**例外，防止 SONAR 程式碼插入這些用戶端上的應用程式。 在用戶端探索到應用程式後，便可以在政策中架構應用程式例外。

請參閱第 425 頁的「管理 SONAR」。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

管理 SONAR

SONAR 是用戶端電腦上主動型威脅防護的一部分，也是 Symantec Endpoint Protection Manager 中病毒和間諜軟體防護政策的一部分。

表 21-1　　管理 SONAR

工作	敘述
瞭解 SONAR 運作方式	瞭解 SONAR 偵測未知威脅的方式。 SONAR 運作方式的相關資訊可幫助您決定如何在安全網路中使用 SONAR。 請參閱第 424 頁的「關於 SONAR」。

工作	敘述
檢查 SONAR 是否已啟用	若要為用戶端電腦提供最完整的防護，您應啟用 SONAR。 SONAR 可與某些其他 Symantec Endpoint Protection 功能交互運作。 SONAR 需要「自動防護」。 您可以使用「用戶端」標籤檢查用戶端電腦上是否已啟用「主動型威脅防護」。 請參閱第 428 頁的「調整用戶端電腦上的 SONAR 設定」。
檢查 SONAR 的預設設定	SONAR 設定是病毒和間諜軟體防護政策的一部分。 請參閱第 367 頁的「關於預設的病毒和間諜軟體防護政策掃描設定」。
確定已啟用智慧型掃描查詢	除啟發式外，SONAR 還使用信譽資料進行偵測。 如果停用「智慧型掃描查詢」，SONAR 只會採用啟發式技術進行偵測。誤報率可能會增加，且 SONAR 提供的防護會受到限制。 請在**「遞送」**對話方塊中啟用或停用「智慧型掃描查詢」。 請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。
監控 SONAR 事件以查是否有偵測誤報	您可以使用 SONAR 日誌監控事件。 您還可以檢視「SONAR 偵測結果」報告 (在「風險報告」下)，以檢視偵測相關資訊。 請參閱第 429 頁的「監控 SONAR 偵測結果來查看是否有誤報」。 請參閱第 539 頁的「監控端點防護」。
調整 SONAR 設定	您可以針對 SONAR 偵測到的某些類型的威脅變更偵測動作。 您可能希望變更偵測動作以減少偵測誤報率。 您還可能希望針對高風險或低風險啟發式偵測啟用或停用通知。 請參閱第 428 頁的「調整用戶端電腦上的 SONAR 設定」。 請參閱第 427 頁的「處理和避免 SONAR 偵測誤報」。
防止 SONAR 偵測已知安全的應用程式	SONAR 可能會偵測您希望在用戶端電腦上執行的檔案或應用程式。 可以使用「例外」政策為要允許的特定檔案、資料夾或應用程式指定例外。對於 SONAR 隔離的項目，您可以為 SONAR 日誌中隔離的項目建立例外。 您還可能希望設定 SONAR 動作以記錄和允許偵測。您可以使用應用程式探索，以便 Symantec Endpoint Protection 瞭解用戶端電腦上的合法應用程式。 在 Symantec Endpoint Protection 瞭解您在網路中使用的應用程式後，您可以將 SONAR 動作變更為「隔離」。 **附註：**如果您將高風險偵測對應的動作設定為「只記錄」，則可能會為您的用戶端電腦帶來潛在威脅。 請參閱第 427 頁的「處理和避免 SONAR 偵測誤報」。

工作	敘述
阻止 SONAR 檢查某些應用程式	在某些情況下，當 SONAR 將程式碼插入應用程式中進行檢查時，應用程式可能變得不穩定或無法執行。可以針對應用程式建立檔案、資料夾或應用程式例外。 請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。
管理 SONAR 偵測變更 DNS 或主機檔案的應用程式的方式	可以使用 SONAR 政策設定，全域調整 SONAR 處理 DNS 或主機檔案變更偵測的方式。可以使用「例外」政策來架構特定應用程式的例外。 請參閱第 428 頁的「調整用戶端電腦上的 SONAR 設定」。 請參閱第 482 頁的「針對會變更 DNS 或主機檔案的應用程式建立例外」。
允許用戶端將有關 SONAR 偵測的資訊傳送給賽門鐵克	賽門鐵克建議您在用戶端電腦上啟用傳送。用戶端送出的偵測相關資訊有助於賽門鐵克解決威脅。此資訊有助於賽門鐵克建立更好的啟發式技術，進而產生較低的偵測誤報率。 請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

處理和避免 SONAR 偵測誤報

對於某些內部自訂應用程式，SONAR 可能會做出偵測誤報。此外，如果您停用「智慧型掃描查詢」，則來自 SONAR 的誤報數目會增加。

請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

一般而言，您可以變更 SONAR 設定以減輕偵測誤報率。您也可以為 SONAR 偵測為誤報的特定檔案或特定應用程式建立例外。

警告：如果您將高風險偵測對應的動作設定為「只記錄」，則可能會為您的用戶端電腦帶來潛在威脅。

表 21-2 處理 SONAR 誤報

工作	敘述
記錄 SONAR 高風險啟發式偵測與使用應用程式探索	您可能需要在一段短時間時內將高風險啟發式偵測對應的偵測動作設為**「記錄」**。同時，請讓應用程式探索執行相同的一段時間。Symantec Endpoint Protection 會探索您在網路上執行的合法程序。然而，這麼做可能無法隔離某些真正的偵測結果。 請參閱第 285 頁的「收集有關用戶端電腦執行的應用程式資訊」。 在該段時間之後，您應將偵測動作重新設為**「隔離」**。 **附註：**如果您針對低風險啟發式偵測使用主動模式，會增加偵測誤報的可能性。依預設會停用主動模式。 請參閱第 428 頁的「調整用戶端電腦上的 SONAR 設定」。
為 SONAR 建立例外以允許安全應用程式	您可以使用下列方式，為 SONAR 建立例外： ■ 使用 SONAR 日誌為已偵測到且隔離的應用程式建立例外 您可以從 SONAR 日誌為偵測誤報建立例外。如果項目已隔離，Symantec Endpoint Protection 會在隔離所中重新掃描該項目後還原項目。用戶端收到更新的定義檔之後，會重新掃描隔離所中的項目。 請參閱第 484 頁的「從日誌事件建立例外」。 請參閱第 389 頁的「架構 Windows 用戶端處理隔離項目的方式」。 ■ 使用例外政策為特定檔案名稱、資料夾名稱或應用程式指定例外。 您可以從 SONAR 偵測中排除整個資料夾。您可能需要排除自訂應用程式所在的資料夾。 請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

調整用戶端電腦上的 SONAR 設定

若要降低偵測誤報率，您可能需要變更 SONAR 動作。若要變更顯示在您用戶端電腦上的偵測通知數目，您可能也需要變更 SONAR 動作。

附註：當此網域在雲端主控台中註冊時，部分選項旁會顯示雲端圖示。當密集型防護政策生效時，該政策僅針對 14.0.1 用戶端覆寫這些選項。

調整用戶端電腦上的 SONAR 設定

1 在「病毒和間諜軟體防護」政策中，選取 **SONAR** 。

2 確認已勾選**「啟用 SONAR」**。

附註：啟用 SONAR 時，可疑行為偵測會自動開啟。啟用 SONAR 時，無法關閉可疑行為偵測。

3 在「**掃描詳細資料**」下，變更高或低風險啟發式威脅對應的動作。

您可以為低風險偵測啟用主動模式。此設定會增加SONAR對低風險偵測的靈敏度。它可能會增加偵測誤報率。

4 您也可以選擇變更顯示在用戶端電腦上的通知相關設定。

5 在「**系統變更事件**」下，變更「**偵測到 DNS 變更**」或「**偵測到主機檔案變更**」對應的動作。

附註：「提示」動作可能導致用戶端電腦上出現許多通知。**「忽略」**之外的任何動作都可能會導致主控台上有許多日誌事件，並傳送電子郵件通知給管理員。

警告：如果將動作設定為**「攔截」**，則可能會攔截用戶端電腦上重要的應用程式。

例如，如果將**「偵測到DNS變更」**對應的動作設定為**「攔截」**，可能會發生攔截VPN用戶端等應用程式的情形。如果將**「偵測到主機檔案變更」**對應的動作設為**「攔截」**，則可能會攔截需要存取主機檔案的應用程式。您可以使用 DNS 或主機檔案變更例外，允許特定應用程式進行 DNS 或主機檔案變更。

請參閱第 482 頁的「針對會變更 DNS 或主機檔案的應用程式建立例外」。

6 在「**可疑行為偵測**」下，您可以變更高或低風險偵測對應的動作。

如果已停用 SONAR，則可以啟用或停用可疑行為偵測。

7 按下「**確定**」。

請參閱第 425 頁的「管理 SONAR」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

監控 SONAR 偵測結果來查看是否有誤報

用戶端會收集 SONAR 偵測結果，並且上傳到管理伺服器。 結果會儲存在 SONAR 日誌中。

若要判斷哪些程序合法而哪些程序具有安全風險，請參閱日誌的以下各欄：

事件	事件類型與用戶端針對程序採取的動作，例如清除事件或記錄事件。請檢視下列事件類型： ■ 可能為合法性最低的程序會列為**「發現潛在風險」**事件。 ■ 可能為安全風險的程序會列為**「發現安全風險」**事件。
應用程式	程序名稱。
應用程式類型	SONAR 掃描偵測到的惡意軟體類型。

檔案/路徑　　程序啟動時所在路徑的名稱。

從**「事件」**欄可馬上看出偵測的程序是否為安全風險或合法性最低的程序。然而，發現的潛在風險不一定是合法程序，而發現的安全風險也不一定是惡意程序。因此，您需要檢視**「應用程式類型」**和**「檔案/路徑」**等欄，以瞭解相關資訊。例如，您可能認得第三方合法應用程式的應用程式名稱。

監控 SONAR 偵測結果來查看是否有誤報

1. 在主控台中，按下**「監控器」>「日誌」**。
2. 在「日誌」標籤的**「日誌類型」**下拉式清單中，按下 **SONAR**。
3. 從**「時間範圍」**清單方塊中，選取一個最接近上次變更掃描設定時間的時間。
4. 按下**「其他設定」**。
5. 在**「事件類型」**下拉式清單中，選取下列其中一個日誌事件：
   - 若要檢視所有偵測的程序，確定已選取**「全部」**。
   - 若要檢視已評估為安全風險的程序，請按下**「發現安全風險」**。
   - 若要檢視已評估且已記錄為潛在風險的程序，請按下**「發現潛在風險」**。
6. 按下**「檢視日誌」**。
7. 在辨識合法應用程式和安全風險之後，請在例外政策中為其建立例外。

   您可以直接從「SONAR 日誌」窗格中建立例外。

請參閱第 484 頁的「從日誌事件建立例外」。

變更竄改防護設定

「竄改防護」為伺服器及用戶端上執行的賽門鐵克應用程式提供即時防護。它可阻擋病蟲、特洛伊木馬程式、病毒和安全風險等這些非賽門鐵克的程序影響賽門鐵克資源。您可以架構用戶端，以攔截或記錄嘗試修改賽門鐵克資源的動作。您可以為「竄改防護」偵測的應用程式建立例外。

竄改防護設定會針對所選群組進行全域架構。

變更竄改防護設定

1. 在主控台中，按下**「用戶端」**。
2. 在**「政策」**標籤的**「設定」**下，按下**「一般設定」**。
3. 在**「竄改防護」**標籤上，勾選或取消勾選**「防護賽門鐵克安全軟體不受竄改或關閉」**。
4. 在**「如果應用程式嘗試竄改或關閉賽門鐵克安全軟體，要執行的動作」**下的清單方塊中，選取下列其中一個記錄動作。
5. 按下**「確定」**。

請參閱第 481 頁的「在 Windows 用戶端上建立竄改防護例外」。

22

管理應用程式控制、裝置控制和系統鎖定

本章包含以下主題：

關於應用程式控制、系統鎖定和裝置控制

若要監控和控制用戶端電腦上的應用程式行為，可以使用應用程式控制和系統鎖定。應用程式控制會在已定義的應用程式嘗試存取用戶端電腦系統資源時，加以允許或攔截。系統鎖定則只會允許已核准的應用程式在用戶端電腦上執行。若要管理存取用戶端電腦的硬體裝置，可以使用裝置控制。

警告：應用程式控制和系統鎖定是進階安全功能，僅應由具經驗的管理員進行架構。

應用程式控制、系統鎖定和裝置控制可用來完成下列工作。

應用程式控制	■ 防止惡意軟體佔據應用程式。 ■ 限制可執行的應用程式。 ■ 防止使用者變更組態檔。 ■ 保護特定的登錄機碼。 ■ 保護特定資料夾，例如 \WINDOWS\system。 可使用「應用程式控制」和「裝置控制」政策架構應用程式控制和裝置控制。 請參閱第 433 頁的「設定應用程式控制」。
系統鎖定	■ 控制用戶端電腦上的應用程式。 ■ 攔截嘗試執行或將自己載入現有應用程式的幾乎所有的特洛伊木馬程式、間諜軟體或惡意軟體。 系統鎖定能確保系統維持在已知且受信任的狀態。 **附註：**如果未審慎實作系統鎖定，則可能會導致網路發生嚴重問題。賽門鐵克建議您在特定階段實作系統鎖定。 可在**「用戶端」**頁面上的**「政策」**標籤中架構系統鎖定。 請參閱第 445 頁的「架構系統鎖定」。
裝置控制	■ 攔截或允許不同類型的裝置附加到用戶端電腦，例如 USB、紅外線和 FireWire 裝置。 ■ 攔截或允許序列埠和平行埠。 請參閱第 463 頁的「管理裝置控制」。

應用程式控制與裝置控制在 32 位元和 64 位元 Windows 電腦上均受支援。

自 14 版起，Mac 電腦上即支援使用裝置控制。

設定應用程式控制

應用程式控制會在已定義的應用程式嘗試存取用戶端電腦系統資源時，加以允許或攔截。您可以允許或攔截對特定登錄機碼、檔案和資料夾的存取。您也可以定義哪些應用程式可以執行、哪些應用程式不能透過異常程序終止，以及哪些應用程式可以呼叫 DLL。

使用下列步驟可在一組用戶端電腦上設定應用程式控制。

表 22-1 設定應用程式控制

步驟	敘述
開啟政策並啟用預設應用程式控制規則集	「應用程式控制」政策包含預先定義的規則集，而這些規則集預設會停用。您可以啟用任何需要的規則集，然後將政策套用至群組。預先定義的規則集是在生產模式而非測試模式下進行架構。但是，您應該將設定變更為測試模式，然後在測試網路中測試這些規則，之後才將這些規則套用至生產網路。 請參閱第 435 頁的「啟用和測試預設應用程式規則」。
新增其他應用程式控制規則 (選擇性)	如果預設規則集不符合您的需求，請新增規則集與規則。此工作通常只應由進階管理員執行。 請參閱第 438 頁的「將自訂規則新增至應用程式控制」。
針對應用程式新增例外	應用程式控制會在部分應用程式中插入程式碼來對其進行檢查，如此可能會讓電腦上執行的應用程式變慢。如有必要，您可以從應用程式控制中排除部分應用程式。可使用例外政策針對應用程式控制新增檔案例外或資料夾例外。 請參閱第 475 頁的「從掃描中排除檔案或資料夾」。
檢視應用程式控制日誌	如果您要測試新的政策或是對問題進行疑難排解，則應該監控此日誌中的應用程式控制事件。 在測試模式和生產模式中，應用程式控制事件均是記錄在 Symantec Endpoint Protection Manager 的應用程式控制日誌中。在用戶端電腦上，應用程式控制和裝置控制事件會顯示在「控制」日誌中。 一項應用程式控制動作可能會顯示有重複或多個日誌項目。例如，explorer.exe 在嘗試複製檔案時，會設定檔案存取遮罩的寫入位元和刪除位元。Symantec Endpoint Protection 會記錄該事件。如果複製動作因應用程式控制規則攔截這個動作而失敗，explorer.exe 會嘗試僅使用存取遮罩中的刪除位元來複製檔案。Symantec Endpoint Protection 會針對該複製嘗試記錄另外一個事件。 請參閱第 563 頁的「檢視日誌」。
阻止或允許使用者啟用或停用應用程式控制 (選擇性)	在極少數情況下，應用程式控制可能會干擾用戶端電腦上執行的某些安全應用程式。您可能想要允許使用者停用此選項來對問題進行疑難排解。在混合模式或用戶端模式下，使用**「用戶端使用者介面設定」**對話方塊中的**「允許使用者啟用和停用應用程式裝置控制」**設定。 請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

您也可以使用系統鎖定，在用戶端電腦上允許核准的應用程式或是攔截未核准的應用程式。

請參閱第 445 頁的「架構系統鎖定」。

啟用和測試預設應用程式規則

應用程式控制包括由一或多個規則組成的預設規則集。預設應用程式控制規則集會隨 Symantec Endpoint Protection Manager 一起安裝。預設規則集在安裝時是停用的。要在應用程式控制政策中使用預設規則集，您必須啟用它們並將政策套用至用戶端群組。

如需常見預先定義之規則的說明，請參閱：強化 Symantec Endpoint Protection (SEP)：使用應用程式與裝置控制政策來提升安全性

在下列工作中，您可以啟用和測試**「攔截向 USB 磁碟機寫入內容」**規則集。

啟用預設應用程式規則集

1. 在主控台中，按下**「政策」**>**「應用程式與裝置控制」**，然後在**「工作」**下方，按下**「新增應用程式控制政策」**。
2. 在**「概述」**窗格中，輸入政策的名稱和說明。
3. 按下**「應用程式控制」**。
4. 在**「應用程式控制」**窗格中，勾選您要實作的每個規則集旁的**「已啟用」**核取方塊。

   例如，在**「攔截向 USB 磁碟機寫入內容」**規則集旁，勾選「已啟用」欄中的核取方塊。
5. 要檢閱規則集的規則，請選取規則，按下**「編輯」**，然後按下**「確定」**。

   請參閱第 438 頁的「將自訂規則新增至應用程式控制」。
6. 將**「生產」**變更為**「測試 (只記錄)」**。
7. 指派政策給群組，然後按下**「確定」**。

測試攔截向 USB 磁碟機寫入內容規則集

1. 在用戶端電腦上，連接 USB 磁碟機。
2. 開啟「Windows 檔案總管」，然後連按兩下 USB 磁碟機。
3. 以滑鼠右鍵按下視窗，然後按下**「新增」**>**「資料夾」**。

   如果應用程式控制已生效，就會出現**「無法建立資料夾」**錯誤訊息。

請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。

請參閱第 435 頁的「關於應用程式控制與裝置控制政策的結構」。

關於應用程式控制與裝置控制政策的結構

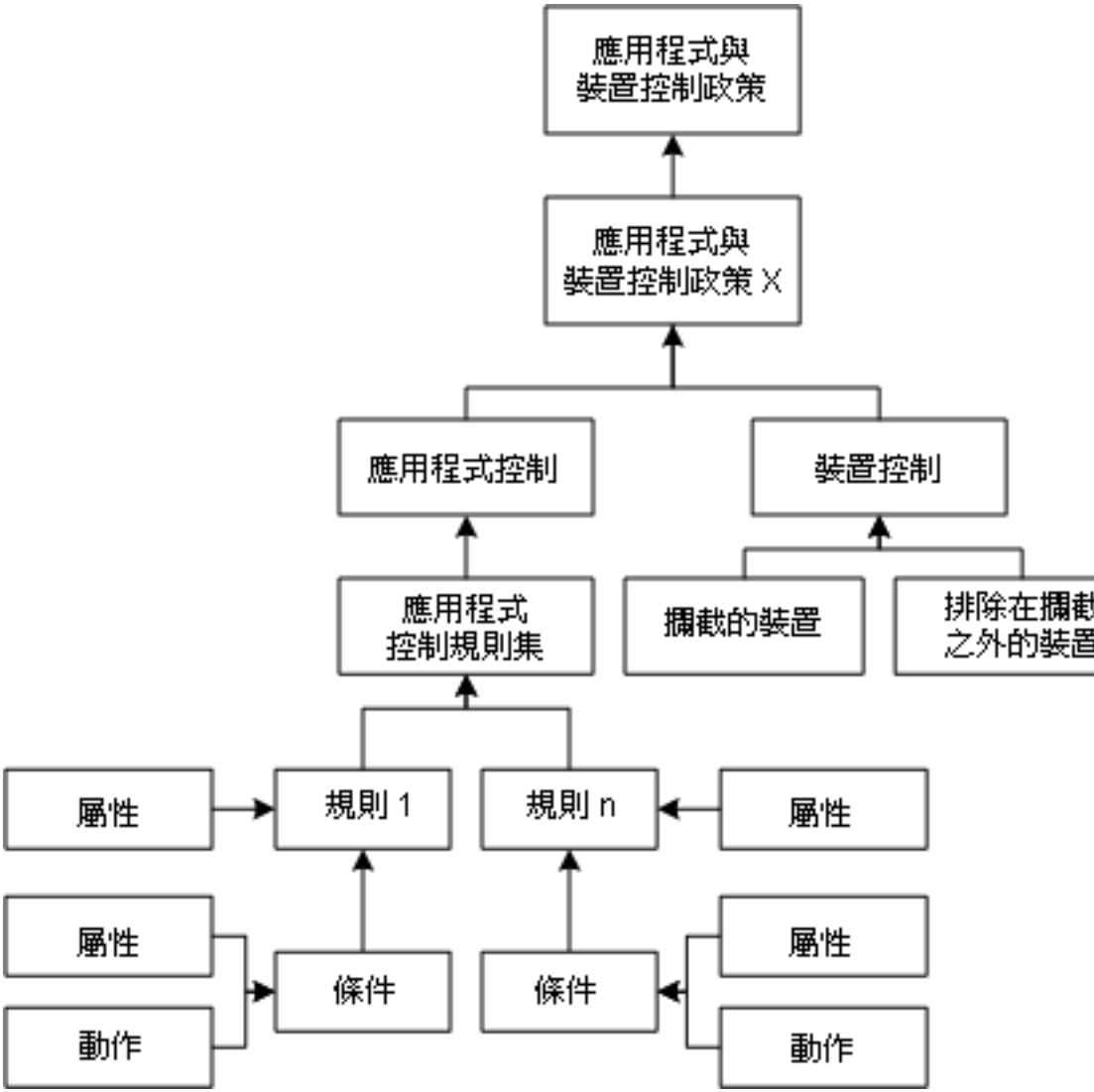
「應用程式與裝置控制」政策分兩個部分：

- 「應用程式控制」包含一或多個規則集。每個規則集都包含一或多個規則。您可以架構各項規則的屬性、條件和動作：
  - **「規則」**：定義您要監控的應用程式。

  - **「條件」**：監控規則中定義之應用程式的指定操作。條件也包含觀察到指定操作時要採取的動作。
  - 新增規則和條件時，您需要指定條件的特定**「屬性」**以及符合條件時要採取的動作。每種條件類型包含的屬性皆不同。
- 裝置控制包含攔截的裝置清單及不攔截的裝置清單。您可以新增至這兩份清單，並管理其中的內容。

圖 22-1 說明應用程式和裝置控制元件，以及兩者之間的關係。

圖 22-1　　應用程式與裝置控制政策結構



請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。
請參閱第 433 頁的「設定應用程式控制」。
請參閱第 438 頁的「將自訂規則新增至應用程式控制」。
請參閱第 463 頁的「管理裝置控制」。

將自訂規則新增至應用程式控制

如果預設規則集不符合您的需求，請新增規則集與規則。您可以修改隨政策安裝的預先定義的規則集。

- 規則集是一個配置區，其中包含一或多個允許或攔截動作的規則。
- 規則集中的規則則定義一或多個程序或應用程式。您也可以排除不要監控的程序。
- 每個規則包含要套用至特定程序的條件和動作。對於各項條件，您可以架構符合條件時要採取的動作。您可以架構規則只套用於某些應用程式，也可以架構規則排除動作套用於其他應用程式。

請參閱第 435 頁的「關於應用程式控制與裝置控制政策的結構」。

使用下列步驟來自行新增應用程式規則：

- 步驟 1：新增自訂規則集和規則
- 步驟 2：為規則定義應用程式或程序
- 步驟 3：將條件和動作新增至規則
- 步驟 4：在將規則套用至生產網路前先測試規則。
  請參閱第 444 頁的「測試應用程式控制規則」。

步驟 1：新增自訂規則集和規則

最佳實務準則是建立一個規則集，並在其中納入所有允許、攔截和監控指定工作的動作。另一方面，如果您有多個工作，則應該建立多個規則集。例如，如果您想要攔截所有嘗試寫入抽取式磁碟機的動作，並且想要攔截對特定應用程式進行篡改的應用程式，則應該建立兩個規則集。您可以按需新增及啟用任何數目的規則集與規則。

例如，BitTorrent 是一項用於點對點檔案共用的通訊協定，其本身並不安全。BitTorrent 會散佈電影、遊戲、音樂和其他檔案。BitTorrent 可謂散佈威脅最簡單的方法之一。惡意軟體會隱藏在透過點對點網路來共用的檔案內。您可以使用應用程式控制來攔截對 BitTorrent 通訊協定的存取。您也可以使用點對點驗證和入侵預防。請參閱第 531 頁的「透過架構點對點驗證攔截遠端電腦」。

架構規則及其條件時，請考慮順序問題，以免發生無法預期的結果。此工作通常只應由進階管理員執行。

請參閱第 441 頁的「新增應用程式控制規則的最佳實務準則」。

新增自訂規則集和規則

1 開啟應用程式控制政策。

請參閱第 435 頁的「啟用和測試預設應用程式規則」。

2 在「**應用程式控制**」面板的預設規則集清單下方，按下「**新增**」。

若要修改預先定義的規則集，請將其選取，然後按下「**編輯**」。例如，若要監控存取 BitTorrent 通訊協定的應用程式，請選取「**攔截從抽取式磁碟機執行程式 [AC2]**」。

3 在「**新增應用程式控制規則集**」對話方塊中，為規則集輸入名稱和敘述。

4 在「規則」下方，選取「**規則 1**」，然後在「**屬性**」標籤上，為規則輸入有意義的名稱和敘述。

若要新增其他規則，請按下「**新增**」>「**新增規則**」。

步驟 2：為規則定義應用程式或程序

每項規則均必須包含至少一個要在用戶端電腦上監控的應用程式或程序。您也可以從規則中排除特定應用程式。

為規則定義應用程式或程序

1 選取規則後，在「**屬性**」標籤的「**套用此規則至下列程序**」旁邊，按下「**新增**」。

2 在「**新增程序定義**」對話方塊中，輸入應用程式名稱或程序名稱，例如`bittorrent.exe`。

如果您想將這項規則套用至某組應用程式以外的其他所有應用程式，請在這個步驟中定義代表全部之意的萬用字元 (*)。然後，在「**請勿套用此規則至下列程序**」旁邊，列出需要當作例外的應用程式。

3 按下「**確定**」。

「**啟用此規則**」核取方塊預設為啟用狀態。如果取消勾選此選項，則不會套用規則。

步驟 3：將條件和動作新增至規則

條件可控制嘗試在用戶端電腦上執行的應用程式或程序的行為。每種條件類型均有專屬的屬性來指定條件要尋找的情況。

每個條件均各自設有當條件成立時，要對程序採取的特定動作。動作 (「**終止程序**」動作除外) 一律會套用至您為*「規則」* (而非*「條件」*) 定義的程序。

警告：「終止程序」動作會終止呼叫者程序或是提出要求的應用程式。呼叫者程序是您在規則中 (而非在條件中) 定義的程序。對目標程序執行的其他動作則在條件中定義。

請參閱第 442 頁的「選擇用於規則之條件的最佳實務準則」。

條件	敘述
登錄存取嘗試	允許或攔截對用戶端電腦上登錄設定的存取
檔案和資料夾存取嘗試	允許或攔截對用戶端電腦上所定義檔案或資料夾的存取
啟動程序嘗試	允許或攔截在用戶端電腦上啟動程序的動作。
終止程序嘗試	允許或攔截在用戶端電腦上終止程序的動作。例如，您可能需要攔截將特定應用程式停止的動作。 **警告：**則「終止程序嘗試」條件會參考*「目標」*程序。如果您對 Symantec Endpoint Protection 或其他重要程序使用**「終止程序嘗試」**條件，然後使用**「終止程序」**動作來刪除嘗試刪除 Symantec Endpoint Protection 的程序。
載入 DLL 嘗試	允許或攔截在用戶端電腦載入 DLL 的動作。

將條件和動作新增至規則

1. 在**「規則」**下，選取您新增的規則，按下**「新增」**>**「新增條件」**，然後選擇條件。

   請參閱第 442 頁的「選擇用於規則之條件的最佳實務準則」。

   例如，按下**「啟動程序嘗試」**，即可新增要在用戶端電腦存取 BitTorrent 通訊協定時套用的條件。

2. 在**「屬性」**標籤上，選取應該或不應該啟動的程序：

   - 指定要啟動的程序：
     在**「套用至下列*實體*」**旁邊，按下**「新增」**。
   - 排除不要啟動的程序：
     在**「請勿套用至下列程序」**旁邊，按下**「新增」**。

3. 在**「新增*實體*定義」**對話方塊中，輸入程序名稱、DLL 或登錄機碼。

   例如，若要新增 BitTorrent，請輸入其檔案路徑和可執行檔，例如：
   `C:\Users\UserName\AppData\Roaming\BitTorrent`

   若要將條件套用至特定資料夾中的所有程序，最佳實務準則是使用 *folder_name** 或 *folder_name***。一個星號即包括指名資料夾中全部的檔案和資料夾。使用 *folder_name*** 可包含指名資料夾中各個檔案和資料夾，以及各個子資料夾中各個檔案和資料夾。

4. 按下**「確定」**。

5. 在條件的**「動作」**標籤上，選取要採取的動作。

   例如，若要在 Textpad 嘗試啟動 Firefox 時加以攔截，請按下**「攔截存取」**。

6 核取**「啟用記錄」**和**「通知使用者」**，然後新增要向用戶端電腦使用者顯示的訊息。

例如，輸入 **Textpad tries to launch Firefox**。

7 按下**「確定」**。

此時會顯示新規則集，並會針對測試模式架構此規則集。 您應該先測試新規則集，再將其套用至用戶端電腦。

新增應用程式控制規則的最佳實務準則

您應該審慎規劃自訂應用程式控制規則。建立應用程式控制規則時，請記住以下最佳實務準則。

表 22-2 應用程式控制規則的最佳實務準則

最佳實務準則	敘述	範例
考慮規則順序	應用程式控制規則的運作方式類似於大多數網路型防火牆規則，兩者都是使用第一個規則相符的功能。 如果滿足多個條件時，第一個規則會是套用的唯一規則，除非為此規則架構的動作為**「繼續處理其他規則」**。	您希望防止所有使用者在 USB 磁碟機上移動、複製和建立檔案。 您具有一個現有規則，該規則具有一個條件允許寫入存取名為 Test.doc 的檔案。 您可以將第二個條件新增至這個現有規則集，以攔截所有 USB 磁碟機。 在這種情況下，使用者仍可以建立和修改 USB 磁碟上的 Test.doc 檔案。 在規則集中，**「允許存取」**Test.doc 的條件會在**「攔截存取」** USB 磁碟機的條件之前。 當滿足清單中**「攔截存取」** USB 磁碟機的條件前面的條件時，便不會處理這個「攔截存取」條件。
使用正確的動作	**「終止程序嘗試」**條件會允許或攔截應用程式在用戶端電腦上終止呼叫程序的動作。 此條件不會允許或攔截使用者採用平常的方法停止應用程式，例如按下「檔案」功能表中的「結束」。	Process Explorer 是一項工具，可顯示已開啟或載入的 DLL 程序，以及程序使用哪些資源。 您可能希望在 Process Explorer 嘗試終止特定應用程式時終止 Process Explorer。 使用**「終止程序嘗試」**條件和**「終止程序」**動作建立此類型的規則。 您可以將此條件套用至 Process Explorer 應用程式。 您可以將此規則套用至您不希望 Process Explorer 終止的一個或多個應用程式。
每個目標各使用一個規則集	建立一個規則集，並在其中納入所有允許、攔截或監控特定工作的動作。	您想要攔截所有嘗試寫入抽取式磁碟機的動作，並且想要攔截對特定應用程式進行篡改的應用程式。 若要實現這些目標，應該建立兩個不同的規則集，而不是建立單一規則集。

最佳實務準則	敘述	範例
謹慎使用「**終止程序**」動作	當呼叫程序滿足所架構的條件時，「**終止程序**」動作會刪除該程序。 只有進階管理員才可使用「**終止程序**」動作。通常，您應該改用「**攔截存取**」動作。	您希望在任何程序啟動 Winword.exe 時隨時終止 Winword.exe。 您可以建立一個規則，並使用「**啟動程序嘗試**」條件和「**終止程序**」動作架構此規則。 您將條件套用於 Winword.exe，並且將規則套用於全部的程序。 您可能希望此規則終止 Winword.exe，但此規則未執行這個動作。 如果您嘗試從「Windows 檔案總管」啟動 Winword.exe，包含此組態的規則會終止 Explorer.exe，而非 Winword.exe。如果使用者直接啟動 Winword.exe，則仍可執行該程式。請改用「**攔截存取**」動作來攔截目標程序，或 Winword.exe。
在將規則投入生產環境之前先測試規則	規則集的「**測試 (只記錄)**」選項僅會記錄動作，而不會將動作套用至用戶端電腦。在將規則切換回生產模式之前，請先以測試模式執行規則達某段可接受的時間長度。在此期間，可檢閱應用程式控制日誌，並確認規則是否會按計劃運作。	測試選項將會減少因未考量規則的所有可能性而引起的潛在意外。 請參閱第 444 頁的「測試應用程式控制規則」。

請參閱第 438 頁的「將自訂規則新增至應用程式控制」。

請參閱第 442 頁的「選擇用於規則之條件的最佳實務準則」。

選擇用於規則之條件的最佳實務準則

您可以新增自訂應用程式控制規則和條件，以防止使用者開啟應用程式、寫入檔案或共用檔案。如不知該如何設定規則，不妨參考預設規則集。例如，您可以編輯「**攔阻應用程式執行**」規則集，以檢視如何使用「**啟動程序嘗試**」條件。

請參閱第 438 頁的「將自訂規則新增至應用程式控制」。

表 22-3 用於規則的一般條件

規則	條件
防止使用者開啟應用程式	當應用程式滿足下列條件之一時，您可以攔截它： ■ **啟動程序嘗試** 例如，若要防止使用者傳輸 FTP 檔案，您可以新增規則來攔截使用者從指令提示啟動 FTP 用戶端。 ■ **載入 DLL 嘗試** 例如，如果您新增在用戶端電腦上攔截 Msvcrt.dll 的規則，則使用者將無法開啟 Microsoft WordPad。 此規則還會攔截使用 DLL 的任何其他應用程式。
防止使用者寫入特定檔案	您可能想要允許使用者開啟某個檔案，但不能修改檔案。例如，檔案可能包含員工應檢視但不該編輯的財務資料。 您可以建立規則，將檔案的唯讀存取權限授予使用者。 例如，您可以新增規則，來允許您在記事本中開啟文字檔案而不允許您編輯此檔案。 針對此類型的規則使用**「檔案和資料夾存取嘗試」**條件。
在 Windows 電腦上攔截檔案共用	您可以在 Windows 電腦上停用本機檔案和列印共用。 包括下列條件： ■ **登錄存取嘗試** 新增所有相關的 Windows 安全性和共用登錄機碼。 ■ **啟動程序嘗試** 指定伺服器服務程序 (svchost.exe)。 ■ **載入 DLL 嘗試** 指定「安全性」和「共用」標籤的 DLL (rshx32.dll、ntshrui.dll) 。 ■ **載入 DLL 嘗試** 指定伺服器服務 DLL (srvsvc.dll)。 您可以將各個條件的動作設定為**「攔截存取」**。 您還可以使用防火牆規則來阻止或允許用戶端電腦共用檔案。 請參閱第 316 頁的「允許用戶端瀏覽網路中的檔案和印表機」。
防止使用者執行點對點應用程式	您可以防止使用者在其電腦上執行點對點應用程式。 您可以建立具有**「啟動程序嘗試」**條件的自訂規則。 在此條件中，您必須指定所有要攔截的點對點應用程式，例如 LimeWire.exe 或 *.torrent。 您可以將條件的動作設定為**「拒絕存取」**。 使用「入侵預防」政策攔截來自點對點應用程式的網路流量。使用防火牆政策攔截傳送和接收點對點應用程式流量的通訊埠。 請參閱第 325 頁的「管理入侵預防」。 請參閱第 291 頁的「建立防火牆政策」。

規則	條件
攔截嘗試寫入 DVD 光碟機	目前，應用程式控制不具有可直接攔截 CD/DVD 寫入的預設規則。相反地，您可以使用**「新增條件」**和**「檔案和資料夾存取嘗試」**條件建立攔截寫入 CD 或 DVD 磁碟機之特定 DLL 的規則。 您還應建立設定 Windows 登錄機碼的主機完整性政策，以攔截對 DVD 磁碟機的寫入嘗試。 請參閱第 524 頁的「設定主機完整性」。 請參閱：如何在 Windows 7 中攔截 CD/DVD 寫入

測試應用程式控制規則

新增應用程式控制規則後，您應該在自己的網路中測試這些規則。「應用程式控制」政策中使用的規則集若發生架構錯誤，可能會使電腦或伺服器無法運作。用戶端電腦可能會失敗，或是其與 Symantec Endpoint Protection Manager 之間的通訊可能會遭到攔截。測試好規則後，即可將其套用至您的生產網路。

步驟 1：將規則集設定為測試模式

您可以將模式設定為測試模式來測試規則集。測試模式會建立一個日誌項目，用以指示何時套用規則集中的規則 (實際上並不會套用這些規則)。

預設規則預設會使用生產模式。自訂規則預設會使用測試模式。您應該同時測試預設和自訂規則集。

您可能希望個別測試規則集中的規則。您可以在規則集中啟用或停用規則來測試各個規則。

將規則集變更為測試模式

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 在**「應用程式控制政策」**下方，按下**「應用程式控制」**。
3. 在**「應用程式控制規則集」**清單中，針對規則集按下**「測試/正式」**欄中的下拉式箭頭，然後按下**「測試 (只記錄)」**。

請參閱第 433 頁的「設定應用程式控制」。

步驟 2：將「應用程式與裝置控制」政策套用至測試網路中的電腦

如果您建立了新的「應用程式與裝置控制」政策，請將此政策套用至測試網路中的用戶端。

請參閱第 275 頁的「指派政策給群組或位置」。

步驟 3：監控應用程式控制日誌

規則集在測試模式下執行一段時間後，可檢查日誌是否有任何錯誤。在測試模式和生產模式中，應用程式控制事件均是記錄在 Symantec Endpoint Protection Manager 的應用程式控制日誌中。在用戶端電腦上，應用程式控制和裝置控制事件會顯示在「控制」日誌中。

一項應用程式控制動作可能會顯示有重複或多個日誌項目。例如，explorer.exe 在嘗試複製檔案時，會設定檔案存取遮罩的寫入位元和刪除位元。Symantec Endpoint Protection 會記錄該事件。如果複製動作因應用程式控制規則攔截這個動作而失敗，explorer.exe 會嘗試僅使用存取遮罩中的刪除位元來複製檔案。Symantec Endpoint Protection 會針對該複製嘗試記錄另外一個事件。

請參閱第 563 頁的「檢視日誌」。

步驟 4：將規則集變更回生產模式

如果規則如預期般執行，可將規則集模式變更回生產模式。

架構系統鎖定

系統鎖定透過攔截未核准的應用程式來控制一組用戶端電腦上的應用程式。 您可以設定系統鎖定以允許指定清單 (許可清單) 上僅有的應用程式。 許可清單包括所有已核准的應用程式；任何其他應用程式則會在用戶端電腦上遭到攔截。 或者，可以設定系統鎖定以攔截指定清單 (黑名單) 上僅有的應用程式。 黑名單包括所有未核准的應用程式；用戶端電腦上被允許的任何其他應用程式。

附註：系統鎖定允許的所有應用程式受 Symantec Endpoint Protection 中的其他保護功能支配。

許可清單或黑名單可包括檔案指紋清單和特定的應用程式名稱。 檔案指紋清單是檔案總和檢查碼和電腦路徑位置的清單。

您可以使用「應用程式與裝置控制」政策而不使用系統鎖定來控制特定的應用程式，也可以既使用「應用程式與裝置控制」政策又使用系統鎖定。

您需要針對網路中的每個群組或位置設定系統鎖定。

表 22-4 系統鎖定步驟

動作	敘述
步驟 1：建立檔案指紋清單	您可以建立一個檔案指紋清單，其中包含允許或不允許在用戶端電腦上執行的應用程式。 使用檔案指紋清單作為系統鎖定中許可清單或黑名單的一部分。 當您執行系統鎖定時，需要使用包括您想要列入許可清單或黑名單的所有應用程式的檔案指紋清單。例如，您的網路可能包括 Windows Vista 32 位元、Windows Vista 64 位元和 Windows XP SP2 用戶端。 您可以針對許可清單中的每一個用戶端影像建立檔案指紋清單。 您可透過下列方法建立檔案指紋清單： ■ Symantec Endpoint Protection 提供了一個可建立檔案指紋清單的總和檢查碼公用程式。 此公用程式會隨 Symantec Endpoint Protection 一起安裝在用戶端電腦上。 使用此公用程式在指定路徑中建立特定應用程式或所有應用程式的總和檢查碼。 使用此方法產生在黑名單模式下執行系統鎖定時使用的檔案指紋。 請參閱第 449 頁的「以 checksum.exe 建立檔案指紋清單」。 ■ 使用「收集檔案指紋清單」指令，在單一電腦或一小群電腦上建立檔案指紋清單。 在 12.1.6 或更新版本中，您可以從主控台執行「收集檔案指紋清單」指令。指令會收集包含目標電腦上每個應用程式的檔案指紋清單。 例如，您可能會在執行金影像的電腦上執行指令。 在許可清單模式下執行系統鎖定時，您可以使用此方法。請注意，您使用此指令產生的檔案指紋清單無法修改。重新執行此指令時，檔案指紋清單會自動更新。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。 ■ 使用任何第三方總和檢查碼公用程式來建立檔案指紋清單。 **附註：**在 12.1.6 或更新版本中，如果您在自己的網路中執行 Symantec EDR，可能會看到來自 Symantec EDR 的檔案指紋清單。 請參閱第 452 頁的「系統鎖定與 Symantec EDR 黑名單規則之間的互動」。
步驟 2：將檔案指紋清單匯入 Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager 必須提供清單，您才能在系統鎖定架構中使用檔案指紋清單。 使用總和檢查碼工具建立檔案指紋清單時，您必須將清單手動匯入 Symantec Endpoint Protection Manager。 請參閱第 451 頁的「在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單」。 使用收集檔案指紋清單指令建立檔案指紋清單時，產生的清單會自動在 Symantec Endpoint Protection Manager 主控台中提供使用。 您也可以從 Symantec Endpoint Protection Manager 匯出現有的檔案指紋清單。

動作	敘述
步驟3：建立已核准或未核准應用程式的應用程式名稱清單	可以使用任意文字編輯器來建立一個文字檔，其中包括您所需許可清單或黑名單中的應用程式的檔案名稱。與檔案指紋清單不同，可以直接將這些檔案匯入系統鎖定架構。匯入檔案後，應用程式會以個別項目出現在系統鎖定架構中。 也可以在系統鎖定架構中手動輸入個別的應用程式名稱。 **附註：**當以黑名單模式啟用系統鎖定時，大量的指定應用程式可能會影響用戶端電腦效能。 請參閱第 453 頁的「建立應用程式名稱清單以匯入系統鎖定架構中」。
步驟 4：設定及測試系統鎖定架構	在測試模式下，系統鎖定處於停用且不攔截任何應用程式。所有未核准應用程式都會被記錄，但不會遭到攔截。需要使用**「系統鎖定」**對話方塊中的**「記錄未核准的應用程式」**選項測試整個系統鎖定架構。 若要設定和執行測試，請完成下列步驟： ■ 將檔案指紋清單新增到系統鎖定架構。 在許可清單模式下，檔案指紋是已核准的應用程式。 在黑名單模式下，檔案指紋是未核准的應用程式。 ■ 新增個別應用程式名稱或將應用程式名稱清單匯入系統鎖定架構。 可以匯入應用程式名稱清單，不用在系統鎖定架構中逐一輸入名稱。 在許可清單模式下，應用程式是已核准的應用程式。 在黑名單模式下，應用程式是未核准的應用程式。 ■ 執行一段時間的測試。 在測試模式下執行系統鎖定的時間應夠長，以便客戶端執行其平常的應用程式。 通常可能是一週的時間範圍。 請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。
步驟5：檢視未核准的應用程式，並視需要修改系統鎖定架構	執行一段時間的測試後，可以檢查未核准的應用程式清單。 可以在**「系統鎖定」**對話方塊中檢查狀態，以檢視未核准的應用程式清單。 記錄的事件也會出現在「應用程式控制」日誌中。 可以決定是否新增更多應用程式至檔案指紋或應用程式清單中。啟用系統鎖定之前，也可以視需要新增或移除檔案指紋清單或應用程式。 請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

動作	敘述
步驟 6：啟用系統鎖定	系統鎖定預設會在許可清單模式下執行。 您可架構系統鎖定以改在黑名單模式下執行。 當在許可清單模式中啟用系統鎖定時，會攔截不在核准的應用程式清單上的所有應用程式。當在黑名單模式下啟用系統鎖定時，會攔截在未核准的應用程式清單上的所有應用程式。 **附註：**確定在啟用系統鎖定之前，已測試您的架構。 如果攔截了必要的應用程式，用戶端電腦可能無法重新啟動。 請參閱第 460 頁的「在許可清單模式下執行系統鎖定」。 請參閱第 461 頁的「在黑名單模式下執行系統鎖定」。
步驟7：更新進行系統鎖定所需的檔案指紋清單	您可能會隨時間變更網路中執行的應用程式。 可以根據需要更新或移除檔案指紋清單。 您可以用下列方式更新檔案指紋清單： ■ 請手動附加、取代或合併您匯入的檔案指紋清單。 您無法將檔案指紋清單附加至您使用收集檔案指紋清單指令產生的指紋清單。 您可以使用指令產生的清單附加匯入的清單。 在該情況下，如果您重新執行指紋指令，則必須重新建立附加的清單。 請參閱第 452 頁的「手動更新 Symantec Endpoint Protection Manager 中的檔案指紋清單」。 請參閱第 451 頁的「在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單」。 ■ 自動更新您匯入的現有檔案指紋清單。 也可以自動更新您匯入的應用程式或應用程式名稱清單。 請參閱第 454 頁的「自動更新系統鎖定的許可清單或黑名單」。 請參閱第 453 頁的「建立應用程式名稱清單以匯入系統鎖定架構中」。 ■ 重新執行收集檔案指紋清單指令以自動更新指令產生的指紋清單。 當您重新執行此指令時，新清單會自動取代現有清單。 **附註：**在將用戶端電腦新增到網路中後，您可能想要重新測試整個系統鎖定架構。 可以將新的用戶端移動到獨立群組或測試網路及停用系統鎖定。 或者，您可以保持系統鎖定啟用，並在只記錄模式下執行架構。 也可以依照下一個步驟中的描述，測試個別檔案指紋或應用程式。 請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

動作	敘述
步驟8：當系統鎖定啟用後，在新增或移除選取的項目之前對其進行測試	當系統鎖定啟用後，在系統鎖定架構中新增或移除個別檔案指紋、應用程式名稱清單或特定應用程式前，可以對它們進行測試。 如果有許多檔案指紋清單並且其中一部分不再使用，您可能想要移除清單。 **附註：**從系統鎖定新增或移除檔案指紋清單或特定應用程式時，請小心。 從系統鎖定新增或移除項目可能會有風險。 可能會攔截用戶端電腦上的重要應用程式。 ■ 測試選取項目。 使用**「移除前測試」**，將特定的檔案指紋清單或特定應用程式記錄為未核准。 執行此測試時，會啟用系統鎖定，但不攔截所選取的任何應用程式，或選取的檔案指紋清單中的任何應用程式。 而是系統鎖定將應用程式記錄為未核准。 ■ 檢查「應用程式控制」日誌。 日誌項目會出現在「應用程式控制」日誌中。 如果此日誌不包含測試的應用程式項目，則可以確定用戶端未使用這些應用程式。 請參閱第 462 頁的「當系統鎖定已啟用後，在新增或移除選取的項目之前對它們進行測試」。

請參閱第 433 頁的「設定應用程式控制」。

以 checksum.exe 建立檔案指紋清單

您可以使用 checksum.exe 公用程式來建立檔案指紋清單。 此清單包含位於電腦上指定路徑中每個執行檔或 DLL 的以下內容：

- 路徑
- 檔案名稱
- 對應的總和檢查碼

然後，將檔案指紋清單匯入 Symantec Endpoint Protection Manager，以用於您的系統鎖定組態中。

此公用程式會隨 Symantec Endpoint Protection 一起安裝在用戶端電腦上。

請參閱第 451 頁的「在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單」。

請參閱第 445 頁的「架構系統鎖定」。

您還可使用第三方公用程式或「收集檔案指紋清單」指令來建立檔案指紋清單。

請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

以 checksum.exe 建立檔案指紋清單

1 在包含要建立其檔案指紋清單之影像的電腦上，開啟命令提示視窗。

電腦必須已安裝了 Symantec Endpoint Protection 用戶端軟體。

2 瀏覽到用戶端安裝資料夾，其中包含 checksum.exe 檔案。一般而言，檔案位於以下資料夾中：

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\

3 輸入下列指令：

```
checksum.exe outputfile.txt path
```

其中：

- *outputfile.txt* 為產生之文字檔案的名稱，其中包含指定磁碟機上所有應用程式的總和檢查碼。
- *path* 為您要在其上收集總和檢查碼資訊的電腦上的檔案路徑。

附註：若要針對 C 磁碟機上的所有檔案執行總和檢查碼，必須在 *path* 的末尾新增正斜線。否則，該指令僅在 `checksum.exe` 所在資料夾中執行。

輸出檔案中的每一行格式如下：

checksum_of_the_filefull_pathname_of_the_exe_or_DLL

以空格分隔總和檢查碼值和完整路徑名稱。

checksum.exe 輸出的範例如下所示：

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
```

語法範例

下列是您可以用來為 C 磁碟機上所有檔案建立指紋清單的語法範例：

```
checksum.exe cdrive.txt c:/
```

此指令會建立名稱為 cdrive.txt 的檔案。它包含所有可執行檔和 DLL (在執行所在之電腦的 C 磁碟機上找到) 的總和檢查碼和檔案路徑。

下列是您可以用來在用戶端電腦上建立資料夾指紋的語法範例：

```
checksum.exe blocklist.txt c:\Files
```

此指令會建立名稱為 blocklist.txt 的檔案。 該檔案包含「檔案」資料夾中找到的任何執行檔和 DLL 的總和檢查碼和檔案路徑。

在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單

Symantec Endpoint Protection Manager 主控台必須提供檔案指紋清單，以便將這些清單新增到系統鎖定架構。 使用 checksum.exe 公用程式或第三方總和檢查碼工具建立檔案指紋清單時，必須手動匯入這些清單。 還可以合併檔案指紋清單。

您使用收集檔案指紋清單指令建立的檔案指紋清單會自動在主控台提供使用。 您不需匯入它們。 您不可修改使用收集檔案指紋清單指令建立的檔案指紋清單。 不過，您可以將指令產生的檔案指紋清單與另一個檔案指紋清單合併。 如果您再次執行此指令以重新產生清單，則必須再次手動合併清單。

請參閱第 445 頁的「架構系統鎖定」。

請參閱第 449 頁的「以 checksum.exe 建立檔案指紋清單」。

匯入或合併檔案指紋清單

1. 在主控台中，按下**「政策」**。
2. 在**「政策」**下方，展開**「政策元件」**，然後按下**「檔案指紋清單」**。
3. 在**「工作」**下，按下**「新增檔案指紋清單」**。
4. 在**「歡迎使用新增檔案指紋精靈」**中，按**「下一步」**。
5. 在**「新檔案指紋的相關資訊」**面板中，鍵入新清單的名稱和敘述。
6. 按**「下一步」**。
7. 在**「建立檔案指紋」**面板中，選取下列選項之一：
   - **透過匯入指紋檔案建立檔案指紋**
   - **透過合併多個現有檔案指紋建立檔案指紋**
     只有在您已匯入多個檔案指紋清單時，才可使用此選項。
8. 按**「下一步」**。
9. 執行下列其中一項動作：
   - 指定所建立的檔案指紋的路徑。 您可以瀏覽尋找該檔案。
   - 選取您要合併的指紋清單。
10. 按**「下一步」**。
11. 按下**「關閉」**。
12. 按下**「完成」**。

    匯入或合併的指紋清單會顯示在**「政策 > 政策元件 > 檔案指紋清單」**下的**「政策」**標籤下方。

手動更新 Symantec Endpoint Protection Manager 中的檔案指紋清單

在執行系統鎖定一段時間之後，您可能會想要更新檔案指紋清單。您可以附加、取代或移除已匯入的現有檔案指紋清單中的項目。您無法直接編輯 Symantec Endpoint Protection Manager 中任何現有的檔案指紋清單。

若您要將指紋清單合併到不同名稱的新清單，請使用**「新增檔案指紋精靈」**。

如果您使用收集檔案指紋清單指令建立指紋清單，則不可附加、取代或移除項目。不過，您可以將指令產生的清單附加至匯入的清單。如果您重新執行此指令，則必須再次手動更新指紋清單。

您無法修改 Symantec EDR 傳送至 Symantec Endpoint Protection Manager 的任何檔案指紋清單。

請參閱第 451 頁的「在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單」。

請參閱第 445 頁的「架構系統鎖定」。

更新 Symantec Endpoint Protection Manager 中的檔案指紋清單

1. 在主控台中，按下**「政策」**。
2. 在**「政策」**下方，展開**「政策元件」**，然後按下**「檔案指紋清單」**。
3. 在**「檔案指紋清單」**窗格中，選取要編輯的指紋清單。
4. 按下 **Edit**。
5. 在**「編輯檔案指紋精靈」**中，按**「下一步」**。
6. 執行下列其中一個動作：
   - 按下**「附加一個指紋檔案到這個檔案指紋」**，新增檔案至現有的檔案。
   - 按下**「附加其他檔案指紋到這個檔案指紋」**，以合併您已經匯入的檔案指紋清單。
   - 按下**「使用新清單取代現有清單」**。
   - 按下**「移除同時出現在新清單中的任何指紋」**。
7. 執行下列其中一個動作：
   - 按下**「瀏覽」**找出檔案，或輸入您要附加、取代或移除之檔案指紋清單的完整路徑。
   - 選取您要合併的檔案指紋。
8. 按**「下一步」**>**「關閉」**>**「完成」**。

系統鎖定與 Symantec EDR 黑名單規則之間的互動

如果您的網路包括 Symantec EDR，您可能會在 Symantec EDR 的系統鎖定組態中看到黑名單。

Symantec EDR 黑名單以下列方式與系統鎖定組態互動：

- Symantec Endpoint Protection Manager 從 Symantec EDR 接收黑名單規則時，Symantec Endpoint Protection Manager 會為所有網域和群組以黑名單模式啟用系統鎖定。
- 黑名單規則顯示於系統鎖定組態中的 Symantec Endpoint Protection Manager 檔案指紋清單內。您無法從 Symantec EDR 修改檔案指紋清單。
- 如果您架構了具有以許可清單模式啟用之系統鎖定的用戶端群組，設定將予以保留且 Symantec Endpoint Protection Manager 不會使用 Symantec EDR 黑名單規則。
- 如果您停用系統鎖定並刪除 Symantec EDR 黑名單，Symantec Endpoint Protection Manager 會自動重新啟用系統鎖定並套用黑名單。
- 如果您停用系統鎖定但不刪除 Symantec EDR 黑名單，在您重新啟用系統鎖定之前，其將保留為停用狀態。

附註：Symantec EDR 會直接將許可清單規則傳送至 Symantec Endpoint Protection 用戶端。Symantec EDR 不會將許可清單檔案指紋傳送至 Symantec Endpoint Protection Manager。

請參閱第 460 頁的「在許可清單模式下執行系統鎖定」。

請參閱第 461 頁的「在黑名單模式下執行系統鎖定」。

請參閱第 397 頁的「將用戶端群組架構為使用私用伺服器進行信譽查詢和提交」。

建立應用程式名稱清單以匯入系統鎖定架構中

您可將應用程式名稱清單匯入系統鎖定架構。您可能想要匯入應用程式名稱清單，而不是將應用程式名稱逐一新增至系統鎖定架構。

根據預設，合併應用程式名稱清單中最多可包含 512 個應用程式。您可以在 conf.properties 檔案中變更該數目上限。

您可以使用任何文字編輯器，建立應用程式名稱清單檔案。

檔案中的每一行可包含用空格分隔的下列項目：

- 檔案名稱
  如果使用路徑名稱，則必須放在引號內。
- 測試模式
  值應為 1 或 Y (表示啟用)，或者 0 或 N (表示停用)。如果欄位保留空白，表示停用測試模式。如果要指定比對模式，您必須包含值。
- 比對模式 (萬用字元或規則運算式)
  值應為 1 或 Y (表示規則運算式比對)，或者 0 或 N (表示萬用字元比對)。如果欄位保留空白，就會使用萬用字元比對。

附註：測試模式欄位會啟用或停用清單中每個應用程式的**「增加前測試」**或**「移除前測試」**選項。當您使用**「僅記錄應用程式」**選項來測試整個系統鎖定架構時，會忽略測試模式欄位。

每一行都應使用下列語法：

```
filename test_mode matching_mode
```

例如：

```
aa.exe
bb.exe 0 1
cc.exe 1
dd.exe 1 0
"c:\program files\ee.exe" 0 0
```

將此清單匯入系統鎖定時，個別應用程式會出現在系統鎖定架構中，且具有下列設定：

表 22-5　　比對模式設定的範例

應用程式名稱	「增加前測試」或「移除前測試」	比對模式
aa.exe	已停用	萬用字元
bb.exe	已停用	規則運算式
cc.exe	已啟用	萬用字元
dd.exe	已啟用	萬用字元
c:\program files\ee.exe	已停用	萬用字元

請參閱第 445 頁的「架構系統鎖定」。

自動更新系統鎖定的許可清單或黑名單

Symantec Endpoint Protection Manager 可以自動更新您匯入、合併或附加的現有檔案指紋清單和應用程式名稱清單。

當您在同一台電腦上重新執行此指令時，會自動更新您從收集檔案指紋清單指令所產生的檔案指紋清單。

Symantec Endpoint Protection Manager 可以更新現有清單， 但無法自動上傳新的許可清單或黑名單。

您也可以手動更新現有檔案指紋。

表 22-6 更新系統鎖定的許可清單或黑名單

步驟	敘述
步驟 1：建立已更新的檔案指紋清單或應用程式名稱清單並壓縮檔案	您可以使用 checksum.exe 公用程式或任何第三方公用程式來建立已更新的檔案指紋清單。 您可以使用任何文字編輯器來更新應用程式名稱清單。 這些清單的名稱必須與 Symantec Endpoint Protection Manager 中現存的名稱相同。 請參閱第 449 頁的「以 checksum.exe 建立檔案指紋清單」。 無法直接更新您從收集檔案指紋清單指令所產生的指紋清單。您可以將指令產生的清單與另一個清單合併，或是在匯入的清單上附加指令產生的清單。 自動更新功能需要檔案指紋和應用程式名稱清單的壓縮檔案 (zip 檔案)。 您可以在 Windows 或任何壓縮公用程式中使用檔案壓縮功能來壓縮檔案。
步驟 2：建立 index.ini 檔案	index.ini 檔案指定 Symantec Endpoint Protection Manager 應更新哪一個檔案指紋清單和應用程式名稱清單。 您可以使用任何文字編輯器來建立 index.ini 檔案，然後將該檔案複製到指定的 URL。 請參閱第 456 頁的「建立 index.ini 檔案以供自動更新用於系統鎖定的許可清單和黑名單」。
步驟 3：使壓縮檔案和 index.ini 可供 Symantec Endpoint Protection Manager 使用	Symantec Endpoint Protection Manager 使用 UNC、FTP 或 HTTP/HTTPS，在指定的 URL 擷取 index.ini 檔案和 zip 檔案。 Symantec Endpoint Protection Manager 使用 index.ini 檔案中的指示來更新指定的檔案。 當您啟用自動更新時，Symantec Endpoint Protection Manager 會根據您設定的排程定期檢查此 URL 是否有已更新的檔案。 對於 UNC，僅支援 JCFIS 共用。不支援 DFS 共用。 **附註：**如果無法使用 UNC、FTP 或 HTTP/HTTPS，您可以將 index.ini 和更新的檔案指紋及應用程式名稱檔案直接複製到下列資料夾：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content。這些檔案應解壓縮。 如果 Symantec Endpoint Protection Manager 無法使用 UNC、FTP 或 HTTP/HTTPS 來更新檔案，便會檢查此資料夾。
步驟 4：在管理主控台中啟用自動許可清單和黑名單更新	您必須在 Symantec Endpoint Protection Manager 主控台中啟用自動更新現有的許可清單或黑名稱。 您可使用 Symantec Endpoint Protection Manager 的**「檔案指紋更新」**對話方塊，啟用更新功能及指定排程和 URL 資訊。 請參閱第 457 頁的「針對系統鎖定啟用許可清單和黑名單的自動更新」。
步驟 5：檢查許可清單或黑名單的自動更新狀態	您可以在主控台中檢查狀態，以確定 Symantec Endpoint Protection Manager 完成更新。 請參閱第 457 頁的「檢查系統鎖定的自動許可清單或黑名單更新狀態」。

請參閱第 452 頁的「手動更新 Symantec Endpoint Protection Manager 中的檔案指紋清單」。

請參閱第 445 頁的「架構系統鎖定」。

建立 index.ini 檔案以供自動更新用於系統鎖定的許可清單和黑名單

自動更新功能需要 index.ini 檔案。您可以使用任何文字編輯器建立此檔案。

附註：如果您在文字檔案中使用非英文字元，您應使用沒有位元組順序標記 (Byte Order Mark, BOM) 字元的 UTF-8 來編輯和儲存此檔案。

index.ini 檔案可指定下列項目：

- 包含已更新檔案指紋清單和應用程式名稱清單之壓縮檔案的版本和名稱。
- 您要更新之檔案指紋清單和應用程式名稱清單的名稱。
- 使用應用程式名稱清單的用戶端群組名稱。

現有的檔案指紋清單或群組必須已經存在於 Symantec Endpoint Protection Manager 中。群組必須啟用系統鎖定。檔案指紋清單和應用程式名稱清單必須可從指定的壓縮檔案取得。

您必須使用下列語法建構 index.ini 檔案：

```
[Revision]
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description

[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE


[ApplicationNameList - domain name or Default]
existing group path="updated list" REPLACE/APPEND/REMOVE
```

例如，您可以在 index.ini 檔案中使用下面幾行：

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
Description=NewUpdates

[FingerprintList - Default]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE
```

```
[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE

[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

請參閱第 454 頁的「自動更新系統鎖定的許可清單或黑名單」。

請參閱第 453 頁的「建立應用程式名稱清單以匯入系統鎖定架構中」。

針對系統鎖定啟用許可清單和黑名單的自動更新

您可以將 Symantec Endpoint Protection Manager 架構為自動更新用於系統鎖定的許可清單和黑名單。

若要自動更新您使用收集檔案指紋清單指令產生的檔案指紋清單，請再次執行此指令。

在管理主控台中啟用自動許可清名單和黑名單更新

1. 在主控台的**「管理員」**標籤上，按下**「伺服器」**。
2. 用滑鼠右鍵按下相關伺服器，然後選取**「編輯伺服器屬性」**。
3. 在**「伺服器屬性」**對話方塊中，選取**「檔案指紋更新」**標籤。
4. 在**「檔案指紋更新」**標籤上，勾選**「自動更新許可清單或黑名單」**。
5. 輸入 index.ini 和壓縮檔案所在位置的 URL。

   如果想要使用 UNC 或 FTP，您也必須為 index.ini 和內容指定使用者名稱和密碼。
6. 在**「排程」**下方，您可以指定 Symantec Endpoint Protection Manager 嘗試更新許可清單或黑名單的頻率，也可以使用預設設定。
7. 按下**「確定」**。

請參閱第 454 頁的「自動更新系統鎖定的許可清單或黑名單」。

檢查系統鎖定的自動許可清單或黑名單更新狀態

在 Symantec Endpoint Protection Manager 更新許可清單或黑名單之後，您可以透過數種方式檢查更新狀態。

檢查系統鎖定的自動許可清單或黑名單更新狀態

- 在主控台中，執行下列其中一個動作：

- 在「**管理員**」標籤上，選取站台。類似下列內容的訊息隨即出現：**更新修訂為「20120528 R016 *敘述*」的許可清單和黑名單成功。**
- 在「**監視器**」標籤上，檢視「**系統日誌: 伺服器活動**」。 事件類型通常會顯示成類似於「**檔案指紋更新**」。
- 在「**政策**」標籤的「**政策元件**」下方，檢查檔案指紋清單敘述。敘述會顯示成類似於「**修訂: 20120528 R016 *敘述***」。

請參閱第 454 頁的「自動更新系統鎖定的許可清單或黑名單」。

請參閱第 563 頁的「檢視日誌」。

啟用系統鎖定前設定和測試系統鎖定架構

一般來說，需要在測試模式下執行一周或足夠時間的系統鎖定，以讓用戶端執行其典型的應用程式。 在確定系統鎖定設定不會對使用者造成問題後，可以啟用系統鎖定。

在測試模式下執行系統鎖定時，系統鎖定處於停用。 系統鎖定不會攔截任何應用程式。 而是記錄但不攔截未核准的應用程式，以便您可以在啟用系統鎖定前檢閱清單。 可以檢閱「控制」日誌中的日誌項目。 也可以在「**系統鎖定**」對話方塊中檢閱未核准的應用程式。

附註：也可以建立防火牆規則，以允許用戶端上已核准的應用程式。

啟用系統鎖定前設定和測試系統鎖定架構

1. 在主控台中，按下「**用戶端**」，然後在「**用戶端**」下方找到要設定系統鎖定的群組。
2. 在「**政策**」標籤上，按下「**系統鎖定**」。
3. 按下「**記錄未核准的應用程式**」，以便在測試模式下執行系統鎖定。

   此選項會記錄用戶端目前正在執行的未核准的應用程式。
4. 選取「**許可清單模式**」或「**黑名單模式**」。
5. 在「**應用程式檔案清單**」的「**檔案指紋清單**」下，新增或移除檔案指紋清單。

   若要新增清單，該清單必須在 Symantec Endpoint Protection Manager 中可供使用。

   請參閱第 451 頁的「在 Symantec Endpoint Protection Manager 中匯入或合併檔案指紋清單」。

6 若要新增應用程式名稱清單，請在**「應用程式檔案清單」**的**「檔案名稱」**下，按下**「匯入」**。

指定要匯入的應用程式名稱清單，然後按下**「匯入」**。清單中的應用程式以個別項目的形式出現在系統鎖定架構中。

附註：應用程式名稱清單必須是指定檔案名稱、測試模式和比對模式的文字檔案。

請參閱第 453 頁的「建立應用程式名稱清單以匯入系統鎖定架構中」。

7 若要新增個別應用程式，請在**「應用程式檔案清單」**的**「檔案名稱」**下，按下**「新增」**。

8 在**「新增檔案定義」**對話方塊中，指定檔案 (.exe 或 .dll) 的完整路徑名稱。

可以使用標準字串或規則運算式語法來指定名稱。 名稱可以包括萬用字元 (* 代表任意字元，? 代表單一字元)。名稱也可以包括環境變數，例如 %ProgramFiles% 代表程式檔案目錄的位置，而 %windir% 代表 Windows 安裝目錄的位置。

9 預設會保持選取**「使用萬用字元比對 (支援 * 和 ?)」**，或如果在檔案名稱使用了規則運算式，請改為按下**「使用規則運算式比對」**。

10 如果您只想在該檔案在特定磁碟機類型上執行時允許它，請按下**「僅比對下列磁碟機類型內的檔案」**。

取消選取不要包含的磁碟機類型。 根據預設會選取所有磁碟機類型。

11 如果您希望依照裝置 ID 類型進行比對，請選取**「僅比對下列裝置 ID 類型的檔案」**，然後按下**「選取」**。

12 在清單中按下需要的裝置，然後按下**「確定」**。

13 按下**「確定」**開始測試。

一段時間後，便可以檢視未核准的應用程式清單。如果重新開啟**「用於*群組名稱*的系統鎖定」**對話方塊，可以查看測試的執行時間。

檢視測試已記錄但沒有攔截的未核准的應用程式

1 在**「用於*群組名稱*的系統鎖定」**對話方塊中，按下**「檢視未核准的應用程式」**。

2 在**「未核准的應用程式」**對話方塊中，檢視應用程式。

這個清單包含應用程式執行的時間、電腦的主機名稱、用戶端的使用者名稱，以及執行檔檔名等資訊。

3 決定要處理未核准應用程式的方式。

若是許可清單模式，則可以將要允許的應用程式名稱新增至核准的應用程式清單。若是黑名單模式，則可以移除要允許的應用程式的名稱。

4 如果變更了檔案指紋清單或個別應用程式，並且想要重新執行測試，請在**「未核准的應用程式」**對話方塊中，按下**「重設測試」**。否則，按下**「關閉」**。

5 完成測試後，便可以啟用系統鎖定。

請參閱第 445 頁的「架構系統鎖定」。

在許可清單模式下執行系統鎖定

可以將系統鎖定架構為僅允許用戶端電腦上核准的應用程式。將僅允許執行核准的清單上的應用程式。將攔截其他所有應用程式。核准的清單稱為許可清單。核准的應用程式受 Symantec Endpoint Protection 的其他保護功能支配。

附註：預設情況下，當啟用系統鎖定時，系統鎖定會在許可清單模式下行。

只有在符合下列條件時，才應該將系統鎖定架構為在許可清單模式下執行：

- 使用**「記錄未核准的應用程式」**選項測試了系統鎖定架構。
- 已確定核准的應用程式清單中列出了用戶端電腦需要執行的全部應用程式。

警告：從系統鎖定新增或移除檔案指紋清單或特定應用程式時，請小心。從系統鎖定新增或移除項目可能會有風險。可能會攔截用戶端電腦上的重要應用程式。

請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

附註：如果您執行以許可清單模式啟用的系統鎖定，Symantec Endpoint Protection Manager 不會從 Symantec EDR 套用任何黑名單規則。

請參閱第 452 頁的「系統鎖定與 Symantec EDR 黑名單規則之間的互動」。

在許可清單模式下執行系統鎖定

1 在主控台中，按下**「用戶端」**。

2 在**「用戶端」**下，選取要設定系統鎖定的群組。

如果您選取子群組，則必須關閉父群組的繼承功能。

3 在**「政策」**標籤上，按下**「系統鎖定」**。

4 在**「系統鎖定」**下，選取**「啟用系統鎖定」**，攔截用戶端嘗試執行的任何未核准的應用程式。

5 在**「應用程式檔案清單」**下，選取**「許可清單模式」**。

6 在「**核准的應用程式**」下，確認已包括用戶端電腦執行的所有應用程式。

警告：您必須將用戶端電腦要執行的所有應用程式包含在核准的應用程式清單中。否則，可能導致某些用戶端電腦無法重新啟動，或阻止使用者執行重要應用程式。

7 若要在用戶端攔截應用程式時在用戶端電腦上顯示訊息，請勾選「**如果攔截到應用程式時通知使用者**」。

8 按下「**確定**」。

請參閱第 445 頁的「架構系統鎖定」。

請參閱第 208 頁的「停用群組繼承」。

在黑名單模式下執行系統鎖定

您可以啟用系統鎖定以便攔截用戶端電腦上未核准的應用程式清單。未核准的清單中的所有應用程式都會遭到攔截。未核准的清單稱為黑名單。所有其他應用程式都會被允許。允許的應用程式依 Symantec Endpoint Protection 的其他防護功能而定。

附註：如果您在網路中執行 Symantec EDR，Symantec EDR 組態會影響系統鎖定黑名單組態。

請參閱第 452 頁的「系統鎖定與 Symantec EDR 黑名單規則之間的互動」。

只有符合下列條件時，才能架構系統鎖定來攔截未核准的應用程式：

- 使用「**記錄未核准的應用程式**」選項測試了系統鎖定架構。
- 您確定用戶端電腦所應攔截的所有應用程式都列在未核准的應用程式清單中。

請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

警告：從系統鎖定新增或移除檔案指紋清單或特定應用程式時，請小心。從系統鎖定新增或移除項目可能會有風險。可能會攔截用戶端電腦上的重要應用程式。

在黑名單模式下執行系統鎖定

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」下，選取要設定系統鎖定的群組。

如果您選取子群組，則必須關閉父群組的繼承功能。

請參閱第 208 頁的「停用群組繼承」。

3 在「**政策**」標籤上，選取「**系統鎖定**」。

4 在「**系統鎖定**」對話方塊中，選取「**啟用系統鎖定**」。

5 在「**應用程式檔案清單**」下，選取「**黑名單模式**」。

6 在「**未核准的應用程式**」下，確定您已包含用戶端電腦所應攔截的所有應用程式。

附註：大量的具名應用程式可能會降低您的用戶端電腦效能。

7 若要在用戶端攔截應用程式時在用戶端電腦上顯示訊息，請勾選「**如果攔截到應用程式時通知使用者**」。

8 按下「**確定**」。

請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

請參閱第 445 頁的「架構系統鎖定」。

當系統鎖定已啟用後，在新增或移除選取的項目之前對它們進行測試

系統鎖定啟用一段時間後，您可能想要新增或移除檔案指紋清單或特定應用程式。隨著時間的演變，您可能已經累積許多不再使用的檔案指紋清單。或者，使用者需要的應用程式可能發生變更。

在新增或移除選取的項目之前，需要對它們進行測試，以便用戶端電腦不會攔截重要的應用程式。 在黑名單模式下，系統鎖定會攔截新增到組態的所有新項目。 在許可清單模式下，系統鎖定會攔截移除的所有現有項目。 系統鎖定預設會以許可清單模式執行。

附註：測試個別項目時，系統鎖定處於啟用狀態。系統鎖定會繼續攔截不屬於測試部分的應用程式。

可以測試個別檔案指紋清單，以確保用戶端電腦不再使用清單中的應用程式。也可以測試在系統鎖定架構中指定的個別應用程式。

當系統鎖定停用後，可以測試整個系統鎖定架構，而非特定項目。

當系統鎖定已啟用後，在新增或移除選取的項目之前對它們進行測試

1 在主控台中，按下「**用戶端**」。

2 在「**用戶端**」下，找到要從系統鎖定中移除的項目所對應的群組。

3 在「**政策**」標籤上，按下「**系統鎖定**」。

系統鎖定架構應該已經啟用。

- 若是許可清單模式，則應知道要測試的現有檔案指紋清單或特定應用程式名稱。
- 若是黑名單模式，則應新增要測試的新檔案指紋清單或應用程式名稱。

請參閱第 460 頁的「在許可清單模式下執行系統鎖定」。

請參閱第 461 頁的「在黑名單模式下執行系統鎖定」。

4 在許可清單模式下，在**「應用程式檔案清單」**下，勾選要測試的現有檔案指紋清單或應用程式旁的**「移除前測試」**。

系統鎖定會繼續允許這些應用程式，但它們會被記錄為未核准的應用程式。

如果匯入了應用程式名稱清單，則**「移除前測試」**欄位已經填入了資料。

5 按下**「確定」**開始測試。

如果重新開啟**「用於*群組名稱*的系統鎖定」**對話方塊，可以查看測試的執行時間。通常，您可能需要執行一周或更長時間的測試。

測試後，可以檢查「應用程式控制」日誌。如果已測試的應用程式出現在「應用程式控制」日誌中，則可以確定使用者在執行這些應用程式。可以決定是否將測試的項目作為系統鎖定架構的一部分加以保留。

如果決定現在要攔截已測試的項目，請執行下列其中一項動作：

- 如果許可清單已啟用，請在**「用於*群組名稱*的系統鎖定」**對話方塊中，選取測試的項目並按下**「移除」**。
- 如果黑名單模式已啟用，請在**「用於*群組名稱*的系統鎖定」**對話方塊中，取消選取**「增加前測試」**。

警告：在許可清單模式中，系統鎖定會攔截檔案指紋清單中的任何應用程式和從組態中移除的特定應用程式名稱。在黑名單模式中，系統鎖定會攔截檔案指紋清單中的任何應用程序和新增到組態中的特定應用程式名稱。

請參閱第 458 頁的「啟用系統鎖定前設定和測試系統鎖定架構」。

請參閱第 445 頁的「架構系統鎖定」。

管理裝置控制

裝置控制指定用戶端電腦上要允許或攔截的硬體裝置。您可以使用預設硬體裝置清單和「裝置控制」政策來管理裝置控制，也可以自行新增硬體裝置清單。

表 22-7 管理裝置控制

步驟	敘述
檢視 Symantec Endpoint Protection Manager 中的預設硬體裝置清單	根據預設，Symantec Endpoint Protection Manager 包含一個硬體裝置清單。此清單顯示在 Symantec Endpoint Protection Manager 的**「政策」**標籤的**「政策元件」**下。您可以使用此清單選取用戶端電腦上要控制的裝置。 如果要控制的裝置未包含在此清單中，則必須先新增該裝置。 請參閱第 465 頁的「關於硬體裝置清單」。

步驟	敘述
將裝置新增至硬體裝置清單 (如有必要)	將裝置新增至裝置清單時，您需要裝置的類別 ID 或裝置 ID。 您無法新增自訂的 Mac 裝置。您只能使用提供的裝置類型。 請參閱第 467 頁的「新增硬體裝置至硬體裝置清單中」。 請參閱第 466 頁的「使用 DevViewer 取得 Windows 電腦的裝置廠商或型號」。
在裝置控制政策中允許或攔截裝置	指定您要允許或攔截哪些從用戶端存取的裝置。 請參閱第 464 頁的「允許或攔截用戶端電腦上的裝置」。

在 Mac 用戶端上，裝置控制會包含在 SymDaemon 服務中。無需重新啟動 Windows 用戶端或 Mac 用戶端，裝置控制即會運作。

請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。

請參閱第 695 頁的"依據平台的**「裝置控制」**差異"。

允許或攔截用戶端電腦上的裝置

您可以使用「應用程式與裝置控制」政策來架構裝置控制。開始之前，將您需要的任何裝置新增至**「硬體裝置」**清單。

請參閱第 467 頁的「新增硬體裝置至硬體裝置清單中」。

自 14 版起，您可以架構 Windows 與 Mac 裝置控制。

為 Windows 用戶端架構裝置控制

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 按下**「裝置控制」**。
3. 在**「攔截的裝置」**下，按下**「新增」**。
4. 在**「裝置選取」**視窗中，選取一個或多個裝置。 如有必要，請確定是否攔截特定的通訊埠，就會排除裝置。

   附註：通常，絕不應該攔截鍵盤。

5. 按下**「確定」**。
6. 在**「不攔截的裝置」**下，按下**「新增」**。
7. 在**「裝置選取」**視窗中，選取一個或多個裝置。
8. 如果您希望通知使用者，請勾選**「當裝置被攔截時通知使用者」**。
9. 按下**「確定」**。

為 Mac 用戶端架構裝置控制 (自 14 版起)

1. 在主控台中開啟「應用程式與裝置控制」政策。
2. 在**「Mac 設定」**下方，按下**「裝置控制」**。
3. 在**「攔截的裝置」**下，按下**「新增」**。
4. 在**「裝置選取」**視窗中，從清單中選取裝置。您一次僅可以新增一個裝置。

   若視窗底部的欄位可用，請填寫。如果您將這些欄位保留為空白，此類型的所有裝置都將被攔截。

   您也可使用規則運算式來定義裝置廠商、裝置型號或序號。請參閱**「Mac 裝置控制」**視窗中的說明，以瞭解詳細資訊。

   若要從 Mac 的連線裝置取得序號、型號或廠商名稱，請使用安裝檔案中的 DeviceInfo 工具。您可在 `Tools/DeviceInfo` 下找到此工具及其指示。
5. 按下**「確定」**。
6. 在**「不攔截的裝置」**下，按下**「新增」**。
7. 在**「裝置選取」**視窗中，從清單中選取裝置，定義已排除的裝置，然後按下**「確定」**。
8. 如果您希望通知使用者，請勾選**「當裝置被攔截時通知使用者」**。
9. 按下**「確定」**。

請參閱第 463 頁的「管理裝置控制」。

請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。

關於硬體裝置清單

Symantec Endpoint Protection Manager 包含一個硬體裝置清單。 此清單預設包含一些裝置。您可以在架構裝置控制時使用這些裝置。

請參閱第 463 頁的「管理裝置控制」。

您可以將裝置新增到此清單。 您無法編輯或刪除任何預設裝置。

您無法新增自訂的 Mac 硬體裝置。

依裝置 ID 或類別 ID 識別裝置。您可以使用下列值之一，將裝置新增至此清單。您可以使用工具來判斷裝置 ID 或類別 ID。若為 Windows，請移至 Tools\DevViewer。若為 Mac，請移至 Tools\DeviceInfo。

請參閱第 466 頁的「使用 DevViewer 取得 Windows 電腦的裝置廠商或型號」。

類別 ID

類別 ID 指的是 Windows GUID。 每種裝置類型都有關聯的類別和 ClassGuid。 ClassGuid 是十六進位值，格式如下：

{00000000-0000-0000-0000-000000000000}

裝置 ID	裝置 ID 是裝置的專屬 ID。裝置 ID 語法內含敘述性的字串，使之較類別 ID 更易於閱讀。 新增裝置 ID 時，可使用裝置的特定 ID。或者，您可在裝置 ID 字串中使用萬用字元，以標示非專屬的裝置群組。您可以使用星號 (*) 表示零或更多其他字元，或使用問號 (?) 表示任何數值單一字元。 以下為特定 USB SanDisk 裝置的裝置 ID： USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\00020714O6&0 以下是使用萬用字元指示 USB SanDisk 裝置的裝置 ID： USBSTOR\DISK&VEN_SANDISK* 以下是使用萬用字元指示 USB 裝置的裝置 ID： USBSTOR\DISK* 以下是使用萬用字元指示 USB 儲存裝置的裝置 ID： USBSTOR*

使用 DevViewer 取得 Windows 電腦的裝置廠商或型號

您可以使用 Symantec DevViewer 工具取得類別 ID (GUID) 或裝置 ID。您可以使用「Windows 裝置管理員」取得類別 ID。

取得裝置 ID 後，您可使用萬用字元進行修改，標示為非專屬的裝置群組。

使用 DevViewer 工具取得類別 ID 或裝置 ID

1. 在透過 MySymantec 取得的完整產品安裝檔案中，找到 `Tools\DevViewer` 資料夾，然後將 `DevViewer.exe` 工具複製到用戶端電腦。

   請參閱 MySymantec 入門指南。
2. 在用戶端電腦上，執行 `DevViewer.exe`。
3. 展開裝置樹狀結構，然後找到需要裝置 ID 或 GUID 的裝置。

   例如，展開**「磁碟機」**，然後選取該類別中的裝置。
4. 在右窗格中，在裝置 ID (開頭為 [裝置 ID]) 上按下滑鼠右鍵，然後按下**「複製裝置 ID」**。
5. 按下**「結束」**。
6. 在管理伺服器上，將裝置 ID 貼到硬體裝置清單中。

從控制台取得裝置 ID

1. 從「控制台」開啟「裝置管理員」。

   「裝置管理員」的路徑取決於 Windows 作業系統。例如，在 Windows 7 中，按下**「開始」>「控制台」>「系統」>「裝置管理員」**。
2. 在**「裝置管理員」**對話方塊中，以滑鼠右鍵按下裝置，再按下**「屬性」**。

3 在該裝置的「**屬性**」對話方塊中，從「**詳細資訊**」標籤選取裝置 ID。

依據預設，裝置 ID 為第一個顯示的值。

4 複製 ID 字串。

5 按下「**確定**」。

請參閱第 467 頁的「新增硬體裝置至硬體裝置清單中」。

新增硬體裝置至硬體裝置清單中

在取得硬體裝置的類別 ID 或裝置 ID 後，您可以將硬體裝置新增至預設「硬體裝置」清單。您接著可以從「應用程式與裝置控制」政策的裝置控制部分存取此預設清單。

請參閱第 465 頁的「關於硬體裝置清單」。

新增硬體裝置至硬體裝置清單中

1 在主控台中，按下「**政策**」。

2 在「**政策**」下，展開「**政策元件**」然後按「**硬體裝置**」。

3 在「**工作**」下方，按下「**新增硬體裝置**」。

4 輸入要新增裝置的名稱。

類別 ID 和裝置 ID 依慣例會用大括號 (`{ }`) 括住。您可能需要將大括號取代為萬用字元 `?`。

5 選取「**類別 ID**」或「**裝置 ID**」，然後貼上從「Windows 裝置管理員」或 DevViewer 工具複製的 ID。

6 您可以使用萬用字元來定義一組裝置 ID。例如，您可以使用下列字串：`*IDE\DVDROM*`。

請參閱第 466 頁的「使用 DevViewer 取得 Windows 電腦的裝置廠商或型號」。

7 按下「**確定**」。

23

管理例外

本章包含以下主題：

管理 Symantec Endpoint Protection 中的例外

您可以在 Symantec Endpoint Protection Manager 主控台中管理 Symantec Endpoint Protection 的例外。

表 23-1　　管理例外

工作	敘述
了解例外	使用例外可將項目排除在用戶端電腦上的掃描範圍之外。 請參閱第471頁的「關於以作業系統為基礎的掃描中的例外」。
檢視 Symantec Endpoint Protection 自動排除掃描的檔案和資料夾類型	Symantec Endpoint Protection 會針對某些第三方應用程式和賽門鐵克的某些產品自動建立例外或排除項。 您也可以架構個別的掃描，以便僅掃描特定副檔名並略過任何其他副檔名。 請參閱第 365 頁的「關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾」。

工作	敘述
建立掃描例外	可以直接在「例外」政策中新增例外，也可以從**「監視器」**頁面上的日誌事件新增例外。 請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。 請參閱第 484 頁的「從日誌事件建立例外」。
限制使用者可在用戶端電腦上架構的例外類型 (僅限 Windows)	根據預設，用戶端電腦上的使用者具有有限的例外架構權限。您可以進一步限制使用者，以免其針對病毒和間諜軟體掃描或 SONAR 建立例外。 使用者永遠無法強制執行應用程式偵測，也永遠沒有建立「竄改防護」例外的權限。 使用者也無法建立應用程式控制的檔案例外。 請參閱第 483 頁的「限制使用者可在用戶端電腦上架構的例外類型」。
查看日誌，是否有可能要為其建立例外的偵測。	在 Symantec Endpoint Protection 執行偵測後，您可以從日誌事件建立偵測的例外。 例如，您可能希望針對掃描會偵測、但使用者要求下載的檔案建立例外。 請參閱第 484 頁的「從日誌事件建立例外」。
建立入侵預防特徵的例外	您可以指定入侵預防的例外。 您還可以針對入侵預防設定排除主機清單。 入侵預防例外會在「入侵預防」政策中架構。 請參閱第 331 頁的「為 IPS 特徵建立例外」。

針對哪種類型的掃描使用哪些 Windows 例外？

表 23-2 列出了在版本 14 MPx 及更早版本中，針對哪種類型的掃描使用例外政策中的哪些例外類型。

表 23-2 版本 14.0.1 及更早版本的例外名稱

Symantec Endpoint Protection Manager 14.0.1 及更早版本	用戶端限制 (位於 Symantec Endpoint Protection Manager)*	Windows 用戶端	例外適用功能
應用程式	應用程式例外	應用程式例外	■ 自動防護 ■ 手動掃描 ■ 排程掃描 ■ 下載鑑識 ■ SONAR
要監控的應用程式	無	無	應用程式控制
憑證	無	無	■ 自動防護 ■ 手動掃描 ■ 排程掃描 ■ 下載鑑識 ■ SONAR
DNS 或主機檔案變更	DNS 或主機檔案變更例外	DNS 或主機檔案變更例外 > 應用程式	SONAR
副檔名	副檔名例外	安全風險例外 > 副檔名	■ 自動防護 ■ 手動掃描 ■ 排程掃描
檔案	檔案例外	安全風險例外 > 檔案	■ 自動防護 ■ 手動掃描 ■ 排程掃描 ■ SONAR ■ 應用程式控制
資料夾	資料夾例外： ■ 安全風險例外 ■ SONAR 例外	安全風險例外 > 資料夾 SONAR 例外	■ 自動防護 ■ 手動掃描 ■ 排程掃描 ■ SONAR ■ 應用程式控制
已知風險	已知風險例外	安全風險例外 > 已知風險	■ 自動防護 ■ 手動掃描 ■ 排程掃描 ■ SONAR
信任的 Web 網域	信任的 Web 網域例外	安全風險例外 > Web 網域	下載鑑識

Symantec Endpoint Protection Manager 14.0.1 及更早版本	用戶端限制 (位於 Symantec Endpoint Protection Manager)*	Windows 用戶端	例外適用功能
竄改防護例外	無	無	竄改防護所保護的應用程式

*用戶端限制是可以在用戶端上顯示或隱藏以供用戶端使用者新增的例外。在雲端主控台中新增的例外無法在 Symantec Endpoint Protection Manager 中的用戶端上啟用或停用。

請參閱第 483 頁的「限制使用者可在用戶端電腦上架構的例外類型」。

請參閱第 515 頁的「Symantec Endpoint Protection Manager 例外政策如何與雲端主控台互動？」。

關於以作業系統為基礎的掃描中的例外

通常，例外是您要從掃描中排除的項目，如檔案或 Web 網域。

Symantec Endpoint Protection 會從病毒和間諜軟體掃描中自動排除某些檔案。

您可能想要使用例外減少掃描執行的時間。例如，您可以從掃描中排除檔案、資料夾和副檔名。若減少掃描時間，則可能會提高用戶端電腦的系統效能。

也可以使用例外來偵測應用程式，或變更當 Symantec Endpoint Protection 偵測到應用程式或當應用程式啟動時的預設行為。

附註：您無法為單一病毒和間諜軟體掃描建立例外。例如，如果您建立檔案例外，Symantec Endpoint Protection 會對所有病毒和間諜軟體掃描 (「自動防護」、「下載鑑識」以及任何管理員定義或使用者定義的掃描) 套用此例外。

例外可套用於特定用戶端類型 (Windows、Mac 或 Linux)。您可以分別為每個用戶端類型架構例外。

表 23-3　作業系統類型和掃描例外

用戶端類型	例外
Windows 用戶端	■ 檔案 ■ 資料夾 ■ 已知風險 ■ 副檔名 ■ 信任的 Web 網域 ■ 要監控的應用程式 ■ 應用程式 ■ 竄改防護

用戶端類型	例外
Mac 用戶端	■ 檔案或資料夾例外
Linux 用戶端	■ 資料夾或副檔名例外

請參閱第 365 頁的「關於 Symantec Endpoint Protection 從病毒和間諜軟體掃描排除的檔案和資料夾」。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

建立病毒和間諜軟體掃描的例外

可為 Symantec Endpoint Protection 建立不同類型的例外。

您建立的任何例外會優先於使用者可能定義的任何例外。 在用戶端電腦上，使用者無法檢視您建立的例外。 使用者僅能檢視自己建立的例外。

病毒和間諜軟體掃描的例外也適用於「下載鑑識」。

表 23-4 為 Symantec Endpoint Protection 建立例外

工作	敘述
從病毒和間諜軟體掃描中排除檔案	在 Windows 和 Mac 用戶端上支援。 從 Windows 用戶端上的病毒和間諜軟體掃描、SONAR 或應用程式控制，依名稱排除檔案。 請參閱第 475 頁的「從掃描中排除檔案或資料夾」。
從病毒和間諜軟體掃描中排除資料夾	在 Windows、Mac 和 Linux 用戶端上受支援。 從病毒和間諜軟體掃描、SONAR 或 Windows 用戶端上的所有掃描中排除資料夾。 在 Windows 和 Linux 用戶端上，您可以選擇將病毒和間諜軟體掃描的例外限制為自動防護或是排程和隨選掃描。 如果您執行的應用程式將許多暫存檔案寫入資料夾，則可能需要從自動防護中排除該資料夾。 自動防護會在檔案寫入時加以掃描，因此您可以透過將例外限制為排程和隨選掃描來提升電腦效能。 您可能需要從排程和隨選掃描中排除不常使用的資料夾或是包含封存檔案或封裝檔案的資料夾。 例如，排程或隨選掃描不常使用的深度封存檔案可能會降低電腦效能。 只有在存取任何檔案或寫入任何檔案到資料夾時，自動防護才會透過掃描來保護資料夾。 請參閱第 475 頁的「從掃描中排除檔案或資料夾」。

工作	敘述
從病毒和間諜軟體掃描中排除已知風險	在 Windows 用戶端上支援。 從病毒和間諜軟體掃描中排除已知風險。掃描會忽略此風險，但是，您可以架構例外以便掃描記錄偵測。任何情況下，用戶端軟體都不會在偵測到指定的風險時通知使用者。 如果使用者針對架構為忽略的已知風險架構自訂動作，則 Symantec Endpoint Protection 會忽略自訂動作。 安全風險例外不適用於 SONAR。 請參閱第 478 頁的「從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險」。
從病毒和間諜軟體掃描中排除檔案副檔名	在 Windows 和 Linux 用戶端上支援。 從病毒和間諜軟體掃描中排除任何含指定副檔名的檔案。 副檔名例外不適用於 SONAR 或 Power Eraser。 請參閱第 478 頁的「從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名」。
監控應用程式以為應用程式建立例外	在 Windows 用戶端上支援。 使用**「要監控的應用程式」**例外來監控特定的應用程式。當 Symantec Endpoint Protection 探索到應用程式時，便可以建立例外以指定 Symantec Endpoint Protection 處理應用程式的方式。 如果停用應用程式探索，「要監控的應用程式」例外會針對指定的應用程式強制執行應用程式探索。 請參閱第 479 頁的「在 Windows 用戶端上監控應用程式以建立應用程式的例外」。

工作	敘述
指定病毒和間諜軟體掃描如何處理受監控的應用程式	在 Windows 用戶端上支援。 使用應用程式例外以指定套用到受監控的應用程式的 Symantec Endpoint Protection 動作。 動作類型決定 Symantec Endpoint Protection 是否在偵測到應用程式或在應用程式執行時套用動作。 Symantec Endpoint Protection 在應用程式啟動或執行時，對應用程式套用「終止」、「隔離」或「移除」動作。 它在偵測到應用程式時會套用「只記錄」或「忽略」動作。 與檔案名稱例外不同，應用程式例外是一種雜湊型的例外。 不同的檔案可以具有相同的名稱，但檔案雜湊會獨特地標識應用程式。 此應用程式例外是 SHA-2 雜湊的例外。 在 Symantec Endpoint Protection 探索到應用程式後，可以為其建立例外的應用程式會出現在**「例外」**對話方塊中。 可以要求 Symantec Endpoint Protection 監控特定的應用程式以進行探索。 請參閱第 479 頁的「指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式」。 請參閱第 285 頁的「收集有關用戶端電腦執行的應用程式資訊」。
從病毒和間諜軟體掃描中排除 Web 網域	在 Windows 用戶端上支援。 「下載鑑識」會掃描使用者試圖從網站及其他入口網站下載的檔案。「下載鑑識」會作為病毒和間諜軟體掃描的一部分執行。 您可以為已知安全性的特定 Web 網域架構例外。 您必須啟用「下載鑑識」，例外才會生效。 **附註：**如果用戶端電腦使用帶驗證功能的代理，您必須為 Symantec URL 指定信任的 Web 網域例外。透過使用例外，可以讓用戶端電腦與 Symantec Insight 及其他重要的賽門鐵克網站進行通訊。 請參閱下列文章： ■ 如何測試 Insight 與賽門鐵克授權伺服器的連線 ■ 允許 Symantec Endpoint Protection 連線到賽門鐵克信譽與授權伺服器所需排除的代理伺服器 請參閱第 480 頁的「從 Windows 用戶端上的掃描中排除信任的 Web 網域」。

工作	敘述
為竄改防護建立檔案例外	在 Windows 用戶端上支援。 竄改防護可保護用戶端電腦不受竄改賽門鐵克程序和內部物件之程序的攻擊。當竄改防護偵測到一個可能會修改賽門鐵克架構設定或 Windows 登錄值的程序時，就會攔截該程序。 一些第三方應用程式會無意地嘗試修改賽門鐵克程序或設定。可能需要允許安全應用程式修改賽門鐵克設定。您可能想要停止用戶端電腦上特定登錄區或特定檔案的竄改防護。 在某些情況下，「竄改防護」可能會攔截螢幕閱讀器或部份其他輔助技術應用程式。可以建立檔案例外，讓應用程式可在用戶端電腦上執行。「竄改防護」不支援資料夾例外。 請參閱第 481 頁的「在 Windows 用戶端上建立竄改防護例外」。
允許應用程式變更 DNS 或主機檔案	在 Windows 用戶端上支援。 可以建立應用程式例外以變更 DNS 或主機檔案。SONAR 通常會防止 DNS 或主機檔案變更之類的系統變更。例如，您可能需要針對 VPN 應用程式建立例外。 請參閱第 482 頁的「針對會變更 DNS 或主機檔案的應用程式建立例外」。
排除憑證	在 Windows 用戶端上受支援 (自 14.0.1 起)。 您可以排除掃描某個憑證。排除憑證可避免其被標示為可疑。例如，下載鑑識掃描可能會將內部工具上的自我簽署憑證標示為可疑。 請參閱第 482 頁的「在 Windows 用戶端上從掃描中排除憑證」。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

請參閱第 484 頁的「從日誌事件建立例外」。

從掃描中排除檔案或資料夾

您可以分別為檔案或資料夾新增例外。如果您想建立多個檔案的例外，請重複此程序。

既可以在 Windows 用戶端上又可以在 Mac 用戶端上架構檔案或資料夾例外。在 Windows 用戶端上，檔案例外可套用到病毒和間諜軟體掃描、SONAR，以及應用程式控制。資料夾例外適用於病毒和間諜軟體掃描，以及 SONAR。

在 Windows 用戶端上從掃描中排除檔案

1. 在「**例外政策**」頁面上，按下「**例外**」。
2. 在「**例外**」下方，按下「**新增**」>「**Windows 例外**」>「**檔案**」。

3 在「**前置變數**」下拉式方塊中，選取常用資料夾。

選取 **[無]** 以輸入絕對路徑與檔案名稱。

選取前置字元時，可在不同的 Windows 作業系統中使用例外。

4 在「**檔案**」文字方塊中，輸入檔案名稱。

若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[無]**，請鍵入完整的路徑名稱。

附註：路徑必須使用反斜線來表示。

---

5 在「**指定將排除此檔案的掃描類型**」下，選取掃描類型 (「**安全風險**」、**SONAR** 或「**應用程式控制**」)。

您必須選取至少一種類型。

6 若是安全風險掃描，請在「**指定安全風險掃描的類型**」下，選取「**自動防護**」、「**排程和隨選**」或「**全部掃描**」。

請參閱說明，以取得為何要將例外限制為特定類型的安全風險掃描的相關資訊。

7 按下「**確定**」。

在 Windows 用戶端上從掃描中排除資料夾

1 在「**例外政策**」頁面上，按下「**例外**」。

2 在「**例外**」下，按下「**新增**」>「**Windows 例外**」>「**資料夾**」。

3 在「**前置變數**」下拉式方塊中，選取常用資料夾。

選取 **[無]** 以輸入絕對路徑與檔案名稱。

選取前置字元時，可在不同的 Windows 作業系統中使用例外。

4 在「**資料夾**」文字方塊中，輸入資料夾名稱。

若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[無]**，請鍵入完整的路徑名稱。

附註：路徑必須使用反斜線來表示。

---

5 在「**指定排除此資料夾的掃描類型**」下，選取掃描類型 (「**安全風險**」、**SONAR**、「**應用程式控制**」或「**全部**」)。

您必須選取至少一種類型。

6 若是安全風險掃描，請在「**指定安全風險掃描的類型**」下，選取「**自動防護**」、「**排程和隨選**」或「**全部掃描**」。

請參閱說明，以取得為何要將例外限制為特定類型的安全風險掃描的相關資訊。

7 按下「**確定**」。

從 Mac 用戶端上的掃描中排除檔案或資料夾

1 在「**例外政策**」頁面上，按下「**例外**」。

2 在「**例外**」下方，按下「**新增**」>「**Mac 例外**」>「**檔案或資料夾的安全風險例外**」。

3 在「**檔案或資料夾的安全風險例外**」下的「**前置變數**」下拉式方塊中選擇一般資料夾。

選取 **[無]** 以輸入絕對路徑與檔案名稱。

4 在「**檔案**」或「**資料夾**」文字方塊中，鍵入檔案或資料夾的名稱。

若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[無]**，請鍵入完整的路徑名稱。

附註：資料夾路徑必須用正斜線表示。

5 按下「**確定**」。

從 Linux 用戶端上的掃描中排除資料夾

1 在「**例外政策**」頁面上，按下「**例外**」。

2 在「**例外**」下方，按下「**新增**」>「**Linux 例外**」。

3 按下「**資料夾**」。

4 在「**新增資料夾例外**」對話方塊中，您可以選擇前置變數，鍵入資料夾名稱，以及是否要包含子資料夾。

若您選擇一個前置變數，路徑應與前置字元有關。若您選擇 **[無]**，請鍵入完整的路徑名稱。

附註：資料夾路徑必須用正斜線表示。

5 指定安全風險掃描的類型。選取「**自動防護**」、「**排程和隨選**」或「**全部掃描**」，然後按下「**確定**」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

請參閱第 478 頁的「從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名」。

從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險

用戶端軟體偵測到的安全風險會顯示在**「已知安全風險例外」**對話方塊中。

已知安全風險清單包含有關風險嚴重性的資訊。

從 Windows 用戶端上的病毒和間諜軟體掃描中排除已知風險

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 在**「例外」**下，按下**「新增」>「Windows 例外」>「已知風險」**。
3. 在**「新增已知安全風險例外」**對話方塊中，選取要從病毒和間諜軟體掃描中排除的一或多個安全風險。
4. 如果您想要記錄該偵測事件，勾選**「偵測到安全風險時記錄」**。

   如果您未勾選此選項，用戶端會在偵測到選取風險時忽略該風險。用戶端也因此不會記錄該偵測事件。
5. 按下**「確定」**。
6. 架構完此政策後，按下**「確定」**。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名

您可以新增多個副檔名至例外。在您建立例外之後，您無法為相同的政策建立其他副檔名例外。您必須編輯現有的例外。

您一次僅可以新增一個副檔名。如果您在**「新增」**文字方塊中輸入多個副檔名，政策會將這些項目視作一個副檔名進行處理。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

從 Windows 用戶端和 Linux 用戶端上的病毒和間諜軟體掃描中排除副檔名

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 在**「例外」**下方，按下**「新增」>「Windows 例外」>「副檔名」**或**「新增」>「Linux 例外」>「副檔名」**。
3. 在文字方塊中，輸入要排除的副檔名，然後按下**「新增」**。
4. 在**「指定安全風險掃描的類型」**下，選取**「自動防護」**、**「排程和隨選」**或**「全部掃描」**。
5. 將任何其他副檔名新增至例外。
6. 按下**「確定」**。

請參閱第 475 頁的「從掃描中排除檔案或資料夾」。

在 Windows 用戶端上監控應用程式以建立應用程式的例外

當 Symantec Endpoint Protection 探索到受監控的應用程式時，該應用程式會出現在**「應用程式例外」**對話方塊中。可以在「例外」政策中建立應用程式的例外動作。該應用程式還會出現在相關日誌中，並且可以從日誌中建立例外。

如果停用應用程式探索，「要監控的應用程式」例外會針對指定的應用程式強制執行應用程式探索。

在 Windows 用戶端上監控應用程式以建立應用程式的例外

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 按下**「新增」>「Windows 例外」>「要監控的應用程式」**。
3. 在對話方塊中鍵入應用程式名稱。

   例如，您可以輸入如下的可執行檔名稱：

   foo.exe
4. 按下**「新增」**。
5. 按下**「確定」**。

請參閱第 284 頁的「監控在用戶端電腦執行的應用程式與服務」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

請參閱第 479 頁的「指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式」。

請參閱第 484 頁的「從日誌事件建立例外」。

指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式

可以監控特定應用程式，以便可以建立 Symantec Endpoint Protection 處理應用程式的方式的例外。在 Symantec Endpoint Protection 探索到應用程式並且管理主控台接收到事件後，應用程式會出現在**「應用程式例外」**對話方塊的應用程式清單中。如果網路中的用戶端電腦尚未探索到任何應用程式，則應用程式清單顯示空白。

應用程式清單包括監控的應用程式以及使用者下載的檔案。當 Symantec Endpoint Protection 偵測到應用程式或當應用程式執行時，Symantec Endpoint Protection 會套用動作。

應用程式也會出現在**「DNS 和主機檔案變更例外」**的清單中。

指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 按下**「新增」>「Windows 例外」>「應用程式」**。

3 在「**檢視**」下拉式方塊中，選取「**全部**」、「**受監控的應用程式**」或「**使用者允許的應用程式**」。

4 選取要為其建立例外的應用程式。

5 在「**動作**」下拉式方塊中，選取「**忽略**」、「**只記錄**」、「**隔離**」、「**終止**」或「**移除**」。

當掃描偵測到應用程式為不良或惡意時，會套用「**忽略**」和「**只記錄**」動作。當應用程式啟動時，會套用「**終止**」、「**隔離**」和「**移除**」動作。

6 按下「**確定**」。

請參閱第 479 頁的「在 Windows 用戶端上監控應用程式以建立應用程式的例外」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

請參閱第 284 頁的「監控在用戶端電腦執行的應用程式與服務」。

請參閱第 482 頁的「針對會變更 DNS 或主機檔案的應用程式建立例外」。

從 Windows 用戶端上的掃描中排除信任的 Web 網域

您可以從病毒和間諜軟體掃描和從 SONAR 中排除 Web 網域。排除信任的 Web 網域時，始終會允許使用者從該網域內的任何位置下載的任何檔案。不過，自動防護和其他定義的掃描仍會掃描該檔案。

依據預設，下載鑑識會排除出現在「**Internet 信任的網站**」清單上的網站，該清單位於「**Internet Explorer**」>「**工具**」>「**網際網路選項**」>「**安全性**」。您可以從「**病毒和間諜軟體防護**」政策的「下載鑑識」設定中架構此設定。

如果停用「下載鑑識」或「自動防護」，則也會停用信任的 Web 網域例外。

附註：架構例外時請務必小心。您建立的每個例外都會降低電腦的安全性設定檔。考慮傳送任何可疑的誤報進行檢查，而不是開啟永久的掃描排除。一律使用 Symantec Endpoint Protection 提供的多層防護。

報告可疑的錯誤的偵測 (誤報)

支援的 Web 網域例外

建立 Web 網域例外時，請遵循以下準則：

- 指定信任的 Web 網域例外時，您必須以 URL 或 IP 位址形式輸入單一網域。一次只能指定一個網域。
- 不支援通訊埠編號。
- 指定 URL 時，例外只會使用 URL 的網域名稱部分。您可以在 URL 之前附加 HTTP 或 HTTPS (不區分大小寫)，但是例外會套用至這兩個通訊協定。

- 當您指定 IP 位址時，例外會同時套用至指定的 IP 位址及其對應的主機名稱。如果使用者透過其 URL 瀏覽到某個位置，Symantec Endpoint Protection 會將主機名稱解析成 IP 位址並套用例外。您只能在 IP 位址之前附加 HTTP (不區分大小寫)。
- 下載鑑識和 SONAR 均會排除該網域，而不論使用者是否透過 HTTP 或 HTTPS 瀏覽至網域。
- 針對 FTP 位置，您必須指定 IP 位址。不支援 FTP URL。
- 支援將萬用字元 * 與信任的 Web 網域的例外搭配使用。

從 Windows 用戶端上的掃描中排除信任的 Web 網域

1. 在**「例外政策」**頁面上，按下**「新增」>「Windows 例外」>「信任的 Web 網域」**。
2. 在**「新增信任的 Web 網域例外」**對話方塊中，輸入要排除的網域名稱或 IP 位址。

   請參閱第 480 頁的"支援的 Web 網域例外"。
3. 按下**「確定」**。
4. 重複此程序可新增更多 Web 網域例外。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

在 Windows 用戶端上建立竄改防護例外

可以為「竄改防護」建立檔案例外。如果竄改防護會對您用戶端電腦上的已知安全性應用程式造成干擾，則您可能希望建立竄改防護例外。例如，「竄改防護」可能會攔截像螢幕閱讀器這類的輔助技術應用程式。

您需要知道與輔助技術應用程式相關聯的檔案名稱。然後您就可以建立例外，允許應用程式執行。

附註：「竄改防護」不支援資料夾例外。

在 Windows 用戶端上建立竄改防護例外

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 按下**「新增」>「Windows 例外」>「竄改防護例外」**。
3. 在**「新增竄改防護例外」**對話方塊的**「前置變數」**下拉式方塊中選擇一般資料夾。

   選擇前置字元時，可在不同的 Windows 作業系統使用例外。

   若您想輸入絕對路徑與檔案名稱，請選擇**[無]**。

4 在「**檔案**」文字方塊中，輸入檔案名稱。

若您選擇一個前置字元，路徑應與前置字元有關。若您將前置字元選為 **[NONE]**，請鍵入完整的路徑名稱。

必須指定檔案名稱。「竄改防護」不支援資料夾例外。如果輸入資料夾名稱，「竄改防護」不會排除具有該名稱的資料夾中的所有檔案。它只會排除具有該指定名稱的檔案。

5 按下「**確定**」。

請參閱如何在 Symantec Endpoint Protection 12.1 中從 Symantec Endpoint Protection Manager 收集竄改防護日誌。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

針對會變更 DNS 或主機檔案的應用程式建立例外

您可以針對會變更 DNS 或主機檔案的特定應用程式建立例外。SONAR 可能會防止 DNS 或主機檔案變更之類的系統變更。例如，您可能需要針對 VPN 應用程式建立例外。

您可以監控特定應用程式，以便建立 DNS 或主機檔案變更例外。在 Symantec Endpoint Protection 探索到應用程式且管理主控台接收事件時，該應用程式會顯示在應用程式清單中。如果網路中的用戶端電腦尚未探索到任何應用程式，則應用程式清單顯示空白。

請使用 SONAR 設定來控制 SONAR 全域偵測 DNS 或主機檔案變更的方式。

針對會變更 DNS 或主機檔案的應用程式建立例外

1 在「**例外政策**」頁面上，按下「**例外**」。

2 按下「**新增**」>「**Windows 例外**」>「**DNS 或主機檔案變更例外**」。

3 選取要為其建立例外的應用程式。

4 在「**動作**」下拉式方塊中，選取「**忽略**」、「**只記錄**」、「**提示**」或「**攔截**」。

當掃描偵測到應用程式對 DNS 或主機檔案進行變更時，就會套用動作。

5 按下「**確定**」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

請參閱第 479 頁的「指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式」。

請參閱第 428 頁的「調整用戶端電腦上的 SONAR 設定」。

在 Windows 用戶端上從掃描中排除憑證

自 14.0.1 起，您可以個別為憑證新增例外，以防止憑證簽署的檔案被掃描和偵測為可疑檔案。例如，公司內部開發的工具會使用自我簽署憑證。從掃描排除此憑證可防止自動防護、下載鑑識、SONAR 或其他掃描將其簽署的檔案偵測為可疑檔案。

憑證排除僅支援 X.509 和 base64 憑證類型。當您新增憑證例外時，將需要 DER 或 base64 編碼檔案 (.cer) 中的公用憑證的複本。

以下產品不支援憑證排除：

- 記憶體攻擊緩和
- 主動型威脅防護系統變更事件
- 竄改防護
- 壓縮檔案內憑證簽署的檔案

無需在用戶端電腦上的憑證儲存區中安裝排除的憑證，排除即可運作。如果憑證例外和黑名單規則之間發生衝突，則會優先採用黑名單規則。

您只能透過 Symantec Endpoint Protection Manager 政策，而不能透過 Symantec Endpoint Protection 用戶端介面設定，新增憑證例外。

附註：如果已從雲端主控台取消註冊 Symantec Endpoint Protection Manager，則只能在其中新增憑證例外。如果已註冊 Symantec Endpoint Protection Manager，請使用雲端主控台來新增或管理憑證例外。

在 Windows 用戶端上從掃描中排除憑證

1. 在**「例外政策」**頁面上，按下**「例外」**。
2. 在**「例外」**下方，按下**「新增」>「Windows 例外」>「憑證」**。

   如果已在雲端主控台中註冊 Symantec Endpoint Protection Manager，這個選項不會出現。請改為在雲端主控台中新增憑證例外。
3. 在**「憑證檔案」**下方，按下**「瀏覽」**來瀏覽至您要排除的憑證，然後按下**「確定」**。
4. 確認**「憑證資訊」**下方的值對您要排除的憑證來說是正確的，然後按下**「確定」**。

   若要針對多個憑證建立例外，請重複此程序。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

限制使用者可在用戶端電腦上架構的例外類型

您可以架構限制，使用戶端電腦上的使用者無法為病毒和間諜軟體掃描或SONAR建立例外。依預設，允許使用者架構例外。

無論限制設定為何，用戶端電腦上使用者都無法建立竄改防護例外。

使用者也無法建立應用程式控制的檔案例外。

限制使用者可在用戶端電腦上架構的例外類型

1 請在「**例外政策**」頁面上，按下「**用戶端限制**」。

2 在「**用戶端限制**」下，取消勾選任何您不希望使用者在用戶端電腦上架構的例外。

3 架構完此政策後，按下「**確定**」。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

從日誌事件建立例外

您可以針對病毒和間諜軟體掃描、SONAR、應用程式控制和「竄改防護」從日誌事件中建立例外。

附註：無法針對提早啟動防惡意軟體偵測從日誌事件建立例外。

表 23-5 例外和日誌類型

例外類型	日誌類型
檔案	風險日誌
資料夾	風險日誌 SONAR 日誌
已知風險	風險日誌
副檔名	風險日誌
應用程式	風險日誌 SONAR 日誌
信任的 Web 網域	風險日誌 SONAR 日誌
竄改防護	應用程式控制日誌
DNS 或主機檔案變更	SONAR 日誌

Symantec Endpoint Protection 必須已偵測到您要為其建立例外的項目。當使用日誌事件建立例外時，您可指定應包含例外的例外政策。

從日誌事件建立例外

1. 在「**監視器**」標籤上，按下「**日誌**」標籤。
2. 在「**日誌類型**」下拉式清單中，選取「風險」日誌、SONAR 日誌或「應用程式與裝置控制」日誌。
3. 如果選取了「應用程式與裝置控制」，請從「**日誌內容**」清單中選取「**應用程式控制**」。
4. 按下「**檢視日誌**」。
5. 在「**時間範圍**」旁，選取過濾日誌的時間間隔。
6. 選取要為其建立例外的一個或多個項目。
7. 在「**動作**」旁，選取要建立的例外類型。

   對於所選取的項目，您選取的例外類型必須有效。
8. 按下「**套用**」或「**開始**」。
9. 在對話方塊中，移除任何您不想包含在例外中的項目。
10. 對於安全風險，如果要 Symantec Endpoint Protection 記錄偵測，請勾選「**偵測到安全風險時記錄**」。
11. 選取所有應使用例外的例外政策。
12. 按下「**確定**」。

請參閱第 539 頁的「監控端點防護」。

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

24

管理整合

本章包含以下主題：

管理 Symantec Endpoint Protection 中的整合

Symantec Endpoint Protection Manager 中的整合政策可讓您管理與您環境中使用之其他賽門鐵克產品的整合。

表 24-1 管理整合

整合	說明
Web Security Services (WSS) 流量重新導向	(WSS) 流量重新導向 (WTR) 會將 Symantec Web Security Service 功能整合至 Symantec Endpoint Protection。您可以為您在 Symantec Web Security Service 中架構的代理自動架構 (PAC) 檔案指定 URL。您也可以啟用本機代理服務，以進一步精細控制網頁流量重新導向。 請參閱第 486 頁的「架構 WSS 流量重新導向」。

架構 WSS 流量重新導向

自 14.0.1 MP1 版起，Web Security Service (WSS) 流量重新導向 (WTR) 會將 Symantec Web Security Service 功能整合至 Symantec Endpoint Protection。Symantec Web Security Service 提供大量連線選項，以安全地重新導向網頁流量，無論使用者是在內部部署還是在企業網路外。Symantec Web Security Service 提供數種存取方法。如需詳細資訊，請參閱：

Web Security Service 存取方法

藉由向 Symantec Endpoint Protection 新增 WSS 流量重新導向，您可以自動化網頁流量重新導向至 Symantec Web Security Service，並保護使用 Symantec Endpoint Protection 之每個端點上的網頁流量。

若要在 Symantec Endpoint Protection Manager 內使用此功能，您必須具有有效的 Web Security Service 訂購授權。請聯絡您的客戶代表取得 Web Security Service 授權。

- WSS 流量重新導向的運作方式
- 架構 WSS 流量重新導向

WSS 流量重新導向的運作方式

Symantec Endpoint Protection 使用 WSS 流量重新導向功能更新代理組態瀏覽器設定。每當使用者使用網頁瀏覽器存取網站時，瀏覽器都會透過最近的雲端託管 Web Security Service 傳送所有網頁瀏覽器流量，如代理自動架構 (PAC) 檔案所定義。根據預先定義的組態，Symantec WSS 代理可以重新導向、允許或攔截流量。

自 14.2 起，您可以透過 WSS 允許進階用戶端驗證，以根據傳送網頁流量的使用者，對網頁流量進行更精細的控制。

支援 WSS 流量重新導向的瀏覽器如下：

- Microsoft Internet Explorer 9 - 11
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

架構 WSS 流量重新導向

1. 在 Symantec Endpoint Protection Manager 中，按下**「政策」>「整合」**，然後開啟**「整合」**政策。
2. 按下**「WSS 流量重新導向」>「啟用 WSS 流量重新導向」**。
3. 在**「代理自動架構 (PAC) 檔案 URL」**下，輸入有效的 PAC 檔案 URL。

   可從網路中負責管理 Symantec Web Security Service 的管理員處取得此 URL。只能在 Symantec Endpoint Protection Manager 中架構或編輯此 URL。
4. 您可以新增 WSS 整合 Token，來收集建立每個使用者規則的精細資訊。

   如果預設的 2968 不適用於您的環境，您可以定義流量攔截通訊埠。

5 (選擇性)：按下**「在用戶端上安裝 Symantec Web Security Service 根憑證，以便保護加密流量」**，在 Symantec Endpoint Protection 用戶端上安裝適當的根憑證來保護加密流量。

6 按下**「確定」**。

將政策指派給用戶端群組後，Firefox 使用者必須重新啟動瀏覽器，才會套用 WSS 流量重新導向設定。

附註： 如果您在**「用戶端使用者介面控制設定」**下按下**「混合控制」**，然後按下**「自訂」**，則用戶端使用者介面設定中不存在可用於架構 WSS 流量重新導向的選項。

25

測試安全政策

本章包含以下主題：

測試 Symantec Endpoint Protection Manager 政策

您可能需要先評估 Symantec Endpoint Protection 或測試政策，然後才能將它們下載到用戶端電腦。 您可以使用 Symantec Endpoint Protection Manager 政策來測試下列功能，以確保產品能在用戶端電腦上正確運作。

表 25-1 您可以測試的功能

功能	請參閱本主題
病毒和間諜軟體防護	若要測試預設病毒和間諜軟體防護政策，請從以下位置下載 EICAR 測試病毒： http://www.eicar.org/86-0-Intended-use.html 請參閱第 490 頁的「測試病毒和間諜軟體防護政策」。
SONAR	下載 Socar.exe 測試檔以確認 SONAR 運作是否正常

功能	請參閱本主題
Insight	如何測試 Insight 與賽門鐵克授權伺服器的連線能力
入侵預防	測試預設 IPS 政策
應用程式控制	請參閱第 490 頁的「攔截程序在用戶端電腦上啟動」。 請參閱第 491 頁的「防止使用者寫入用戶端電腦上的登錄」。 請參閱第 492 頁的「防止使用者寫入特定檔案」。 請參閱第 494 頁的「新增和測試攔截 DLL 的規則 」。 請參閱第 495 頁的「新增和測試終止程序的規則」。

測試病毒和間諜軟體防護政策

若要測試並檢查病毒和間諜軟體防護政策是否起作用，您可以使用測試病毒檔 eicar.com。EICAR 測試病毒是歐洲電腦防毒研究協會 (European Institute for Computer Antivirus Research，EICAR) 所開發的文字檔，其提供了簡單且安全的方式來測試大多數的防毒軟體。您可以使用它來確認用戶端防毒部分的運作情況。

測試病毒和間諜軟體防護政策

1. 在用戶端電腦上，從 EICAR 網站下載防毒測試檔，網址如下：

   http://2016.eicar.org/86-0-Intended-use.html
2. 執行 EICAR 測試檔。

   系統會顯示通知，表示發現風險。
3. 在 Symantec Endpoint Protection Manager 的「**監視器**」頁面上，按下「**日誌**」。
4. 在「**日誌**」標籤的「**日誌類型**」下拉式清單中，按「**風險**」，再按下「**檢視日誌**」。
5. 在「**風險日誌**」頁面上，會出現「**發現病毒事件**」。

攔截程序在用戶端電腦上啟動

FTP 用戶端是將檔案從伺服器傳輸至用戶端電腦的常見方式。若要防止使用者傳輸檔案，您可以新增規則來攔截使用者從命令提示字元啟動 FTP 用戶端。

新增攔截程序在用戶端電腦上啟動的規則

1. 開啟應用程式控制政策，然後在「**應用程式控制**」窗格中按下「**新增**」。
2. 在「**應用程式控制規則集**」對話方塊的「**規則**」清單中選取規則，然後在「**屬性**」標籤的「**規則名稱**」文字方塊中輸入 **ftp_ blocked_from_cmd**。
3. 在「**套用此規則至下列程序**」右側，按下「**新增**」。

4 在「**新增程序定義**」對話方塊的「**要比對的程序名稱**」下方，輸入 **cmd.exe**，然後按下「**確定**」。

5 在「**應用程式控制規則集**」對話方塊的「**規則**」清單下方，按下「**新增條件**」>「**啟動程序嘗試**」。

6 在「**屬性**」標籤的「**敘述**」文字方塊中，輸入 **no ftp from cmd**。

7 在「**套用此規則至下列程序**」右側，按下「**新增**」。

8 在「**新增程序定義**」對話方塊的「**要比對的程序名稱**」下方，輸入 **ftp.exe**，然後按下「**確定**」。

9 在「**應用程式控制規則集**」對話方塊的「**動作**」標籤上，按下「**攔截存取**」、「**啟用記錄**」和「**通知使用者**」。

10 在「**通知使用者**」下方，輸入 **ftp is blocked if launched from the cmd**。

11 按下「**確定**」兩次，然後將政策指派給群組。

測試規則。

測試攔截程序在用戶端電腦上啟動的規則

1 在用戶端電腦上，開啟命令提示字元。

2 在命令提示字元視窗中，輸入 **ftp**，然後按 **Enter** 鍵。

由於已指定規則，FTP 用戶端不會開啟。

防止使用者寫入用戶端電腦上的登錄

您可以保護特定的登錄機碼，防止使用者存取或修改登錄中的任何登錄機碼或值。您可以允許使用者檢視登錄機碼，但不能重新命名或修改登錄機碼。

若要測試功能：

- 新增測試登錄機碼。
- 新增可以讀取但無法寫入登錄機碼的規則。
- 嘗試將新值加入到登錄機碼。

新增測試登錄機碼

1 在用戶端電腦上，開啟指令行並輸入 **regedit**，以開啟登錄檔編輯器。

2 在登錄檔編輯器中，展開 HKEY_LOCAL_MACHINE\Software，然後建立名為 test 的新登錄機碼。

防止使用者寫入用戶端電腦上的登錄

1 開啟應用程式控制政策，然後在「**應用程式控制**」窗格中按下「**新增**」。

2 在「**應用程式控制規則集**」的「**規則**」清單下方，按下「**新增**」>「**新增規則**」。

3 在「**屬性**」標籤的「**規則名稱**」文字方塊中，輸入 **HKLM_write_not_allowed_from_regedit**。

4 在「**套用此規則至下列程序**」右側，按下「**新增**」。

5 在「**新增程序定義**」對話方塊的「**要比對的程序名稱**」下方，輸入 **regedit.exe**，然後按下「**確定**」。

6 在「**應用程式控制規則集**」對話方塊的「**規則**」清單下方，按下「**新增**」>「**新增條件**」>「**登錄存取嘗試**」。

7 在「**屬性**」標籤的「**敘述**」文字方塊中，輸入「**登錄存取**」。

8 在「**套用此規則至下列程序**」右側，按下「**新增**」。

9 在「**新增登錄機碼定義**」對話方塊的「**登錄機碼**」文字方塊中，輸入 **HKEY_LOCAL_MACHINE\software\test**，然後按下「**確定**」。

10 在「**應用程式控制規則集**」對話方塊的「**動作**」標籤上，按下「**讀取嘗試**」群組方塊中的「**允許存取**」、「**啟用記錄**」和「**通知使用者**」。

11 在「**通知使用者**」下方，輸入「**允許讀取**」。

12 在「**建立、刪除或寫入嘗試**」群組方塊中，按下「**攔截存取**」、「**啟用記錄**」和「**通知使用者**」。

13 在「**通知使用者**」下方，輸入「**攔截寫入**」。

14 按下「**確定**」兩次，然後將政策指派給群組。

測試規則。

測試攔截寫入登錄的規則

1 套用政策之後，在用戶端電腦的登錄檔編輯器中，展開 HKEY_LOCAL_MACHINE\Software。

2 按下先前建立名為 test 的登錄機碼。

3 用滑鼠右鍵按下測試機碼，然後按下「**新增**」，再按「**字串值**」。

您應無法將新值加入到測試登錄機碼。

防止使用者寫入特定檔案

您可能會想要使用者可以檢視但無法修改檔案。例如，檔案可能包含員工應檢視但不該編輯的財務資料。

您可以建立應用程式和裝置控制規則，將檔案的唯讀存取權限授予使用者。例如，您可以新增規則，來允許您在記事本中開啟文字檔案而不允許您編輯此檔案。

新增防止使用者寫入特定檔案的規則

1 開啟應用程式控制政策，然後在**「應用程式控制」**窗格中按下**「新增」**。

2 在**「應用程式控制規則集」**的**「規則」**清單下方，按下**「新增」>「新增規則」**。

3 在**「屬性」**標籤的**「規則名稱」**文字方塊中，輸入 **1.txt in c read allowed write terminate**。

4 在**「套用此規則至下列程序」**右側，按下**「新增」**。

5 在**「新增程序定義」**對話方塊的**「要比對的程序名稱」**下方，輸入 **notepad.exe**，然後按下**「確定」**。

6 在**「應用程式控制規則集」**對話方塊的**「規則」**清單下方，按下**「新增」>「新增條件」>「檔案和資料夾存取嘗試」**。

7 在**「屬性」**標籤的**「敘述」**文字方塊中，輸入 **file access launched** 。

8 在**「套用此規則至下列程序」**右側，按下**「新增」**。

9 在**「新增檔案或資料夾定義」**對話方塊中，將 **c:\1.txt** 輸入**「要比對的檔案或資料夾名稱」**群組方塊的文字方塊中，然後按下**「確定」**。

10 在**「應用程式控制規則集」**對話方塊的**「動作」**標籤上，選取**「讀取嘗試」**群組方塊中的**「允許存取」**，然後勾選**「啟用記錄」**和**「通知使用者」**。

11 在**「通知使用者」**下方，輸入**「允許讀取」**。

12 在**「建立、刪除或寫入嘗試」**群組方塊中，按下**「攔截存取」**、**「啟用記錄」**和**「通知使用者」**。

13 在**「通知使用者」**下方，輸入 **writing to block Notepad**。

14 按兩次**「確定」**，然後將政策指派給用戶端電腦群組。

測試規則。

測試防止使用者寫入特定檔案的規則

1 在用戶端電腦上，開啟「檔案總管」，找到 c:\ 磁碟機，然後按下**「檔案」>「新增」>「文字文件」**。

如果您使用「記事本」建立檔案，檔案會是唯讀檔案。

2 將檔案重新命名為 1.txt。

確定檔案儲存到 c:\ 資料夾。

3 在「記事本」中開啟 c:\1.txt 檔案。

您可以開啟檔案但無法編輯它。

新增和測試攔截 DLL 的規則

您可能會想防止使用者開啟特定應用程式。攔截使用者開啟應用程式的方法之一，就是攔截應用程式執行所需的 DLL。若要攔截 DLL，您可以建立攔截 DLL 載入的規則。當使用者嘗試開啟應用程式時，即無法開啟應用程式。

例如，Msvcrt.dll 檔案包含用來執行如 Microsoft WordPad 等多項 Windows 應用程式的程式碼。如果您新增規則來攔截用戶端電腦上的 Msvcrt.dll，就無法開啟 Microsoft WordPad

---

附註：以「重視安全性」為前提撰寫的某些應用程式可能會將 DLL 植入解讀為惡意動作。請採取因應措施來攔截植入或移除 DLL。

新增攔截 DLL 的規則

1. 開啟應用程式控制政策，然後在**「應用程式控制」**窗格中按下**「新增」**。
2. 在**「應用程式控制規則集」**的**「規則」**清單下方，按下**「新增」>「新增規則」**。
3. 在**「屬性」**標籤的**「規則名稱」**文字方塊中，輸入**「攔截使用者開啟 Microsoft Wordpad」**。
4. 在**「套用此規則至下列程序」**右側，按下**「新增」**。
5. 在**「新增程序定義」**對話方塊的**「要比對的程序名稱」**下方，輸入 **C:\Program Files\Windows NT\Accessories\wordpad.exe**，然後按下**「確定」**。
6. 在**「應用程式控制規則集」**對話方塊的**「規則」**清單下方，按下**「新增」>「新增條件」>「載入 DLL 嘗試」**。
7. 在**「屬性」**標籤的**「敘述」**文字方塊中，輸入**「已攔截 DLL」**。
8. 在**「套用至下列 DLL」**右側，按下**「新增」**。
9. 在**「新增 DLL 定義」**對話方塊中，將 **MSVCRT.dll** 輸入**「要比對的 DLL 名稱」**群組方塊的文字方塊中，然後按下**「確定」**。
10. 在**「應用程式控制規則集」**對話方塊的**「動作」**標籤上，按下**「攔截存取」**、**「啟用記錄」**和**「通知使用者」**。
11. 在**「通知使用者」**下方，輸入**「應無法載入 WordPad」**。
12. 按兩次**「確定」**，然後將政策指派給用戶端電腦群組。

    測試規則。

測試攔截 DLL 的規則

- 在用戶端電腦上，嘗試開啟 Microsoft WordPad。

新增和測試終止程序的規則

Process Explorer 是一項工具，可顯示已開啟或載入的 DLL 程序，以及程序使用哪些資源。您也可以使用 Process Explorer 終止程序。您可以新增一項規則：如果使用者使用 Process Explorer 嘗試終止「小算盤」應用程式，即終止 Process Explorer。

新增終止程序的規則

1. 開啟應用程式控制政策，然後在**「應用程式控制」**窗格中按下**「新增」**。
2. 在**「應用程式控制規則集」**的**「規則」**清單下方，按下**「新增」>「新增規則」**。
3. 在**「屬性」**標籤的**「規則名稱」**文字方塊中，輸入**「如果 Process Explorer 嘗試終止 calc.exe，即終止 Process Explorer」**。
4. 在**「套用此規則至下列程序」**右側，按下**「新增」**。
5. 在**「新增程序定義」**對話方塊的**「要比對的程序名稱」**下方，輸入 **procexp.exe**，然後按下**「確定」**。
6. 在**「應用程式控制規則集」**對話方塊的**「規則」**清單下方，按下**「新增」>「新增條件」>「終止程序嘗試」**。
7. 在**「屬性」**標籤的**「敘述」**文字方塊中，輸入**「已停止 DLL」**。
8. 在**「套用此規則至下列程序」**右側，按下**「新增」**。
9. 在**「新增程序定義」**對話方塊中，將 **calc.exe** 輸入**「要比對的程序名稱」**群組方塊的文字方塊中，然後按下**「確定」**。
10. 在**「應用程式控制規則集」**對話方塊的**「動作」**標籤上，按下**「終止程序」**、**「啟用記錄」**和**「通知使用者」**。
11. 在**「通知使用者」**下方，輸入**「如果您嘗試從 procexp 終止 calc，procexp 即會終止」**。
12. 按下**「確定」**兩次，然後將政策指派給群組。

    測試規則。

測試終止程序的規則

1. 在用戶端電腦上，從下列網址下載並執行免費版本的 Process Explorer：

   http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
2. 在 Windows 中開啟「小算盤」。
3. 開啟 Process Explorer。
4. 在 **Process Explorer** 視窗中，用滑鼠右鍵按下 `calc.exe` 程序，然後按下 **Kill Process**。

   Process Explorer 即會終止。

測試預設 IPS 政策

若要測試預設 IPS 政策，您必須先觸發用戶端電腦上的事件。

測試預設 IPS 政策

1. 重新命名可執行檔 (.exe) 為 jpeg (.jpg)。
2. 將 .jpg 檔案上傳到 Web 伺服器\站台。
3. 在用戶端電腦上，使用網頁瀏覽器開啟重新命名的可執行檔。

附註：若要開啟重新命名的可執行檔，您必須使用 IP 位址存取 Web 伺服器\站台。例如，您可以輸入：**http://*web server IP address*/*renamed executable*.jpg**

---

4. 如果用戶端上的 IPS 政策運作正常，會發生下列事件：
   - 您應無法開啟 .jpg 檔案。
   - 通知區域圖示中的訊息指出用戶端已攔截 .jpg 檔案。
   - 您可以開啟安全日誌並尋找指出用戶端已攔截 .jpg 檔案的日誌項目。

部分 5

從 Symantec Endpoint Protection Cloud 入口網站管理用戶端

26

使用 Symantec Endpoint Protection Cloud 入口網站

本章包含以下主題：

Symantec Endpoint Protection 14.2 雲端主控台簡介

https://embed.ustudio.com/embed/DXPQbyHsEtqf/Uh8109teSTtB

雲端主控台納入了進階能見度和控制，以偵測並矯正您環境中的新興威脅。

雲端主控台還利用 Symantec Endpoint Protection 的進階機器學習功能來提供可疑檔案的能見度，以及防惡意軟體之基於政策的密集型控制。進階機器學習不需要特徵即可確定已阻止您環境中的威脅。

下列是在註冊 Symantec Endpoint Protection Manager 網域時取得的功能的高階摘要：

- 使用密集型防護政策搜尋並攔截可疑偵測

- 可針對低頻寬環境最佳化的產品組態
- 利用集中的黑名單和許可清單的整合式錯誤管理
- 用於管理進階功能的現代雲端主控台

請參閱第 499 頁的「在 Symantec Endpoint Protection Manager Console 的雲端主控台中註冊 14.1/14.2 網域」。

在 Symantec Endpoint Protection Manager Console 的雲端主控台中註冊 14.1/14.2 網域

若要使用雲端主控台，您必須先從 Symantec Endpoint Protection Manager Console 的**「首頁」**註冊您的網域。

附註：最多可以註冊 10 個網域。

---

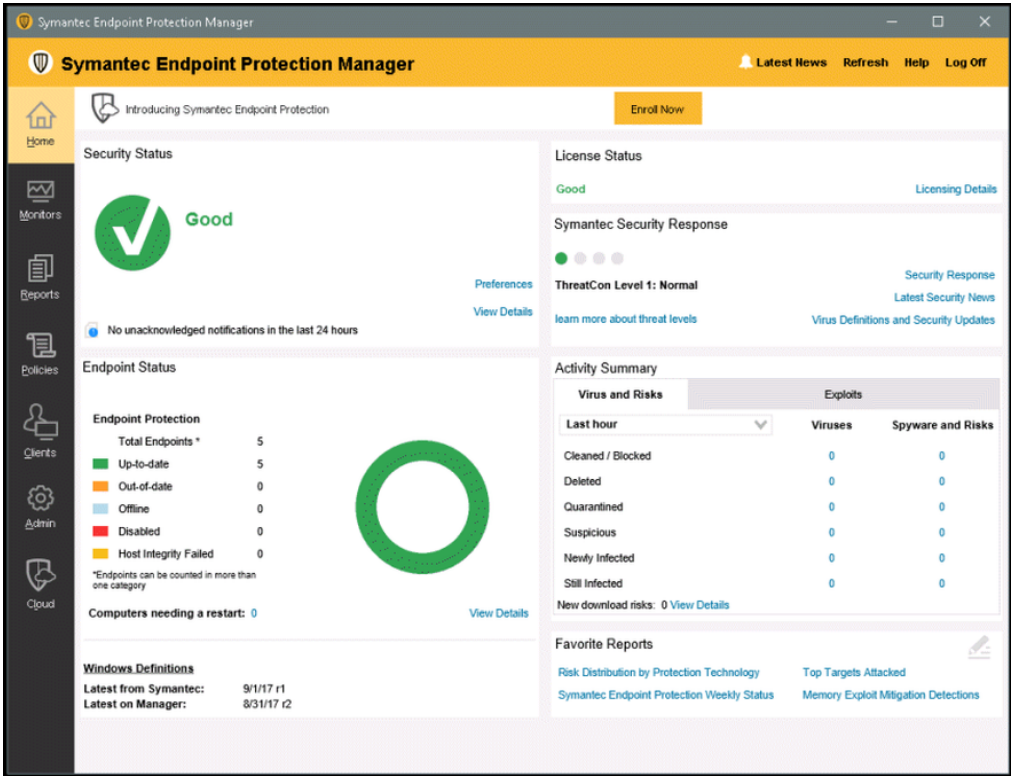
https://embed.ustudio.com/embed/DXPQbyHsEtqf/USbzokAGGD77

附註：**向雲端主控台註冊會使用 .MSI 檔案安裝 Symantec Endpoint Protection Manager Bridge。開始註冊之前，將應用程式與裝置控制置於測試 (只記錄) 模式以及將系統鎖定置於只記錄模式。只有在此類政策套用至執行 Symantec Endpoint Protection Manager 所在的伺服器且政策攔截 .MSI 安裝時，此情況才適用。

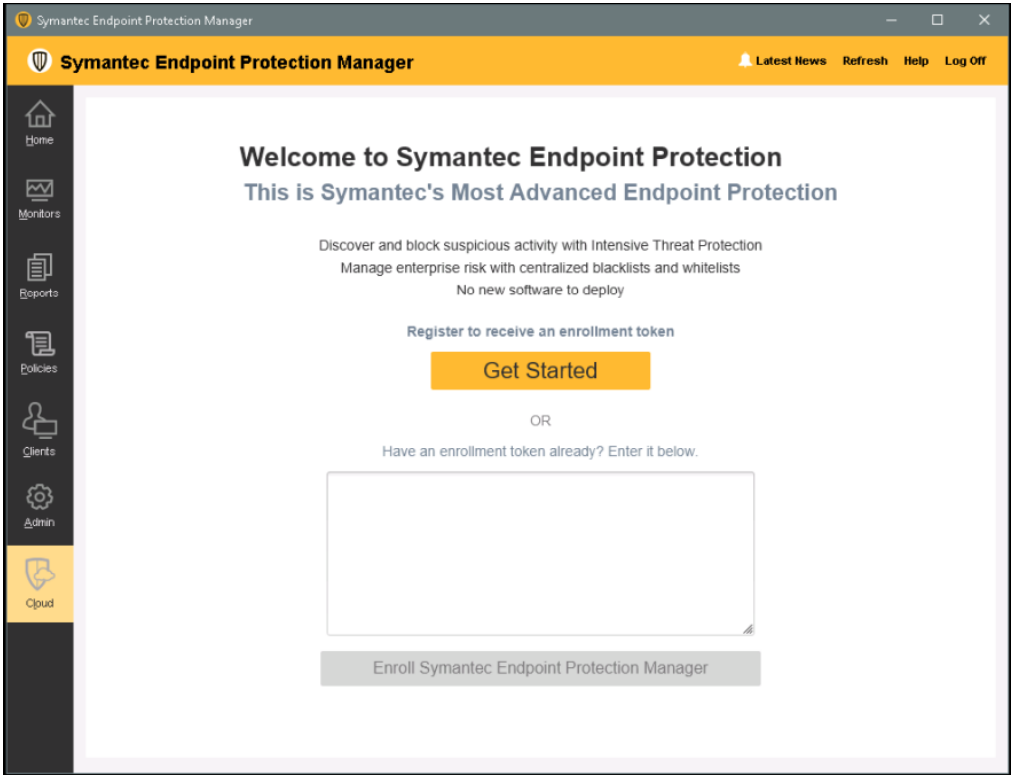
請參閱啟用和測試預設應用程式規則和啟用系統鎖定前設定和測試系統鎖定組態。

開始註冊

◆ 在 Symantec Endpoint Protection Manager 主控台中，按下**「立即註冊」**。


Symantec Endpoint Protection Manager
Symantec Endpoint Protection Manager
Latest News
Refresh
Help
Log Off
Home
Monitors
Reports
Policies
Clients
Admin
Cloud
Introducing Symantec Endpoint Protection
Enroll Now
Security Status
Good
Preferences
View Details
No unacknowledged notifications in the last 24 hours
License Status
Good
Licensing Details
Symantec Security Response
ThreatCon Level 1: Normal
learn more about threat levels
Security Response
Latest Security News
Virus Definitions and Security Updates
Endpoint Status
Endpoint Protection
Total Endpoints * 5
Up-to-date 5
Out-of-date 0
Offline 0
Disabled 0
Host Integrity Failed 0
*Endpoints can be counted in more than one category
Computers needing a restart: 0
View Details
Windows Definitions
Latest from Symantec: 9/1/17 r1
Latest on Manager: 8/31/17 r2
Activity Summary
Virus and Risks
Exploits
Last hour
Viruses
Spyware and Risks
Cleaned / Blocked 0 0
Deleted 0 0
Quarantined 0 0
Suspicious 0 0
Newly Infected 0 0
Still Infected 0 0
New download risks: 0 View Details
Favorite Reports
Risk Distribution by Protection Technology
Top Targets Attacked
Symantec Endpoint Protection Weekly Status
Memory Exploit Mitigation Detections

註冊頁面隨即出現。


Symantec Endpoint Protection Manager
Symantec Endpoint Protection Manager
Latest News
Refresh
Help
Log Off
Home
Monitors
Reports
Policies
Clients
Admin
Cloud
Welcome to Symantec Endpoint Protection
This is Symantec's Most Advanced Endpoint Protection
Discover and block suspicious activity with Intensive Threat Protection
Manage enterprise risk with centralized blacklists and whitelists
No new software to deploy
Register to receive an enrollment token
Get Started
OR
Have an enrollment token already? Enter it below.
Enroll Symantec Endpoint Protection Manager

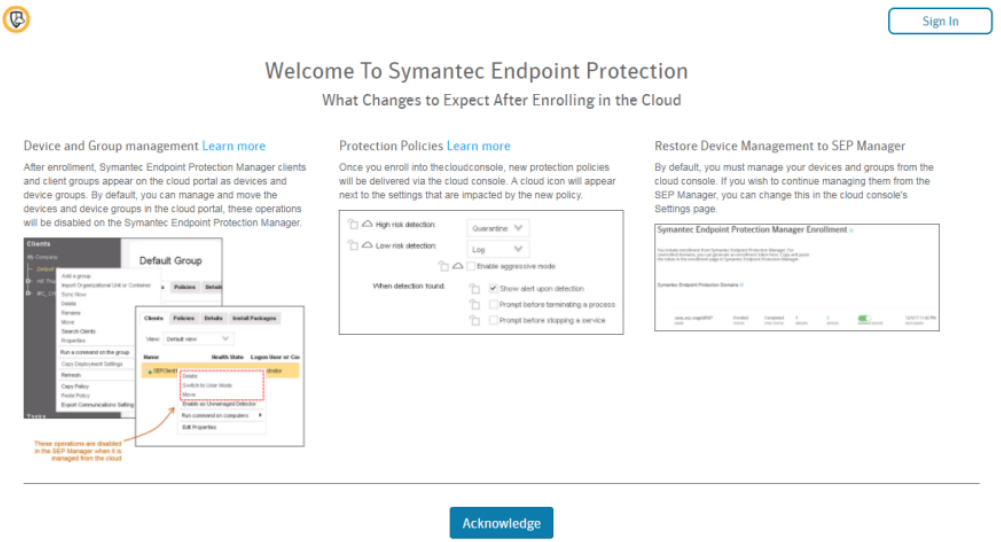
取得註冊碼

1 在 Symantec Endpoint Protection Manager 的「**雲端**」頁面上，按下「**開始使用**」。

附註：如果遇到隱私權錯誤，則可能需要安裝憑證。請參閱下列文章：

使用網頁瀏覽器來檢視管理主控台時發生憑證錯誤

認可頁面隨即出現。

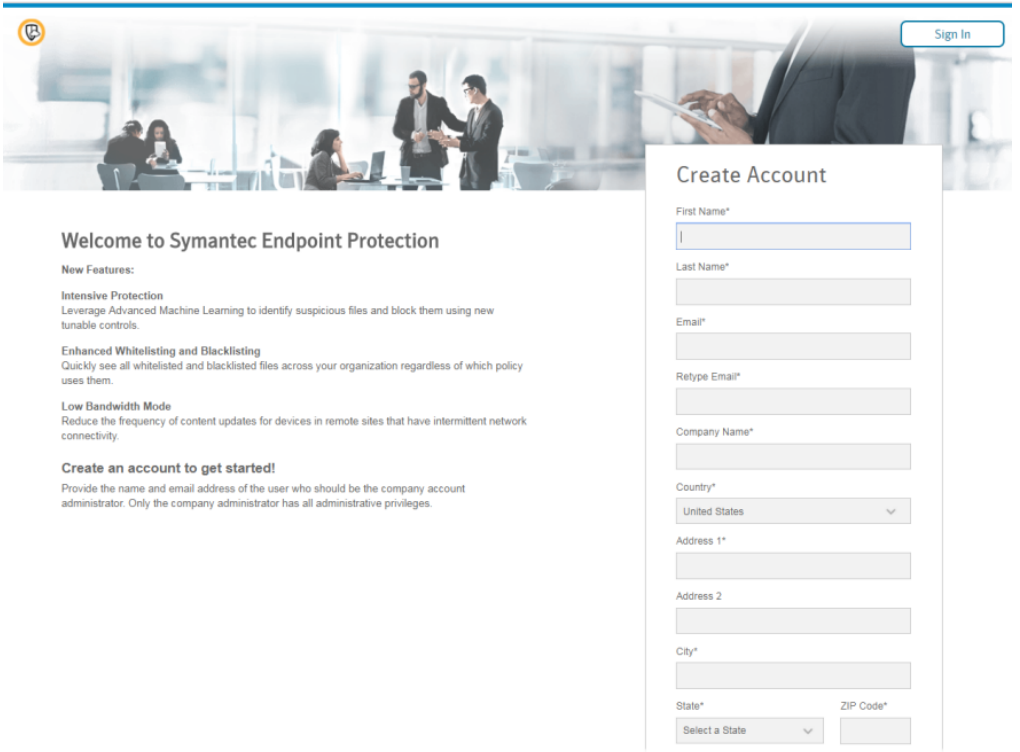


2 按下「**認可**」。

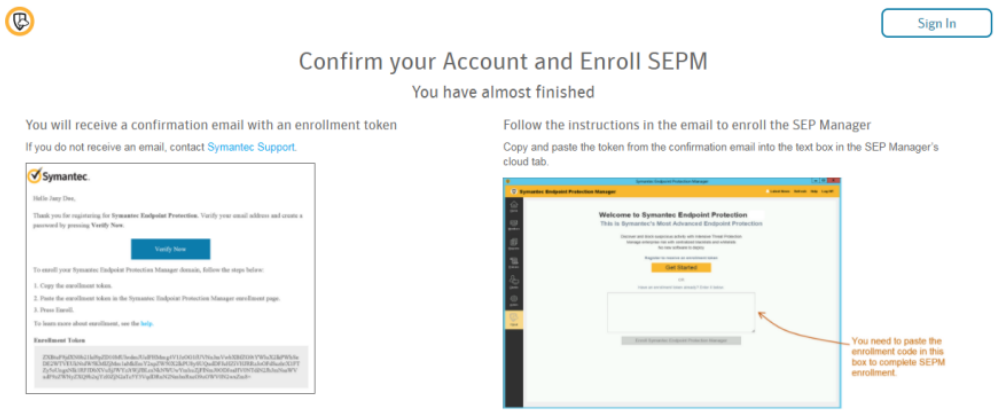
附註：請確定您已閱讀相關頁面以瞭解註冊 Symantec Endpoint Protection Manager 網域後，裝置 (用戶端) 和群組管理中將會發生的變更。

3 建立帳戶或使用現有憑證登入 (如果有的話)。

4 若要建立帳戶，請在表單中輸入您的資訊，並選取「**建立帳戶**」。您提供的電子郵件地址可用來傳送您的驗證和網域註冊資訊。



確認頁面隨即出現。



5 接收驗證電子郵件時，在電子郵件中選取**「驗證」**來驗證您的帳戶。

完成註冊

1 從電子郵件複製註冊碼，並將代碼貼上 Symantec Endpoint Protection Manager 註冊頁面。

2 註冊之後，您的所有裝置會出現在雲端主控台中。裝置包含您的用戶端和用戶端群組。依據預設，Symantec Endpoint Protection Manager 會管理拓樸。如果您想要從雲端主控台管理群組和裝置，稍後在雲端主控台的**「設定」>「Symantec Endpoint Protection Manager 註冊」**中，僅針對登入的網域關閉**「管理裝置」**選項。

如果您使用 Active Directory 或第三方 API 來管理裝置，則應該保持停用此選項。

警告：每當您對裝置群組結構進行變更時，均會延遲 10 分鐘，變更才會在 Symantec Endpoint Protection Manager 中出現。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓樸變更。變更可能不會生效。

附註：網域註冊後，雲端主控台一律會管理支援雲端的政策，而不論**「管理裝置」**設定為何。

---

3 選取**「註冊」**。

您會看見確認訊息。

4 現在您可以使用 Symantec Endpoint Protection Manager**「首頁」**橫幅中的**「啟動」**按鈕來登入雲端主控台。

如何將註冊網域雲端主控台功能與內部部署 Symantec Endpoint Protection Manager 相比較

註冊 Symantec Endpoint Protection Manager 網域後，可以在雲端主控台和 Symantec Endpoint Protection Manager 中管理政策。

表 26-1 功能參考

Symantec Endpoint Protection 雲端主控台	Symantec Endpoint Protection Manager
裝置、裝置群組 預設由 Symantec Endpoint Protection Manager 管理 註冊設定中的「**管理裝置**」選項會控制雲端主控台是否組織裝置和裝置群組。 **附註：**每當您對裝置群組結構進行變更時，均會延遲 10 分鐘，變更才會在 Symantec Endpoint Protection Manager 中出現。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓樸變更。變更可能不會生效。	**用戶端、用戶端群組** 當網域的主要裝置選項(「**管理裝置**」)已啟用時，您必須使用雲端主控台來組織用戶端和用戶端群組。 如果您使用 Symantec Endpoint Protection Manager、Active Directory，或使用第三方 API 來管理裝置，則應該停用此選項。 **附註：**雲端主控台一律會管理其支援的政策，而不論「**管理裝置**」設定為何。Symantec Endpoint Protection Manager 會繼續管理在雲端主控台中無法使用的任何政策。
政策群組	沒有對應的組態。
政策繼承 在雲端主控台中，政策繼承永遠為啟用狀態。不過，您始終可以直接將政策套用至子群組，以覆寫父系政策。	**政策繼承** 在 Symantec Endpoint Protection Manager 中，如果您想要直接將政策套用至子群組，則必須停用政策繼承。 **附註：**如果您取消註冊網域，從雲端主控台直接套用至子群組的任何 MEM 政策都會套用至子群組及其位置，而不論 Symantec Endpoint Protection Manager 繼承設定為何。
雲端主控台中的可用政策： ■ 密集型防護政策 ■ 系統政策 (僅限低頻寬選項) ■ 許可清單政策 ■ 黑名單政策 ■ MEM 政策	**其他政策將繼續在 Symantec Endpoint Protection Manager 中進行管理：** ■ 防火牆政策 ■ 入侵預防政策 ■ 應用程式與裝置控制政策 ■ LiveUpdate 政策 ■ 主機完整性政策 ■ 除 Bloodhound、SONAR 啟發式、下載鑑識和掃描動作以外的病毒和間諜軟體防護政策選項 **附註：**Symantec Endpoint Protection 15 提供完整的雲端管理主控台。

Symantec Endpoint Protection 雲端主控台	Symantec Endpoint Protection Manager
密集型防護政策 網域註冊後自動套用至 Windows 用戶端 (自 14.0.1 版起) 針對 Windows 用戶端取代病毒和間諜軟體防護政策中的一些設定	**病毒和間諜軟體防護政策中的下載鑑識、Bloodhound 和 SONAR 設定** 當網域已在雲端主控台中註冊時，下列設定不適用於 Symantec Endpoint Protection 14.0.1 用戶端： ■ 病毒和間諜軟體防護政策偵測動作 ■ Bloodhound 設定 ■ 下載鑑識靈敏度滑動軸 ■ 下載鑑識感染狀況、首次出現和內部網路選項 ■ SONAR 啟發式偵測、SONAR 主動模式和 SONAR 可疑行為設定 如果您取消註冊網域，這些設定仍將用於舊版用戶端以及 14.0.1 用戶端。 **附註：**預設的「密集型防護」攔截層級較「病毒和間諜軟體防護」政策中的最主動 Bloodhound 設定不主動。如果您目前的政策將 Bloodhound 指定在其最高層級，則可能需要增加密集型防護層級。
許可清單政策 即使取消註冊網域，您在雲端中建立的任何許可清單政策都會出現在 Symantec Endpoint Protection Manager 中。	**例外政策** 來自雲端主控台的項目會出現在**「例外」**清單中。
黑名單政策 即使將網域取消註冊，您在雲端中建立的任何黑名單政策仍會出現在 Symantec Endpoint Protection Manager 中。 **附註：**黑名單政策是一種應用程式控制類型，其使用 Symantec Endpoint Protection Manager 中的 SONAR 技術來強制執行其規則。它不會使用 Symantec Endpoint Protection Manager 中的應用程式控制驅動程式。	**例外政策** 來自雲端主控台的黑名單政策並非掃描例外。但是，來自雲端主控台的黑名單項目會出現在**「例外」**清單中。

Symantec Endpoint Protection 雲端主控台	Symantec Endpoint Protection Manager
雲端主控台例外類型 ■ 憑證 ■ 檔案名稱 ■ 網域 ■ 雜湊 ■ 路徑 ■ 副檔名 ■ IPS 主機	**僅限 Symantec Endpoint Protection Manager 例外類型** 網域註冊後，只能為雲端主控台中不支援的類型建立例外。 ■ 已知風險 ■ 副檔名 ■ 竄改防護 ■ DNS 和主機檔案變更 ■ 要監控的應用程式 ■ Linux 例外 ■ Mac 例外
系統政策：低頻寬選項 預設值為關閉。	沒有對應的選項。 只能在雲端主控台中啟用或停用低頻寬選項。 Symantec Endpoint Protection Manager 會顯示低頻寬狀態。您可以在**「外部通訊」>「雲端設定」**中查看是否已啟用低頻寬選項。 Symantec Endpoint Protection Manager 還會管理低頻寬運作所需的 LiveUpdate AML 內容。
攻擊緩和政策 政策選項可與 Symantec Endpoint Protection Manager 中的選項相比。	**記憶體攻擊緩和政策** 當網域已在雲端註冊時，無法架構政策設定。
低頻寬政策需要將低頻寬 AML 內容下載至用戶端。 內容不受控制或是顯示在雲端主控台中。	**低頻寬 AML 內容**。 內容類型已下載至 Symantec Endpoint Protection Manager 或用戶端，使得低頻寬選項能夠運作。
瀏覽器隔離政策 **應用程式隔離政策** **平台安全政策** **信任的更新程式政策** 這些政策需要應用程式隔離的授權。	裝置僅直接從雲端主控台接收 Application Isolation 政策。無法在 Symantec Endpoint Protection Manager 中架構這些政策。 **附註：**如果您的裝置透過 Symantec Endpoint Protection Manager 進行註冊，隔離政策不會出現在 Symantec Endpoint Protection Manager 中。 Symantec Endpoint Protection Manager 不會收集任何與這些政策相關的日誌。
應用程式控制政策 需要授權。	**應用程式與裝置控制政策** **系統鎖定** 您可以繼續使用這些 Symantec Endpoint Protection Manager 政策，但與雲端中的 Application Control 可能存在某些衝突。

Symantec Endpoint Protection 雲端主控台	Symantec Endpoint Protection Manager
管理員角色 ■ 超級管理員 ■ 限制的管理員 ■ 檢視者	**管理員角色** ■ 系統管理員 ■ 管理員 (基於網域) ■ 限制的管理員 (基於政策) 雲端主控台管理員和 Symantec Endpoint Protection Manager 管理員未以任何形式連結。
主控台逾時 您無法變更此逾時期間。逾時為 30 分鐘。	**主控台逾時** 預設為 1 小時。您可以變更逾時。
無法使用。 所有政策變更會即時發生。	**「活動訊號」**選項

Symantec Endpoint Protection Manager 如何與雲端主控台互動

本節列出了在雲端主控台中註冊 Symantec Endpoint Protection Manager 網域時可能發生的一些預期行為。

- 雲端主控台與 Symantec Endpoint Protection Manager 之間的通訊和註冊
- 授權、安裝、升級、資料庫
- 網域、網站、遠端複製
- 群組、用戶端、位置
- 政策和繼承

雲端主控台與 Symantec Endpoint Protection Manager 之間的通訊和註冊

- 如果 Symantec Endpoint Protection Manager 連接器無法取得雲端主控台的存取 Token，它會每小時重試一次。
- 透過 Symantec Endpoint Protection Manager 連線的用戶端可能不會立即在雲端主控台中顯示正確的線上狀態。在線上狀態變更後，可能需要 5-10 分鐘才能看到目前狀態的準確反映。
  檢查用戶端是否已連線至管理伺服器且受保護
- 管理伺服器與 Amazon Web Services (AWS) 伺服器的系統時間相差必須在 10 分鐘以內。否則，註冊會失敗，並且您會看到以下錯誤訊息：

```
Enrollment in the cloud console cannot complete because the Symantec Endpoint
Protection Manger computer date and time does not match the current date
and time. Change the setting in the Control Panel, and then retry the
enrollment.
```

若要解決時間不相符問題，請將 Symantec Endpoint Protection Manager 伺服器與網路時間通訊協定 (NTP) 同步。請參閱下列各項以取得詳細資訊：
http://www.ntp.org

- 您可以使用以下日誌來疑難排解失敗的註冊：`BRIDGE_INSTALL.log`、`catalinaWs.out`、`Cloud-0.log`、`scm-server-0.log` 和 `semapisrv_access_log.date.log`。所有這些檔案皆位於 Symantec Endpoint Protection Manager 安裝資料夾內的 \tomcat\logs 中。

請參閱第 499 頁的「在 Symantec Endpoint Protection Manager Console 的雲端主控台中註冊 14.1/14.2 網域」。

請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。

授權、安裝、升級、資料庫

- 無需單獨授權即可在雲端主控台中使用或註冊；雲端主控台授權是免費的。只需要 Symantec Endpoint Protection 的授權。
- 無法從雲端主控台升級管理伺服器。
- 無法從雲端備份或還原內嵌資料庫或 Symantec Endpoint Protection Manager 設定。仍在 Symantec Endpoint Protection Manager 中備份和還原資料庫與設定。
- 若要釋放授權，Symantec Endpoint Protection Manager 資料庫會根據所指定的天數刪除未連線至網域的用戶端。在雲端主控台中，30 天後會自動刪除這些用戶端，且無法架構此間隔。首先會刪除 Symantec Endpoint Protection Manager 資料庫中的用戶端，然後刪除雲端主控台中的用戶端。請參閱第 86 頁的「從資料庫清除過時的用戶端以使更多授權可用」。

網域、網站、遠端複製

- 對於每個網站，可在雲端主控台中針對每個網站註冊一個 Symantec Endpoint Protection Manager 網域。即使網域位於不同的網站，也無法註冊多個網域。如果您使用相同的雲端主控台帳戶，也無法註冊單獨的 Symantec Endpoint Protection Manager 網域。
- 對於具有兩個 Symantec Endpoint Protection Manager (共用 SQL Server 資料庫且架構進行容錯移轉)的網站，您可以從其中一個管理伺服器註冊一個網域。在每個管理伺服器與雲端主控台之間通訊的 Bridge 服務一次在一個管理伺服器上執行。該服務首先在具有較高伺服器優先順序的管理伺服器上執行。如果第一個 Bridge 服務當機，則會改為執行第二個管理伺服器的服務。一次只能從雲端主控台管理一個網域。雲端主控台與每個管理伺服器之間的同步會同時發生。

表 26-2 顯示當您註冊 Symantec Endpoint Protection Manager 網域時雲端主控台支援的網站組態。

表 26-2 雲端主控台支援的網站組態

網站組態	在雲端主控台上受支援
一個網站、一台電腦上的一個 Symantec Endpoint Protection Manager (僅搭配內嵌資料庫)	是
一個網站、一台電腦上的一個 Symantec Endpoint Protection Manager，搭配第二台電腦上的 Microsoft SQL Server 資料庫	是
一個網站、多個 Symantec Endpoint Protection Manager	是
多個網站、每個網站上的一個 Symantec Endpoint Protection Manager，搭配遠端複製*	是 (自 14.2 版起)
多個網站、每個網站上的多個 Symantec Endpoint Protection Manager，搭配遠端複製*	是 (自 14.2 版起)

* 僅支援遠端複製夥伴關係中一個網站上的一個 Symantec Endpoint Protection Manager 向雲端進行註冊。

請參閱第 518 頁的「向雲端主控台中的遠端複製夥伴註冊網站」。

群組、用戶端、位置

- 如果您在雲端主控台中重新命名「**我的公司**」，Symantec Endpoint Protection Manager 中的群組名稱不會變更。
- 雲端管理功能需要受管用戶端。無法管理非受管用戶端，或將使用雲端功能的政策套用至非受管用戶端。如果將使用雲端功能的政策套用至非受管用戶端，該政策會預設為對等的舊 Symantec Endpoint Protection 選項。
- 版本 14、14 MP1、14 MP2 和舊版 12.1.x 用戶端電腦會顯示在雲端主控台中，但不支援任何新的雲端式功能。
- 如果雲端主控台中的「**管理裝置**」選項處於開啟狀態，則雲端主控台會管理裝置。如果處於關閉狀態，則 Symantec Endpoint Protection Manager 會管理裝置。
  如果搭配使用 Active Directory 與 Symantec Endpoint Protection Manager 來管理群組和用戶端，則 Symantec Endpoint Protection Manager 會自動管理裝置。在此情況下，無法將「**管理裝置**」切換至雲端主控台。此設定會將裝置組織的控制僅返回到 Symantec Endpoint Protection Manager。它不影響任何群組的政策防護。您可以繼續從雲端主控台管理進階政策功能。
- 每當您對裝置群組結構進行變更時，均會延遲 10 分鐘，變更才會在 Symantec Endpoint Protection Manager 中出現。反之亦然。此行為類似於 Symantec Endpoint Protection Manager 遠端複製運作的方式。在延遲期間，您不應該嘗試進行其他拓樸變更。

- 如果在雲端主控台中新增包含以下任何特殊字元的群組或政策：**/ \ * ? < > | : "**，這些字元將在 Symantec Endpoint Protection Manager 中轉換為破折號。例如，如果您在 Symantec Endpoint Protection Manager 上命名群組 `Europe***`，則此群組會標示為 `Europe---`。
- 雲端主控台不支援位置。因此，如果 Symantec Endpoint Protection Manager 群組具有多個位置且每個位置使用不同的政策 (共用或非共用)，則只有預設位置的政策將會同步並套用至雲端主控台上對等的群組。在雲端主控台重新與 Symantec Endpoint Protection Manager 同步之後，雲端主控台中該群組的政策將作為共用政策套用至 Symantec Endpoint Protection Manager 上對等群組中的所有位置。此程序將同時套用到 Symantec Endpoint Protection Manager 中的記憶體攻擊緩和政策和例外政策。
- 雲端主控台不支援透過 IPv6 的連線。透過 IPv6 網路註冊 Symantec Endpoint Protection Manager，導致以下錯誤：

  ```
  An error has occurred requesting the status for this enrollment token.
  Symantec Endpoint Protection Manager cannot connect to the cloud console.
  Check the network connection and try again.
  ```

政策和繼承

- 只能從雲端管理 14.0.1/14.1、14.0.1 MP1、14.0.1 MP2 和 14.2 用戶端的政策設定。
  仍必須直接從 Symantec Endpoint Protection Manager 管理低於 14.0.1 之用戶端的政策設定。但是存在例外。如果從雲端套用例外政策，且用戶端支援例外類型，則例外會套用至用戶端 (無論版本為何)。記憶體攻擊緩和政策會套用至所有 14 版用戶端及更新版本。
- 來自雲端的政策不會遵循 Symantec Endpoint Protection Manager 的政策繼承組態。相反地，它們會遵循在雲端中定義的繼承規則。
- 在病毒和間諜軟體防護政策中，當網域在雲端主控台中註冊時，部分選項旁會顯示雲端圖示。當密集型防護政策生效時，該政策僅針對 14.0.1/14.1、14.0.1 MP1、14.0.1 MP2 和 14.2 用戶端覆寫這些選項。
- 在 Symantec Endpoint Protection Manager 中，於雲端主控台中建立和指派的第一個預設雲端政策會附加一個 `v` 和數字 (`#`)，如下所示：`預設 MEM 政策 v1`。如果取消註冊並重新註冊 Symantec Endpoint Protection Manager 網域，則會在政策名稱後面附加額外的 `v#`。例如，`預設 MEM 政策 v1` 可能會變為`預設 MEM 政策 v1 v1` 或`預設 MEM 政策 v1 v3`。
- 對於 Symantec Endpoint Protection Manager 例外政策與雲端主控台黑名單和許可清單政策之間的差異：
  請參閱第 515 頁的「Symantec Endpoint Protection Manager 例外政策如何與雲端主控台互動？」。

請參閱第 504 頁的「如何將註冊網域雲端主控台功能與內部部署 Symantec Endpoint Protection Manager 相比較」。

關於雲端式群組和政策 (14.1/14.2)

雲端式群組

在雲端主控台中註冊之後，Symantec Endpoint Protection Manager 的群組會自動顯示在雲端主控台中。用戶端電腦在雲端主控台中顯示為裝置。雲端主控台不支援位置。

雲端式政策

在雲端主控台中註冊 Symantec Endpoint Protection Manager 網域時，您可以從雲端主控台建立套用至 Symantec Endpoint Protection Manager 用戶端群組的政策。這些政策會向下推送至 Symantec Endpoint Protection Manager，而其會將政策派送至用戶端。

您可以在雲端主控台中建立下列政策：

- 密集型防護政策
- 許可清單政策
- 黑名單政策
- 系統政策，用於低頻寬選項
- 記憶體攻擊緩和政策

Symantec Endpoint Protection Manager 群組的政策繼承不會套用至來自雲端的政策。您可以在**「用戶端」>「政策」**標籤中，藉由出現在政策說明旁的雲端圖示識別雲端式政策。

表 26-3　　雲端圖示

圖示	敘述
	此群組不會從其雲端主控台中的父系繼承政策。政策會直接套用至群組。
	此群組會從其雲端主控台中的父系繼承政策。

請參閱第 508 頁的「Symantec Endpoint Protection Manager 如何與雲端主控台互動」。

在低頻寬環境中更新用戶端

何謂低頻寬模式？

自 14.1 起，低頻寬模式是至少符合下列其中一個準則的這些環境的新選項：

- 需要較不頻繁的病毒和間諜軟體、SONAR 和 IPS 內容更新
- 對雲端的連線能力較低

低頻寬用戶端較不常接收更新。賽門鐵克每週會更新低頻寬內容一次。在低頻寬模式下，您可以使用主動模式政策更好地調整端點上的安全性。

請參閱第 384 頁的「Symantec Endpoint Protection 如何使用進階機器學習？」。

您必須在雲端主控台中註冊，才能使用低頻寬政策。低頻寬預設為關閉。

- 在雲端主控台中，於系統政策中啟用低頻寬模式。
- 確定 LiveUpdate 下載低頻寬內容。
  下載低頻寬內容至 Symantec Endpoint Protection Manager
- 建立取得低頻寬內容的用戶端群組。
  針對低頻寬用戶端建立群組

啟用低頻寬模式之後，您可以在**「預設」**檢視和**「防護技術」**檢視的**「用戶端」**標籤中查看其狀態。您也可以根據低頻寬內容派送產生報告。

請參閱第 514 頁的"在於低頻寬模式下執行的用戶端上執行報告"。

啟用低頻寬模式

請在雲端主控台的「系統政策」中啟用或停用低頻寬模式。

啟用低頻寬

1. 在雲端主控台中，移至**「政策」**。
2. 按下**「顯示過濾器」**下拉式清單，並選取**「政策類型」**來依政策類型排序。
3. 選取要編輯的低頻寬政策的**「名稱」**。

   附註：建立政策時，您會在政策建立程序完成時看見政策頁面。

4. 使用**「在低頻寬模式下執行」**選項旁的滑動軸，來啟用或停用**「在低頻寬模式下執行」**。
5. 按下**「儲存政策」**。

下載低頻寬內容至 Symantec Endpoint Protection Manager

依據預設會下載和啟用進階機器學習內容。您可以使用以下程序來驗證已啟用它們。

下載低頻寬內容至 Symantec Endpoint Protection Manager

1. 在 Symantec Endpoint Protection Manager Console 中，按下**「管理員」>「本機網站」>「編輯網站屬性」**。
2. 按下以選取**「LiveUpdate」**標籤，然後按下**「要下載的內容類型」**旁的**「變更選定內容」**。
3. 確定已勾選**「進階機器學習」**旁的方塊。
4. 按下**「確定」>「確定」**儲存變更。

在 LiveUpdate 內容政策中包含低頻寬內容

1 在 Symantec Endpoint Protection Manager 主控台中，前往**「政策」>「LiveUpdate」**，然後編輯指派給群組 (包含啟用低頻寬的用戶端) 的政策。

2 按下**「LiveUpdate 內容」**，然後連按兩下**「LiveUpdate 內容政策」**。

3 在**「Windows 設定」**下方，按下**「安全性定義檔」**。

4 確保已勾選**「進階機器學習」**方塊。

5 按下**「確定」**儲存變更。

請參閱第 163 頁的「關於 LiveUpdate 下載的內容類型」。

針對低頻寬用戶端建立群組

針對低頻寬用戶端建立群組

1 在雲端主控台中，按下**「裝置」**，然後在**「我的公司」**下新增子群組。

如果您無法新增子群組，請在雲端主控台 (**「設定」>「Symantec Endpoint Protection Manager 註冊」**) 中啟用**「管理裝置」**。否則，請在 Symantec Endpoint Protection Manager 中新增群組。如果您使用 Active Directory 同步，請透過 Active Directory 新增群組。

2 將「系統政策」套用至您先前架構為使用低頻寬的群組。在裝置群組上，按下**「套用政策」**，新增系統政策，然後按下**「送出」**。

3 在 Symantec Endpoint Protection Manager 主控台中，確保您先前架構的 LiveUpdate 內容政策已套用至您建立的群組。您在 Symantec Endpoint Protection Manager 中啟用或停用的政策繼承僅會套用至 Symantec Endpoint Protection Manager 政策，而不會套用至雲端主控台裝置政策。

您可能必須預留一些時間供群組從雲端主控台同步。

在於低頻寬模式下執行的用戶端上執行報告

您可執行報告以列出接收低頻寬內容的用戶端。

在於低頻寬模式下執行的用戶端上執行報告

1 在 Symantec Endpoint Protection Manager 主控台中，按下**「報告」>「快速報告」**，然後進行下列選擇：

- 報告類型：**電腦狀態**
- 選取報告：**低頻寬內容派送**

2 選取時間範圍：**更多選項的其他設定**。

3 按下**「建立報告」**。

Symantec Endpoint Protection Manager 例外政策如何與雲端主控台互動？

例外政策如何在雲端主控台上運作？

雲端主控台並非支援 Symantec Endpoint Protection Manager 支援的所有例外。在雲端主控台中註冊 Symantec Endpoint Protection Manager 網域之後，會根據例外類型將雲端主控台中的原始 Symantec Endpoint Protection Manager 例外政策分為兩種政策類型。這些雲端式政策稱為黑名單政策和許可清單政策。雲端政策不支援的例外仍保留在 Symantec Endpoint Protection Manager 例外政策中。在雲端主控台和 Symantec Endpoint Protection Manager 同步之後，會將雲端式政策重新匯入 Symantec Endpoint Protection Manager 中。

例如，假設在 Symantec Endpoint Protection Manager 中建立名為*「SEPM 例外政策」*的政策。此政策包含「應用程式」例外、「信任的 Web 網域」例外和「要監控的應用程式」例外。在雲端主控台中註冊之後，*「SEPM 例外政策」*中的雲端式例外會分為兩種政策。這些政策稱為*「匯入的 SEPM 例外政策 (BL)」*和*「匯入的 SEPM 例外政策 (WL)」*。黑名單政策僅透過「應用程式」例外建立，而許可清單政策則透過「應用程式」例外和「網域」例外建立。原始的 Symantec Endpoint Protection Manager *「SEPM 例外政策」*會保留「要監控的應用程式」例外。在雲端主控台與 Symantec Endpoint Protection Manager 同步之後，Symantec Endpoint Protection Manager 會顯示指派給同一個群組的三個政策：*「SEPM 例外政策」*、*「匯入的 SEPM 例外政策 (BL) v1」*和*「匯入的 SEPM 例外政策 (WL) v1」*。

請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。

此外，雲端主控台的許可清單和黑名單政策並非支援 Symantec Endpoint Protection Manager 例外政策支援的所有動作。雲端主控台之許可清單政策中的「應用程式」例外僅支援**「忽略」**動作。雲端主控台之黑名單政策中的「應用程式」例外僅支援**「隔離」**動作。如果在 Symantec Endpoint Protection Manager 例外政策中新增「應用程式」例外，然後在雲端主控台中註冊 Symantec Endpoint Protection Manager，則雲端主控台政策中的動作會自動變更。對於許可清單政策，**「只記錄」**動作會轉換為**「忽略」**動作。**「終止」**和**「移除」**動作會轉換為**「隔離」**動作。將這些政策重新匯入 Symantec Endpoint Protection Manager 中之後，管理伺服器會保留雲端主控台政策中的動作。

請參閱第 479 頁的「在 Windows 用戶端上監控應用程式以建立應用程式的例外」。

雲端主控台支援和不支援哪些例外？

在 Windows 用戶端上，雲端主控台支援以下例外：

黑名單政策：

- 雜湊 (SHA-256)

許可清單政策：

- 憑證
- 檔案名稱

- 網域
- 雜湊
- 檔案路徑
- 副檔名
- IPS 主機

在雲端主控台中註冊 Symantec Endpoint Protection Manager 之後，Symantec Endpoint Protection Manager 例外政策中的 Windows 例外會轉換為以下政策類型和例外類型：

表 26-4 Windows 例外及其轉換為雲端主控台例外的方式

Symantec Endpoint Protection Manager 例外政策	黑名單政策	許可清單政策
應用程式	雜湊 (僅限 SHA-256)	雜湊 (僅限 SHA-256)
憑證	不適用	憑證
檔案 > 安全風險/SONAR	不適用	檔案名稱
資料夾 > 安全風險/SONAR	不適用	路徑
信任的 Web 網域	不適用	網域

以下 Windows 例外將保留在 Symantec Endpoint Protection Manager 例外政策中，但在雲端主控台中不受支援：

- 要監控的應用程式
- 副檔名
- 檔案 - 應用程式控制
- 資料夾 - 應用程式控制
- 已知風險
- 竄改防護例外
- DNS 或主機檔案變更例外

雲端主控台不支援 Linux 用戶端例外或 Mac 用戶端例外。所有 Linux 例外項目和 Mac 例外項目均保留在 Symantec Endpoint Protection Manager 例外政策中。

附註：您也可以使用從 Symantec Endpoint Protection Manager 匯出之總和檢查碼的 .csv 檔案，將例外直接新增至雲端主控台。此檔案指紋清單包含位於電腦上指定路徑中之每個執行檔或 DLL 的路徑、檔案名稱以及對應的總和檢查碼。使用 checksum.exe 建立檔案指紋清單

請參閱第 469 頁的「針對哪種類型的掃描使用哪些 Windows 例外？」。

使用者可在 Windows 用戶端上新增的例外

Symantec Endpoint Protection Manager 例外政策允許您讓 Windows 用戶端上的使用者新增例外 (稱為用戶端限制)。

如果 Symantec Endpoint Protection Manager 在雲端主控台中註冊，則 Symantec Endpoint Protection Manager 不會顯示以下用戶端限制：

- 應用程式例外
- 檔案例外
- 資料夾例外 > 安全風險例外/SONAR 例外
- 信任的 Web 網域例外
- 憑證例外

附註：此外，在雲端式例外政策所控制的 Windows 用戶端上，這些例外不會顯示在用戶端使用者介面中。

無論是否已註冊 Symantec Endpoint Protection Manager，Symantec Endpoint Protection Manager 都不會顯示以下用戶端限制。

- DNS 或主機檔案變更例外
- 副檔名例外
- 已知風險例外

請參閱第 483 頁的「限制使用者可在用戶端電腦上架構的例外類型」。

註冊例外政策以及將其與雲端主控台同步的問題

- 只有在原始 Symantec Endpoint Protection Manager 例外政策包含黑名單政策和許可清單政策支援的例外時，才會自動在雲端主控台中建立黑名單政策或許可清單政策。否則，雲端主控台會忽略例外政策。
- 註冊之後，只有已指派的 Symantec Endpoint Protection Manager 例外政策會與雲端主控台同步，然後這些政策將重新匯入 Symantec Endpoint Protection Manager 中。未指派的政策與非雲端式例外政策一起保留在 Symantec Endpoint Protection Manager 中。此外，如果已指派的 Symantec Endpoint Protection Manager 例外政策沒有黑名單例外或許可清單例外，則會針對該群組在雲端主控台中建立對應的空白黑名單政策和/或空白許可清單政策。
- 註冊之後，您可以在 Symantec Endpoint Protection Manager 中建立和指派非雲端式例外政策。但是，這些政策必須僅包含以 Symantec Endpoint Protection Manager 為基礎的例外，而非雲端式例外。如果您建立和指派雲端式黑名單政策或許可清單政策，這些政策會自動同步並匯入到 Symantec Endpoint Protection Manager 中。

- 取消註冊網域之後，在雲端主控台中建立的例外政策仍會保留在 Symantec Endpoint Protection Manager 中。但是，這些雲端式政策會從 Symantec Endpoint Protection Manager 中的群組取消指派。您可以合併、重新指派或刪除這些政策 (如果您不再需要這些政策)。
- 如果將 Symantec Endpoint Protection Manager 例外政策匯入雲端主控台且該政策具有應用程式例外，則這些例外會在政策匯入後遺失。您必須手動將應用程式例外重新新增至雲端主控台的黑名單和許可清單政策。雲端主控台會保留其他類型的例外，例如憑證例外。

向雲端主控台中的遠端複製夥伴註冊網站

如何在雲端主控台中註冊網站？

自 14.2 版起，可在雲端主控台中註冊的一個網站，與不在雲端主控台中註冊的其他網站之間設定遠端複製。您可以註冊一個網站作為主要網站。所有其他網站可以直接與主要網站進行遠端複製，或彼此進行遠端複製。例如，如果網站 A 為主要網站，將網站 A 註冊到雲端主控台。可以架構網站 B 和網站 C 與網站 A 進行遠端複製。也可以架構網站 B 與網站 A 進行遠端複製，並架構網站 C 與網站 B 進行遠端複製。

表 26-5　　註冊多個遠端複製網站的程序

工作	敘述
步驟 1：遠端複製兩個網站，然後在雲端主控台中註冊。	註冊主要網站之前遠端複製所有政策、群組和日誌事件，以避免任何資料庫衝突。 也可以在雲端中註冊主要網站後，新增遠端複製夥伴。 主要網站可以有多個夥伴網站。 請參閱第 645 頁的「立即遠端複製資料」。 請參閱第 637 頁的「什麼是網站以及遠端複製如何運作？」。
步驟 2：註冊主要網站。	選擇並註冊一個網站作為主要網站，以執行註冊和任何進一步的動作，例如建立政策。 對於具有多個管理伺服器的網站，您只需要註冊其中一個管理伺服器。任何其他管理伺服器均會自動註冊。 不要在雲端主控台中註冊第二個網站或夥伴網站。 請參閱第 499 頁的「在 Symantec Endpoint Protection Manager Console 的雲端主控台中註冊 14.1/14.2 網域」。

工作	敘述
步驟 3：等待執行同步。	在註冊的主要網站和雲端主控台同步後，會在主要網站上發生下列事件： ■ Bridge 服務會自動安裝在所有管理伺服器上。不過，Bridge 服務僅對曾用於在雲端主控台中註冊的管理伺服器有效。 ■ 主要網站會同步報告事件與雲端主控台。 ■ 主要網站針對未連線到此網站的所有用戶端上傳群組、裝置、政策、日誌事件、用戶端套件，以及定義檔。 ■ 主要網站從雲端主控台接收政策、日誌與指令，並立即將資料傳遞至與此網站進行通訊的用戶端。 將 Symantec Endpoint Protection Manager 網域註冊到雲端主控台後，會發生什麼情況
步驟 4：遠端複製主要網站及任何夥伴網站。	排程遠端複製，以便這兩個網站具有相同的註冊資料。執行遠端複製後，夥伴網站上會發生下列事件： ■ 夥伴網站會根據與主要網站的遠端複製排程，從雲端主控台接收內容。然後，連線到夥伴網站的用戶端會收到此資料。 ■ 夥伴網站會從主要網站取得註冊詳細資料。這些詳細資料會顯示在**「雲端」**頁面 > **「疑難排解」**頁面上。 ■ 夥伴網站的管理伺服器不會安裝 Bridge 服務。因此，夥伴網站不會直接與雲端主控台同步。 請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。
步驟 5：(選擇性) 將群組和裝置的控制切換至雲端主控台。	依據預設，當您註冊未遠端複製的 Symantec Endpoint Protection Manager 網域時，雲端主控台會管理用戶端群組結構。依據預設，當您註冊已遠端複製的網站時，Symantec Endpoint Protection Manager 會管理群組結構。 ■ 如果 Symantec Endpoint Protection Manager 為主要網站，您可以在主要網站上新增群組和政策，然後便會在夥伴網站上進行遠端複製。 ■ 如果將雲端主控台設為主要網站，請先執行與夥伴網站的遠端複製。此遠端複製可確保您在夥伴網站上新增的群組和政策同步到雲端主控台。 若要將控制切換到雲端主控台，請在雲端主控台的**「設定」**>**「Symantec Endpoint Protection Manager 註冊」**中進行註冊後，啟用**「管理裝置」**選項。

您無法針對遠端複製的夥伴執行容錯移轉或負載平衡。

請參閱第 629 頁的「設定容錯移轉和負載平衡」。

附註：如果您架構 Content Analysis 系統設定，請在主要網站上進行架構，以便此功能在雲端主控台上可用。如果在夥伴網站上架構 CAS，CAS 設定不會與雲端主控台同步。

架構 Symantec Endpoint Protection 以使用 Content Analysis 系統

在雲端主控台中註冊的網站之間移除與還原遠端複製

如果您移除主要網站和夥伴網站之間的夥伴關係，會一併移除與雲端主控台的夥伴關係。

若要還原與主要網站的夥伴關係，請使用**「新增現有遠端複製夥伴」**精靈。

您也可以直接在雲端主控台中註冊夥伴網站，以作為個別網站。在此情況下，您必須建立不同的 Symantec Cyber Defense Manager 帳戶。若要還原與主要網站的夥伴關係，您必須取消註冊夥伴網站。然後，在主要網站上，使用**「管理伺服器組態精靈」**重新架構夥伴關係。

附註：作為最佳實務準則，將夥伴網站保留為個別網站，且請勿嘗試還原與主要網站的遠端複製。

請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。

疑難排解雲端主控台中的網站遠端複製

取得主要網站註冊和遠端複製的相關資訊：

- 尋找遠端複製事件。
  在主要網站上，開啟**「系統日誌」**>**「管理」**日誌類型，並尋找**「遠端複製事件」**事件類型。
  請參閱第 563 頁的「檢視日誌」。
- 查看夥伴網站的註冊狀態。
  在夥伴網站上，**「註冊狀態」**顯示為**「已註冊」**。
  「連線狀態」等其他欄位則顯示**「無」**。
  若要顯示註冊資訊，請按下**「雲端」**頁面 >**「疑難排解」**。

部分 6

監控、報告和強制執行合規性

27

管理主機完整性以強制執行安全政策

本章包含以下主題：

主機完整性的運作方式

主機完整性可確保用戶端電腦受到防護並遵從公司的安全性政策。主機完整性政策可用於定義、強制執行和還原用戶端的安全性，以保護企業網路和資料的安全。

表 27-1 在用戶端電腦上強制執行安全性遵從的程序

步驟	敘述
步驟 1：用戶端電腦在本機執行主機完整性檢查。	管理伺服器會將主機完整性政策下載到所指派群組中的用戶端電腦。用戶端電腦會執行主機完整性檢查，它會將每台電腦的組態與您新增至主機完整性政策的要求進行比較。 主機完整性政策會檢查是否存在防毒軟體、修正程式、修補程式，以及其他安全性要求。例如，政策會檢查作業系統是否套用了最新的修正程式。 請參閱第 524 頁的「設定主機完整性」。
步驟 2：通過或未通過主機完整性檢查	■ 如果電腦符合政策的全部要求，表示通過主機完整性檢查。 ■ 如果電腦不符合政策的全部要求，表示未通過主機完整性檢查。您也可以設定政策以忽略不符合的需求，使檢查能夠通過。 請參閱第 529 頁的「允許主機完整性檢查在需求失敗時通過」。 您也可以在防火牆政策中設定點對點驗證，此驗證可授予或攔截對於已安裝用戶端之遠端電腦的入埠存取。 請參閱第 531 頁的「透過架構點對點驗證攔截遠端電腦」。
步驟 3：非遵從電腦矯正失敗的主機完整性檢查 (選擇性)	■ 如果主機完整性檢查失敗，您可以架構用戶端來加以矯正。若要矯正，用戶端會下載並安裝遺漏的軟體。您可以架構用戶端或一般使用者在預先定義的需求或自訂需求中進行矯正。接著，主機完整性會重新檢查用戶端電腦是否已安裝軟體。 請參閱第 526 頁的「設定預先定義主機完整性需求的矯正」。 ■ 如果驗證矯正的主機完整性檢查仍然失敗，用戶端會套用隔離所政策。您可以使用隔離所政策將更嚴格的限制套用到失敗的電腦。 請參閱第 530 頁的「針對失敗的主機完整性檢查建立隔離所政策」。 ■ 如果用戶端位於「隔離所」位置，主機完整性檢查會繼續執行並嘗試矯正。檢查頻率和矯正設定依架構主機完整性政策的方式而定。在用戶端經過矯正並通過主機完整性檢查之後，用戶端就會自動移出「隔離所」位置。在某些情況下，您可能需要手動矯正用戶端電腦。
步驟 4：用戶端繼續監控遵從狀態	主機完整性檢查會主動監控每個用戶端的遵從狀態。一旦用戶端的遵從狀態變更，電腦的權限也會變更。 ■ 如果您變更主機完整性政策，它會在下一次出現活動訊號時下載至用戶端。用戶端接著會執行「主機完整性」檢查。 ■ 當主機完整性檢查正在進行時，如果用戶端切換至具有不同主機完整性政策的位置，則用戶端會停止此項檢查。此停止包括任何矯正嘗試。如果新的位置無法使用矯正伺服器連線，使用者可能會看見逾時訊息。檢查完成後，用戶端會捨棄結果。接著，用戶端會根據位置的新政策，立即執行新的「主機完整性」檢查。 您可以在遵從日誌中檢視主機完整性檢查的結果。 請參閱第 563 頁的「檢視日誌」。

設定主機完整性

使用主機完整性政策，可確保您網路中的用戶端電腦符合組織的安全政策。

表 27-2 列出了您使用主機完整性政策設定安全性遵從所需要執行的步驟。

表 27-2 設定主機完整性政策的工作

步驟	敘述
步驟 1：新增主機完整性政策，用於檢查用戶端電腦的需求並針對非遵從電腦強制執行矯正動作	新增政策時，請執行下列工作： 1 選擇您想要用戶端電腦檢查的需求類型。為每種類型的軟體 (如應用程式、檔案和修補程式) 建立單獨的需求。 請參閱第 524 頁的「關於主機完整性需求」。 請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。 2 針對非遵從用戶端電腦架構矯正動作。 矯正需要用戶端電腦安裝或要求用戶端使用者安裝所需的軟體。 請參閱第 526 頁的「設定預先定義主機完整性需求的矯正」。 3 設定檢查需求以及嘗試矯正的順序。例如，應該以特定的順序完成更新，以便在使用者必須重新啟動用戶端電腦之前套用所有更新。
步驟 2：設定主機完整性檢查和通知的選項	■ 架構主機完整性檢查的執行頻率。 請參閱第 528 頁的「架構主機完整性檢查頻率的設定」。 ■ 架構使用者是否可以取消矯正。 請參閱第 527 頁的「允許使用者延遲或取消主機完整性矯正」。 ■ 設定當主機完整性檢查通過或失敗時顯示於用戶端電腦的通知。使用通知來告訴一般使用者下一步的動作。例如，一般使用者可能需要允許新修補程式在用戶端電腦上下載並安裝。 請參閱第 529 頁的「架構主機完整性檢查的通知」。
步驟 3：設定點對點強制執行	如果測試主機完整性遵從性的用戶端電腦與已遵從用戶端電腦位於同一網路，則您可以設定點對點強制執行。您主要是針對檔案共用使用點對點強制執行。 請參閱第 531 頁的「透過架構點對點驗證攔截遠端電腦」。
步驟 4：針對非遵從電腦和未經矯正的電腦設定隔離所政策 (選擇性)	如果用戶端電腦執行主機完整性檢查失敗並且未執行矯正，您可以使用隔離所政策隔離電腦。 請參閱第 530 頁的「針對失敗的主機完整性檢查建立隔離所政策」。

關於主機完整性需求

建立新主機完整性政策時，請決定要新增的需求類型。

每個需求都會指定下列項目：

- 檢查的條件
  例如，需求將會檢查最新病毒定義檔集是否已經安裝在用戶端電腦上。
- 如果用戶端未能通過條件需求，用戶端應該採取什麼矯正動作
  例如，矯正動作可以包括用戶端可下載並安裝缺少的病毒定義檔所在的 URL。

表 27-3 列出了您可以使用的需求類型。

表 27-3 主機完整性政策的需求類型

類型	敘述
預先定義的需求	使用預先定義的需求來檢查特定應用程式或檔案是否已經在用戶端上安裝並執行。預先定義的需求可以檢查以下任一類型的應用程式的狀態：防毒軟體、防間諜軟體、防火牆、修正程式或服務套件。例如，修正程式需求可檢查用戶端電腦是否執行特定的作業系統修正程式。 如果預先定義的需求沒有足夠的詳細資料，請新增自訂需求並撰寫指令碼。 請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。
範本中的自訂需求	範本為預先定義的自訂需求，是賽門鐵克為經常執行的工作所撰寫。例如，用戶端可以檢查是否已在過去 42 天內變更密碼。您也可以基於範本來撰寫自訂需求指令碼。 利用「主機完整性政策 LiveUpdate 服務」可以取得範本需求，您必須首先設定 LiveUpdate，以將主機完整性範本下載至管理伺服器。 請參閱第 532 頁的「從範本新增自訂需求」。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。
自訂需求	如果預先定義的需求和範本均無法提供您需要的檢查種類，請使用自訂需求。自訂需求包括與預先定義的需求相同的欄位，但是會提供更多的彈性。例如，您可以包括不位於預先定義之防間諜軟體應用程式清單的防間諜軟體應用程式。 而在自訂需求中包括類似的應用程式，可大大簡化必要應用程式的管理。例如，Internet Explorer 和 Mozilla Firefox 之類的網際網路瀏覽器都可納入同一個需求中。 請參閱第 532 頁的「撰寫自訂的需求指令碼」。

請參閱第 524 頁的「設定主機完整性」。

將預先定義的需求新增至主機完整性政策

主機完整性政策中預先定義的需求將檢查用戶端電腦是否執行以下任何類型的應用程式，例如：防毒軟體、防間諜軟體、防火牆等。

您可決定特定應用程式，例如適用於 Windows 7 作業系統的特定修補程式。然後，您可以指定用戶端電腦取得修補程式的路徑。

將預先定義的需求新增至主機完整性政策

1 在主控台中，開啟某個主機完整性政策。

2 在「**主機完整性政策**」頁面上，按下「**需求**」>「**新增**」。

3 在「**新增需求**」對話方塊中，按下「**選取需求**」下拉式清單，選取預先定義的需求，然後按下「**確定**」。

4 架構此需求的設定和矯正選項，然後按下「**確定**」。

請參閱第 526 頁的「設定預先定義主機完整性需求的矯正」。

如需詳細資訊，請按下「**說明**」。

5 按下「**確定**」。

6 將政策指派給群組或位置。

7 按下「**確定**」。

請參閱第 532 頁的「從範本新增自訂需求」。

請參閱第 532 頁的「撰寫自訂的需求指令碼」。

啟用和停用主機完整性需求

將需求新增至主機完整性政策時，依預設將啟用需求。您必須先停用這些需求，等到有需要時再啟用。例如，測試主機完整性政策時，您可以暫時停用需求。

啟用與停用主機完整性需求

1 在主控台中，開啟主機完整性政策並按下「**需求**」。

2 在「**需求**」頁面上，進行下列任一工作：

- 若要啟用需求，請勾選所選取需求的「**啟用**」核取方塊。
- 若要停用需求，請取消勾選所選取需求的「**啟用**」核取方塊。

3 按下「**確定**」。

請參閱第 524 頁的「設定主機完整性」。

設定預先定義主機完整性需求的矯正

如果用戶端「主機完整性」檢查顯示需求失敗，則您可以架構還原必要檔案的政策。此用戶端將透過下載、安裝或執行所需的應用程式來還原檔案，以符合需求。用戶端電腦接著便可通過主機完整性檢查。

您可以在新增預先定義需求的相同對話方塊中設定矯正。您不僅可以指定用戶端下載矯正檔案的路徑，也可以指定如何實作矯正程序。

您還可以讓使用者控制何時矯正其電腦。例如，重新啟動可能會讓使用者遺失工作，因此使用者可能想要將矯正延遲到當天結束時進行。

在下載、安裝或執行還原需求的指令之後，用戶端一律會重新測試需求。此外，用戶端還會記錄結果為 pass 或 fail。

設定預先定義主機完整性需求的矯正

1 在主控台中，開啟某個主機完整性政策並新增一個預先定義的需求。

請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。

2 在「**新增需求**」對話方塊中，按下「**如果尚未在用戶端安裝 <需求類型>，請安裝**」。

3 按下「**下載安裝套件**」。

4 在「**下載 URL**」文字方塊中，輸入可將安裝檔案下載到用戶端電腦的 URL。

5 在「**執行指令**」文字方塊中，執行下列其中一個工作：

- 如果您要讓用戶端使用者執行安裝，請將文字方塊保留空白。
- 如果您要安裝自動執行，請輸入 **%F%**。
  %F% 變數代表最後下載的檔案。您可以使用可從「**開始**」>「**執行**」執行的任何指令。例如，若要安裝 Vista 的修正程式，請鍵入指令 **%Systemroot%\system32\wusa.exe /quiet /norestart %F%**。

6 可以選擇性地設定延遲或取消矯正的選項，然後按下「**確定**」。

請參閱第 527 頁的「允許使用者延遲或取消主機完整性矯正」。

7 按下「**確定**」。

請參閱第 529 頁的「允許主機完整性檢查在需求失敗時通過」。

允許使用者延遲或取消主機完整性矯正

您可以允許使用者將矯正延遲到比較方便的時間。如果使用者針對某個需求在安裝軟體後必須重新啟動其電腦，則可能需要等待以後再重新啟動電腦。

如果使用者延遲矯正，則可能會發生以下任一事件：

- 用戶端會記錄該事件。「主機完整性」狀態會顯示為失敗，因為不符合需求。使用者隨時都可從用戶端手動執行新的「主機完整性」檢查。
- 用戶端執行另一次「主機完整性」檢查前，「主機完整性」檢查矯正訊息視窗都不會顯示。如果使用者選擇在 5 分鐘內提醒，但「主機完整性」檢查是每隔 30 分鐘執行一次，則訊息視窗會等到 30 分鐘後才顯示。為了避免造成使用者困惑，您可能需要將最短時間設定和「主機完整性」檢查頻率設定同步。
- 如果使用者在下次「主機完整性」檢查之前延遲矯正，則使用者的選擇會被覆寫。

- 如果使用者延遲矯正動作且用戶端接收到更新的政策，矯正可用的時間長度則會重設為新的最大值。

允許使用者延遲或取消主機完整性矯正

1. 在主控台中，開啟某個主機完整性政策並新增一個需求。

   請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。

2. 在「**新增需求**」對話方塊中，設定矯正。

   請參閱第 526 頁的「設定預先定義主機完整性需求的矯正」。

3. 在需求的對話方塊中，執行下列其中一項工作，然後按下「**確定**」：

   - 若要讓用戶端使用者延遲下載檔案，請勾選「**指定下載失敗時要等待多久後再次嘗試下載**」。
   - 若要讓用戶端使用者取消矯正，請勾選「**允許使用者取消下載主機完整性矯正**」。

4. 按下「**確定**」。
5. 按下「**進階設定**」。
6. 在「**進階設定**」頁面的「**矯正對話方塊選項**」下方，架構取消矯正的選項。
7. 若要在用戶端電腦上新增自訂訊息，請按下「**設定其他文字**」。

   使用者按下「**詳細資訊**」時，此處鍵入的訊息會顯示在用戶端矯正視窗中。

8. 按下「**確定**」。

架構主機完整性檢查頻率的設定

您可架構主機完整性檢查的執行方式，以及檢查結果的處理方式。

在您新增或更新主機完整性政策之後，它就會在出現下一次活動訊號時，下載至用戶端。然後，用戶端會執行主機完整性檢查。

如果使用者切換至具有不同政策的位置，而此時正在執行主機完整性檢查，則用戶端會停止此項檢查。如果政策有要求，則這個停止動作還包含矯正嘗試。如果新的位置無法使用矯正伺服器連線，使用者可能會看見逾時訊息。檢查完成後，用戶端會捨棄結果。接著，用戶端會根據位置的新政策，立即執行新的「主機完整性」檢查。

如果新位置使用相同的政策，則用戶端會保留所有的「主機完整性」計時器設定。唯有在政策設定有需要時，用戶端才會執行新的「主機完整性」檢查。

架構主機完整性檢查頻率的設定

1. 在主控台中，開啟主機完整性政策，然後按下「**進階設定**」。
2. 在「**進階設定**」頁面，「**主機完整性檢查選項**」下，設定主機完整性檢查頻率。
3. 按下「**確定**」。

請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。

請參閱第 529 頁的「允許主機完整性檢查在需求失敗時通過」。

允許主機完整性檢查在需求失敗時通過

即使使用者的電腦未能通過主機完整性檢查，使用者也可能需要繼續工作。即使特定的需求失敗，您也可以讓主機完整性檢查通過。用戶端將記錄結果，但會忽略結果。

您可以針對特定的需求套用此設定。如果您要將這項設定套用至所有的需求，您必須分別在每項需求上啟用此設定，設定預設為停用。

允許主機完整性檢查在需求失敗時通過

1. 在主控台中，開啟主機完整性政策。
2. 新增預先定義的需求或自訂需求，然後按下**「確定」**。

   請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。

   請參閱第 532 頁的「撰寫自訂的需求指令碼」。
3. 在需求的對話方塊上，勾選**「即使這項要求失敗，也允許主機完整性檢查通過」**，然後按下**「確定」**。
4. 按下**「確定」**。

架構主機完整性檢查的通知

用戶端執行「主機完整性」檢查時，您可以架構發生下列狀況時出現的通知：

- 主機完整性檢查失敗時。
- 主機完整性檢查失敗後再次檢查通過時。

「主機完整性」檢查的結果會出現在用戶端的「安全日誌」中。這些資訊會上傳至管理伺服器**「監控器」**頁面的「遵從日誌」中。

用戶端的「安全日誌」包含多個窗格。如果您選取「主機完整性」檢查事件類型，左下方窗格會列出各個需求已通過還是未通過。右下方窗格會列出需求的條件。您可以架構用戶端，使資訊不出現在右下方窗格中。雖然進行疑難排解時可能需要這項資訊，但是您可能不希望使用者檢視這項資訊。例如，您可能寫入指定登錄值或檔案名稱的自訂需求。「安全日誌」仍會記錄詳細資訊。

您也可以啟用通知，使得使用者能夠選擇立即下載軟體，或延遲矯正。

請參閱第 527 頁的「允許使用者延遲或取消主機完整性矯正」。

架構主機完整性檢查的通知

1 在主控台中，開啟主機完整性政策。

2 在「**主機完整性**」頁面上，按下「**進階設定**」。

3 在「**進階設定**」頁面的「**通知**」下，若要顯示詳細的需求資訊，請勾選「**顯示詳細的主機完整性記錄**」。

用戶端的「安全日誌」右下方窗格會顯示「主機完整性」需求的完整資訊。

4 勾選下列任何選項：

- **主機完整性檢查失敗時顯示通知訊息**。
- **主機完整性檢查失敗後再次檢查通過時顯示通知訊息**。

5 若要加入自訂訊息，請按下「**設定其他文字**」，然後輸入其他文字內容，上限為 512 個字元，並且按下「**確定**」。

6 架構完此政策後，按下「**確定**」。

針對失敗的主機完整性檢查建立隔離所政策

您對主機完整性檢查失敗的用戶端電腦使用隔離所政策，嘗試矯正，然後再次矯正失敗。用戶端電腦矯正失敗之後，會自動切換至隔離所位置，在其中對該電腦套用隔離所政策。請使用隔離所政策對失敗的電腦套用更嚴格的限制。您可以對隔離所政策使用任何類型的保護政策。例如，您可以套用會封鎖電腦對 Internet 之存取權的隔離所防火牆政策。

當用戶端電腦位於隔離所位置時，您可以架構主機完整性檢查來繼續執行並嘗試矯正電腦。您可能也需要手動矯正電腦。

針對失敗的主機完整性檢查建立隔離所政策

1 在主控台中，按下「**用戶端**」，再按下「**政策**」標籤。

2 在「**政策**」標籤中，按下「**主機完整性檢查失敗時的隔離政策**」旁的「**新增政策**」。

3 在「**新增隔離所政策**」對話方塊中，選擇政策類型，然後按「**下一步**」。

4 選擇是否使用現有政策、建立新政策或匯入政策檔，然後按「**下一步**」。

5 執行下列其中一項工作：

- 在「**新增政策**」對話方塊中選擇政策，然後按下「**確定**」。
- 在「**政策類型**」對話方塊中架構政策，然後按下「**確定**」。
- 在「**匯入政策**」對話方塊中，找到 `.dat` 檔案並按下「**匯入**」。

請參閱第 526 頁的「設定預先定義主機完整性需求的矯正」。

請參閱第 524 頁的「關於主機完整性需求」。

透過架構點對點驗證攔截遠端電腦

您可以使用點對點驗證，允許遠端用戶端電腦 (對等者) 連線至同一企業網路內的其他用戶端電腦 (驗證者)。驗證者會暫時攔截遠端電腦的入埠 TCP 和 UDP 流量，直到遠端電腦通過主機完整性檢查。當遠端電腦實際上在遠端時，您可以使用此強制執行技術。此技術利用 Symantec Endpoint Protection 防火牆的進階功能來增強共用檔案的存取。

主機完整性檢查會驗證遠端電腦的下列特性：

- 遠端電腦已安裝 Symantec Endpoint Protection。
- 遠端電腦已通過主機完整性檢查。

如果遠端電腦通過主機完整性檢查，則驗證者會允許來自遠端電腦的入埠連線。

如果遠端電腦未通過主機完整性檢查，則驗證者會繼續攔截遠端電腦。您可以指定要攔截遠端電腦多久時間，等過了這段時間，才能再次嘗試連線至驗證者。您也可以指定一律允許某些遠端電腦，即使它們無法通過主機完整性檢查。如果您沒有啟用遠端電腦的主機完整性政策，則遠端電腦會通過主機完整性檢查。

點對點驗證資訊會出現在防網路和主機侵入流量日誌中。

附註：點對點驗證適用於伺服器控制和混合控制，但不適用於用戶端控制。

透過架構點對點驗證攔截遠端電腦

1. 在主控台中，開啟某個防火牆政策。
2. 在**「防火牆政策」**頁面上，按下**「點對點驗證設定」**。
3. 在**「點對點驗證設定」**頁面中，勾選**「啟用點對點驗證」**。
4. 架構頁面上所列的每個值。

   如需這些選項的詳細資訊，請按下**「說明」**。
5. 若要允許遠端電腦不經驗證就可連線到用戶端電腦，請勾選**「從驗證範圍中排除主機」**，然後按下**「排除的主機」**。

   用戶端電腦允許傳送至**「主機」**清單中所列電腦的流量。
6. 在**「排除的主機」**對話方塊中，按下**「新增」**，新增不必經過驗證的遠端電腦。
7. 在**「主機」**對話方塊中，定義主機的 IP 位址、IP 範圍或子網路，然後按下**「確定」**。
8. 在**「排除的主機」**對話方塊中，按下**「確定」**。
9. 按下**「確定」**。
10. 如果系統顯示提示，請將政策指派至某個群組。

請參閱第 291 頁的「建立防火牆政策」。

請參閱第 524 頁的「設定主機完整性」。

請參閱第 280 頁的「防止使用者在用戶端電腦上停用防護」。

從範本新增自訂需求

您可以新增賽門鐵克建立的常用自訂需求，而無需從草稿撰寫自訂需求。使用 LiveUpdate 將主機完整性內容下載至管理伺服器。主機完整性內容包括多個範本。然後，您可以將自訂需求從範本新增至主機完整性政策。

若要取得最新的主機完整性範本，您必須將 LiveUpdate 內容政策架構為下載主機完整性內容。

如果您是第二次匯入需求，而且已存在相同名稱的需求，則匯入的需求將不會覆寫現有的需求。但在**「需求」**表格中，匯入的需求名稱旁邊會顯示編號 2。

從範本新增自訂需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在**「主機完整性政策」**頁面上，按下**「需求」>「新增」**。
3. 在**「新增需求」**對話方塊中，按下**「選取需求」**下拉式清單，選取預先定義的需求，然後按下**「確定」**。
4. 在**「主機完整性線上更新」**對話方塊中，展開**「範本」**，然後選取範本類別。
5. 在要新增的每個範本旁邊，按下**「新增」**。
6. 按下**「匯入」**。
7. 按下**「確定」**。

請參閱第 524 頁的「關於主機完整性需求」。

請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。

請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。

撰寫自訂的需求指令碼

自訂需求比預先定義的需求提供更多的彈性。例如，您可以新增預先定義應用程式清單中未納入的應用程式。

若要建立自訂需求，您可以將一或多個函數或 **IF..THEN** 陳述式新增至指令碼中。執行指令碼時，「主機完整性」檢查會搜尋 **IF** 節點下所列的條件。接著根據該條件，執行 **THEN** 節點下所列的動作。隨即傳回結果 (`pass` 或 `fail`)。

在要檢查的一個指令碼中新增許多不同條件時，這個設定會套用到整個自訂需求指令碼。這個選擇可能會影響您決定是要建立多個小型自訂需求，還是建立包含多個步驟的大型自訂需求。

撰寫自訂的需求指令碼

1. 在主控台中，開啟某個主機完整性政策。
2. 在「**主機完整性政策**」頁面上，按下「**需求**」>「**新增**」。
3. 在「**新增需求**」對話方塊中，按下「**選取需求**」下拉式清單，選取預先定義的需求，然後按下「**確定**」。
4. 在「**自訂需求**」對話方塊中，輸入需求的名稱。

   需求名稱會顯示在用戶端電腦中。名稱會向使用者顯示需求通過與否，或提示使用者下載軟體。
5. 若要新增條件，請在「**自訂的需求指令碼**」下方，按下「**新增**」，然後按下 **IF..THEN**。

   附註：如果您先新增一個函數或 **IF..THEN** 陳述式但沒有填寫欄位，則會顯示錯誤：如果您不想新增陳述式，請在陳述式上按一下滑鼠右鍵，然後按下「**刪除**」。
6. 在 **IF** 節點下反白顯示空白條件，然後在右窗格中選取條件。

   「主機完整性」檢查會搜尋用戶端電腦上的條件。
7. 在「**選取條件**」下拉式清單下，指定其他必要的資訊。
8. 在「**自訂的需求指令碼**」下方，按下 **THEN**，然後按下「**新增**」。

   THEN 陳述式提供條件為 True 時應採取的動作。
9. 按下以下任何選項：
   - **IF..THEN**
     使用巢狀 **IF..THEN** 陳述式定義檢查條件和條件評估為 True 時採取的動作。
   - **功能**
     使用函數定義矯正動作，例如下載檔案。
   - **傳回**
     使用傳回陳述式，指定條件評估結果通過或失敗。各個自訂需求的末尾必須是通過或未通過的陳述式。
   - **註解** (選擇性)
     使用註解，說明您新增的條件、函數或陳述式等功能。
10. 在右窗格中，定義已新增的條件。

    若需這些選項的詳細資訊，請按下「**說明**」。
11. 若要新增更多的巢狀陳述式、條件或函數，請在「**自訂的需求指令碼**」下，在節點上按下滑鼠右鍵，然後按下「**新增**」。
12. 必要時，重複步驟 9 至 11。

13 若不論結果如何，都要使「主機完整性」檢查通過，請勾選**「即使這項要求失敗，也允許主機完整性檢查通過」**。

14 按下**「確定」**。

請參閱第 537 頁的「使用自訂需求程序檔建立測試主機完整性政策」。

請參閱第 525 頁的「將預先定義的需求新增至主機完整性政策」。

關於登錄條件

您可以指定哪些 Windows 登錄設定要作為自訂需求的 **IF..THEN** 陳述式的一部分進行檢查。此外，還可以指定變更登錄值的方法。 只有 `HKEY_CLASSES_ROOT`、`HKEY_CURRENT_USER`、`HKEY_LOCAL_MACHINE`、`HKEY_USERS` 和 `HKEY_CURRENT_CONFIG` 是受支援的登錄設定。

指定登錄機碼時，務必留意下列考量：

- 機碼名稱不可超過 255 個字元。
- 如果登錄機碼末尾含有反斜線 (\)，則被視為登錄機碼。例如：
  `HKEY_LOCAL_MACHINE\SOFTWARE\`
- 如果登錄機碼末尾沒有反斜線，則被視為登錄名稱。例如：
  `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

指定登錄值時，務必留意下列考量：

- 值名稱不可超過 255 個字元。
- 您可以檢查 DWORD (十進位)、二進位 (十六進位) 或字串形式的值。
- 若是 DWORD 值，您可以檢查值是否低於、等於、不等於或大於指定值。
- 若是字串值，您可以檢查值資料是否等於或包含特定字串。如果您要以區分大小寫的方式進行字串比較，請勾選**「符合大小寫」**核取方塊。
- 若是二進位值，您可以檢查值資料是否等於或包含特定片段的二進位資料。以十六進位元組來表示資料。如果您指定值「包含」，還可指定此資料的位移。如果位移保留空白，則會搜尋特定二進位資料的值。十六進位編輯方塊中允許的值為 `0` 到 `9` 以及 `a` 到 `f`。

以下是登錄值的範例：

DWORD	`12345` (十進位)
二進位	`31 AF BF 69 74 A3 69` (十六進位)
字串	`ef4adf4a9d933b747361157b8ce7a22f`

撰寫要在用戶端執行指令碼的自訂需求

在自訂主機完整性需求中，您可指定函數，讓用戶端執行指令碼。您可以使用程序檔命令語言 (如 JScript 或 VBScript) 來搭配 Microsoft Windows Script Host 執行。

撰寫要在用戶端執行指令碼的自訂需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在「**主機完整性政策**」頁面上，按下「**需求**」>「**新增**」。
3. 在「**新增需求**」對話方塊中，按下「**選取需求**」下拉式清單，選取預先定義的需求，然後按下「**確定**」。

   請參閱第 532 頁的「撰寫自訂的需求指令碼」。
4. 在「**自訂需求**」對話方塊的「**自訂的需求指令碼**」下方，選取要新增功能的節點。
5. 按下「**新增**」，再按下「**功能**」。
6. 按下「**公用程式: 執行指令碼**」。
7. 輸入指令碼的檔案名稱，例如 **myscript.js**。
8. 輸入指令碼的內容。
9. 在「**執行指令**」文字欄位中，輸入用來執行指令碼的指令。

   使用 **%F** 來指定指令碼檔案名稱。指令碼會在系統路徑位置執行。
10. 若要指定允許 **Execute** 指令完成的時間長度，請選取下列其中一個選項：
    - **不等候**
      如此一來只要成功執行，動作就會傳回 true，而不會等到完成執行。
    - **等候執行完成**
    - **輸入最長時間**
      輸入以秒為單位的時間。如果 `Execute` 指令未在指定時間內完成，便會終止檔案的執行。
11. 此外，如果不再需要檔案，您也可以取消勾選「**在執行完成或終止之後，刪除暫存檔**」。

    如果選取「**不等候**」，則這個選項停用。
12. 此外，您也可以取消勾選「**顯示新程序視窗**」，表示不要看到視窗顯示執行指令碼的需求。

撰寫要設定檔案時間戳記的自訂需求

在自訂主機完整性需求中，您可以指定「**設定時間戳記**」函數，以建立 Windows 登錄設定來儲存目前的日期和時間。然後再使用「**檢查時間戳記**」條件，來檢查建立時間戳記後，是否已經超過了指定的時間長度。

例如，如果主機完整性檢查每2分鐘執行一次，您可以指定動作以較長的間隔(如一天)執行。在此情況下，就會移除儲存的時間值。您可以設定指令碼執行如下：

- 當用戶端收到新的設定檔
- 當使用者手動執行主機完整性檢查

撰寫要設定檔案時間戳記的自訂需求

1. 在主控台中，開啟某個主機完整性政策。
2. 在**「主機完整性政策」**頁面上，按下**「需求」>「新增」**。
3. 在**「新增需求」**對話方塊中，按下**「選取需求」**下拉式清單，選取預先定義的需求，然後按下**「確定」**。

   請參閱第 532 頁的「撰寫自訂的需求指令碼」。
4. 在**「自訂需求」**對話方塊的**「自訂的需求指令碼」**下方，選取要新增功能的節點。
5. 按下**「新增」**，再按下**「功能」**。
6. 按下**「公用程式: 設定時間戳記」**。
7. 針對儲存日期和時間資訊的登錄設定，鍵入名稱，最多 255 個字元。

   例如，輸入**上次檔案更新的日期和時間：**

比較目前時間與儲存的時間值

1. 撰寫自訂需求指令碼。

   請參閱第 532 頁的「撰寫自訂的需求指令碼」。
2. 在**「自訂需求」**對話方塊的**「自訂的需求指令碼」**下方，選取要新增條件的節點。
3. 按下**「新增」**，然後按下 **IF..THEN**。
4. 按下**「公用程式: 檢查時間戳記」**。
5. 鍵入您之前為所儲存時間登錄設定所輸入的名稱。
6. 指定以分鐘、小時、天或週為單位的時間長度。

   如果超過指定的時間長度，或登錄設定值空白，則**「設定時間戳記」**函數會傳回True值。

編寫自訂需求以增加登錄 DWORD 值。

針對自訂需求，您可以增加Windows登錄DWORD值。如果機碼不存在，**「增加登錄 DWORD 值」**功能會建立該機碼。

編寫自訂需求以增加登錄 DWORD 值

1. 在主控台中，新增具有自訂需求指令碼的主機完整性政策。

   請參閱第 532 頁的「撰寫自訂的需求指令碼」。
2. 在**「自訂需求」**對話方塊的**「自訂的需求指令碼」**下方，選取要新增功能的節點。

3 按下「**新增**」，再按「**功能**」。

4 按下「**登錄: 增加登錄 DWORD 值**」。

5 在「**登錄機碼**」欄位中輸入要檢查的登錄機碼。

6 在「**值名稱**」欄位中輸入要檢查的值名稱。

7 按下「**確定**」。

使用自訂需求程序檔建立測試主機完整性政策

您為此測試建立的政策僅用於示範目的。政策會偵測是否存在作業系統，當偵測到時會產生 `fail`事件。一般來說，您會因為其他原因產生`fail`事件。

請完成下列工作：

- 使用自訂需求指令碼新增主機完整性政策，該指令碼可檢查用戶端電腦上的作業系統。
  請參閱第 537 頁的「使用自訂需求指令碼建立測試主機完整性政策」。
- 測試已建立的主機完整性政策。
  請參閱第 538 頁的「測試用戶端電腦上的主機完整性政策」。

使用自訂需求指令碼建立測試主機完整性政策

1 在主控台中，開啟某個主機完整性政策。

2 在「**主機完整性政策**」頁面上，按下「**需求**」>「**新增**」。

3 在「**新增需求**」對話方塊中，按下「**選取需求**」下拉式清單，選取預先定義的需求，然後按下「**確定**」。

4 在「**名稱**」方塊中，輸入自訂需求的名稱。

5 在「**自訂需求**」對話方塊的「**自訂的需求指令碼**」下的「**在下方插入陳述式**」上按下滑鼠右鍵，然後按下「**新增**」> **IF .. THEN**。

6 在右窗格的「**選取條件**」下拉式清單中，按下「**公用程式: 作業系統是**」。

7 在「**作業系統**」下，勾選用戶端電腦所執行且您可以測試的一或多個作業系統。

8 在「**自訂的需求指令碼**」下的「**THEN //在此插入陳述式**」上按下滑鼠右鍵，然後按下「**新增**」>「**功能**」>「**公用程式: 顯示訊息對話方塊**」。

9 在「**訊息方塊的標題**」欄位中，輸入訊息標題中要顯示的名稱。

10 在「**訊息方塊的文字**」欄位中，輸入您希望訊息顯示的文字。

11 在左窗格的「**自訂的需求指令碼**」下方，按下「**通過**」。

12 在右窗格的「**需求結果會傳回**」下，勾選「**失敗**」，然後按下「**確定**」。

13 按下「**確定**」。

14 在「**主機完整性政策**」對話方塊的左面板中，按下「**指派政策**」。

15 在「**指派主機完整性政策**」對話方塊中，選取要指派政策給哪些群組，然後按下「**指派**」。

在「**指派主機完整性政策**」對話方塊中，按下「**是**」，指派主機完整性政策的變更。

附註：一項主機完整性政策可以指派給多個群組，但一個群組只能具有一項主機完整性政策。您可以用不同的政策來取代現有政策。

測試用戶端電腦上的主機完整性政策

1 在主控台中，按下「**用戶端**」>「**用戶端**」。

2 在「**用戶端**」下方，按下並反白顯示包含您套用主機完整性政策的用戶端電腦的群組。

3 在「**工作**」下方，按下「**對群組執行指令**」>「**更新內容**」，然後按下「**確定**」。

4 登入執行用戶端的電腦並注意出現的訊息方塊。

因為規則觸發了`fail`測試，所以會出現訊息方塊。測試後，停用或刪除測試政策。

請參閱第 532 頁的「撰寫自訂的需求指令碼」。

請參閱第 536 頁的「編寫自訂需求以增加登錄 DWORD 值。」。

請參閱第 535 頁的「撰寫要在用戶端執行指令碼的自訂需求」。

28

使用報告和日誌監控防護

本章包含以下主題：

監控端點防護

Symantec Endpoint Protection 會收集網路安全性事件的相關資訊。 您可以使用日誌和報告檢視這些事件，也可透過通知方式在發生事件時隨時通知您。

您可以使用報告和日誌來判定下列種類問題的答案：

- 哪些電腦已受感染？
- 哪些電腦需要掃描？
- 網路內偵測出哪些風險？

表 28-1 監控端點防護工作

工作	敘述
檢閱網路的安全性狀態	下列清單說明了部分您可執行以監控用戶端電腦安全性狀態的工作。 ■ 檢視未安裝的用戶端數量。 請參閱第 544 頁的「執行有關用戶端部署狀態的報告」。 ■ 檢視已離線的電腦數量。 請參閱第 542 頁的「尋找離線電腦」。 ■ 取得已偵測病毒的計數以及其他安全性風險，並檢視各病毒與安全性風險的詳細資料。 請參閱第 544 頁的「檢視風險」。 ■ 取得網路中未受保護電腦的計數，並檢視每部電腦的詳細資訊。 請參閱第 547 頁的「檢視系統防護」。 ■ 檢視病毒和間諜軟體定義檔為最新的電腦數量。 請參閱第 547 頁的「檢視系統防護」。 ■ 檢視用戶端電腦的即時作業狀態。 請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。 ■ 檢閱網路中執行的程序。 請參閱第 429 頁的「監控 SONAR 偵測結果來查看是否有誤報」。 ■ 找出哪些電腦已指派至哪些群組。 ■ 檢視安裝在您網路中的用戶端和 Symantec Endpoint Protection Manager 伺服器上的 Symantec Endpoint Protection 軟體版本清單。 請參閱第 543 頁的「產生網路中安裝的 Symantec Endpoint Protection 版本的清單」。 ■ 檢視用戶端電腦上的授權資訊，其中包括有效基座個數、已過度部署基座個數、已過期的基座個數，以及到期日。 請參閱第 84 頁的「檢查 Symantec Endpoint Protection Manager 中的授權狀態」。 請參閱第 546 頁的「檢視每日或每週狀態報告」。
找出需要保護的用戶端電腦	您可以執行下列工作，檢視或尋找哪些電腦需要額外進行防護： ■ 檢視已停用 Symantec Endpoint Protection 的電腦數量。 請參閱第 547 頁的「檢視系統防護」。 ■ 檢視病毒和間諜軟體定義檔已過期的電腦數量。 請參閱第 547 頁的「檢視系統防護」。 ■ 尋找最近未掃描的電腦。 請參閱第 542 頁的「尋找未掃描電腦」。 ■ 檢視攻擊目標和來源。 請參閱第 545 頁的「檢視攻擊目標和來源」。 ■ 檢視事件日誌。 請參閱第 563 頁的「檢視日誌」。

工作	敘述
防護您的用戶端電腦	您可以從主控台執行指令，保護用戶端電腦。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。 例如，您可以消除用戶端電腦上的安全風險。 請參閱第 351 頁的「檢查掃描動作及重新掃描識別出的電腦」。
架構通知，以便在發生安全性事件時發出警示	您可以建立並架構在發生某些安全相關事件時啟動通知。 例如，您可以設定用戶端電腦發生入侵嘗試時提出通知。 請參閱第 577 頁的「設定管理員通知」。
為正在進行的監控建立自訂快速報告和排程報告	您可以建立和產生自訂的快速報告，也可以排程含有所要檢視資訊的自訂報告定期執行。 請參閱第 559 頁的「執行和自訂快速報告」。 請參閱第 561 頁的「如何執行排程報告」。 請參閱第 560 頁的「儲存和刪除自訂報告」。 請參閱第 547 頁的「架構報告偏好」。
將用戶端日誌使用的空間量減到最少	基於安全理由，您可能需要將日誌記錄保留一段較長的時間。 然而，如果您有許多用戶端，可能會產生大量的用戶端日誌資料。 如果您的管理伺服器空間不夠，您可能需要減少日誌大小，並縮短資料庫保留日誌的時間。 您可以執行下列工作，來減少日誌資料量： ■ 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。 請參閱第 625 頁的「指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器」。 ■ 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。 請參閱第 626 頁的「指定日誌大小以及在資料庫中保留日誌項目的時間長度」。 ■ 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。 ■ 減少各管理伺服器所管理的用戶端數目。 ■ 減少活動訊號頻率，這會控制用戶端日誌多久上傳一次到伺服器。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。 ■ 在將日誌資料插入資料庫之前，減少日誌資料所儲存目錄的空間。 請參閱第 627 頁的「關於增加用於用戶端日誌資料的伺服器磁碟空間」。

工作	敘述
將日誌資料匯出至集中位置	如果您要在集中的位置存放整個網路的所有日誌，日誌資料匯出會很有用。 如果您要使用試算表等第三方程式組織或運用資料，也可以使用日誌資料匯出的方式。 您也可能想在刪除日誌記錄之前，先匯出日誌的資料。 您可以將某些日誌中的資料匯出至逗號分隔文字檔。 您可以將其他日誌的資料匯出至稱為傾印檔的 Tab 分隔文字檔，或匯出至 Syslog 伺服器。 請參閱第 624 頁的「將日誌資料匯出至文字檔」。 請參閱第 623 頁的「將資料匯出至 Syslog 伺服器」。 請參閱第 568 頁的「檢視其他網站的日誌」。
使用報告和日誌進行問題疑難排解	您可以使用報告針對部分問題進行疑難排解。 請參閱第 668 頁的「報告問題疑難排解」。

附註：Symantec Endpoint Protection 會從管理伺服器上的事件日誌，提取報告中所顯示的事件。 事件日誌包含用戶端電腦時區的時間戳記。 當管理伺服器收到事件時，會將事件的時間戳記轉換成格林威治標準時間 (GMT)，再插入資料庫中。 當您建立報告時，報告軟體會以您檢視報告所在電腦的當地時間，來顯示事件資訊。

尋找未掃描電腦

您可以列出需要掃描的電腦。

請參閱第 539 頁的「監控端點防護」。

尋找未掃描電腦

1. 在主控台中，按下**「報告」**。
2. 在**「快速報告」**標籤上，指定下列資訊：

報告類型	選取**「掃描」**。
所選報告	選取**「未掃描電腦」**。

3. 按下**「建立報告」**。

尋找離線電腦

您可以列出離線的電腦。

用戶端離線的原因有幾個。您可以利用幾種方式來識別離線的電腦並針對這些問題採取補救措施。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

尋找離線電腦

1. 在主控台上，按下**「首頁」**。
2. 在**「首頁」**頁面的**「端點狀態」**窗格中，按代表離線電腦數量的連結。
3. 若需離線電腦的更多資訊，請按**「檢視詳細資料」**連結。

檢視電腦狀態日誌中的離線用戶端電腦

1. 在主控台中，按下**「監視器」**。
2. 在**「日誌」**標籤的**「日誌類型」**清單方塊中，按下**「電腦狀態」**。
3. 按下**「其他設定」**。
4. 在「線上狀態」清單方塊中，按下**「離線」**。
5. 按下**「檢視日誌」**。

   依預設，在過去 24 小時離線的電腦清單會出現。此清單包括每部電腦的名稱、IP 位址以及上次登入其伺服器的時間。您可以調整時間範圍，顯示在您想要查看的任何時間範圍內離線的電腦。

產生網路中安裝的 Symantec Endpoint Protection 版本的清單

您可以從 Symantec Endpoint Protection Manager 執行快速報告，這個報告會提供網路中安裝的 Symantec Endpoint Protection 軟體版本的清單。當您想要從舊版的 Symantec Endpoint Protection 升級或移轉軟體時，此清單可能很實用。此清單包括本機和遠端電腦。

您可以使用 MHTML 網頁封存檔格式儲存此報告。

請參閱第 563 頁的「列印和儲存報告副本」。

產生列出 Symantec Endpoint Protection 軟體版本的報告

1. 在主控台中，按下**「報告」**。
2. 在**「報告類型」**中，選取**「電腦狀態」**。
3. 在**「選取報告」**中，選取**「Symantec Endpoint Protection 產品版本」**。
4. 按下**「建立報告」**。

產生詳細的用戶端電腦清單，包括 Symantec Endpoint Protection 軟體版本

1. 在主控台中，按下**「監視器」**，然後按下**「日誌」**標籤。
2. 在**「日誌類型」**中，選取**「電腦狀態」**。

3 視需要調整「**時間範圍**」，然後按下「**檢視日誌**」。

4 捲動以尋找「**版本**」欄。按下標頭，以依版本號碼排序。

按下「**檢視套用的過濾器**」以調整日誌過濾。按下「**匯出**」以匯出清單。按下用戶端電腦，然後按下「**詳細資料**」以查看其詳細資料。

請參閱第 563 頁的「檢視日誌」。

請參閱第 130 頁的「選擇升級用戶端軟體的方法」。

請參閱第 121 頁的「Symantec Endpoint Protection 的升級資源」。

執行有關用戶端部署狀態的報告

您可以執行多個有關您用戶端部署狀態的報告。例如，您可以查看成功或未成功安裝的用戶端數。 您也可以查看哪些用戶端上安裝了何種防護技術，以及有關用戶端電腦的系統資訊。

請參閱第 539 頁的「監控端點防護」。

檢視已部署用戶端的狀態

1 在主控台中，按下「**報告**」。

2 在「**快速報告**」標籤上，按下「**電腦狀態**」報告類型，然後按下其中一個報告：

- 如需瞭解用戶端的部署狀態，請按下「**部署報告**」。
- 如需瞭解用戶端的防護狀態，請按下「**用戶端清查詳細資料**」。

3 按下「**建立報告**」。

檢視風險

您可以取得關於網路風險的資訊。

請參閱第 539 頁的「監控端點防護」。

檢視受感染和有風險的電腦

1 在主控台中，按下「**報告**」。

2 在「**快速報告**」標籤上，指定下列資訊：

報告類型	**風險**
所選報告	**受感染和處於風險的電腦**

3 按下「**建立報告**」。

為了更佳瞭解不啟用某些功能的好處和風險，您可以執行「依防護技術顯示風險分佈」報告。此報告提供下列資訊：

- 以特徵為基礎的病毒和間諜軟體偵測
- SONAR 偵測
- 「下載鑑識」偵測
- 入侵預防和瀏覽器防護偵測

檢視各類型防護技術所偵測到的風險

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	**風險**
所選報告	**依防護技術顯示風險分佈**

3 按下**「建立報告」**。

檢視新偵測到的風險

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	**風險**
所選報告	**網路中偵測到的新風險**

3 按下**「建立報告」**。

檢視綜合性風險報告

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	**風險**
選取報告	**綜合性風險報告**

3 按下**「建立報告」**。

檢視攻擊目標和來源

您可以檢視攻擊目標和來源。

請參閱第 539 頁的「監控端點防護」。

檢視前幾名遭攻擊目標

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	選取**「防網路和主機侵入」**。
選取報告	選取**「前幾名遭攻擊目標」**。

3 按下**「建立報告」**。

檢視前幾名攻擊來源

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	選取**「防網路和主機侵入」**。
選取報告	選取**「前幾名攻擊來源」**。

3 按下**「建立報告」**。

包含下列統計資料的完整報告：

- 前幾名攻擊類型
- 前幾名遭攻擊目標
- 前幾名攻擊來源
- 前幾名流量通知

檢視關於攻擊目標和來源的完整報告

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤上，指定下列資訊：

報告類型	選取**「防網路和主機侵入」**。
選取報告	選取**「完整報告」**。
「架構」選項	您可以選取要納入完整報告中的報告。

3 按下**「建立報告」**。

檢視每日或每週狀態報告

「每日狀態報告」可提供下列資訊：

- 採取了已清除、可疑、已攔截、已隔離、已刪除、新感染和仍受感染動作的病毒偵測結果數。
- 病毒定義檔派送時間表
- 前 10 大風險及感染

「每週狀態報告」可提供下列資訊：

- 電腦狀態
- 病毒偵測
- 防護狀態快照
- 病毒定義檔派送時間表
- 依日期顯示風險分佈
- 前 10 大風險及感染

請參閱第 539 頁的「監控端點防護」。

檢視每日狀態報告

1 在主控台中，按下**「首頁」**。

2 在**「首頁」**的**「我的最愛報告」**窗格中，按下**「Symantec Endpoint Protection 每日狀態」**或**「Symantec Endpoint Protection 每週狀態」**。

檢視系統防護

系統防護包含下列資訊：

- 病毒定義檔為最新的電腦數量。
- 病毒定義檔已過期的電腦數量。
- 已離線的電腦數量。
- 已停用的電腦數量。

請參閱第 539 頁的「監控端點防護」。

檢視系統防護

1 在主控台中，按下**「首頁」**。

系統防護顯示於**「端點狀態」**窗格中。

2 在**「端點狀態」**窗格中，按**「檢視詳細資料」**以檢視更多的系統防護資訊。

架構報告偏好

您可以架構下列報告偏好：

- **「首頁」**和**「監視器」**頁顯示選項
- **「安全狀態」**臨界值
- 用於日誌和報告以及舊版日誌檔上傳的顯示選項

您設定的安全狀態臨界值，可決定何時將 Symantec Endpoint Protection Manager 的**「首頁」**的安全狀態訊息視為不良。臨界值是以百分比表示，設定將網路視為違反安全性政策的時機。

例如，您可以設定病毒定義過時的電腦數量百分比，以觸發不良安全狀態。您也可以設定需要將定義檔視為過期的天數。Symantec Endpoint Protection 會按下列方式，在計算特徵或定義檔是否過期時，判斷哪些項目是最新的。其標準是最新的病毒定義和 IPS 特徵日期，這可以從執行主控台的管理伺服器取得。

若需可設定的偏好選項相關資訊，可按下**「偏好」**對話方塊各個標籤上的**「說明」**。

架構報告偏好

1. 在主控台的**「首頁」**上，按下**「偏好」**。
2. 根據要設定的偏好類型，按下以下其中一個標籤：
   - **首頁和監視器**
   - **安全狀態**
   - **日誌和報告**
3. 設定要變更的選項值。
4. 按下**「確定」**。

從獨立式網頁瀏覽器登入報告

您可以從與您的管理伺服器連線的獨立式網頁瀏覽器，存取**「首頁」**、**「監視器」**和**「報告」**頁面。然而，使用獨立式瀏覽器時，所有其他主控台功能都無法使用。

報告頁面和日誌頁面通常會以安裝管理伺服器時所用的語言顯示。若要在使用遠端主控台或瀏覽器時顯示這些頁面，您必須在所使用的電腦上安裝適當的字型。

若要從網頁瀏覽器存取報告，您必須具備下列資訊：

- 管理伺服器的主機名稱。
- 管理伺服器的使用者名稱和密碼。

附註：針對支援正在使用的 Symantec Endpoint Protection 版本的最低瀏覽器版本檢查系統需求。不支援更低的網頁瀏覽器版本。

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

從獨立式網頁瀏覽器登入報告

1 開啟網頁瀏覽器。

2 按照以下格式，在位址文字方塊中輸入預設的報告 URL：

https://*SEPMServer*:8445/reporting

其中 *SEPMServer* 是管理伺服器的主機名稱或 IP 位址。如需支援的網頁瀏覽器清單，請參閱：所有 Endpoint Protection 版本的版本說明、新修正和系統需求。

IP 位址包括 IPv4 和 IPv6。必須用方括弧括住 IPv6 位址。例如：
https://[*SEPMServer*]:8445

附註：在瀏覽器中輸入 HTTPS 獨立式報告 URL 時，瀏覽器可能會顯示警告。出現警告是因為管理伺服器使用自我簽署憑證。若要解決這個問題，您可以在瀏覽器的信任憑證儲存區中安裝憑證。 憑證僅支援主機名稱，所以請在 URL 中使用主機名稱。 如果使用 localhost、IP 位址或完整網域名稱，警告還是會出現。

如果您使用 12.1 並且是從版本 11 移轉，Symantec Endpoint Protection 11 版的預設報告 URL 為 http://*SEPMServer*:8014/reporting。您必須更新瀏覽器的書籤。

3 當出現登入對話方塊時，請輸入您的使用者名稱和密碼，然後按下**「登入」**。

如果您使用超過一個網域，請在**「網域」**文字方塊中鍵入您的網域名稱。

關於 Symantec Endpoint Protection Manager 報告類型

以下是可用的報告類別：

- 快速報告，可視需要執行。
- 排程報告，根據您架構的排程自動執行。

報告包含從您的管理伺服器以及與這些伺服器通訊的用戶端電腦收集到的事件資料。 您可以自訂報告來提供想要檢視的資訊。

快速報告是預先定義的報告，不過您可以自訂這些報告，並儲存用來建立自訂報告的過濾條件。 您可以使用自訂過濾條件建立自訂排程報告。 當您排程要執行的報告時，可以架構它以電子郵件傳送給一或多個收件者。

排程報告預設通常為執行。 您可以針對尚未執行的任何排程報告變更此設定。 您也可以刪除單一或所有排程報告。

表 28-2 可作為快速報告和排程報告的報告類型

報告類型	敘述
稽核	顯示用戶端和位置目前使用之政策的相關資訊。 此報告包含關於政策修改活動的資訊，如事件時間和類型、政策修改、網域、網站、管理員以及敘述。
應用程式與裝置控制	顯示攔截某些類型行為之事件的相關資訊。 這些報告包括應用程式安全性警示、攔截的目標及攔截的裝置等相關資訊。 攔截的目標可能是 Windows 登錄機碼、DLL、檔案和程序。
合規性	顯示已通過或未通過主機完整性檢查之用戶端數量的相關資訊。
電腦狀態	顯示網路中電腦作業狀態 (例如哪些電腦關閉了安全功能) 的相關資訊。這類報告包括有關版本、尚未登入伺服器的用戶端、用戶端清查及線上狀態等的資訊。
欺敵	顯示欺敵活動的相關資訊，例如報告欺敵活動的前幾個電腦或使用者，以及觸發的前幾個欺敵工具。
防網路和主機刺探利用	顯示入侵預防、防火牆攻擊、防火牆流量和封包以及記憶體攻擊緩和的相關資訊。 「防網路和主機刺探利用」報告可以追蹤電腦活動，以及該電腦與其他電腦及網路的互動狀況。其記錄的資訊包括嘗試透過網路連線進出電腦的流量。記憶體攻擊緩和事件列出了終止應用程式或攔截攻擊以防止其攻擊應用程式的緩和技術。
風險	顯示管理伺服器及其用戶端上風險事件的相關資訊。 其包含有關SONAR掃描的資訊。
掃描	顯示病毒和間諜軟體掃描活動的相關資訊。
系統	顯示事件時間、事件類型、網站、網域、伺服器及嚴重性等級等的相關資訊。 「系統」報告包含有助於疑難排解用戶端問題的資訊。

如果您的網路包含多個網域，多個報告可讓您檢視所有網域、單一或數個網站的資料。 所有快速報告均預設為顯示適用於您選取要建立之報告的所有網域、群組、伺服器等。

請參閱第 559 頁的「執行和自訂快速報告」。

請參閱第 561 頁的「如何執行排程報告」。

下一節依照名稱及其一般內容來說明報告。您可以針對所有報告架構「基本設定」和「進階設定」，以精簡所要檢視的資料。您也可以命名並儲存自訂過濾器，以便日後執行相同的自訂報告。

表 28-3 稽核報告

報告名稱	說明
使用的政策	此報告顯示用戶端和位置目前所使用的政策。此項資訊包含網域名稱、群組名稱，以及套用於各個群組的政策序號。

表 28-4 應用程式與裝置控制報告

報告名稱	說明
含最多警示之應用程式控制日誌的前幾名群組	此報告由一個圓形圖與一些相對長條組成。它會顯示含應用程式控制日誌的群組，這些日誌已產生最大量的安全警示。
前幾名被攔截目標	此報告由一個圓形圖與下列目標 (如果有) 組成： ■ 前幾名檔案 ■ 前幾名登錄機碼 ■ 前幾名程序 ■ 前幾名模組 (dll)
前幾名被攔截裝置	此報告由一個圓形圖組成，會顯示最常被攔截而不能存取網路的裝置。

表 28-5 合規性報告

報告名稱	敘述
主機完整性狀態	此報告顯示通過或未通過電腦上所執行主機完整性檢查的用戶端。
按合規性失敗摘要的用戶端	此報告由一個長條圖組成，其中顯示： ■ 按控制失敗事件的類型 (例如防毒、防火牆或 VPN) 列出的唯一工作站計數 ■ 群組內的用戶端總數
合規性失敗詳細資料	此報告由一個表格組成，會按控制失敗顯示唯一電腦。它會顯示每個失敗中涉及的準則和規則，以及已部署的用戶端百分比和失敗的百分比。
按位置的非合規性用戶端	此報告由一個表格組成，會顯示合規性失敗事件。這些事件會按其位置顯示在群組中。此項資訊包括失敗的唯一電腦，以及失敗總計百分比和位置失敗百分比。

表 28-6 電腦狀態報告

報告名稱	說明
病毒定義檔派送	此報告顯示用於整個網路的唯一病毒定義檔版本，以及使用每種定義檔版本的電腦數量和百分比。

報告名稱	說明
最近未更新的電腦	此報告顯示最近未更新的所有電腦清單。它也會顯示電腦的作業系統、IP 位址、使用者名稱和上次變更其狀態的時間。
Symantec Endpoint Protection 產品版本	此報告顯示網路中所有 Symantec Endpoint Protection 產品版本的版本號碼清單。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
入侵預防特徵分佈	此報告顯示用於整個網路的 IPS 特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
下載防護特徵分佈	此報告顯示用於整個網路的下載防護特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
SONAR 特徵分佈	此報告顯示用於整個網路的 SONAR 特徵檔案版本。它也包含使用各版本的網域和伺服器，還有使用各版本的電腦數量和百分比。
用戶端清查	此報告由一個長條圖組成，會顯示每一項的電腦總數和百分比： ■ 作業系統 ■ 總記憶體 ■ 可用記憶體 ■ 總計磁碟空間 ■ 可用磁碟空間 ■ 處理器類型
合規性狀態分佈	此報告由一個圓形圖與一些相對長條組成，這些長條會按群組或按子網路顯示合規性通過和未通過情況。它會顯示合規的電腦數量和百分比。
用戶端線上狀態	此報告由一些圓形圖及對應於每個群組或每個子網路的相對長條組成。它會顯示線上的電腦百分比。 線上具有下列意義： ■ 若是推送模式下的用戶端，線上代表用戶端目前已連線至伺服器 ■ 若是提取模式下的用戶端，線上代表用戶端在最後兩個用戶端活動訊號期間內，已連上伺服器 ■ 若是遠端據點中的用戶端，線上代表用戶端在上次遠端複製時處於線上狀態
有最新政策的用戶端	此報告由對應於每個群組或每個子網路的圓形圖組成。它會顯示套用最新政策的電腦數量和百分比。
依群組顯示用戶端數目	此報告由一個表格組成，會按群組列出主機資訊。它會顯示用戶端和使用者數量。如果您使用多個網域，此項資訊會按網域顯示。

報告名稱	說明
安全狀態摘要	此報告會反映網路的一般安全狀態，並顯示有下列狀態的電腦數量和百分比： ■ 防毒引擎關閉 ■ 自動防護關閉 ■ 竄改防護關閉 ■ 需要重新啟動 ■ 主機完整性檢查失敗 ■ 網路威脅防護關閉
防護內容版本	此報告顯示用於整個網路的所有主動型防護內容版本。針對下列每種防護類型，會顯示一個圓形圖： ■ 分解程式版本 ■ Eraser 引擎版本 ■ SONAR 內容版本 ■ SONAR 引擎版本 ■ 商用應用程式清單版本 ■ 內容處理程式引擎版本 ■ 允許的應用程式清單版本 ■ 賽門鐵克安全機制應變中心已新增的內容類型
Symantec Endpoint Protection 授權狀態	此報告包含試用授權到期的天數以及新增授權的指示。
用戶端清查詳細資料	此報告包含用戶端清查的詳細資料，例如電腦規格和特徵。
用戶端軟體遞送 (快照) 僅限排程報告	此報告由一個表格組成，用於追蹤用戶端套件部署進度。快照資訊可讓您瞭解遞送的進度情況，以及尚未完全部署的用戶端數量。
某段時間內的線上/離線用戶端 (快照) 僅限排程報告	此報告由折線圖和表格組成，會顯示線上或離線的用戶端數量。針對每個前幾項目標顯示一個圖表。目標是群組或作業系統。
某段時間內有最新政策的用戶端 (快照) 僅限排程報告	此報告由一個折線圖組成，會顯示已套用最新政策的用戶端。對於每個前幾名用戶端顯示一個圖表。
某段時間內的非合規用戶端 (快照) 僅限排程報告	此報告由一個折線圖組成，會顯示某段時間內未通過主機完整性檢查的用戶端百分比。對於每個前幾名用戶端顯示一個圖表。
病毒定義遞送 (快照) 僅限排程報告	此報告會列出已遞送到用戶端的病毒定義檔套件版本。此項資訊有助於從主控台追蹤新病毒定義檔的部署進度。

報告名稱	說明
部署報告	此報告摘要說明了用戶端安裝和部署的狀態。

表 28-7 防網路和主機刺探利用報告

報告名稱	說明
前幾名遭攻擊目標	此報告由一個圓形圖組成，其中包括攻擊數量和百分比、攻擊類型和嚴重性及攻擊分佈等資訊。您可以使用群組、子網路、用戶端或通訊埠作為目標來檢視資訊。
前幾名攻擊來源	此報告由一個圓形圖組成，會顯示對您網路發動攻擊的前幾部主機。它包括攻擊數量和百分比、攻擊類型和嚴重性及攻擊分佈等資訊。
前幾名攻擊類型	此報告由一個圓形圖組成，其中包括事件數量和百分比、群組和嚴重性及按群組的事件類型和數量等資訊。
前幾名攔截的應用程式	此報告由一個圓形圖組成，會顯示遭攔截而無法存取您網路的前幾個應用程式。它包括攻擊數量和百分比、群組和嚴重性及按群組的事件類型和數量等資訊。
某段時間內的攻擊	此報告由一或多個折線圖組成，會顯示所選時段內的攻擊。例如，如果時間範圍是上個月，則報告會顯示上個月每天的攻擊總數。它會包括攻擊的數量和百分比。您可以檢視所有電腦的攻擊情況，或是按前幾名作業系統、使用者、IP 位址、群組或攻擊類型進行檢視。
依嚴重性顯示安全事件	此報告由一個圓形圖組成，會顯示網路中按嚴重性分級之安全事件的總數和百分比。
某段時間內攔截的應用程式	此報告由一個折線圖和一個表格組成。它會顯示在您選取的時段內遭攔截而無法存取您網路的應用程式總數。它包括事件時間、攻擊數量和百分比。您可以顯示所有電腦的資訊，或是按群組、IP 位址、作業系統或使用者來顯示資訊。
某段時間內的流量通知	此報告由一個折線圖組成，會顯示某段時間內基於防火牆規則違規的通知數量。計入的規則就是您在「防火牆政策規則」清單的「記錄」欄位中已勾選「傳送電子郵件警示」選項的規則。您可以在此報告中，顯示所有電腦的資訊，或是按群組、IP 位址、作業系統或使用者來顯示資訊。
前幾名流量通知	此報告由一個圓形圖和一些相對長條組成，會列出群組或子網路，以及通知數和百分比。它會顯示根據您架構為務必通知之防火牆規則違規情況所產生的通知數。計入的規則就是您在「防火牆政策規則」清單的「記錄」欄位中已勾選「傳送電子郵件警示」選項的規則。您可以檢視按前幾名群組或子網路分組的全部、流量日誌或封包日誌的資訊。
記憶體攻擊緩和偵測	此報告顯示已攔截或允許的記憶體攻擊緩和類型的數量。

報告名稱	說明
完整報告	此報告在單一報告中提供下列「網路威脅防護」資訊： ■ 前幾名攻擊類型 ■ 依群組顯示前幾名遭攻擊目標 ■ 依子網路顯示前幾名遭攻擊目標 ■ 依用戶端顯示前幾名目標 ■ 前幾名攻擊來源 ■ 依群組顯示前幾名流量通知 (流量) ■ 依群組顯示前幾名流量通知 (封包) ■ 依子網路顯示前幾名流量通知 (流量) ■ 依子網路顯示前幾名流量通知 (封包) ■ 此報告包括所有網域的資訊

表 28-8 風險報告

報告名稱	說明
受感染和處於風險的電腦	此報告由兩個表格組成。其中一個表格會列出有病毒感染的電腦，而另一個表格會列出有尚未矯正之安全風險的電腦。
動作清單	此報告由一個表格組成，會顯示偵測到風險時可能採取的所有動作數量。可能的動作有「已清除」、「可疑」、「已攔截」、「已隔離」、「已刪除」、「擱置修復」、「已記錄商用或強制偵測」、「新感染」和「仍受感染」。此資訊也會顯示在 Symantec Endpoint Protection 首頁上。
風險偵測數目	此報告由一個圓形圖、一個風險表格以及一個相關相對長條組成。它會按網域、伺服器或電腦顯示風險偵測數量。如果您用的是舊版 Symantec AntiVirus 用戶端，則此報告會使用伺服器群組，而非網域。
網路中偵測到的新風險	此報告由一個表格和一個分佈圓形圖組成。針對每一個新風險，表格會提供下列資訊： ■ 風險名稱 ■ 風險類別或類型 ■ 第一次搜尋到的資料 ■ 組織中的第一次發生 ■ 最先偵測到它的掃描類型 ■ 發現它時它所在的網域 (舊版電腦上為伺服器群組) ■ 發現它的伺服器 (舊版電腦上的父系伺服器) ■ 發現它的群組 (舊版電腦上為父系伺服器) ■ 發現它的電腦，以及當時登入的使用者名稱 圓形圖會按目標選取類型顯示新風險分佈：網域 (舊版電腦上為伺服器群組)、群組、伺服器 (舊版電腦上為父系伺服器)、電腦或使用者名稱。

報告名稱	說明
前幾名風險偵測交叉比對	此報告由一個 3D 長條圖組成，透過兩個變數將病毒和安全風險偵測進行交叉比對。您可以選取電腦、使用者名稱、網域、群組、伺服器或風險名稱，作為 x 和 y 軸變數。此報告會顯示每個座標軸變數的前五個實例。如果您已選取電腦為變數之一，而受感染的電腦少於 5 部，則圖中可能顯示未感染的電腦。 **附註：**對於執行舊版 Symantec AntiVirus 的電腦，會使用伺服器群組和父系伺服器，而不是網域和伺服器。
下載風險分佈	此報告顯示下載鑑識所偵測到的檔案數量，並按敏感程度進行分組。會向找到的檔案提供詳細報告。您也可以在執行報告之前，按 URL、Web 網域、應用程式和使用者允許的方式分組檔案。
風險分佈摘要	此報告由一個圓形圖和一個相關長條圖組成，會顯示所選目標類型中每個唯一項目的相對百分比。例如，如果選擇的目標是風險名稱，則圓形圖會顯示每個唯一風險的切片。每個風險名稱會顯示一個長條，詳細資料包括偵測數目及其佔偵測總數的百分比。目標包括風險名稱、網域、群組、伺服器、電腦、使用者名稱、來源、風險類型或風險嚴重性。對於執行舊版 Symantec AntiVirus 的電腦，會使用伺服器群組和父系伺服器，而不是網域和伺服器。
某段時間內的風險分佈	此報告由一個表格及一個相對長條組成，表格會顯示單位時間內偵測到病毒和安全風險數量。
依防護技術顯示風險分佈	此報告顯示每個防護技術的病毒和安全風險偵測數量。
SONAR 偵測結果	此報告由一個圓形圖和一些長條圖組成，會顯示下列資訊： ■ 標記為風險但您已經將其新增至網路中允許的例外的應用程式清單 ■ 已偵測到並確認為風險的應用程式清單 ■ 已偵測到但風險狀態仍待確認的應用程式清單 每份清單上，此報告都顯示公司名稱、應用程式雜湊及版本，以及涉及到的電腦。對於允許的應用程式，此報告還會顯示允許的來源。

報告名稱	說明
SONAR 威脅分佈	此報告由一個圓形圖組成，以數個相對長條和一個摘要表格顯示偵測出的前幾名應用程式名稱。這些偵測包括「商用應用程式清單」和「強制偵測」清單上的應用程式。第一個摘要表格包含應用程式名稱以及偵測數目和百分比。 摘要表格顯示每個偵測的下列資訊： ■ 應用程式名稱和雜湊 ■ 應用程式類型，鍵盤側錄程式、特洛伊木馬程式、病蟲、遠端控制或商用鍵盤側錄程式 ■ 公司名稱 ■ 應用程式版本 ■ 報告該偵測的唯一電腦數量 ■ 偵測中的前三名路徑名稱 ■ 上次偵測日期
某段時間內的 SONAR 威脅偵測	此報告由一個折線圖組成，會顯示所選時間範圍內的主動型威脅偵測數目。它也包含具有相對長條的表格，會列出某段時間內偵測出的威脅總數。
前幾名風險的動作摘要	此報告會列出網路中發現的前幾名風險。對於每個風險，此報告都會顯示動作摘要長條，會顯示偵測到風險時所採取的每項動作百分比。動作包括「已隔離」、「已清除」、「已刪除」等。此報告也會顯示每一個特定動作為第一個架構的動作、第二個架構的動作、兩者皆非或不明的時間百分比。
通知數	此報告由一個圓形圖以及一個相關相對長條組成。圖表會顯示根據您架構為務必通知之防火牆規則違規情況所觸發的通知數。它會包括每個通知的類型和數量。
某段時間內的通知數	此報告由一個折線圖組成，會顯示所選時間範圍內網路中的通知數。它也包含一個表格，會列出某段時間內的通知數和百分比。您可以過濾資料，使其按通知類型、確認狀態、建立者和通知名稱顯示。
每週爆發	此報告顯示指定時間範圍內每週偵測到病毒和安全風險的數目以及相對長條。時間範圍為一天時，會顯示過去一週的情況。
綜合性風險報告	此報告預設會包含所有的分佈報告和新風險報告。不過，您可以將其架構為僅包含特定的報告。此報告包括所有網域的資訊。
Symantec Endpoint Protection 每日狀態	此報告包含過去 24 小時內網路事件的病毒偵測情況、介入情況和定義狀態。
Symantec Endpoint Protection 每週狀態	此報告包含過去一週內端點電腦的授權狀態和病毒偵測統計資料。除非另有說明，資料反映的是累計值。

表 28-9 掃描報告

報告名稱	說明
掃描統計長條圖	此報告由一個長條圖組成，您可以在此選取掃描中的下列資訊的分佈方式： ■ 按掃描時間 (秒) ■ 按偵測到的風險數 ■ 按具有偵測的檔案數 ■ 按掃描的檔案數 ■ 按掃描時省略的檔案數 您也可以架構 Bin 寬度和長條圖中使用的 Bin 數目。Bin 寬度是用於選定群組的資料間隔。Bin 數目則會指定長條圖重複幾次資料間隔。 顯示的資訊包括項目數、最大值和最小值，以及平均值和標準誤差。 您可能會想要變更報告值，以使報告長條圖中產生最大量的資訊。例如，您可能會想要考慮所檢視的網路規模和資訊量。
依上次掃描時間顯示電腦	此報告按上次掃描時間顯示安全網路內的電腦清單。它也包含 IP 位址和掃描時登入的使用者名稱。
未掃描電腦	此報告顯示安全網路中尚未掃描的電腦清單，並提供下列資訊： ■ IP 位址 ■ 上次掃描的時間 ■ 目前使用者或上次掃描時登入的使用者的名稱

表 28-10 系統報告

報告名稱	說明
產生錯誤的前幾名用戶端	此報告由一個圓形圖組成，會顯示每個警告狀況和錯誤狀況。圖表會按用戶端顯示相對錯誤數和相對警告數及百分比。
產生錯誤的前幾名伺服器	此報告由一個圓形圖組成，會顯示每個警告狀況和錯誤狀況。圖表會按伺服器顯示相對錯誤數和相對警告數及百分比。
某段時間內的資料庫遠端複製失敗	此報告由一個折線圖與一個相關表格組成，會列出所選時間範圍內的遠端複製失敗。
網站狀態報告	此報告會顯示所有網站運作狀態的即時摘要，以及本機網站上所有伺服器的相關資訊。
WSS 整合 Token 使用情況	此報告摘要說明了使用 WSS 流量重新導向進行用戶端驗證的整合 Token 的使用情況。

執行和自訂快速報告

快速報告係指預先定義的自訂報告。這些報告包含從您的管理伺服器以及與這些伺服器通訊的用戶端電腦收集到的事件資料。快速報告可根據您為報告架構的特定設定提供關於事件的資訊。您可以儲存報告設定，以便日後可執行相同的報告，並且可以列印和儲存報告。

快速報告屬於靜態報告，可根據您在報告中指定的時間範圍提供特定資訊。您也可以利用日誌即時監控各個事件。

執行快速報告

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤的**「報告類型」**清單方塊中，選取要執行的報告類型。

3 在**「選取報告」**清單方塊中，選取要執行的報告名稱。

4 按下**「建立報告」**。

自訂快速報告

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤的**「報告類型」**清單方塊中，選取要自訂的報告類型。

3 在**「選取報告」**清單方塊中，選取要自訂的報告名稱。

如需「**網路遵從狀態**」報告與「**遵從狀態**」報告，請在「**狀態**」清單方塊中，選擇要使用的已儲存過濾架構或保留預設過濾的架構。

您可選擇「**前幾名風險偵測關聯**」報告的「**X 軸**」與「**Y 軸**」清單方塊，指定檢視報告的方式。

可選擇「**掃描統計長條圖**」報告的「**Bin 寬度**」與「**Bin 數目**」。

有些報告可在「**群組**」清單方塊中，指定報告結果分組方式。有些報告可在「**目標**」欄位中選擇過濾報告結果的目標。

4 在「**使用儲存的過濾**」清單方塊中，選取要使用的儲存過濾架構，或使用預設過濾。

5 在**「您要使用什麼過濾設定?」下方**的**「時間範圍」**清單方塊中，選取報告的時間範圍。

6 如果您已選取「**設定特定日期**」，則使用「**開始日期**」和「**結束日期**」清單方塊。這些選項可設定您要檢視資訊的時間間隔。

產生電腦狀態報告後選取**「設定特定日期」**，您可指定檢視自日期和時間欄位指定時間後，尚未登記於伺服器的電腦的所有相關項目。

7 如果您要架構報告的其他設定，請按下**「其他設定」**，並設定您想要的選項。

您可以按下**「更多相關資訊」**，以檢視上下文關聯說明的過濾選項敘述。

附註：過濾選項文字方塊，接受萬用字元，並可不區分大小寫搜尋相符項目。ASCII 星號字元是唯一可當做萬用字元使用的星號字元。

如果您日後要再次執行此報告，則可以儲存報告架構設定。

8 按下**「建立報告」**。

請參閱第 560 頁的「儲存和刪除自訂報告」。

請參閱第 563 頁的「列印和儲存報告副本」。

請參閱第 561 頁的「如何執行排程報告」。

儲存和刪除自訂報告

您可以將自訂報告設定儲存在過濾條件中，以便日後再次產生相同的報告。儲存設定時，設定會儲存到資料庫中。您提供給過濾的名稱會顯示在適用於該類型之日誌和報告的**「使用儲存的過濾」**清單方塊中。

附註：您儲存的過濾架構設定僅供您的使用者登入帳戶使用。其他具有報告權限的使用者無法存取您儲存的設定。

請參閱第 562 頁的「編輯用於排程報告的過濾」。

您可以刪除您所建立的任何報告架構。刪除架構後，您就無法再使用該報告。預設報告架構名稱會出現在**「使用儲存的報告」**清單方塊中，畫面會重新填入預設架構設定。

附註：如果您從管理伺服器刪除管理員，可以選擇儲存刪除的管理員所建立的報告。 報告的擁有權會變更，而且報告名稱也會變更。 新報告名稱的格式為 `"OriginalName('AdminName')"`。例如，由管理員 **JSmith** 建立名為 `Monday_risk_reports` 的報告，會重新命名為 `Monday_risk_reports(JSmith)`。

請參閱第 241 頁的「關於管理員帳戶和存取權限」。

儲存自訂報告

1 在主控台中，按下**「報告」**。

2 在**「快速報告」**標籤中，從清單方塊選擇一項報告類型。

3 變更報告的任何基本設定或其他設定。

4 按下**「儲存過濾」**。

5 在「**過濾器名稱**」文字方塊中，輸入此報告過濾的敘述性名稱。過濾新增至「**使用儲存的過濾**」清單時，只會顯示該名稱的前 32 個字元。

6 按下「**確定**」。

7 當出現確認對話方塊時，按下「**確定**」。

在您儲存過濾之後，該過濾會顯示在適用於相關報告和日誌的「**使用儲存的過濾**」清單方塊中。

刪除自訂報告

1 在主控台中，按下「**報告**」。

2 在「**快速報告**」標籤上，選取報告類型。

3 在「**使用儲存的過濾**」清單方塊中，選取要刪除的過濾名稱。

4 在「**使用儲存的過濾**」清單方塊旁按下「**刪除**」圖示。

5 當出現確認對話方塊時，按下「**是**」。

如何執行排程報告

排程報告是指根據您所架構之排程自動執行的報告。 排程報告會以電子郵件形式傳送給收件者，因此您必須加入至少一位收件者的電子郵件地址。 執行報告之後，該報告會以 .mht 檔案附件形式由電子郵件傳送給您所架構的收件者。

排程報告中所顯示的資料每小時都會在資料庫中進行更新。 當管理伺服器以電子郵件傳送排程報告時，報告中的資料是一小時內的新資料。

含某段時間內資料的其他報告會根據您針對用戶端日誌所架構的上傳間隔，在資料庫中進行更新。

請參閱第 625 頁的「指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器」。

附註：如果您在站台中有多個伺服器共用資料庫，則只有第一個安裝的伺服器會執行針對該站台所排程的報告。 此預設可以確保站台中的所有伺服器不會同時執行相同的排程掃描。 若要指定不同的伺服器來執行排程報告，則可以在本機站台屬性中架構此選項。

執行排程報告

1 在主控台中，按下「**報告**」。

2 在「**排程報告**」標籤上，按下「**新增**」。

3 在「**報告名稱**」文字方塊中，鍵入描述性名稱，並選擇是否鍵入較長的敘述。

雖然您可以將 255 個以上字元的內容貼到「敘述」文字方塊中，但敘述中只會儲存 255 個字元。

4 若您不要在下次之前執行此報告，可取消勾選「**啟用此排程報告**」核取方塊。

5 從清單方塊選取您要排程的報告類型。

6 從清單方塊選取您要排程的特定報告名稱。

7 從清單方塊選取您要使用之儲存的過濾名稱。

8 在**「執行一次每隔」**文字方塊中，選取您要以電子郵件形式傳送報告給收件者的時間間隔(時數、天數、週數、月數)。 然後輸入您選取的時間間隔值。 例如，如果您要每隔一天傳送報告，請選取天數，然後輸入 2。

9 在**「在以下時間後開始」**文字方塊中，鍵入您要開始執行報告的日期，或者按下行事曆圖示，然後選取日期。 然後從清單方塊選取小時和分鐘。

10 在**「報告收件者」**下方，鍵入電子郵件地址，多個地址則請以逗號分隔。

您必須設定郵件伺服器屬性，電子郵件通知才會生效。

11 按下**「確定」**。

編輯用於排程報告的過濾

您可以變更已排程之任何報告的設定。下次執行報告時，就會使用新的過濾設定。 您也可以根據先前儲存的報告過濾，建立其他的排程報告。

過濾存放區是由建立者所決定，因此當兩個使用者建立同名的過濾時，並不會發生問題。 但是，個別使用者或兩個使用者如果登入預設的 admin 帳戶，則不應該建立同名的過濾。

如果使用者建立同名的過濾，則在兩種情況下會發生衝突：

- 兩個使用者在不同的站台上都登入預設的 admin 帳戶，且兩個都建立同名的過濾。
- 同一個使用者建立過濾後，登入不同的站台，然後立即建立同名的過濾。

如果任一種情況發生在站台複寫進行之前，則使用者會在過濾清單中看到兩個同名的過濾。但只有一個過濾可以使用。如果發生此問題，最好是刪除可用的過濾，然後以不同的名稱重新建立。刪除可用的過濾時，不可用的過濾也會隨之刪除。

請參閱第 560 頁的「儲存和刪除自訂報告」。

附註：當您將儲存的過濾與排程報告相關聯時，請確定過濾不含自訂日期。如果過濾指定了自訂日期，您會在每次報告執行時取得相同的報告。

請參閱第 561 頁的「如何執行排程報告」。

編輯用於排程報告的過濾

1 在主控台中，按下**「報告」**。

2 按下**「排程報告」**。

3 在報告清單中，按下您要編輯的排程報告。

4 按下「**編輯過濾**」。

5 對過濾進行所需的變更。

6 按下「**儲存過濾**」。

若要保留原始的報告過濾，請重新命名此編輯後的過濾。

7 按下「**確定**」。

8 當出現確認對話方塊時，按下「**確定**」。

列印和儲存報告副本

您可以列印報告或儲存快速報告的副本。 您無法列印排程報告。 儲存的檔案或印出的報告均提供報告資料庫中現有資料的快照，因此，您可以保有先前的記錄。

附註：依預設，Internet Explorer 不會列印背景色彩和影像。 如果停用這個列印選項，印出來的報告可能看起來會與當初建立的報告不同。您可以變更瀏覽器的設定，列印背景色彩和影像。

請參閱第 559 頁的「執行和自訂快速報告」。

列印報告副本

1 在「報告」視窗中，按下「**列印**」。

2 在「**列印**」對話方塊中，視需要選取所要的印表機，然後按下「**列印**」。

當您儲存報告時，會儲存以報告資料庫現有資料為依據的安全性環境快照。如果稍後再以相同的過濾架構執行相同的報告，新報告會顯示不同的資料。

儲存報告副本

1 在「報告」視窗中，按下「**儲存**」。

2 在「**檔案下載**」對話方塊中，按下「**儲存**」。

3 在「**另存新檔**」對話方塊的「**儲存於**」選擇對話方塊中，瀏覽至儲存檔案的位置。

4 在「**檔案名稱**」清單方塊中，視需要變更預設的檔案名稱。

5 按下「**儲存**」。

報告會在您選取的位置中以 MHTML 網頁封存格式儲存。

6 在「**下載完成**」對話方塊中，按下「**關閉**」。

檢視日誌

您可以選取一組過濾設定，再根據這些設定從日誌產生要檢視的事件清單。

附註：檢視含大量資料的日誌，而發生資料庫錯誤時，您可能要變更資料庫逾時參數。

如果出現 CGI 或終止程序錯誤，您可能要變更其他逾時參數。

請參閱第 669 頁的「變更檢視報告和日誌的逾時參數」。

報告和日誌始終會以安裝管理伺服器時所用的語言顯示。若要在使用遠端 Symantec Endpoint Protection Manager 主控台或瀏覽器時顯示這些項目，您必須在所使用的電腦上安裝適當的字型。

請參閱第 564 頁的「關於 Symantec Endpoint Protection Manager 日誌類型」。

請參閱第 567 頁的「使用過濾儲存和刪除自訂日誌」。

檢視日誌

1. 在主控台中，按下**「監視器」**。
2. 在**「日誌」**標籤的**「日誌類型」**清單方塊中，選取您要檢視的日誌類型。
3. 對於某些類型的日誌，會顯示**「日誌內容」**清單方塊。如果顯示此方塊，請選取您要檢視的日誌內容。
4. 在**「使用儲存的過濾」**清單方塊中，選取儲存的過濾，或保留**「預設」**值。
5. 從**「時間範圍」**清單方塊選取時間，或保留預設值。如果您選取**「設定特定日期」**，請設定您要顯示哪個或哪些日期和時間之後的項目。
6. 按下**「其他設定」**，限制顯示的項目數。

   您也可以針對所選的日誌類型，設定任何其他可用的**「其他設定」**。

   附註：接受萬用字元和搜尋相符項目的篩選選項欄位不區分大小寫。ASCII 星號字元是唯一可當做萬用字元使用的星號字元。

7. 按下**「檢視日誌」**。

   也可以按下**「儲存過濾」**儲存過濾組態，以便日後產生相同的日誌檢視。

關於 Symantec Endpoint Protection Manager 日誌類型

日誌包含了用戶端架構變更、安全性相關活動及錯誤的相關記錄，這些記錄稱為事件。日誌會顯示這些事件以及所有相關的其他資訊。安全性相關活動包括病毒偵測、電腦狀態，以及進出用戶端電腦流量的相關資訊。

日誌很重要，可以追蹤每一用戶端電腦的活動，及其與其他電腦和網路互動的情形。可以使用這些資料分析網路的整體安全狀態，並修改用戶端電腦上的防護。您可以追蹤與病毒、安全風險和攻擊相關的趨勢。當多人共用一部電腦時，您可能可以識別引入風險的人員，並協助其採取更好的預防措施。

您可以在「**監視器**」頁面的「**日誌**」標籤上檢視日誌資料。

管理伺服器會定期將用戶端中的日誌資訊上傳到管理伺服器。您可以在日誌或報告中檢視這些資訊。由於報告是靜態的，其所包括的詳細資料沒有日誌裡那麼多，因此您可能傾向於使用日誌來監控網路。

除了使用日誌來監控網路，您還可以從各種日誌中採取以下動作：

- 在用戶端電腦上執行指令。
  請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。
- 新增多種類型的例外。
  請參閱第 484 頁的「從日誌事件建立例外」。
- 從「**隔離所**」刪除檔案。
  請參閱第 390 頁的「使用風險日誌刪除用戶端電腦中隔離的檔案」。

表 28-11 描述您可檢視的不同類型內容，以及您可以從各個日誌進行的動作。

表 28-11 日誌類型

日誌類型	內容和動作
稽核	「稽核」日誌包含政策修改活動的資訊。 提供的資訊包括事件時間和類型、修改的政策、相關網域、網站和使用者名稱，以及敘述。 此日誌沒有任何關聯的動作。
應用程式與裝置控制	應用程式控制日誌和裝置控制日誌包含有關某類行為遭攔截的事件資訊。 下列應用程式與裝置控制日誌可供使用： ■ 應用程式控制，包含「竄改防護」資訊 ■ 裝置控制 提供的資訊包括事件發生的時間、採取的動作，以及相關的網域和電腦。此外，還包括相關的使用者、嚴重性、相關的規則、呼叫者程序以及目標。 您可以透過應用程式控制日誌建立應用程式控制或竄改防護例外。 請參閱第 479 頁的「指定 Symantec Endpoint Protection 如何在 Windows 用戶端上處理受監控的應用程式」。
合規性	合規性日誌包含用戶端「主機完整性」的相關資訊。 這些日誌沒有任何關聯的動作。

日誌類型	內容和動作
電腦狀態	「電腦狀態」日誌包括網路用戶端電腦的即時作業狀態資訊。 提供的資訊包括電腦名稱、IP 位址、受感染狀態、防護技術、自動防護狀態、版本和定義檔日期。此外，也包括使用者、上次登入時間、政策、群組、網域，以及需要重新啟動狀態。 您可以從此日誌清除受感染電腦狀態。 **附註：**此日誌包含同時從 Windows 用戶端和 Mac 用戶端收集的資訊。
欺敵	欺敵日誌包含有關用戶端將其作為欺敵活動結果傳送回 Symantec Endpoint Protection Manager 的任何活動的資訊。 欺敵是一組工具，用來向潛在的攻擊者顯示似乎為所需資料和攻擊媒介的項目。您可以使用這些工具來快速地偵測並停止滲透嘗試。欺敵工具和說明檔位於安裝檔案的 `/Tools/Deception` 資料夾中。
防網路和主機刺探利用	防網路和主機刺探利用日誌包含入侵預防、防火牆與記憶體攻擊緩和的相關資訊。 這些日誌包含有關防火牆和入侵預防所受之攻擊的資訊。提供的資訊包括服務阻斷攻擊、通訊埠掃描，以及針對執行檔進行的變更。其中還包含有關通過防火牆的連線 (流量) 以及通過的資料封包的資訊。這些日誌也包含針對電腦進行的某些作業變更，例如偵測網路應用程式，以及架構軟體。
SONAR	SONAR 日誌包含 SONAR 威脅掃描期間所偵測到的威脅相關資訊。這些是即時掃描，可以偵測在您的用戶端電腦上執行的潛在惡意應用程式。 資訊包括發生時間、事件實際動作、使用者名稱、網域、應用程式、應用程式類型、檔案和路徑等項目。 請參閱第 424 頁的「關於 SONAR」。
風險	「風險日誌」包含風險事件的資訊。其中提供的資訊包括事件時間、事件實際動作、使用者名稱、電腦和網域、風險名稱和來源、計數，以及檔案和路徑。
掃描	掃描日誌包含來自 Windows 用戶端和 Mac 用戶端的病毒和間諜軟體掃描活動相關資訊。 日誌提供的資訊包括開始掃描、電腦、IP 位址、狀態、持續時間、偵測、掃描、省略以及網域等項目。 這些日誌沒有任何關聯的動作。
系統	系統日誌包含事件的相關資訊，例如服務何時啟動和停止。 這些日誌沒有任何關聯的動作。

使用過濾儲存和刪除自訂日誌

您可以使用**「基本設定」**和**「其他設定」**架構自訂過濾，來變更所要查看的資訊。您可以將自己的過濾設定儲存到資料庫，以便日後再次產生相同的檢視。儲存設定時，設定會儲存到資料庫中。您提供給過濾的名稱會顯示在適用於該類型之日誌和報告的**「使用儲存的過濾」**清單方塊中。

附註：如果您選取**「過去 24 小時」**作為報告過濾的時間範圍，則 24 小時的時間範圍會從您首次選取過濾時開始算起。如果您重新整理頁面，並不會重設 24 小時範圍的開始時間。如果您選取過濾，然後等待檢視日誌，那麼時間範圍會從您選取過濾時開始算起。而不是從您檢視日誌時開始算起。

如果您要確定過去24小時時間範圍是從現在起算，請選取不同的時間範圍，然後重新選取**「過去 24 小時」**。

使用過濾儲存自訂日誌

1. 在主視窗中，按下**「監視器」**。
2. 在**「日誌」**標籤的**「日誌類型」**清單方塊中，選取您要架構過濾的日誌檢視類型。
3. 對於某些類型的日誌，會顯示**「日誌內容」**清單方塊。如果顯示此方塊，請選取要架構過濾的日誌內容。
4. 在**「使用儲存的過濾」**清單方塊中，選取您要作為開始的過濾。例如，選取預設過濾。
5. 在**「您要使用什麼過濾設定」**下方，按下**「其他設定」**。
6. 變更任何設定。
7. 按下**「儲存過濾」**。
8. 在顯示對話方塊的**「過濾名稱」**方塊中，輸入要用於此日誌過濾架構的名稱。當儲存的過濾新增至過濾清單時，只會顯示該名稱的前 32 個字元。
9. 按下**「確定」**，新的過濾名稱便會新增至**「使用儲存的過濾」**清單方塊中。
10. 當出現確認對話方塊時，按下**「確定」**。

刪除儲存的過濾

1. 在**「使用儲存的過濾」**清單方塊中，選取您要刪除的日誌過濾名稱。
2. 在**「使用儲存的過濾」**清單方塊旁，按下**「刪除」**圖示。
3. 當提示您確認要刪除過濾時，按下**「是」**。

檢視其他網站的日誌

如果您想要檢視其他網站的日誌，您必須從 Symantec Endpoint Protection Manager 主控台登入遠端據點的伺服器。如果您擁有遠端據點伺服器的帳戶，您可以執行遠端登入並檢視該網站的日誌。

如果您已架構遠端複製夥伴，您可以選擇將所有日誌從遠端複製夥伴複製到本機夥伴，反之亦然。如果您選擇遠端複製日誌，依據預設當您檢視任何日誌時，您會同時看見您網站與遠端複製網站的資訊。如果您想要看見單一網站，您必須過濾資料，將其限制在您想要檢視的位置。如果您選擇遠端複製日誌，請確定您有充足的磁碟空間可以儲存其他所有遠端複製夥伴的日誌。

請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。

檢視其他網站的日誌

1. 開啟網頁瀏覽器。
2. 在位址文字方塊中輸入以下內容，如下所示：

   http://*SEPMServer*:9090

   其中 *SEPMServer* 是伺服器名稱或 IP 位址。

   IP 位址可以是 IPv4 或 IPv6。必須用方括弧括住 IPv6 位址：**http://[*SEPMServer*]:9090**

   主控台開始下載。您登入的電腦必須已安裝 Java Runtime Environment (JRE)。如果沒有，您會收到下載和安裝提示。遵照提示安裝 JRE。
3. 在主控台登入對話方塊中，輸入您的使用者名稱和密碼。
4. 如果**「伺服器」**文字方塊沒有自動填寫，如下所示，在其中輸入伺服器名稱或 IP 位址和通訊埠編號 8443：

   http://*SEPMServer*:8443
5. 按下**「登入」**。

29

管理通知

本章包含以下主題：

管理通知

通知可警示管理員及電腦使用者潛在的安全問題。

當您在架構一些通報類型時，會包括預設值。這些指導方針會根據您環境的大小提供合理的設定值，但您還可能需要另行調整。必須經過測試和錯誤才能讓您在過多與過少通報之間找出最適合您環境的平衡點。將臨界值設為初始限值，然後試行幾天。幾天之後，您可以調整通知設定。

以病毒、安全風險和防火牆事件偵測為例，假設您網路中的電腦數目少於 100 台。此網路的合理設定方式是架構一個可在一分鐘內偵測兩個風險事件的通報。如果您有 100 到 1000 台電腦，合理的設定方式是在一分鐘內偵測五個風險事件。

您可以在「**監視器**」頁面中管理通知。您可以使用「**首頁**」頁面決定需要注意、但未認可的通知數量。

表 29-1 列出管理通知可執行的工作。

表 29-1 通知管理

工作	敘述
瞭解通知	瞭解通知的運作方式。 請參閱第 570 頁的「通知的運作方式」。
確認電子郵件伺服器已架構為啟用電子郵件通知	若要以電子郵件傳送通知，需要正確架構 Symantec Endpoint Protection Manager 和電子郵件伺服器。 請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。
檢閱預先架構的通知	檢閱 Symantec Endpoint Protection 提供的預先架構的通知。 請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。
檢視未認可的通知	檢視及回應未認可的通知。 請參閱第 575 頁的「檢視和認可通知」。
架構新通知	您可以選擇建立通知，以提醒您及其他管理員相關的重要問題。 請參閱第 577 頁的「設定管理員通知」。 請參閱第 236 頁的「關於開啟遠端用戶端的通知」。
建立通知過濾	您可以選擇建立過濾，以擴大或限制所有已觸發通知的檢視範圍。 請參閱第 576 頁的「儲存和刪除管理通知過濾器」。

通知的運作方式

通知針對潛在的安全性問題，向管理員和使用者發出警示。例如，通知可以針對過期授權或病毒感染，向管理員發出警示。

事件可觸發通知。出現新的安全風險、用戶端電腦發生硬體變更，或是試用授權過期，都有可能觸發通知。觸發通知後，系統可能會採取相應動作。動作可以將通知記錄在日誌中，也可以執行批次檔或可執行檔，亦或傳送電子郵件。

附註：使用電子郵件通知必須正確架構 Symantec Endpoint Protection Manager 與電子郵件伺服器之間的通訊。

您可以設定通知的節流器期間。節流器期間指定必須經過多久時間，才能檢查通知條件中的新資料。如果通知條件有節流器期間，僅在期間內首次出現觸發條件時才會發出通知。例如，假設發生大規模病毒攻擊，而您有架構好的通知條件，在病毒感染了網路中的五台電腦時即會傳送電子郵件。如果將該通知條件的節流器期間設定為 1 小時，伺服器在攻擊過程中每小時只會傳送一封通知電子郵件。

附註：如果您針對重要事件的相關通知，將**「調節器期間」**設定為**「無」**，則應該確保用戶端可以立即上傳重要事件。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。

請參閱第 569 頁的「管理通知」。

請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。

請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。

請參閱第 577 頁的「設定管理員通知」。

請參閱第 575 頁的「檢視和認可通知」。

有哪些類型的通知，何時傳送它們？

Symantec Endpoint Protection Manager 提供了針對管理員的通知。您可以自訂其中大部分通知，以符合您的特定需求。例如，您可以新增篩選器，將觸發條件僅限定為特定伺服器。或者，您也可以設定通知在觸發時採取特定動作。

根據預設，安裝 Symantec Endpoint Protection Manager 時會啟用其中的部分通知。預設啟用的通知架構為記錄到伺服器，並傳送電子郵件給系統管理員。

請參閱第 569 頁的「管理通知」。

請參閱第 578 頁的「從其他版本升級會如何影響通知條件」。

表 29-2　　預先架構的通知

通知	敘述
驗證失敗	在定義的時段中可架構的登入失敗次數會觸發驗證失敗通知。您可以設定觸發通知必須發生的登入失敗次數及時段。
已變更用戶端清單	現有用戶端清單有所變更時，將觸發此通知。預設會啟用此通知條件。 用戶端清單變更可包括： ■ 新增用戶端 ■ 變更用戶端名稱 ■ 刪除用戶端 ■ 變更用戶端的硬體 ■ 變更用戶端的非受管偵測程式狀態 ■ 用戶端模式變更

通知	敘述
用戶端安全性警示	在發生下列任一安全性事件時，即觸發此通知： ■ 遵從事件 ■ 防網路和主機侵入事件 ■ 流量事件 ■ 封包事件 ■ 裝置控制事件 ■ 應用程式控制事件 您可以修改此通知以指定判斷這些通知何時觸發的事件類型、嚴重性和頻率。 其中的某些發生類型會要求您同時在關聯的政策中啟用記錄。 **附註：**如果您將通知調節器期間設定為**「無」**，則應確定用戶端可以立即上傳重大事件。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。
欺詐偵測	當攻擊者嘗試接觸或修改欺詐時，欺詐工具會記錄事件。會在以下情況下觸發通知： ■ 攻擊者通過用戶端的防禦。 ■ 攻擊者擷取用戶端電腦的相關資訊。 ■ 攻擊者嘗試在企業網路內以其他攻擊形式使用用戶端電腦。
下載防護內容過時	警示管理員有關過時的下載防護內容。您可以指定觸發通知的定義檔期限。
檔案信譽查詢警示	將檔案提交至賽門鐵克進行信譽檢查時警示管理員。SONAR和下載鑑識使用檔案信譽查詢並自動將檔案提交至賽門鐵克。 **「檔案信譽偵測」**通知預設為啟用。
偵測到強制性應用程式	當偵測到商用應用程式清單上的應用程式或偵測到管理員所監控應用程式清單上的應用程式時，會觸發此通知。
IPS 特徵過時	警示管理員有關過時的 IPS 特徵。您可以指定觸發通知的定義檔期限。

通知	敘述
授權問題	**已付費授權到期** 此通知會警示管理員和合作夥伴 (選擇性) 已付費授權到期或即將到期。 預設會啟用此通知。 **過度部署** 此通知會警示管理員和合作夥伴 (選擇性) 有關過度部署的已付費授權。 預設會啟用此通知。 **試用授權到期** 此通知警示管理員已過期的試用授權和60、30和7天內將到期的試用授權。 根據預設，如果有試用授權，則會啟用此通知。根據預設，如果您的授權應進行升級或已付款，則不會啟用此通知。
記憶體攻擊緩和偵測	當偵測到 Windows 漏洞攻擊時，會觸發此通知。
網路負載警示：病毒和間諜軟體完整定義檔的要求	在要求完整定義檔集的用戶端過多以及存在潛在網路頻寬問題時，警示管理員。 預設會啟用此通知。
新發現的應用程式	應用程式探索偵測到新的應用程式時，會觸發此通知。
偵測到新風險	每當病毒和間諜軟體掃描偵測到新風險時就會觸發此通知。 **附註：**如果您將通知調節器期間設定為**「無」**，則應確定用戶端可以立即上傳重大事件。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。
新軟體套件	當下載新軟體套件或發生下列情況時，會觸發此通知: ■ LiveUpdate下載用戶端套件。 ■ 管理伺服器已升級。 ■ 主控台手動匯入用戶端套件。 ■ LiveUpdate 具有新的安全性定義檔或引擎內容。 您可以指定是僅根據新的安全性定義檔，還是僅根據新的用戶端套件，或是同時根據兩者觸發通知。 預設會啟用此通知。
新使用者允許的下載	當用戶端電腦允許「下載鑑識」所偵測到的應用程式時，會觸發此通知。管理員可以使用此資訊，協助評估應攔截還是允許應用程式。

通知	敘述
建議使用 Power Eraser	定期掃描無法修復感染時警示管理員，以便管理員可使用 Power Eraser。 預設會啟用此通知。
風險爆發	此通知會警示管理員有關安全風險的爆發。您可以設定新風險的發生次數和類型，以及這些新風險必須發生在什麼時段才會觸發此通知。發生類型包括發生於任何電腦、發生於一台電腦或發生於多台電腦。 預設會啟用此通知條件。 **附註：**如果您將通知調節器期間設定為**「無」**，則應確定用戶端可以立即上傳重大事件。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。
伺服器健康狀態	伺服器健康狀態問題會觸發此通知。此通知會列出伺服器名稱、健康狀態、原因以及最後一次的上線或離線狀態。 預設會啟用此通知。
單一風險事件	在偵測到單一風險事件時會觸發此通知，並且提供關於風險的詳細資訊。詳細資料包括涉及的使用者和電腦，以及管理伺服器所採取的動作。 **附註：**如果您將通知調節器期間設定為**「無」**，則應確定用戶端可以立即上傳重大事件。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。
SONAR 定義檔過時	警示管理員有關過時的 SONAR 定義檔。您可以指定觸發通知的定義檔期限。
系統事件	當發生特定系統事件時，會觸發此通知，且通知中會提供偵測到的此類事件數目。系統事件包括管理伺服器活動、複寫失敗、備份和系統錯誤。
非受管電腦	當管理伺服器在網路上偵測到非受管電腦時，會觸發此通知。此通知提供有關各非受管電腦的 IP 位址、MAC 位址和作業系統等詳細資料。
升級授權到期	升級授權授予從舊版的 Symantec Endpoint Protection Manager 升級到目前版本。 當此升級授權即將到期時，會觸發此通知。 此通知僅會在升級後出現。
病毒定義檔過時	警示管理員有關過時的病毒定義檔。您可以指定觸發通知的定義檔期限。 預設會啟用此通知。

關於合作夥伴通知

當管理伺服器偵測到用戶端的已付費授權即將到期或已到期時，它會傳送通知給系統管理員。同樣地，管理伺服器可以在偵測到授權過度部署時，也傳送通知給管理員。

但是，在上述兩種情況中，若要解決問題，都需要購買新授權或續購。在許多安裝中，伺服器管理員可能沒有進行此類購買的權限，而仰賴賽門鐵克合作夥伴執行此工作。

管理伺服器提供維護合作夥伴的聯絡人資訊的功能。此資訊可在安裝伺服器時提供。在主控台的「授權」窗格中進行安裝後，系統管理員還可以隨時提供或編輯合作夥伴資訊。

提供合作夥伴聯絡人資訊給管理伺服器時，與已付費授權相關的通知和過度部署授權通知都會自動傳送給管理員和合作夥伴。

請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。

建立管理伺服器與電子郵件伺服器之間的通訊

要讓管理伺服器傳送自動電子郵件通知，您必須架構管理伺服器與電子郵件伺服器之間的連線。

請參閱第 569 頁的「管理通知」。

建立管理伺服器與電子郵件伺服器之間的通訊

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下，選取您要與電子郵件伺服器建立連線的管理伺服器。
3. 在**「工作」**下方，按下**「編輯伺服器屬性」**。
4. 在**「伺服器屬性」**對話方塊中，按下**「電子郵件伺服器」**標籤。
5. 輸入電子郵件伺服器設定。

   若需設定這個對話方塊選項的詳細資料，請按下**「說明」**。
6. 按下**「確定」**。

請參閱在 Endpoint Protection Manager Console 中傳送測試電子郵件訊息失敗。

檢視和認可通知

您可以檢視未認可的通知或所有通知，可以認可未認可的通知，可以檢視目前在主控台中架構的所有通知條件。

「首頁」頁面上的**「安全狀態」**窗格會指出過去 24 小時內發生的未認可通知數。

請參閱第 569 頁的「管理通知」。

檢視最近未認可的通知

1 在主控台中，按下**「首頁」**。

2 在**「首頁」**頁面的**「安全狀態」**窗格中，按下**「檢視通報」**。

此時**「通知」**標籤下會顯示最近未認可的通知清單。

3 (可選) 在通知清單的**「報告」**欄中，按下文件圖示 (如果有)。

通報報告將出現於不同的瀏覽器視窗內。如果沒有文件圖示，則會在通知清單的**「訊息」**欄中顯示所有通知資訊。

檢視所有通知

1 在主控台中，按下**「監視器」**，然後按下**「通知」**標籤。

2 (可選) 在**「通知」**標籤的**「使用儲存的過濾」**功能表中，選取儲存的過濾。

請參閱第 576 頁的「儲存和刪除管理通知過濾器」。

3 (可選) 在**「通知」**標籤的**「時間範圍」**功能表中，選取一個時間範圍。

4 在**「通報」**標籤上，按下**「檢視通報」**。

認可通知

1 檢視通知。

請參閱第 576 頁的「檢視最近未認可的通知」。

請參閱第 576 頁的「檢視所有通知」。

2 在**「通知」**標籤的通知清單中，按下**「認可」**欄中的紅色圖示以確認通知。

檢視所有已架構的通知條件

1 在主控台中，按下**「監視器」**。

2 在**「監視器」**頁面的**「通知」**標籤上，按**「通知條件」**。

此時將顯示在主控台中架構的所有通知條件。您可以利用選取**「顯示通知類型」**功能表內的通知類型來過濾清單。

儲存和刪除管理通知過濾器

您可以使用過濾器在主控台中擴大或限制管理通知的檢視範圍。您可以儲存新過濾器，也可以刪除以前儲存的過濾器。

請參閱第 575 頁的「檢視和認可通知」。

請參閱第 569 頁的「管理通知」。

您可以建立使用下列任意條件組合的已儲存過濾器：

- **時間範圍**

- **認可狀態**
- **通知類型**
- **建立者**
- **通知名稱**

例如，您可以建立一個過濾器，以便僅顯示過去 24 小時內發佈的未認可風險爆發通知。

新增通知過濾器

1 在主控台中，按下**「監視器」**。

2 在**「監視器」**頁面上的**「通知」**標籤中，按下**「其他設定」**。

3 在**「您要使用什麼過濾設定？」**標題下，為過濾器設定條件。

4 按下**「儲存過濾」**。

5 在**「通知」**標籤的**「過濾器名稱」**方塊中，鍵入過濾器名稱，然後按下**「確定」**。

刪除儲存的通知過濾器

1 在主控台中，按下**「監視器」**。

2 在**「監視器」**頁面上的**「通知」**標籤中，在**「使用儲存的過濾」**功能表上選擇過濾器。

3 在**「使用儲存的過濾」**功能表的右側，按下 **X** 圖示。

4 在**「刪除過濾」**對話方塊中，按下**「是」**。

設定管理員通知

您可以架構通知，以便在發生特定種類的事件時，向您和其他管理員發出警示。您還可以新增觸發通知的條件，以提醒您執行重要工作。例如，您可以新增通知條件，在授權到期或偵測到安全風險時通知您。

觸發通知後，可以執行特定動作，例如：

- 將通知記錄到資料庫。
- 傳送電子郵件給一個或多個人員。
- 執行批次檔案。

附註：若要傳送電子郵件通知，您必須將郵件伺服器架構為與管理伺服器通訊。

請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。

您可以從可用通知類型清單中選擇通知條件。

選擇通知類型後，如下所述進行架構：

- 指定過濾器。
  並非所有通知類型都提供過濾器。如有提供，便可以使用過濾器來限制觸發通知的條件。例如，您可以將通知限制為僅在影響特定群組中的電腦時觸發。
- 指定設定。
  所有通知類型都提供設定，但具體設置因類型而異。例如，風險通知可能會讓您指定觸發通知的掃描類型。
- 指定動作。
  所有通知類型都提供可指定的動作。

附註：如果您針對重要事件的相關通知，將**「調節器期間」**設定為**「無」**，則應該確保用戶端可以立即上載重要事件。相關通知包括：**「用戶端安全性警示」**、**「單一風險事件」**、**「偵測到新風險」**與**「風險爆發」**。**「讓用戶端立即上傳重大事件」**選項預設為啟用，並且是在**「通訊設定」**對話方塊中進行架構。

設定管理員通知

1 在主控台中，按下**「監視器」**。

2 在**「監視器」**頁面的**「通知」**標籤上，按**「通知條件」**。

3 在**「通知」**標籤上，按下**「新增」**，然後按下通知類型。

4 在**「新增通知條件」**對話方塊中，提供下列資訊：
   - 在**「通知名稱」**文字方塊中，鍵入用於標示通知條件的名稱。
   - 在**「您要使用何種過濾設定?」** (如果有) 下，指定通知條件的過濾設定。
   - 在**「您要此通知使用哪些設定?」**下，指定觸發通知的條件。
   - 在**「觸發此通知時應該採取什麼動作?」**下，指定觸發通知時應採取的動作。

5 按下**「確定」**。

請參閱第 569 頁的「管理通知」。

請參閱第 575 頁的「檢視和認可通知」。

從其他版本升級會如何影響通知條件

在新伺服器上安裝 Symantec Endpoint Protection 時，預設會啟用許多預先架構的通知條件。但是，從舊版升級 Symantec Endpoint Protection 將會影響預設啟用的通知條件，還會影響其預設設定。

根據預設，會在新安裝 Symantec Endpoint Protection 時啟用下列通知條件：

- **已變更用戶端清單**
- **新用戶端軟體**

- **過度部署問題**
- **已付費授權問題**
- **風險爆發**
- **伺服器健康狀態**
- **試用軟體授權到期**
- **病毒定義檔過時**

當管理員從舊版升級軟體時，將保留舊版中的所有現有通知條件。但是，現有的**「新軟體套件」**通知條件將變為**「新用戶端軟體」**通知條件。**「新用戶端軟體」**條件具有**「新軟體套件」**條件所沒有的兩個設定：**「用戶端套件」**和**「安全性定義檔」**。升級軟體時，將針對在升級後保留的此類型通知條件啟用上述兩種設定。但是，**「新用戶端軟體」**通知是在升級後建立的條件，根據預設，此通知會啟用**「用戶端套件」**設定，並停用**「安全性定義檔」**設定。

附註：啟用**「新用戶端軟體」**通知條件中的**「安全性定義檔」**設定後，可能會導致傳送大量通知。當存在多個用戶端或存在經常排程的安全定義檔更新時，可能會發生此種情況。如果您不希望接收有關安全定義檔更新的頻繁通知，則可以編輯此通知條件以停用**「安全性定義檔」**設定

數個通知條件可能具有舊版所沒有的新設定，即：**「傳送電子郵件給系統管理員」**。如果對於某個通知條件而言，此設定是新設定，則根據預設，會在升級後對此類型的任何現有條件停用此設定。

如果未在早期安裝中新增預設通知條件類型，則會在升級安裝中新增此通知條件。但是，升級程序無法判斷管理員在早期安裝中故意刪除的預設通知條件。因此，在升級安裝中每個預設通知條件會停用所有下列動作設定，只有一個例外：**「傳送電子郵件給系統管理員」**、**「記錄通知」**、**「執行批次檔」**和**「傳送電子郵件給」**。將上述四項動作全部停用後，將不會處理通知條件，即使條件本身存在也是如此。管理員可以編輯通知條件以啟用任何或所有上述設定。

請注意，**「新用戶端軟體」**通知條件是例外：根據預設，可以在升級過程中新增此通知條件時產生通知。與其他預設的通知條件不同的是，將針對此條件啟用**「記錄通知」**和**「傳送電子郵件給系統管理員」**動作設定。

如果軟體的舊版不支援授權，則會啟用**「升級授權到期」**通知條件。

某些通知條件類型在軟體的舊版中無法使用。根據預設，在升級軟體時，會啟用這些通知條件。

請參閱第 571 頁的「有哪些類型的通知，何時傳送它們？」。

部分 7

在虛擬環境中防護用戶端

30

Symantec Endpoint Protection 與虛擬基礎架構概觀

本章包含以下主題：

在虛擬基礎架構中使用 Symantec Endpoint Protection

Symantec Endpoint Protection 針對虛擬基礎架構提供共用智慧型掃描快取和「虛擬映像例外」功能，可讓您啟用以改善效能。您需要執行一些額外的安裝和架構工作，才能啟用這些功能。

表 30-1 虛擬基礎架構功能及其用途

功能及用途	敘述
使用共用智慧型掃描快取略過已知未受病毒感染的檔案，不進行掃描。	共用智慧型掃描快取會追蹤已知未受病毒感染的檔案。共用智慧型掃描快取可因為不需要重新掃描這些檔案，而減少掃描的負荷。 您可以設定下列類型的共用智慧型掃描快取： ■ 網路型共用智慧型掃描快取 使用任何類型虛擬基礎架構的虛擬用戶端都可以使用網路型共用智慧型掃描快取。以減少掃描的負荷。 **附註：**自 14.0 版起，不再支援啟用 vShield 的共用智慧型掃描快取。 請參閱第 582 頁的「關於共用智慧型掃描快取」。 請參閱第 584 頁的「我必須怎麼做才能使用網路型共用智慧型掃描快取」。
使用「虛擬映像例外」工具，用戶端就可以略過基礎影像檔，不進行掃描。	「虛擬映像例外」工具可讓您將基礎影像檔標記為「安全」，如此就可在掃描期間略過這些檔案，從而減少掃描的負荷。 虛擬映像例外工具僅在虛擬環境中執行。 請參閱第 583 頁的「關於虛擬映像例外工具」。
架構非持續虛擬桌面基礎架構功能。	Symantec Endpoint Protection 用戶端有一項組態設定，會指出用戶端為非持續虛擬用戶端。 您可以針對非持續虛擬桌面基礎架構中離線的 GVM 架構不同的老化期間。 Symantec Endpoint Protection Manager 會移除離線時間超過指定時間的非持續 GVM 用戶端。 請參閱第 598 頁的「在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection」。 請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

Symantec Endpoint Protection Manager 和 Symantec Endpoint Protection 中的防護技術在虛擬基礎架構與實體基礎架構中運作的方式通常相同。 您可以在虛擬基礎架構中，採用與實體基礎架構中相同的方式安裝、架構和使用 Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端。

關於共用智慧型掃描快取

使用共用智慧型掃描快取可改善虛擬基礎架構的效能。Symantec Endpoint Protection 用戶端認定未受感染的檔案會新增到快取中。使用相同病毒定義檔版本的後續掃描都可以忽略共用智慧型掃描快取中的檔案。共用智慧型掃描快取僅用於排程掃描和手動掃描。

網路型共用智慧型掃描快取會當作獨立於 Symantec Endpoint Protection 用戶端的 Web 服務執行。共用智慧型掃描快取使用一個投票系統。用戶端使用最新的內容掃描檔案並判斷該檔案未受感染之後，用戶端會傳送投票至快取。如果檔案受感染，則用戶端不會傳送投票。當檔案的投票計數大於或等於投票計數臨界值時，共用智慧型掃描快取就會將檔案視為未受感染。之

後當另一個用戶端需要掃描相同的檔案時，該用戶端會先查詢共用智慧型掃描快取。如果檔案因目前的內容而標記為未受感染，則用戶端不會掃描該檔案。

當用戶端傳送投票至共用智慧型掃描快取時，快取會檢查用戶端用來掃描檔案的內容版本。如果用戶端沒有最新的內容，則共用智慧型掃描快取會忽略此投票。如果有可用的更新內容，則更新的內容會成為已知的最新內容，且共用智慧型掃描會將投票計數重設為 1。

為了使快取大小易於管理，共用智慧型掃描快取採用了一種刪減演算法。這個演算法會先移除最舊的快取項目，也就是時間戳記最舊的項目。此演算法可確保快取大小不會超過記憶體使用量臨界值。

請參閱第 584 頁的「我必須怎麼做才能使用網路型共用智慧型掃描快取」。

請參閱第 588 頁的「自訂共用智慧型掃描快取設定」。

請參閱第 581 頁的「在虛擬基礎架構中使用 Symantec Endpoint Protection」。

關於虛擬映像例外工具

「虛擬映像例外」工具可讓用戶端略過基礎影像檔的威脅掃描。此功能可降低磁碟 I/O 和 CPU 的資源負載。

Symantec Endpoint Protection 同時對受管型用戶端和非受管用戶端支援虛擬映像例外的使用。

附註：賽門鐵克不支援在實體環境中使用虛擬映像例外工具。

請參閱第 595 頁的「在基礎影像上使用虛擬影像例外工具」。

請參閱第 581 頁的「在虛擬基礎架構中使用 Symantec Endpoint Protection」。

31

安裝和使用網路型共用智慧型掃描快取

本章包含以下主題：

我必須怎麼做才能使用網路型共用智慧型掃描快取

您可以使用網路型共用智慧型掃描快取來改善掃描效能。

表 31-1　　安裝及使用網路型共用智慧型掃描快取的工作

步驟	工作
步驟 1：安裝共用智慧型掃描快取。	請參閱第 585 頁的「實作網路型共用智慧型掃描快取的系統需求」。 請參閱第 586 頁的「安裝和移除網路型共用智慧型掃描快取」。

步驟	工作
步驟 2：在 Symantec Endpoint Protection Manager 的「病毒和間諜軟體」政策中，讓您的虛擬用戶端使用共用智慧型掃描快取。	請參閱第 587 頁的「啟用網路型共用智慧型掃描快取」。

安裝共用智慧型掃描快取之後，可以選擇性執行下列工作：

- 自訂共用智慧型掃描快取的任何服務、快取或日誌設定。
  請參閱第 588 頁的「自訂共用智慧型掃描快取設定」。
- 檢視日誌中的相關事件。
  請參閱第 591 頁的「檢視網路型共用智慧型掃描快取日誌事件」。
- 使用 Windows 效能管理員監控其效能。
  請參閱第 592 頁的「監控網路型共用智慧型掃描快取效能計數器」。

實作網路型共用智慧型掃描快取的系統需求

網路型共用智慧型掃描快取伺服器設計為在獨立式實體或虛擬機器上執行。不應將共用智慧型掃描快取安裝至執行其他資料庫應用程式或高可用性伺服器應用程式 (如 Symantec Endpoint Protection Manager 或 Microsoft SQL Server) 的電腦上。

表 31-2描述虛擬基礎架構執行共用智慧型掃描快取所需的最低系統需求。

表 31-2　網路型共用智慧型掃描快取系統需求

需求	敘述
軟體	■ Windows Server 2008 及更新版本 ■ Windows Server 2012 和 Windows Server 2012 R2 ■ Windows Server 2016 ■ Windows Server 2019 ■ .NET Framework 4
CPU	共用智慧型掃描快取必須安裝在專用伺服器或虛擬機器上。
記憶體	最小 2 GB
可用磁碟空間	最小 100 MB

請參閱第 582 頁的「關於共用智慧型掃描快取」。

請參閱第 586 頁的「安裝和移除網路型共用智慧型掃描快取」。

安裝和移除網路型共用智慧型掃描快取

在您安裝網路型共用智慧型掃描快取之前，請確定已符合所有系統需求，並且以 Windows 管理員的身分登入。可以在獨立式實體或虛擬機器上安裝並執行共用智慧型掃描快取。

附註：您不應在安裝了共用智慧型掃描快取的伺服器的主機名稱中使用 DBCS 或高 ASCII 字元。 您還應避免在用於存取的使用者名稱中使用 DBCS 或高 ASCII 字元。 這些字元會導致共用智慧型掃描快取服務無法啟動。

請參閱第 585 頁的「實作網路型共用智慧型掃描快取的系統需求」。

安裝網路型共用智慧型掃描快取

1. 在 Symantec Endpoint Protection 安裝檔案上，瀏覽到 `Tools/Virtualization/SharedInsightCache` 資料夾。
2. 連按兩下以下檔案，啟動安裝程式：

   `SharedInsightCacheInstallation.msi`

   附註：您可以改為輸入下列指令來啟動相同的安裝程式：

   `msiexec /i SharedInsightCacheInstallation.msi`

3. 在 **Shared Insight Cache Setup** 精靈窗格中，按下 **Next**。
4. 仔細閱讀賽門鐵克軟體授權許可協議，勾選 **I accept the terms of the License Agreement**，然後按下 **Next**。
5. 在 **Destination folder** 窗格中，執行下列工作之一：
   - 按下 **Next**，接受共用智慧型掃描快取的預設位置。
   - 按下 **Change**，瀏覽並選取不同的目的資料夾，按下 **OK**，然後按下 **Next**。
6. 在 **Shared Insight Cache Settings** 窗格中，指定以下共用智慧型掃描快取設定：

Cache Usage (% of Physical Memory)	快取的大小上限。 當快取超過此臨界值時，共用智慧型掃描快取會刪減快取大小。
Listening Port	伺服器用來接聽的通訊埠。
Status Listening Port	伺服器用來溝通伺服器狀態資訊的通訊埠。

7 按下「**安裝**」。

8 當安裝完成時，按下 **Finish**。

請參閱第 588 頁的「自訂共用智慧型掃描快取設定」。

移除共用智慧型掃描快取的作用與停止共用智慧型掃描快取服務的作用相同。如果不確定是否要永久移除共用智慧型掃描快取，可以改為停止服務。

請參閱第 591 頁的「關於停止和啟動網路型共用智慧型掃描快取服務」。

附註：若要移除共用智慧型掃描快取，請使用適當的 Windows 控制台，例如「新增或移除程式」。 您必須具有 Windows 管理員權限才能移除共用智慧型掃描快取。

如果您移除共用智慧型掃描快取，可能也想要停用 Symantec Endpoint Protection Manager 中的共用智慧型掃描快取。 停用共用智慧型掃描快取可避免 Windows 事件日誌在每次用戶端無法聯絡快取時收到通知。

啟用網路型共用智慧型掃描快取

若要透過網路與 Symantec Endpoint Protection 用戶端進行通訊，共用智慧型掃描快取預設不會使用驗證，也不會使用 SSL。如果您將「共用智慧型掃描快取」設定變更為使用「具有 SSL 的基本驗證」或「沒有 SSL 的基本驗證」，則必須指定可存取共用智慧型掃描快取的使用者名稱和密碼。

請參閱第 588 頁的「自訂共用智慧型掃描快取設定」。

啟用網路型共用智慧型掃描快取

1 在 Symantec Endpoint Protection Manager 主控台中，開啟適當的「病毒和間諜軟體防護」政策，然後按下「**其他**」。

2 在「**共用智慧型掃描快取**」標籤中，勾選「**使用網路共用智慧型掃描快取**」。

3 如果在組態檔中啟用了 SSL 驗證，則按下「**需要 SSL**」。

4 在「**主機名稱**」方塊中，輸入您安裝共用智慧型掃描快取所在主機的主機名稱。

5 在「**通訊埠**」方塊中，輸入共用智慧型掃描快取的通訊埠號。

6 (選擇性) 如果您架構了共用智慧型掃描快取驗證：

- 在「**使用者名稱**」方塊中，鍵入使用者名稱。
- (選擇性) 按下「**變更密碼**」將預設密碼 (null) 變更為您為驗證建立的密碼。如果不想使用密碼，請將這些欄位保留空白。

7 按下「**確定**」。

請參閱第 584 頁的「我必須怎麼做才能使用網路型共用智慧型掃描快取」。

自訂共用智慧型掃描快取設定

安裝共用智慧型掃描快取之後，您可以在組態檔中自訂其設定。

架構檔是遵循 .NET Framework 應用程式架構標準的 XML 檔案。如果有無效的架構 (例如有無效的 XML、錯誤的值類型或漏填了必填值)，則共用智慧型掃描快取不會啟動。

如需詳細資訊，請參閱：

組態編輯器工具 (SvcConfigEditor.exe)

表 31-3 描述您可以架構的選項。

表 31-3 共用智慧型掃描快取架構選項

選項和預設值	說明和註解
快取服務接聽通訊埠 預設值為 9005。	服務接聽的通訊埠。用戶端會使用接聽埠傳送檔案的掃描結果，以及提出要求來判斷用戶端是否應掃描檔案。 如果通訊埠的範圍不在 0 到 65535 之間，則服務不會啟動。 如果服務無法接聽指定的通訊埠，則它不會啟動。 `<endpoint address="http://localhost:9005/1"` 依據預設，共用智慧型掃描快取伺服器會接聽所有 IP 位址。若要為 HTTP 或 HTTPS 服務架構接聽 IP 位址，您必須使用 Netsh.exe。共用智慧型掃描快取伺服器會接聽您在這些工具所修改的「IP 接聽清單」中指定的 IP 位址。 Netsh.exe 包含在 Windows Server 2008 中。 如需詳細資訊，請參閱： 設定 HTTP 和 HTTPS
狀態服務接聽通訊埠 預設值為 9006。	伺服器用來溝通伺服器狀態資訊的通訊埠。狀態接聽埠在架構區段中指定的通訊埠上使用以 SOAP 為基礎的介面。此介面提供管理員據以查詢快取伺服器資訊和狀態的機制。 如果這個範圍不在 0 - 65535 之間，則服務不會啟動。 如果服務無法接聽指定的通訊埠，則它不會啟動。
投票計數 預設值為 1。	在共用智慧型掃描快取使用結果之前，必須驗證檔案是否未感染病毒的用戶端數目。 這個值必須小於或等於 15。如果大於 15，則伺服器將使用預設值。 `<cache.configuration vote.count="1" />`

選項和預設值	說明和註解
刪減大小 預設值為 10。	當快取達到記憶體使用量限制時，要從快取移除的記憶體使用量百分比。 這個值必須介於 10 和 100 之間。 如果這個值不在 10 和 100 之間，則伺服器將使用預設值。 **附註：**賽門鐵克建議您保留預設的刪減大小。 `<prune.size="10" />`
記憶體使用量 預設值為 50。	在共用智慧型掃描快取開始刪減快取前，快取大小的百分比。 必須大於或等於 10。 `<mem.usage="50" />`
日誌檔 預設值是 *install_folder*/CacheServer.log	共用智慧型掃描快取日誌的檔案。 `<filevalue="CacheServer.log" />`
日誌等級 預設值為 ERROR。	ALL DEBUG INFO WARN ERROR FATAL OFF 值 OFF 表示共用智慧型掃描快取不記錄任何訊息。 `<level value="ERROR" />` 請參閱第 591 頁的「檢視網路型共用智慧型掃描快取日誌事件」。
日誌大小 預設值為 10000。	日誌的大小 (位元組)，超過這個大小之後，共用智慧型掃描快取會轉增日誌。 `<maximumFileSizevalue="10000" />`
日誌備份 預設值為 1。	刪除最舊的日誌之前要保留的轉增日誌數目。 值 0 表示共用智慧型掃描快取不保留任何備份。負值表示共用智慧型掃描快取保留的備份數不受限制。 `<maxSizeRollBackupsvalue="1" />`

選項和預設值	說明和註解

啟用 SSL
啟用驗證
	依據預設，共用智慧型掃描快取設定為不進行任何驗證，也沒有 SSL。您可以將它變更為「具有 SSL 的基本驗證」、「沒有 SSL 的驗證」，或「沒有 SSL 的基本驗證」。
	
	`<webHttpBinding>`
	`<bindingname="CacheServerBinding">`
	`<!--`
	`Uncomment the appropriate section to get`
	`the desired security.`
	
	`If enabling ssl modify the uri to use https.`
	`A cert will also have to be installed and`
	`registered for the ip/port.`
	`-->`
	`<!-- Basic authentication with SSL.-->`
	`<security mode="Transport">`
	`<transport clientCredentialType="Basic"/>`
	`</security-->`
	`<!-- No authentication with SSL.-->`
	`<security mode="Transport">`
	`<transport clientCredentialType="None"/>`
	`</security-->`
	`<!-- Basic authentication with no SSL.-->`
	`<security mode="TransportCredentialOnly">`
	`<transport clientCredentialType="Basic"/>`
	`</security-->`
	`<!-- No authentication with no SSL. DEFAULT -->`
	`<securitymode="None">`
	`<transportclientCredentialType="Basic"/>`
	`</security>`
	`</binding>`
	`</webHttpBinding>`
	
	請參閱第 587 頁的「啟用網路型共用智慧型掃描快取」。

自訂共用智慧型掃描快取設定

1 瀏覽到以下檔案並將其開啟：

```
C:\Program Files (x86)\Symantec\Shared Insight
Cache\SharedInsightCacheInstallation.exe.config
```

2 視需要進行修改。

3 儲存變更並關閉檔案。

4 重新啟動共用智慧型掃描快取服務。

您必須重新啟動共用智慧型掃描快取服務，日誌等級以外的所有架構設定才會生效。

請參閱第 591 頁的「關於停止和啟動網路型共用智慧型掃描快取服務」。

請參閱第 584 頁的「我必須怎麼做才能使用網路型共用智慧型掃描快取」。

關於停止和啟動網路型共用智慧型掃描快取服務

您可能需要暫時停止共用智慧型掃描快取服務才能排除問題。解決問題後，您可以重新啟動該服務。您可以從「服務控制管理員」啟動和停止服務。

移除共用智慧型掃描快取的作用與停止共用智慧型掃描快取服務的作用相同。如果不確定是否要永久移除共用智慧型掃描快取，可以改為停止服務。

您必須具有 Windows 管理員權限才能停止和啟動共用智慧型掃描快取服務。

請參閱第 593 頁的「排除共用智慧型掃描快取問題 」。

檢視網路型共用智慧型掃描快取日誌事件

您可以檢視共用智慧型掃描快取日誌檔，查看共用智慧型掃描快取建立的任何事件。日誌檔位於安裝資料夾中，名為 `CacheServer.log`。

共用智慧型掃描快取採用下列格式列印日誌：

```
[|] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

例如：

```
[|] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

修改組態檔可指定要用於網路型共用智慧型掃描快取的日誌等級。

表 31-4描述您可以設定的等級。

表 31-4 網路型共用智慧型掃描快取日誌等級

日誌等級	敘述
OFF	OFF 表示不記錄任何事件。
FATAL	FATAL 訊息會要求您採取動作。這些訊息是一些會導致共用智慧型掃描快取停止的錯誤。 例如，某個 FATAL 訊息可能表示伺服器 IP 位址無法使用，這意味著共用智慧型掃描快取無法執行。

日誌等級	敘述
ERROR	ERROR 訊息會要求您採取動作，但相應程序會繼續執行。它們是導致共用智慧型掃描快取發生故障或無法工作的系統錯誤。 您也會接收到 FATAL 訊息的所有日誌項目。 此層級是預設的日誌記錄層級。
WARN	WARN 訊息會指出可能不必要、但不會導致共用智慧型掃描快取失敗的共用智慧型掃描快取行為。 您也會收到 FATAL 訊息和 ERROR 訊息的所有日誌項目。
INFO	INFO 訊息描述共用智慧型掃描快取的一般動作或提供其相關資訊。它們可能指出系統狀態，並有助於驗證行為或追蹤問題。不過，單獨使用時，其目的不在呈報可行動項目。 例如，某個資訊訊息可能指出快取刪減已完成。該訊息不提供問題的詳細資料。它只記錄行為。 您也會收到 FATAL 訊息、ERROR 訊息及 WARN 訊息的所有日誌項目。
DEBUG ALL	DEBUG 和 ALL 日誌層級訊息產生相同的結果。這些日誌等級僅供支援人員排除共用智慧型掃描快取問題。 您也會接收到所有其他日誌層級的所有日誌項目。

只有在需要排除共用智慧型掃描快取的問題時才升高日誌等級。如果升高日誌等級，會使日誌檔開始顯著變大。解決問題後，請恢復為預設的 ERROR 日誌等級。

檢視日誌中的共用智慧型掃描快取事件

- 移至下列位置：

  Installation folder/CacheServer.log

請參閱第 588 頁的「自訂共用智慧型掃描快取設定」。

監控網路型共用智慧型掃描快取效能計數器

您可以在 Windows 效能監視器中檢視網路型共用智慧型掃描快取統計值。共用智慧型掃描快取服務必須正在執行才能檢視其效能計數器。

表 31-5 共用智慧型掃描快取統計值

統計值	敘述
快取中的項目數	此數代表快取中目前的項目數。
快取中已投票為未感染病毒的項目數	此數代表快取中目前已投票為未感染病毒的項目數。

統計值	敘述
快取要求的數目	對共用智慧型掃描快取服務提出的快取要求數目。 此數目只包含收到 200 回應的有效要求數目。此計數器在服務重新啟動時不會繼續。
更新要求的數目	對服務提出的更新要求數目。 此數目只是收到 200 回應的有效要求。此計數器在服務重新啟動時不會繼續。

監控網路型共用智慧型掃描快取效能計數器

1 在指令提示下，輸入下列命令：

```
perfmon
```

2 在「**效能**」視窗中的圖形上按下滑鼠右鍵。

3 選取「**新增計數器**」。

4 在「**效能物件**」下拉式清單中，選取「**共用智慧型掃描快取**」。

5 選取要檢視的計數器，然後按下「**新增**」。

6 按下「**關閉**」。

此時「效能」圖形中會顯示您選取的共用智慧型掃描快取計數器。

如需使用 Windows 效能監視器的詳細資訊，請參閱 Windows 說明文件。

請參閱第 593 頁的「排除共用智慧型掃描快取問題 」。

請參閱第 584 頁的「我必須怎麼做才能使用網路型共用智慧型掃描快取」。

排除共用智慧型掃描快取問題

表 31-6提供了有關如何排除共用智慧型掃描快取問題的建議。

表 31-6 共用智慧型掃描快取疑難排解

問題	說明/解決方法
快取結果出現問題	重新啟動服務。 請參閱第 591 頁的「關於停止和啟動網路型共用智慧型掃描快取服務」。
共用智慧型掃描快取傳回「無結果」回應	共用智慧型掃描快取無法成功執行快取查詢時，會傳回「無結果」回應。如果用戶端要求快取查詢，則「無結果」表示必須對檔案進行掃描。 **附註：**即使共用智慧型掃描快取無法成功執行快取更新，也會傳回「成功」回應。原因是因為更新失敗時，用戶端不需要執行其他動作。

問題	說明/解決方法
懷疑 HTTP 流量出現問題	檢視 HTTP 流量錯誤日誌。HTTP 流量錯誤記錄在以下位置： `%Windir%\System32\Logfiles\HTTPERR`

請參閱第 591 頁的「檢視網路型共用智慧型掃描快取日誌事件」。
請參閱第 592 頁的「監控網路型共用智慧型掃描快取效能計數器」。

32

使用虛擬影像例外

本章包含以下主題：

在基礎影像上使用虛擬影像例外工具

在您建置虛擬機器之前，可以在基礎影像上使用虛擬影像例外工具。虛擬影像例外工具可讓您的用戶端略過基礎影像檔威脅掃描，這會降低磁碟 I/O 的資源負載。它還會改善虛擬桌面基礎架構中的 CPU 掃描程序效能。

Symantec Endpoint Protection 支援針對受管用戶端和非受管用戶端使用虛擬影像例外工具。

附註：您無法在非虛擬環境中使用虛擬影像例外工具。

表 32-1　在基礎影像上使用虛擬影像例外工具的程序

步驟	動作
步驟 1	在基礎影像上，對所有檔案執行完整掃描，以確保檔案是乾淨的。 如果 Symantec Endpoint Protection 用戶端隔離受感染的檔案，您必須修復或刪除隔離的檔案，從隔離所移除它們。 請參閱第 389 頁的「指定自動刪除修復、備份和隔離檔案的時間」。
步驟 2	確定用戶端的隔離所空白。 請參閱第 390 頁的「使用風險日誌刪除用戶端電腦中隔離的檔案」。

步驟	動作
步驟 3	從指令行執行虛擬影像例外工具，以標示基礎影像檔。 請參閱第 596 頁的「執行虛擬影像例外工具」。 請參閱第 727 頁的vietool。
步驟 4	在 Symantec Endpoint Protection Manager 中啟用該功能，以便在掃描執行時用戶端知道尋找並略過標示的檔案。 請參閱第 597 頁的「架構 Symantec Endpoint Protection 以略過基礎影像檔掃描」。
步驟 5	從基礎影像移除虛擬影像例外工具。

虛擬影像例外工具支援本機固定式磁碟機。它會處理符合新技術檔案系統 (NTFS) 標準的檔案。

請參閱第 596 頁的「虛擬映像例外工具的系統需求」。

虛擬映像例外工具的系統需求

系統支援虛擬映像例外工具用於 VMware ESX、Microsoft Hyper-V，以及 Citrix Zen 桌面平台。

該用戶端必須符合下列所有需求：

- 用戶端必須安裝在其中一個支援的虛擬環境中。
- 用戶端必須執行 Symantec Endpoint Protection 用戶端軟體 12.1 版或更新版本。

警告：用戶端版本必須與虛擬映像例外工具版本相同。

如需有關需求和支援的平台的最新資訊，請參閱下列網頁：

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

請參閱第 595 頁的「在基礎影像上使用虛擬影像例外工具」。

執行虛擬影像例外工具

執行虛擬影像例外工具之前，請確保已符合所有系統需求。

警告：用戶端版本必須與虛擬影像例外工具版本相同。

請參閱第 596 頁的「虛擬映像例外工具的系統需求」。

執行虛擬影像例外工具

1. 從安裝檔案的 Symantec Endpoint Protection 工具資料夾，將以下檔案下載到基礎影像：

   `/Virtualization/VirtualImageException/vietool.exe`

2. 以管理權限開啟指令提示。
3. 用正確的引數執行虛擬影像例外工具。

   例如，輸入：`vietool c: --generate`

請參閱第 727 頁的vietool。

架構 Symantec Endpoint Protection 以略過基礎影像檔掃描

您在基礎影像檔上執行虛擬影像例外工具之後，可以在 Symantec Endpoint Protection Manager 中啟用使用虛擬影像例外。啟用這個功能後，虛擬用戶端就會尋找工具所插入的屬性。然後 Symantec Endpoint Protection 會略過掃描包含該屬性的基礎影像檔。

您可以略過「自動防護」掃描或管理員定義掃描 (例如手動掃描或排程掃描) 中未變更的基礎影像檔，不進行掃描。

架構 Symantec Endpoint Protection 使用虛擬影像例外略過掃描基礎影像檔

1. 在主控台上，開啟適當的「病毒和間諜軟體防護」政策。
2. 在**「進階選項」**下，按下**「其他」**。
3. 在**「虛擬影像」**標籤上，勾選要啟用的選項。
4. 按下**「確定」**。

請參閱第 595 頁的「在基礎影像上使用虛擬影像例外工具」。

33

暫時性虛擬桌面基礎架構

本章包含以下主題：

- 在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection
- 針對 VDI 中的非持續訪客虛擬機器設定基礎影像
- 如何針對非持續 VDI 用戶端管理授權計數
- 清除過時的非持續 VDI 用戶端以釋放授權

在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection

表 33-1 在非持續虛擬桌面基礎架構中若要使用 Symantec Endpoint Protection 需執行的工作

步驟	敘述
步驟 1：設定基礎影像。	您可以在基礎影像中架構 Symantec Endpoint Protection 用戶端，以指出其為非持續虛擬用戶端。 請參閱第 599 頁的「針對 VDI 中的非持續訪客虛擬機器設定基礎影像」。
步驟 2：在 Symantec Endpoint Protection Manager 中，架構離線非持續 VDI 用戶端的獨立清除間隔。	Symantec Endpoint Protection Manager 會移除離線超過指定時間的非持續 GVM 用戶端。這項功能可以簡化管理 Symantec Endpoint Protection Manager 中的 GVM。 請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

針對 VDI 中的非持續訪客虛擬機器設定基礎影像

您可以設定基礎影像，以便更簡化使用 Symantec Endpoint Protection Manager 在非持續虛擬桌面基礎架構中管理 GVM 的方式。

表 33-2 針對非持續 GVM 設定基礎影像的工作

步驟	敘述
步驟 1：將 Symantec Endpoint Protection 安裝在基礎影像上。	請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。
步驟 2：在管理伺服器中停用「竄改防護」，以便可以修改登錄。	請參閱第 430 頁的「變更竄改防護設定」。
步驟 3：確保 Symantec Endpoint Protection Manager 會正確計算非持續虛擬用戶端的授權數目。	非持續用戶端的優點在於離線非持續用戶端不會計入已部署授權的數量。只有線上用戶端會計入。若將虛擬用戶端標示為非持續用戶端，您必須在基礎影像中建立登錄機碼。 請參閱第 599 頁的「如何針對非持續 VDI 用戶端管理授權計數」。
步驟 4：在 Symantec Endpoint Protection Manager 中，重新啟用「竄改防護」。	請參閱第 430 頁的「變更竄改防護設定」。

設定完基礎影像之後，可以在 Symantec Endpoint Protection Manager 中針對非持續用戶端架構獨立的清除間隔。

請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

如何針對非持續 VDI 用戶端管理授權計數

管理伺服器會針對實體電腦 (無論電腦是處於線上還是離線狀態) 上的用戶端計算每個授權。如果是虛擬用戶端，管理伺服器僅計算線上非持續用戶端的授權。不計算離線非持續用戶端。如果您擁有的使用者數目超過您擁有的用戶端數目，請使虛擬用戶端成為非持續用戶端。

若將虛擬用戶端標示為非持續用戶端，您必須在基礎影像中建立登錄機碼。

針對非持續 VDI 用戶端管理授權計數

1. 安裝 Symantec Endpoint Protection 用戶端並停用「竄改防護」之後，在基礎影像上開啟登錄編輯器。

   請參閱第 430 頁的「變更竄改防護設定」。

2. 瀏覽到以下其中一個登錄機碼：

   - 在 32 位元系統上：HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\

- 在 64 位元系統上：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\

3 建立一個名為 **Virtualization** 的新子機碼。

4 在 **Virtualization** 子機碼中，建立名為 **IsNPVDIClient** 的 DWORD 類型機碼，然後為其指派值 1。

請參閱第 600 頁的「清除過時的非持續 VDI 用戶端以釋放授權」。

請參閱第 599 頁的「針對 VDI 中的非持續訪客虛擬機器設定基礎影像」。

清除過時的非持續 VDI 用戶端以釋放授權

長時間下來，過時用戶端可能會累積在 Symantec Endpoint Protection Manager 資料庫中。過時用戶端是指未連線至 Symantec Endpoint Protection Manager 達 30 天的用戶端。Symantec Endpoint Protection Manager 預設為每隔 30 天會清除過時用戶端。

如果您不想要等待同樣的天數來清除過時的非持續用戶端，可以為這些用戶端架構獨立的間隔。如果您沒有架構獨立的間隔，則離線非持續虛擬用戶端會按照清除過時實體用戶端的相同間隔進行清除。

線上非持續用戶端會計入已部署授權數量；離線非持續用戶端則不會。

請參閱第 599 頁的「如何針對非持續 VDI 用戶端管理授權計數」。

您也可以在**「用戶端」**頁面上，從檢視篩選離線非持續用戶端。

清除過時的非持續 VDI 用戶端以釋放授權

1 在 Symantec Endpoint Protection Manager 主控台的**「管理員」**頁面上，按下**「網域」**。

2 在**「網域」**樹狀結構中，按下所要的網域。

3 在**「工作」**下，按下**「編輯網域屬性」**。

4 在**「編輯網域屬性」>「一般」**標籤中，核取**「刪除指定的時間內未連線的非持續 VDI 用戶端」**核取方塊，然後將**「天」**的值變更為所要的數字。

「刪除指定的時間內未連線的用戶端」選項必須勾選，才能存取離線非持續VDI用戶端的選項。

5 按下**「確定」**。

請參閱第 598 頁的「在非持續虛擬桌面基礎架構中使用 Symantec Endpoint Protection」。

部分 8

架構和管理管理伺服器

34

在管理伺服器與用戶端之間架構連線

本章包含以下主題：

設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊

Symantec Endpoint Protection Manager 會使用 Apache Web 伺服器與用戶端通訊，並提供報告服務。對於 Symantec Endpoint Protection 14 的新安裝，預設為啟用 HTTPS 通訊。HTTPS 是使用憑證簽署和加密資料的安全通訊協定，可確保通訊的機密性和完整性。

依據預設，12.1 版中的 Web 伺服器針對所有通訊使用未加密的通訊協定 HTTP。如果從 12.1 版升級至 Symantec Endpoint Protection 14，Symantec Endpoint Protection Manager 會在升級期間保留設定。如果您尚未在 12.1 版中啟用 HTTPS，可將 Symantec Endpoint Protection Manager Apache Web 伺服器架構為在升級後使用 HTTPS 連線。

表 34-1 架構與用戶端的 HTTPS 通訊

步驟	敘述
步驟 1：檢查預設 HTTPS 通訊埠是否可用	依據預設，HTTPS 流量會使用通訊埠 443。在某些網路中，通訊埠 443 可能已繫結至其他應用程式或服務。在啟用 HTTPS 通訊之前，您必須檢查預設通訊埠是否可用。 請參閱第 603 頁的「驗證通訊埠可用性」。
步驟 2：視需要變更預設 HTTPS 通訊埠	如果通訊埠 443 無法使用，請從通訊埠範圍的上限部分 (49152-65535)，選擇未使用的通訊埠。將管理伺服器架構為使用新通訊埠。更新管理伺服器清單以反映新通訊埠。 請參閱第 604 頁的「針對用戶端通訊變更 Apache 的 HTTPS 通訊埠」。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。
步驟 3：啟用與用戶端的 HTTPS 通訊	編輯 Apache httpd.conf 檔案，以允許與用戶端的 HTTPS 通訊。測試連線，然後將用戶端切換為 HTTPS 通訊。 請參閱第 604 頁的「啟用 HTTPS 用戶端伺服器通訊」。

請參閱第 137 頁的「管理用戶端伺服器連線」。

驗證通訊埠可用性

某些 Symantec Endpoint Protection Manager 組態會要求變更指派的預設通訊埠，以防止與其他應用程式或服務發生衝突。指派新的通訊埠之前，您必須先檢查並確認其他應用程式或服務未使用新的通訊埠。

驗證通訊埠可用性

- 開啟指令提示並輸入下列區分大小寫的指令：

  ```
  netstat -an | find ":port" | find "LISTENING"
  ```

  其中 *port* 代表要檢查可用性的埠號。例如，若要查看通訊埠 443 是否可用，請輸入：

  ```
  netstat -an | find ":443" | find "LISTENING"
  ```

  如果 `netstat` 指令傳回結果，您必須找到未使用的通訊埠。請使用相同的指令，但將 *port* 取代為您選擇的通訊埠。如果此指令未產生任何結果，便可自由地使用該通訊埠。

請參閱第 604 頁的「針對用戶端通訊變更 Apache 的 HTTPS 通訊埠」。

請參閱第 602 頁的「設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊」。

針對用戶端通訊變更 Apache 的 HTTPS 通訊埠

Apache 的預設 HTTPS 通訊埠為通訊埠 443。如果 Symantec Endpoint Protection Manager 託管其他 HTTPS 網站，通訊埠 443 可能已指派給其中一個網站。您應針對新安裝使用其他通訊埠，以盡量減少與已使用預設通訊埠 443 之任何應用程式之間的衝突。如果您想讓用戶端使用預設通訊埠來與 Symantec Endpoint Protection Manager 進行通訊，應該先驗證該通訊埠是否可用。

附註：如果在部署用戶端軟體後自訂 HTTPS 埠號，則用戶端將失去與管理伺服器的通訊。從包含新連線資訊的伺服器執行下一次用戶端更新之後，將會重新建立通訊。也可以使用通訊更新套件。

使用通訊更新套件部署還原用戶端伺服器通訊

完成此程序之後，啟用 HTTPS 用戶端伺服器通訊。

針對用戶端通訊變更 Apache 的 HTTPS 通訊埠

1 在文字編輯器中，開啟下列檔案：

`SEPM_Install\apache\conf\ssl\sslForClients.conf`

SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。

附註：封閉式資料夾 *SEPM_Install*\apache\conf\ssl\ 可能為唯讀。在該情況下，您可能需要在資料夾內容中取消勾選**「唯讀」**。

2 編輯下列行並以新的埠號取代預設的 443：

```
Listen 443

<VirtualHost _default_: 443>
```

3 儲存檔案，然後關閉文字編輯器。

請參閱第 603 頁的「驗證通訊埠可用性」。

請參閱第 604 頁的「啟用 HTTPS 用戶端伺服器通訊」。

請參閱第 602 頁的「設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊」。

啟用 HTTPS 用戶端伺服器通訊

編輯 httpd.conf 檔案，以使用 HTTPS 通訊協定啟用 Symantec Endpoint Protection Manager 伺服器與用戶端之間的安全通訊。

如果您需要為安全通訊使用替代通訊埠，必須先在 Symantec Endpoint Protection Manager 中變更通訊埠指派。

對於 Symantec Endpoint Protection 14.x 的新安裝，依據預設會啟用 HTTPS 用戶端伺服器通訊。如果從 12.1 版升級至 14.x 版，則用戶端伺服器通訊的設定會予以保留。依據預設，不會為 12.1.x 版啟用 HTTPS 用戶端伺服器通訊。

為 Apache Web 伺服器啟用 HTTPS

1 在文字編輯器中，開啟下列檔案：

```
SEPM_Install\apache\conf\httpd.conf
```

SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。

2 尋找下列文字字串並移除井字號 (#)：

```
#Include conf/ssl/sslForClients.conf
```

3 儲存並關閉檔案。

4 重新啟動 **Symantec Endpoint Protection Manager Webserver** 服務。

停止並重新啟動 Symantec Endpoint Protection Manager Webserver 服務亦會停止和重新啟動 Symantec Endpoint Protection Manager 服務。

請參閱第 661 頁的「停止和啟動 Apache Web 伺服器」。

確認 HTTPS 正常運作

1 在網頁瀏覽器中輸入下列 URL：

https://*SEPMServer*:*port*/secars/secars.dll?hello,secars

其中 *SEPMServer* 是 Symantec Endpoint Protection Manager 的伺服器主機名稱，而 *port* 是 HTTPS 埠號。依據預設，HTTPS 流量會使用通訊埠 443。

2 如果瀏覽器顯示「**確定**」一詞，表示 HTTPS 連線成功。

如果顯示頁面錯誤，請重複前面的步驟，並檢查所有字串的格式是否正確。請同時檢查輸入的 URL 是否正確無誤。

如果您沒有使用憑證授權中心簽署的憑證以及私密金鑰組更新管理伺服器，網頁瀏覽器會顯示憑證不受信任的警告。當您從 URL 存取網站 (與管理伺服器憑證上的主旨名稱不同) 時，會顯示相同的警告，此為預期行為。

將用戶端切換為使用 HTTPS 與 Symantec Endpoint Protection Manager 通訊

1 在 Symantec Endpoint Protection Manager 主控台的「**政策**」標籤中，按下「**政策元件**」>「**管理伺服器清單**」。

2 連按兩下您的用戶端群組和位置使用的管理伺服器清單。如果您只有預設的管理伺服器清單，請複製該清單，然後連按兩下新的清單加以編輯。

也可以按下「**工作**」下的「**新增管理伺服器清單**」。在「**管理伺服器**」下的「**新增**」>「**新伺服器**」中新增伺服器資訊。您可以為伺服器 IP 位址和伺服器名稱分別新增一個「**新伺服器**」項目。

請參閱第 273 頁的「在「政策」頁面中複製和貼上政策」。

3 按下「**使用 HTTPS 通訊協定**」。

只有當您先前已使用認證中心簽章的憑證以及私密金鑰組更新管理伺服器時，才應按下「**使用 HTTPS 通訊協定時驗證憑證**」。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

附註：如果已在 `sslForClients.conf` 檔案中使用自訂 HTTPS 埠號，請從管理伺服器清單編輯伺服器。按下「**自訂 HTTPS 通訊埠**」，然後編輯該通訊埠，使其與先前使用的號碼相符。

按下「**確定**」儲存自訂通訊埠。

---

4 按下「**確定**」儲存管理伺服器清單。

5 如果您已編輯預設管理伺服器清單的複本，請在複本上按下滑鼠右鍵，然後按下「**指派**」，將其指派給每個群組和位置。

請參閱第 634 頁的「指派管理伺服器清單至群組和位置」。

當用戶端接收到更新的管理伺服器清單時，用戶端會切換為使用 HTTPS 與 Symantec Endpoint Protection Manager 進行通訊。用戶端的變更最多可能需要三個活動訊號間隔時間才能完成。

確認用戶端與管理伺服器的通訊

1 在 Symantec Endpoint Protection 用戶端上，按下「**說明**」>「**疑難排解**」>「**伺服器連線狀態**」。

2 在「**上次嘗試連線**」和「**上次成功連線**」下方，確認用於 HTTPS 通訊之伺服器位址和埠號的顯示。

3 按下「**立即連線**」以強制立即連線 (視需要)。

請參閱第 604 頁的「針對用戶端通訊變更 Apache 的 HTTPS 通訊埠」。

請參閱第 602 頁的「設定 Symantec Endpoint Protection Manager 和用戶端之間的 HTTPS 通訊」。

改善用戶端和伺服器效能

Symantec Endpoint Protection Manager 包含各種功能，可用於提升用戶端效能和伺服器效能，同時仍維持高度安全性。

表 34-2 可改善伺服器和用戶端效能的工作

工作	敘述
變更用戶端伺服器通訊設定	使用提取模式取代推送模式，控制管理伺服器下載政策和內容更新至用戶端電腦的頻率。 在提取模式中，管理伺服器可支援更多用戶端。 增加活動訊號間隔，降低用戶端和伺服器間的通訊頻率。 如果每部伺服器服務的用戶端數目少於 100，可將活動訊號間隔時間增加為 15-30 分鐘。 如果為 100 至 1,000 個用戶端，請將活動訊號間隔時間增加為 30-60 分鐘。 更大的網路可能需要更長的活動訊號間隔時間。 將下載隨機設定增加為活動訊號間隔時間的一到三倍。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。 如需有關設定活動訊號間隔的詳細資訊，請參閱《Symantec Endpoint 規模設定及擴充性最佳實務準則》白皮書。
隨機選擇並減少內容更新次數	內容更新的大小和頻率各有不同，實際取決於內容類型和可用性。 您可以使用下列方式，減少下載及匯入完整內容更新集的影響： ■ 將用戶端負載分散到多部管理伺服器。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。 ■ 使用其他方式來派送內容，如「群組更新提供者」或第三方派送工具。 「群組更新提供者」可將伺服器的處理負載轉移到下載內容的用戶端，協助您保留頻寬。 請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。 請參閱第 192 頁的「使用第三方派送工具更新用戶端電腦」。 ■ 隨機選擇 LiveUpdate 下載內容到用戶端電腦的時間。 請參閱第 177 頁的「從 LiveUpdate 伺服器隨機進行內容下載」。 請參閱第 177 頁的「從預設管理伺服器或群組更新提供者隨機進行內容下載」。 ■ 在使用者不主動使用用戶端電腦時下載內容更新。 請參閱第 178 頁的「將 Windows 用戶端更新架構為在用戶端電腦閒置時執行」。
調整掃描以改善電腦效能	您可以變更某些掃描設定，在不降低防護能力的情況下，改善電腦效能。 例如，您可以將掃描架構為忽略信任的檔案或在電腦閒置時執行。 請參閱第 375 頁的「調整掃描以改善電腦效能」。 請參閱第 402 頁的「自訂 Windows 用戶端的自動防護」。

工作	敘述
減少資料庫用戶端日誌量	您可以架構記錄選項，以最佳化儲存需求並符合公司控制保留記錄資料的政策。 資料庫會接收持續產生的項目，並將項目儲存到日誌檔案中。 您必須管理儲存在資料庫中的資料，以確保儲存的資料不會耗盡所有可用的磁碟空間。 資料過多時，會造成執行資料庫的電腦當機。 您可以執行下列工作，來減少日誌資料量： ■ 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。 請參閱第 625 頁的「指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器」。 ■ 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。 請參閱第 626 頁的「指定日誌大小以及在資料庫中保留日誌項目的時間長度」。 ■ 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。 ■ 減少各管理伺服器所管理的用戶端數目。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。 ■ 減少活動訊號頻率，這會控制多久將用戶端日誌上傳到伺服器一次。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。 ■ 在將日誌資料寫入資料庫之前，增加儲存日誌資料之目錄的硬碟空間。 請參閱第 627 頁的「關於增加用於用戶端日誌資料的伺服器磁碟空間」。
執行資料庫維護工作	為提高用戶端與伺服器間的通訊速度，您應該排程定期的資料庫維護工作。 請參閱第 621 頁的「排程自動資料庫維護工作」。

關於伺服器憑證

憑證是用於驗證和加密敏感資料的產業標準。 若要防止傳送通過網路中路由器的資訊，應該對資料進行加密。

為了與用戶端通訊，管理伺服器會使用伺服器憑證。 為了讓管理伺服器利用伺服器憑證識別並驗證自己，Symantec Endpoint Protection Manager 預設會加密資料。 不過，某些情況下，您必須停用伺服器與用戶端之間的加密。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

請參閱第 610 頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。

基於安全起見，您可能也會想要備份憑證。 如果管理伺服器損壞，或是您忘記了金鑰儲存密碼，便可以輕易的擷取該密碼。

請參閱第 649 頁的「備份伺服器憑證」。

請參閱第 612 頁的「更新或還原伺服器憑證」。

請參閱第 651 頁的「產生新的伺服器憑證」。

管理伺服器支援下列的憑證類型：

- JKS 金鑰儲存檔案 (.jks) (預設)
  Java 工具 keytool.exe 會產生金鑰儲存檔案。 Java Cryptography Extension (.jceks) 格式需要有特定版本的 Java Runtime Environment (JRE)。 管理伺服器僅支援使用與管理伺服器上 Java Development Kit 相同版本所產生的 .jceks 金鑰儲存檔案。
  這個金鑰儲存檔案必須包含憑證及私密金鑰。 金鑰儲存密碼必須與金鑰密碼相同。 您可以在以下檔案中找到密碼：
  SEPM_Install\Server Private Key Backup\recovery_*timestamp*.zip
  SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。
  密碼出現在 keystore.password= 行。
- PKCS12 金鑰儲存檔案 (.pfx 或 .p12)
- 憑證和私密金鑰檔案 (.der 或 .pem 格式)
  賽門鐵克支援 .der 或 .pem 格式的未加密憑證及私密金鑰，不支援 Pkcs8 加密的私密金鑰。

更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則

在下列情況中，您可能需要更新安全憑證：

- 您還原用戶端已使用的舊有安全憑證。
- 您想要使用預設憑證 (.JKS) 以外的不同安全憑證。

當用戶端與伺服器使用安全通訊時，伺服器憑證會在伺服器與用戶端之間交換。這樣的交換動作會建立伺服器與用戶端間的信任關係。當伺服器上的憑證變更，信任關係就會破裂，用戶端即無法再通訊。 此問題稱為遺棄用戶端。

附註：請使用此程序來更新一部管理伺服器，或是一次更新多部管理伺服器。

表 34-3 列出了在不遺棄伺服器所管理的用戶端情況下更新憑證的步驟。

表 34-3 更新伺服器憑證的步驟

步驟	敘述
步驟 1：中斷遠端複製關係*	如果要更新的管理伺服器會透過其他管理伺服器進行遠端複製，請中斷遠端複製關係。 請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

步驟	敘述
步驟 2：停用伺服器憑證驗證	停用伺服器與用戶端之間的安全通訊。當您停用驗證時，用戶端會在伺服器更新伺服器憑證時保持連線。 請參閱第 610 頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。
步驟 3：等候所有用戶端接收更新的政策	根據下列因素而定，部署更新政策的程序可能需要一週或更長的時間： ■ 連線到管理伺服器的用戶端數目。大型安裝可能需要數天才能完成此程序，因為受管電腦必須上線才能接收新政策。 ■ 某些使用者可能正在休假，而其電腦為離線狀態。 請參閱第 143 頁的「使用政策序號檢查用戶端伺服器通訊」。
步驟 4：更新伺服器憑證	更新伺服器憑證。如果您也打算升級管理伺服器，請先升級憑證。 請參閱第 126 頁的「升級管理伺服器」。 請參閱第 612 頁的「更新或還原伺服器憑證」。 您必須重新啟動下列服務以使用新的憑證： ■ Symantec Endpoint Protection Manager 服務 ■ Symantec Endpoint Protection Manager Webserver 服務。 ■ Symantec Endpoint Protection Manager API 服務
步驟 5：再次啟用伺服器憑證驗證	再次啟用伺服器與用戶端之間的安全通訊。 請參閱第 610 頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。
步驟 6：等候所有用戶端接收更新的政策	用戶端電腦必須在先前步驟中接收政策變更。
步驟 7：還原遠端複製關係*	如果所更新的管理伺服器會透過其他管理伺服器進行遠端複製，請還原遠端複製關係。 請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

*如果您在 Symantec Endpoint Protection Manager 環境中使用遠端複製，則只需執行這些步驟。

請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

請參閱第 651 頁的「產生新的伺服器憑證」。

在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證

Symantec Endpoint Protection Manager 使用憑證來驗證其與 Symantec Endpoint Protection 用戶端之間的通訊。該憑證亦會數位簽署用戶端從中下載的政策檔案和安裝套件。用戶端將在

管理伺服器清單中儲存憑證的快取複本。如果憑證損毀或無效，用戶端就無法與伺服器通訊。如果您停用安全通訊，則用戶端仍然可與伺服器進行通訊，但不會驗證來自管理伺服器的通訊。

在下列情況下，停用安全通訊以更新憑證：

- 具有單一 Symantec Endpoint Protection Manager 的網站
- 具有多個 Symantec Endpoint Protection Manager 的網站，如果您無法啟用容錯移轉或負載平衡

附註：如果憑證已損毀但卻仍然有效，可執行災難復原作為最佳實務準則。

請參閱第 646 頁的「災難復原最佳實務準則」。

更新憑證且用戶端登入並接收到該憑證之後，再次啟用安全通訊。

在具有多個管理伺服器的網站上更新憑證以及使用容錯移轉或負載平衡時，該憑證會在管理伺服器清單中進行更新。在執行容錯移轉或負載平衡程序期間，用戶端接收到更新的管理伺服器清單和新憑證。

在不中斷與用戶端的通訊的情況下，更新單一管理伺服器網站上的伺服器憑證

1. 在主控台中，按下**「政策」>「政策元件」>「管理伺服器清單」**。
2. 在**「工作」**下方，按下**「複製清單」**，然後按下**「貼上清單」**。
3. 連按兩下清單複本加以編輯，然後進行下列變更：
   - 按下**「使用 HTTP 通訊協定」**。
   - 針對每個伺服器位址，請在**「管理伺服器」**下方，按下**「編輯」**，然後按下**「自訂 HTTP 通訊埠」**。
     將其保留為預設值 8014。如果您使用自訂通訊埠，請在此處使用。
4. 按下**「確定」**，然後再按下**「確定」**。
5. 在清單複本上按下滑鼠右鍵，然後按下**「指派」**。
6. 在主控台上，按下**「用戶端」>「政策」>「一般設定」**。
7. 在**「安全設定」**標籤中，取消勾選**「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全通訊」**，然後按下**「確定」**。
8. 移至步驟 9 之前，在對所有群組進行此變更後等待至少三個活動訊號週期。

   請確定您同樣針對未繼承父群組的群組架構此設定。
9. 更新伺服器憑證。

   請參閱第 612 頁的「更新或還原伺服器憑證」。
10. 按下**「確定」**。

若要重新啟用原始設定，請等待至少三個活動訊號週期，然後重新勾選**「使用數位憑證進行驗證，以啟用管理伺服器與用戶端之間的安全通訊」**，並將原始管理伺服器清單重新指派回您的群組。

在不中斷與用戶端的通訊的情況下，更新多個管理伺服器網站上的伺服器憑證

1. 在主控台上，請確保您的用戶端已架構為負載平衡或容錯移轉到至少一個其他 Symantec Endpoint Protection Manager。

   請參閱第 629 頁的「設定容錯移轉和負載平衡」。

   如果您無法啟用負載平衡或容錯移轉，請使用單一管理伺服器網站程序，以先後停用並重新啟用安全通訊。

2. 更新 Symantec Endpoint Protection Manager 上的伺服器憑證。

   請參閱第 612 頁的「更新或還原伺服器憑證」。

3. 等待至少三個活動訊號週期，然後在網站上更新下一個 Symantec Endpoint Protection Manager 上的伺服器憑證。

4. 重複步驟 2 和 3，直到網站上的每個 Symantec Endpoint Protection Manager 都具有新憑證為止。

附註：由於外出或正在休假的使用者的裝置處於離線狀態，因此可能無法接收這些更新。許多機構會執行容錯移轉方法 30 天或以上，以盡可能擷取多個外出用戶端。您可能想要使用舊憑證讓一個 Symantec Endpoint Protection Manager 持續執行 90 天，以確保這些使用者不會被孤立。

請參閱第 608 頁的「關於伺服器憑證」。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

更新或還原伺服器憑證

伺服器憑證會對伺服器與用戶端間的檔案進行加密和解密。用戶端會利用加密金鑰，連線至伺服器、下載檔案，然後對金鑰進行解密，以驗證其可信度。如果您變更伺服器上的憑證，而沒有手動更新用戶端，則伺服器與用戶端間的加密連線將會中斷。

下列情況下，您必須更新伺服器憑證：

- 不使用還原檔案的情況下，重新安裝 Symantec Endpoint Protection Manager。 更新憑證以還原用戶端已使用的先前憑證。
  請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
- 將某一部管理伺服器取代為另一部管理伺服器，並且使用相同的 IP 和伺服器名稱。
- 在災難復原之後，套用了錯誤的伺服器憑證 (.JKS)。
- 購買了不同的憑證，想要使用該憑證來取代預設的 .JKS 憑證。

請參閱第 608 頁的「關於伺服器憑證」。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

更新或還原伺服器憑證

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**的**「本機網站」**下方，按下您要更新伺服器憑證的管理伺服器。
3. 在**「工作」**下方，按下**「管理伺服器憑證」**，然後按**「下一步」**。
4. 在**「管理伺服器憑證」**面板中，按下**「更新伺服器憑證」**，按**「下一步」**，再按下**「是」**。

   若要維護伺服器用戶端連線，請停用安全連線。

   請參閱第 610 頁的「在不中斷與用戶端的通訊的情況下，更新管理伺服器上的伺服器憑證」。
5. 在**「更新伺服器憑證」**面板中，選擇您要更新為哪一個憑證，然後按**「下一步」**。
6. 針對每種憑證類型，按照面板上的指示操作，然後按下**「完成」**。

   備份伺服器憑證位於 *SEPM_Install*\Server Private Key Backup\recovery_*timestamp*.zip。您可以在相同的 .zip 檔案內的 settings.properties 檔案中，找到金鑰儲存檔案的密碼。 密碼出現在 keystore.password= 行。

   SEPM_Install 預設為 C:\Program Files\Symantec\Symantec Endpoint Protection Manager。
7. 您必須重新啟動下列服務以使用新的憑證：
   - Symantec Endpoint Protection Manager 服務
   - Symantec Endpoint Protection Manager Webserver 服務。
   - Symantec Endpoint Protection Manager API 服務

   請參閱第 128 頁的「停止及啟動管理伺服器服務」。

   請參閱第 661 頁的「停止和啟動 Apache Web 伺服器」。

35

架構管理伺服器

本章包含以下主題：

- 管理 Symantec Endpoint Protection Manager 伺服器和第三方伺服器
- 關於 Symantec Endpoint Protection 伺服器的類型
- 匯出和匯入伺服器設定

管理 Symantec Endpoint Protection Manager 伺服器和第三方伺服器

您可以架構 Symantec Endpoint Protection Manager 整合網路環境中許多不同的伺服器類型。

表 35-1　　伺服器管理

工作	敘述
瞭解有關伺服器的資訊	決定您需要設定的伺服器類型。 請參閱第 616 頁的「關於 Symantec Endpoint Protection 伺服器的類型」。
設定伺服器通訊權限	可以允許或拒絕存取遠端主控台。根據單一電腦或一組電腦的 IP 位址新增例外，即可管理存取。 請參閱第 259 頁的「授予或攔截對遠端 Symantec Endpoint Protection Manager 主控台的存取」。
修改伺服器設定	若要修改資料庫設定，或者在不同的電腦還原資料庫，則可以修改伺服器設定。 請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。

工作	敘述
架構郵件伺服器	若要使用網路中的特定郵件伺服器，必須架構郵件伺服器。 請參閱第 575 頁的「建立管理伺服器與電子郵件伺服器之間的通訊」。
管理目錄伺服器	可以將 Symantec Endpoint Protection 與目錄伺服器整合，協助管理管理員帳戶或建立組織單位。 請參閱第 206 頁的「將 Symantec Endpoint Protection Manager 連線至目錄伺服器」。
如果您使用代理伺服器連線到 Symantec LiveUpdate 伺服器，請架構代理設定	若要設定 Symantec Endpoint Protection Manager 來透過代理伺服器連線到 Internet，您必須架構代理伺服器連線。 請參閱第 172 頁的「架構 Symantec Endpoint Protection Manager 連線到代理伺服器，以便存取 Internet 並從 Symantec LiveUpdate 下載內容」。
匯入或匯出伺服器屬性	您可以將伺服器設定匯出至 xml 檔案，以及重新匯入相同的設定。 請參閱第 617 頁的「匯出和匯入伺服器設定」。
管理伺服器憑證	Symantec Endpoint Protection Manager 伺服器使用伺服器憑證加密資料，供網路中的所有伺服器和用戶端之間進行通訊。伺服器用伺服器憑證識別及自行驗證。可能需要備份、更新或產生新的伺服器憑證。 請參閱第 608 頁的「關於伺服器憑證」。 請參閱第 612 頁的「更新或還原伺服器憑證」。 請參閱第 649 頁的「備份伺服器憑證」。 請參閱第 651 頁的「產生新的伺服器憑證」。
架構伺服器的 SecurID 驗證	如果選擇使用 RSA SecurID 驗證管理員帳戶，您也必須架構管理伺服器，才能與 RSA 伺服器通訊。 請參閱第 245 頁的「搭配 Symantec Endpoint Protection Manager 使用 RSA SecurID 驗證」。
使用 Symantec VIP 為 Symantec Endpoint Protection Manager 架構雙因素驗證	如果您在環境中使用 Symantec VIP 進行雙因素驗證，則可以為使用 Symantec Endpoint Protection Manager 驗證進行驗證的管理員啟用此功能。 請參閱第 247 頁的「使用 Symantec VIP 架構雙因素驗證」。

工作	敘述
將伺服器移到不同的電腦	基於下列原因，您可能必須在電腦之間移動管理伺服器軟體： ■ 必須將管理伺服器從測試環境移到生產環境。 ■ 執行管理伺服器的電腦發生硬體故障。 您可以用下列方式移動管理伺服器軟體： ■ 在另一部電腦安裝管理伺服器並執行遠端複製。 請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。 ■ 使用復原檔案在另一部電腦安裝管理伺服器。 請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。
啟動和停止管理伺服器	管理伺服器會執行成為自動服務。 升級或執行災難復原時，必須停止管理伺服器服務。 請參閱第 128 頁的「停止及啟動管理伺服器服務」。

關於 Symantec Endpoint Protection 伺服器的類型

管理伺服器時，下列定義可能有助於理解：

- 網站
  網站是由通常位於相同公司位置的一或多部管理伺服器以及一個資料庫 (內嵌式資料庫或 Microsoft SQL Server) 所組成。您登入的網站為本機網站，可以直接進行修改。本機網站以外的所有其他網站都稱為遠端據點。使用遠端複製連線網站。
  請參閱第 635 頁的「設定網站和遠端複製」。
- 管理伺服器
  已安裝 Symantec Endpoint Protection Manager 軟體的電腦。從管理伺服器，可以建立政策並將其指派給不同的組織群組。 您可以監控用戶端，檢視報告、日誌和警示，以及架構伺服器和管理員帳戶。單一網站的多個管理伺服器可提供容錯移轉和負載平衡功能。
  請參閱第 629 頁的「設定容錯移轉和負載平衡」。
- 資料庫伺服器
  Symantec Endpoint Protection Manager 使用的資料庫。每個網站都有一個資料庫。 如果您使用的是 SQL Server 資料庫，資料庫可位於與管理伺服器相同或不同的電腦上。
  請參閱第 618 頁的「維護資料庫」。
- 遠端複製夥伴
  兩個網站間建立的關係，用於啟用二者之間資料遠端複製。
  請參閱第 635 頁的「設定網站和遠端複製」。

匯出和匯入伺服器設定

伺服器屬性檔案包含 Symantec Endpoint Protection Manager 的伺服器設定。下列情況下，您可能需要匯出和匯入伺服器屬性檔案：

- 使用災難復原檔案來重新安裝 Symantec Endpoint Protection Manager。
  災難復原檔案未包含伺服器設定。重新安裝 Symantec Endpoint Protection Manager 時，會遺失先前變更的任何預設伺服器設定。您可以使用匯出的伺服器屬性檔案來重新匯入變更後的伺服器設定。
- 您可以先在測試環境中安裝 Symantec Endpoint Protection Manager，稍後再將管理伺服器安裝在生產環境中。您可以將匯出的伺服器屬性檔案匯入生產環境。

請參閱第 614 頁的「管理 Symantec Endpoint Protection Manager 伺服器和第三方伺服器」。

匯出伺服器設定

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下，展開**「本機網站 (網站 *site_name*)」**，然後選取您要匯出的管理伺服器。
3. 按下**「匯出伺服器屬性」**。
4. 選取儲存檔案的位置，並指定檔案名稱。
5. 按下**「匯出」**。

匯入伺服器設定

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下，展開**「本機網站 (網站 *site_name*」)**，然後選取您要匯入設定的管理伺服器。
3. 按下**「匯入伺服器屬性」**。
4. 選取您要匯入的檔案，然後按下**「匯入」**。
5. 按下**「是」**。

36

管理資料庫

本章包含以下主題：

維護資料庫

Symantec Endpoint Protection 支援內嵌資料庫和 Microsoft SQL Server 資料庫。 如果您有 5,000 個以上的用戶端，則應該使用 Microsoft SQL Server 資料庫。

Symantec Endpoint Protection Manager 會自動安裝內嵌資料庫。 該資料庫包含安全政策、架構設定、攻擊資料、日誌及報告等資訊。

在安裝 Symantec Endpoint Protection Manager 後，管理伺服器可能會在數週或數月之後速度開始變慢。為改善管理伺服器的效能，您可能需要縮小資料庫儲存空間，並排程各種資料庫維護工作。

表 36-1 資料庫管理工作

工作	敘述
排程定期的資料庫備份	您應該排程定期的資料庫備份，以防資料庫發生毀損。 請參閱第 648 頁的「備份資料庫和日誌」。 請參閱第 621 頁的「排程自動資料庫備份」。 請參閱第 646 頁的「災難復原最佳實務準則」。 或者，您也可以選擇手動掃除資料庫中的資料，避免在備份發生之前自動掃除資料庫。 請參閱第 627 頁的「從資料庫手動清除日誌資料」。
排程資料庫維護工作	您可以排程資料庫維護工作，以加速管理伺服器與資料庫之間的互動。 您可以排程管理伺服器，使其立即執行下列維護工作，或在使用者不在用戶端電腦上時執行下列維護工作。 ■ 從交易日誌移除未使用的資料。 ■ 重建資料庫表索引，來改善資料庫的排序和搜尋功能。 請參閱第 621 頁的「排程自動資料庫維護工作」。
定期檢查資料庫檔案大小	如果您使用 Microsoft SQL Server 資料庫，而非內嵌資料庫，請確定資料庫不會達到檔案大小的上限。 請參閱第 622 頁的「增加 Microsoft SQL Server 資料庫檔案大小」。
計算所需的資料庫儲存空間	請計算所需的磁碟空間總量後，再決定如何減少儲存空間的大小。 資料庫儲存空間取決於以下因素： ■ 日誌大小和到期時間。 ■ 用戶端電腦數目。 ■ 每月病毒平均數目。 ■ 各日誌所需保留的事件數。 ■ 內容更新次數。 內容更新每次約需 300 MB。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。 請參閱第 183 頁的「還原為舊版 Symantec Endpoint Protection 安全更新」。 ■ 各語言所需保留的用戶端版本數目。 例如，如果您同時具備 32 位元用戶端和 64 位元用戶端，則需要兩倍的語言版本數目。 ■ 必須保留的備份數目。 備份檔案大約佔資料庫大小的 75%，然後再乘以保留的備份複本數。 如需如何計算所需硬碟空間的詳細資訊，請參閱賽門鐵克白皮書：Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書。

工作	敘述
減少日誌資料量	資料庫會接收持續產生的項目，並將項目儲存到日誌檔案中。 您必須管理儲存在資料庫中的資料，以確保儲存的資料不會耗盡所有可用的磁碟空間。 資料過多時，會造成執行資料庫的電腦當機。 您可以執行下列工作，來減少日誌資料量： ■ 只將部分用戶端日誌上傳至伺服器，以及變更上傳用戶端日誌的頻率。 請參閱第625頁的「指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器」。 ■ 指定用戶端電腦在資料庫中可保留的日誌項目數，以及可保留多久的時間。 請參閱第626頁的「指定日誌大小以及在資料庫中保留日誌項目的時間長度」。 ■ 過濾掉重要性較低的風險事件和系統事件，減少轉送到伺服器的資料。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。 ■ 在將日誌資料插入資料庫之前，減少日誌資料所儲存目錄的空間。 請參閱第 627 頁的「關於增加用於用戶端日誌資料的伺服器磁碟空間」。 ■ 減少各管理伺服器所管理的用戶端數目。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。 ■ 減少活動訊號頻率，這會控制用戶端日誌多久上傳一次到伺服器。 請參閱第 141 頁的「使用推送模式或提取模式更新用戶端上的政策和內容」。
將日誌資料匯出至另一部伺服器	基於安全目的，您可能需要將大量的日誌記錄保留更久的時間。 為了將用戶端日誌資料量保持在較低的水平，您可以將日誌資料匯出至另一部伺服器。 請參閱第 624 頁的「將日誌資料匯出至文字檔」。 請參閱第 623 頁的「將資料匯出至 Syslog 伺服器」。
建立僅包含所需防護的用戶端安裝套件	用戶端安裝的防護功能越多，用戶端資訊在資料庫中所佔用的空間越多。 建立僅包含用戶端電腦所需適當防護等級的用戶端安裝套件。 加入的群組越多，用戶端資訊在資料庫中所佔用的空間越多。 請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。
使用「群組更新提供者」下載內容	如果您的頻寬低或是用戶端電腦超過 100 個，請使用「群組更新提供者」下載內容。例如，2,000 個用戶端使用一個「群組更新提供者」下載內容，就等同使用四到五部管理伺服器進行下載。 請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。 若要減少磁碟空間和資料庫大小，您可以減少保留在伺服器上的內容修訂數目。 請參閱第 159 頁的「將 LiveUpdate 中的內容下載至 Symantec Endpoint Protection Manager」。
還原資料庫	要復原損毀的資料庫，您可以將資料庫還原到其最初安裝的電腦上。或者，您可以將資料庫安裝在其他電腦上。 請參閱第 652 頁的「還原資料庫」。

請參閱第 665 頁的「檢查與資料庫的連線」。

資料庫中的資訊會儲存在也稱為資料庫綱要的表格中。您可能需要綱要寫入自訂報表的查詢。如需詳細資訊，請參閱：

Symantec Endpoint Protection Manager 資料庫綱要參考

排程自動資料庫備份

您可以排程在較少使用者登入網路時進行資料庫備份。

您也可以在任何時候備份資料庫。

請參閱第 648 頁的「備份資料庫和日誌」。

排定自動資料庫備份：

1. 在主控台中，按下**「管理員」**>**「伺服器」**。
2. 在**「伺服器」**下方，按下**「本機網站 (我的網站)」**>**「本地主機」**。
3. 在**「工作」**下方，按下**「編輯資料庫屬性」**。
4. 在**「資料庫屬性」**對話方塊的**「備份設定」**標籤中，執行以下工作。
   - 在**「備份伺服器」**下拉式清單中，指定要儲存備份的管理伺服器。
   - 若您因安全目的或公司政策需要儲存日誌複本，請勾選**「備份日誌」**。
     否則，請將此選項保持停用，因為日誌會用掉許多磁碟空間。
   - 若公司政策規定，請指定備份數目。
5. 確定勾選**「排程備份」**，並設定排程。
6. 按下**「確定」**。

排程自動資料庫維護工作

安裝管理伺服器之後，資料庫的空間會不斷地成長。 管理伺服器會在數週或數月之後速度變慢。 為減少資料庫大小，並改善資料庫的回應時間，管理伺服器會執行下列資料庫維護工作：

- 截斷交易日誌。
  在資料庫內所發生的每項變更，交易日誌幾乎都會記錄下來。 管理伺服器會從交易日誌移除未使用的資料。
- 重建索引。
  管理伺服器會重組資料庫表索引，以縮短其花費在排序及搜尋資料庫的時間。

根據預設，管理伺服器會依排程執行這些工作。 您可以立即執行維護工作，或調整排程，讓它在使用者不在電腦上時進行。

附註：您也可以使用 Microsoft SQL Server Management Studio 執行資料庫維護工作。不過，您應該使用 Symantec Endpoint Protection Manager 或 Management Studio 其中之一，而不是同時使用這兩個軟體來執行這些工作。

在需要時執行資料庫維護工作

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下方，按下代表資料庫的圖示。
3. 在**「工作」**下，選取以下任何一個選項：
   - **立即截斷交易日誌**
   - **立即重建索引**
4. 按下**「執行」**。
5. 完成工作後，請按下**「關閉」**。

排程資料庫維護工作自動執行

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下方，按下代表資料庫的圖示。
3. 在**「工作」**下方，按下**「編輯資料庫屬性」**。
4. 在**「一般」**標籤中，勾選下列其中一個選項，或兩個都勾選，然後按下**「排程工作」**並指定每項工作的排程。
   - **截斷資料庫交易日誌**。 此工作的預設排程是每 4 小時一次。
   - **重建索引**。 此工作的預設排程是每個星期日的 2:00。

   警告：如果您使用 SQL Server Management Studio 執行這些工作，請取消勾選這些選項。

請參閱第 621 頁的「排程自動資料庫備份」。

增加 Microsoft SQL Server 資料庫檔案大小

如果您使用 SQL Server 資料庫，請定期檢查資料庫大小，以確保資料庫未達到其大小的上限。如果可以，請增加至 SQL Server 資料庫可容納的最大大小。

請參閱第 621 頁的「排程自動資料庫維護工作」。

增加 Microsoft SQL Server 資料庫大小

1 在 Microsoft SQL 伺服器電腦上，開啟 SQL Server Management Studio。

2 在 Object Explorer 中，展開「資料庫」資料夾，在 **sem5** 上按下滑鼠右鍵，然後按下「**屬性**」。

3 在「**資料庫屬性**」對話方塊中，選取「**檔案**」。

4 在「**資料庫檔案**」下，選取 **sem5_log1**，然後捲動至右側來檢視「**自動成長**」欄。

5 在「**自動成長**」欄中，按下 **...** 按鈕。

6 在「**變更 *sem5_log1* 的自動成長**」對話方塊中，按下「**不限制檔案成長**」，然後按下「**確定**」。

7 按下「**確定**」。

將資料匯出至 Syslog 伺服器

為了增加資料庫中的空間，您可以架構管理伺服器將日誌資料傳送至 Syslog 伺服器。

將日誌資料匯出至 Syslog 伺服器時，您必須架構 Syslog 伺服器接收日誌。

請參閱第 624 頁的「將日誌資料匯出至文字檔」。

將資料匯出至 Syslog 伺服器

1 在主控台中，按下「**管理員**」。

2 按下「**伺服器**」。

3 按下您要匯出日誌資料的本機網站或遠端據點。

4 按下「**架構外部記錄**」。

5 在「**一般**」標籤上，從「**更新頻率**」清單方塊選取將日誌資料傳送至檔案的頻率。

6 在「**主要日誌伺服器**」清單方塊中，選取要傳送日誌的管理伺服器。

如果您使用 SQL Server 並將多個管理伺服器連線到資料庫，請將其中一個伺服器指定為主要日誌伺服器。

7 勾選「**啟用日誌傳輸至 Syslog 伺服器**」。

8 提供下列資訊：

- **Syslog 伺服器**
  輸入您要接收日誌資料的 Syslog 伺服器的 IP 位址或網域名稱。
- **目的通訊埠**
  選取要使用的通訊協定，並輸入 Syslog 伺服器用來接聽 Syslog 訊息的目的通訊埠。
- **日誌設備**

鍵入您要用於 Syslog 架構檔的日誌設備數目，或使用預設值。有效值的範圍介於 0 和 23 之間。

9 在「**日誌過濾**」標籤上，勾選要匯出的日誌。

10 按下「**確定**」。

將日誌資料匯出至文字檔

將日誌資料匯出到文字檔案時，預設檔案位於資料夾中。依據預設，該資料夾路徑為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\dump。項目會暫存在 .tmp 檔案中，直到所有記錄都傳送至文字檔為止。

附註：您無法使用匯出的日誌資料還原資料庫。

表 36-2 顯示日誌資料類型與匯出日誌資料檔案名稱的對應。 日誌名稱未逐一對應「**監視器**」頁「**日誌**」標籤上使用的日誌名稱。

表 36-2 Symantec Endpoint Protection 的日誌文字檔名稱

日誌資料	文字檔名稱
伺服器管理	scm_admin.log
應用程式與裝置控制	agt_behavior.log
伺服器用戶端	scm_agent_act.log
伺服器政策	scm_policy.log
伺服器系統	scm_system.log
用戶端封包	agt_packet.log
用戶端主動型威脅	agt_proactive.log
用戶端風險	agt_risk.log
用戶端掃描	agt_scan.log
用戶端安全	agt_security.log
用戶端系統	agt_system.log
用戶端流量	agt_traffic.log

附註：匯出至文字檔時，匯出記錄的數目可能與您在**「外部記錄」**對話方塊中設定的數目不同。 重新啟動管理伺服器時，會發生這種狀況。 重新啟動管理伺服器後，日誌項目計數會重設為 0，而暫存日誌檔中可能已經有項目。 在這種狀況下，重新啟動後各類型產生的第一個 *.log 檔案包含的項目會多於指定值。 後續匯出的任何日誌檔則會包含正確數目的項目。

匯出日誌資料至文字檔案

1. 在主控台中，按下**「管理員」**。
2. 按下**「伺服器」**。
3. 按下要架構外部記錄的本機網站或遠端據點。
4. 按下**「架構外部記錄」**。
5. 在**「一般」**標籤上，選取將日誌資料傳送至檔案的頻率。
6. 在**「主要日誌伺服器」**清單方塊中，選取要傳送日誌的伺服器。

   如果您是使用 Microsoft SQL，且有多個管理伺服器連接資料庫，只有一部伺服器必須設為主要日誌伺服器。
7. 勾選**「匯出日誌至傾印檔」**。
8. 若有必要，勾選**「限制傾印檔記錄」**，並鍵入您要一次傳送至文字檔的項目數目。
9. 在**「日誌過濾」**標籤上，選取要傳送至文字檔的所有日誌。

   如果您選取的日誌類型可選取嚴重性等級，您必須勾選要匯出的嚴重性等級。
10. 按下**「確定」**。

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

公司政策可能要求您增加資料庫保留的日誌事件的時間與類型。 您可以指定要保留的日誌項目數，以及每個項目保留在用戶端上的天數。

您可以架構是否將每種類型的用戶端日誌上傳到伺服器。還可以架構最大上傳大小。如果您選擇不上傳用戶端日誌，則無法執行下列工作：

- 您無法使用**「監視器」**頁面中的**「日誌」**標籤，從 Symantec Endpoint Protection Manager 主控台檢視用戶端日誌資料。
- 您無法在備份資料庫時備份用戶端日誌。
- 您無法將用戶端日誌資料匯出至檔案或集中式日誌伺服器。

附註：部分用戶端日誌設定是群組限定的，而部分是在病毒和間諜軟體防護政策中設定，可套用到位置。如果您要區分所有遠端用戶端日誌和辦公室用戶端設定，則必須使用群組 (而非位置) 來管理遠端用戶端。

請參閱第 626 頁的「指定日誌大小以及在資料庫中保留日誌項目的時間長度」。

指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器

1. 在主控台上按下**「用戶端」**，然後選取群組。
2. 在**「政策」**標籤的**「與位置無關的政策與設定」**下方，按下**「用戶端日誌設定」**。
3. 在**「用於 *group name* 的用戶端日誌設定」**對話方塊中，設定檔案大小上限和保留日誌項目的天數。
4. 對任何想要用戶端轉送至伺服器的日誌勾選**「上傳到管理伺服器」**。
5. 若是**「安全」**日誌和**「流量」**日誌，設定調節器期間和調節器閒置期間。

   這些設定會決定**「防網路和主機刺探利用」**事件彙整的頻率。
6. 按下**「確定」**。

指定日誌大小以及在資料庫中保留日誌項目的時間長度

若要有助於控制硬碟空間，您可以減少資料庫保留的日誌項目數。您也可以架構項目保留的天數。

附註：「監視器」頁面中 Symantec Endpoint Protection Manager 主控台**「日誌」**標籤上的日誌資訊會以邏輯群組的形式呈現，方便您檢視。**「站台屬性日誌設定」**標籤上的日誌名稱會對應到日誌內容，而非對應到**「監視器」**頁面中**「日誌」**標籤上的日誌類型。

請參閱第 625 頁的「指定用戶端日誌大小以及要上傳哪些日誌到管理伺服器」。

指定日誌大小以及在資料庫中保留日誌項目的時間長度

1. 在主控台中，按下**「管理員」**。
2. 在**「伺服器」**下，展開**「本機站台」**，然後按下資料庫。
3. 在**「工作」**下，按下**「編輯資料庫屬性」**。
4. 在**「日誌設定」**標籤上，為每個類型的日誌設定項目數目和保留日誌項目的天數。
5. 按下**「確定」**。

關於增加用於用戶端日誌資料的伺服器磁碟空間

若您架構將大量用戶端日誌資料頻繁上傳到伺服器，可能會導致伺服器磁碟空間不足問題。如果您必須上傳大量用戶端日誌資料，可能就需要調整某些預設值，以避免發生空間不足的問題。 當您部署到用戶端時，請監控伺服器上日誌插入目錄的空間，並視需要調整這些值。

將日誌轉換成 .dat 檔案，然後寫入至資料庫的預設目錄位於下列預設位置：

`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\log`。

若要調整控制伺服器上可用空間的值，您必須在 Windows 登錄中變更這些值。 需要變更的 Windows 登錄機碼位於伺服器上的 HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM。

表 36-3 列出 Windows 登錄機碼及其預設值，並敘述其作用為何。

表 36-3 包含日誌上傳設定的 Windows 登錄機碼

值名稱	敘述
`MaxInboxSpace`	用於指定分配給目錄的空間，日誌檔案會在此目錄中轉換成 .dat 檔案，之後再儲存到資料庫。 預設值為 8 GB。
`MinDataFreeSpace`	用於指定此目錄應保留可用的最小空間。此機碼可確保使用同一個目錄的其他應用程式有足夠的空間可供執行，而不會對效能有不利的影響。 預設值為 200 MB。
`IntervalOfInboxSpaceChecking`	用於指定管理伺服器在檢查完收件匣中可供日誌資料使用的空間之前，應等待多長時間。 預設值為 30 秒。

請參閱第 618 頁的「維護資料庫」。

從資料庫手動清除日誌資料

如果您要在進行例行資料庫維護時手動掃除日誌，則可以在備份資料庫後執行掃除。

如果您允許自動掃除，而又不常進行資料庫備份，可能會遺失部分日誌資料。如果您定期在執行資料庫備份後執行手動日誌掃除，則可以確保維持所有日誌資料完整保留。如果您必須將日誌保留一段較長時間 (例如一年)，這個程序就很有用。您可以手動清除日誌，但此為選用程序，您並非一定要進行。

請參閱第 648 頁的「備份資料庫和日誌」。

請參閱第 626 頁的「指定日誌大小以及在資料庫中保留日誌項目的時間長度」。

從資料庫手動清除日誌資料

1. 為避免備份前自動進行資料庫掃除，可將網站日誌大小增大至最大值。
2. 視需要執行備份。
3. 在安裝 Symantec Endpoint Protection Manager 的電腦上開啟網頁瀏覽器，並輸入下列 URL：

   https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs

   執行此工作後，所有類型日誌的項目都會儲存在備用的資料庫資料表中。原始資料表會保留到下一次掃除啟動為止。
4. 要清空所有項目，而僅保留最新項目，請執行第二次掃除。原始資料表也會給清除，然後會再次儲存項目。
5. 將「**網站屬性**」對話方塊「**日誌設定**」標籤上的設定改回您偏好的設定。

37

管理容錯移轉和負載平衡

本章包含以下主題：

設定容錯移轉和負載平衡

用戶端電腦必須能夠隨時與管理伺服器保持連線，以下載安全政策並接收日誌事件。

容錯移轉可以在管理伺服器無法使用時保持與 Symantec Endpoint Protection Manager 的通訊。 負載平衡用來透過使用管理伺服器清單在多台管理伺服器之間分配用戶端管理

如果您使用的是 Microsoft SQL Server 資料庫，可以設定容錯移轉和負載平衡。 您可以使用內嵌資料庫設定容錯移轉，但前提是您使用遠端複製。 當您將遠端複製與內嵌資料庫搭配使用時，賽門鐵克建議您不要架構負載平衡，因為可能導致資料不一致和遺失。

表 37-1 列出了您在設定容錯移轉和負載平衡時應執行的工作。

表 37-1 容錯移轉和負載平衡的設定程序

工作	敘述
閱讀容錯移轉和負載平衡的相關資訊。	您應瞭解是否需要以及何時設定容錯移轉和負載平衡的管理伺服器。 請參閱第 630 頁的「關於容錯移轉和負載平衡」。

工作	敘述
安裝其他管理伺服器。	請參閱第 632 頁的「安裝管理伺服器以進行容錯移轉或負載平衡」。 每部管理伺服器的用戶端數量取決於日誌大小等數個因素。 若要計算所需的管理伺服器數量，請參閱： Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書
將管理伺服器新增到管理伺服器清單。	若要設定負載平衡，您需要新增多個管理伺服器到管理伺服器清單中。您可以使用預設的管理伺服器清單，或將管理伺服器新增到新的管理伺服器清單中。管理伺服器清單包含可供用戶端連線的管理伺服器 IP 位址或主機名稱。 請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。
將自訂管理伺服器清單指派給群組。	在建立自訂管理伺服器清單後，您必須將該清單指派給群組。 請參閱第 634 頁的「指派管理伺服器清單至群組和位置」。

請參閱第 635 頁的「設定網站和遠端複製」。

如果管理伺服器離線，或發生用戶端與管理伺服器無法通訊的問題，您也應該解決該問題。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

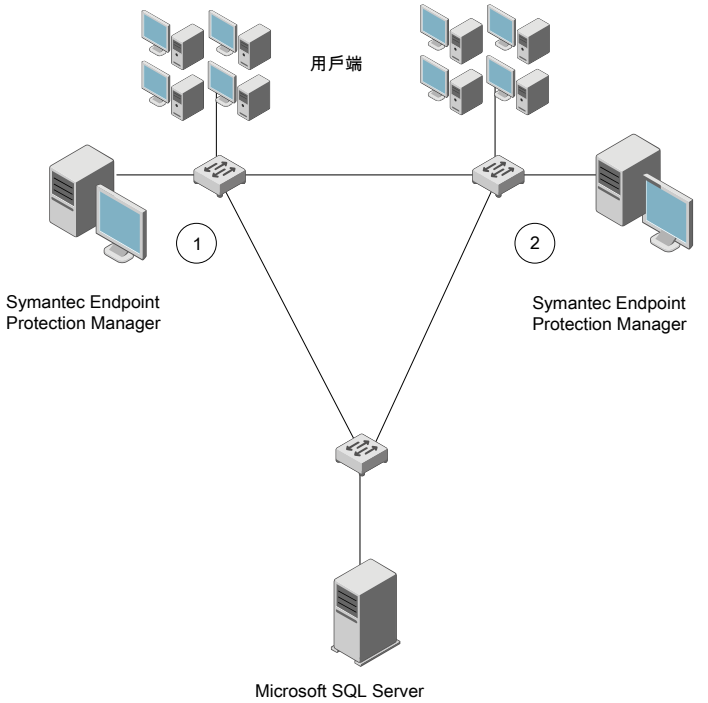
關於容錯移轉和負載平衡

您可以安裝兩個以上的管理伺服器與一個 Microsoft SQL Server 資料庫進行通訊，並將其架構作為容錯移轉或負載平衡之用。 由於只能安裝一個 Symantec Endpoint Protection Manager 與內嵌資料庫進行通訊，所以只有與另一個網站之間進行遠端複製時，才能設定容錯移轉。 當您將遠端複製與內嵌資料庫搭配使用時，賽門鐵克建議您不要架構負載平衡，因為可能導致資料不一致和遺失。

已指派至群組的管理伺服器優先順序清單會發生負載平衡。 您應該將至少兩個管理伺服器新增到網站，以在它們之間自動分配負載。 您安裝的管理伺服器數目可以超過處理用戶端所需的管理伺服器數目，以此可防範個別管理伺服器失效的狀況。 在自訂管理伺服器清單中，各個伺服器會被指派一個優先順序。 新加入網路的用戶端會隨機選取最高優先順序的伺服器進行連線。 如果嘗試的第一個伺服器無法使用，而清單中有其他最高優先順序的伺服器，則會隨機嘗試連線到其中一個伺服器。 如果沒有任何最高優先順序的伺服器可供使用，則用戶端會嘗試連線到清單中其中一個次高優先順序的伺服器。 這個隨機分配用戶端連線的方法會使各個管理伺服器分擔用戶端負載量。

圖 37-1顯示不同子網路中的元件。 管理伺服器與資料庫伺服器可位於相同的子網路中。 伺服器標示為 1 及 2，代表容錯移轉架構。

圖 37-1 容錯移轉組態



在容錯移轉組態中，所有用戶端會在伺服器 1 中傳送和接收流量。如果伺服器 1 離線，所有用戶端會在伺服器 2 中傳送和接收流量，直到伺服器 1 重新上線。在說明圖示中資料庫為遠端安裝，但資料庫也可以安裝於執行 Symantec Endpoint Protection Manager 的電腦中。

如果您想要使用本機伺服器，則您還可能要考慮內容更新的容錯移轉。 執行 LiveUpdate 的所有元件也可以使用更新來源的優先順序清單。 您的管理伺服器可以使用本機 LiveUpdate 伺服器，並在發生故障時移轉至其他實體位置的 LiveUpdate 伺服器。

附註：使用內部 LiveUpdate 伺服器、「群組更新提供者」和網站遠端複製時，不會提供負載平衡功能。 請勿為了負載平衡而設定多個網站。

請參閱第 629 頁的「設定容錯移轉和負載平衡」。

請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。

請參閱第 641 頁的「判斷需要的網站數量」。

請參閱第 635 頁的「設定網站和遠端複製」。

安裝管理伺服器以進行容錯移轉或負載平衡

如果用戶端無法與 Symantec Endpoint Protection Manager 進行通訊，則會使用容錯移轉架構保持通訊。負載平衡則會用來分配管理伺服器之間的用戶端管理。您可以在「管理伺服器」清單中指派管理伺服器的優先順序，以架構容錯移轉和負載平衡。

只有原始 Symantec Endpoint Protection Manager 使用 Microsoft SQL Server 資料庫時，才支援容錯移轉和負載平衡安裝。在用於容錯移轉或負載平衡的電腦上，也必須安裝 SQL Server Native Client 檔案。如果將網站架構為使用內嵌資料庫，請勿安裝用於容錯移轉或負載平衡的伺服器。

安裝管理伺服器以進行容錯移轉或負載平衡

1. 安裝 Symantec Endpoint Protection Manager。

   請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

2. 在**「管理伺服器組態精靈」**面板中，勾選**「自訂組態」**，然後按**「下一步」**。

   請參閱第 37 頁的「安裝後架構 Symantec Endpoint Protection Manager」。

3. 選取您要此伺服器管理的用戶端數目，然後按**「下一步」**。
4. 勾選**「安裝額外的管理伺服器到現有網站」**，然後按**「下一步」**。
5. 在「伺服器資訊」畫面中，接受或變更預設值，然後按**「下一步」**。
6. 在**「Microsoft SQL Server 資訊」**對話方塊中，按下有關安裝 SQL Server 用戶端工具之訊息中的**「確定」**。
7. 在下列文字方塊中輸入遠端伺服器值：

   步驟一告知 Symantec Endpoint Protection Manager 可在何處尋找網路上的 SQL Server，其中包括主機名稱、實例名稱和通訊埠。

   您也可以挑選驗證類型，包括 Windows 驗證或 SQL 驗證。

   - **資料庫伺服器***instance_name*
     SQL Server 通訊埠
     資料庫名稱
     SQL 用戶端資料夾 (本機電腦上)
     如果此文字方塊未自動填入正確路徑，則表示 Microsoft SQL Client Utility 未安裝或未正確安裝。

8. **步驟二**告知 Symantec Endpoint Protection Manager 如何向 SQL Server 進行驗證，並包含資料庫名稱、資料庫使用者和資料庫使用者的密碼。

   安裝該網站的第一個管理伺服器時，您應該已經備妥此資訊。

9. 按**「下一步」**。
10. 指定並確認 Symantec Endpoint Protection Manager admin 帳戶的密碼。

    也可以選擇提供管理員的電子郵件地址。

11 按「**下一步**」。

12 出現警告時，請閱讀簡訊，然後按下**確定**。

13 在「**管理伺服器完成**」面板中，按下「**完成**」。

架構用於負載平衡的管理伺服器清單

架構容錯移轉和負載平衡時，預設會將相同的優先順序指派給管理伺服器。安裝後，如果要變更預設的優先順序，可以使用 Symantec Endpoint Protection Manager 主控台進行變更。只有在網站包含多個管理伺服器時，才能架構負載平衡。

管理伺服器清單中指派為優先順序 1 的伺服器之間，會發生負載平衡。如果多部伺服器指派為優先順序1，用戶端會隨機選擇其中一部伺服器，並與此伺服器建立通訊。如果優先順序為 1 的所有伺服器都出現故障，則用戶端會連線至指派為優先順序 2 的伺服器。

同時提供負載平衡和漫遊功能：

- 啟用 DNS，並且在自訂管理伺服器清單中只放入網域名稱作為唯一項目。
- 啟用 Symantec Endpoint Protection 位置偵測功能，並且為各個位置使用自訂管理伺服器清單。至少針對各個網站建立一個位置。
- 使用提供容錯移轉或負載平衡的硬體裝置。許多這類裝置也提供漫遊設定。

請參閱第 630 頁的「關於容錯移轉和負載平衡」。

架構用於負載平衡的管理伺服器清單

1 在主控台中，按下「**政策**」。

2 展開「**政策元件**」，然後按下「**管理伺服器清單**」。

3 在「**工作**」下方，按下「**新增管理伺服器清單**」。

4 在「**管理伺服器清單**」對話方塊中，按下「**新增**」>「**新伺服器**」。

5 在「**新增管理伺服器**」對話方塊的「**伺服器位址**」方塊中，輸入管理伺服器的完整網域名稱或 IP 位址。

如果您鍵入的是 IP 位址，請確定該位址是靜態的，且所有用戶端都能解析該位址。

6 按下「**確定**」。

7 新增任何其他伺服器。

8 若要架構另一管理伺服器用於負載平衡，請按下「**新增**」>「**新優先順序**」。

9 若要變更用於負載平衡的伺服器的優先順序，請選定伺服器，然後執行下列工作之一：

- 若要使用戶端先連線到該特定伺服器，請按下「**上移**」。

- 若要降低伺服器的優先順序，請按下**「下移」**。

10 按下**「確定」**。

您接著必須將管理伺服器清單套用到群組。

請參閱第 634 頁的「指派管理伺服器清單至群組和位置」。

指派管理伺服器清單至群組和位置

新增政策之後，您必須將該政策指派給群組或 (和) 位置。您也可以使用管理伺服器清單，將用戶端的群組從某個管理伺服器移至另一個管理伺服器。

您必須先完成新增或編輯管理伺服器清單，才能指派清單。

請參閱第 633 頁的「架構用於負載平衡的管理伺服器清單」。

指派管理伺服器清單至群組和位置

1 在主控台中，按下**「政策」**。

2 在**「政策」**頁面中，展開**「政策元件」**，然後按下**「管理伺服器清單」**。

3 在**「管理伺服器清單」**窗格中，選取要指派的管理伺服器清單。

4 在**「工作」**下方，按下**「指派清單」**。

5 在**「套用管理伺服器清單」**對話方塊，勾選要套用管理伺服器清單的群組和位置。

6 按下**「指派」**。

7 按下**「是」**。

在用戶端頁面上指派管理伺服器清單至群組或位置

1 在主控台中，按下**「用戶端」>「政策」**。

2 在**「政策」**標籤中，選取群組，然後取消勾選**「從父群組繼承政策和設定」**。

只有在群組不再從父群組繼承任何政策和設定時，您才能針對該群組設定任何通訊設定。

3 在**「與位置無關的政策與設定」**下方，按下**「通訊設定」**。

4 在**「*group name* 的通訊設定」**對話方塊的**「管理伺服器清單」**下方，選取管理伺服器清單。

與管理伺服器通訊時，您選取的群組就會使用此管理伺服器清單。

5 按下**「確定」**。

38

管理網站和遠端複製

本章包含以下主題：

設定網站和遠端複製

一個網站包含一個資料庫、一或多個管理伺服器以及多個用戶端。依據預設，您將 Symantec Endpoint Protection 部署為單一網站。具有多個資料中心或多處實體位置的組織通常使用多個網站。

遠端複製組態用於備援。一個資料庫內的資料會複製或遠端複製至另一個資料庫上。一個資料庫發生故障時，您仍然可以管理及控制所有用戶端，因為另一個資料庫包含了用戶端資訊。

請參閱第 637 頁的「什麼是網站以及遠端複製如何運作？」。

表 38-1　　設定網站和遠端複製的程序

工作	敘述
步驟 1：確認您是否需要新增另一個網站	設定多個網站和遠端複製之前，請確認是否必要。賽門鐵克建議您只在特定情況下設定多個網站，並且在每個網站陣列中新增最多五個網站。如果您新增額外的網站，請決定哪個網站設計用於您的組織。 請參閱第 640 頁的「決定是否要設定多個網站和遠端複製」。 請參閱第 641 頁的「判斷需要的網站數量」。
步驟 2：在第一個網站上安裝 Symantec Endpoint Protection Manager	第一次安裝 Symantec Endpoint Protection 時，依據預設，您已安裝第一個網站或本機網站。 請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。
步驟 3：在第二個網站上安裝 Symantec Endpoint Protection Manager	透過建立第二個管理伺服器來建立第二個網站。第二個網站歸類為遠端據點，管理伺服器稱為遠端複製夥伴。遠端複製會根據您在初始安裝期間新增第二個網站時的預設排程進行。新增遠端複製夥伴後，您可以變更遠端複製排程以及遠端複製的資料。 請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。 兩個網站間的資料庫第一次遠端複製時，讓遠端複製完整完成。 由於整個資料庫都要經過遠端複製，因此遠端複製可能需要比較長的時間。 您可能想要立即遠端複製資料，而不是等到排程資料庫進行遠端複製。 您也可以將遠端複製排程變更為較早或較晚進行。 如果在一個網站上升級管理伺服器，則必須在所有網站上升級管理伺服器版本。 請參閱第 645 頁的「立即遠端複製資料」。
步驟 4：檢查遠端複製事件的歷程記錄 (選擇性)	如果您需要檢查發生的遠端複製或針對遠端複製事件進行疑難排解，請查看系統日誌。 在第二個管理伺服器中，檢視系統日誌。**「管理」>「遠端複製事件」**事件類型的過濾器。 請參閱第 563 頁的「檢視日誌」。

您還可以將管理伺服器重新架構為透過網路中目前存在的網站遠端複製資料。或者，如果您擁有兩個非遠端複製網站，可以將其中一個轉換為透過第二個網站遠端複製的網站。

請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。

- 架構 Symantec Endpoint Protection 後，您應該備份包含所有架構變更的資料庫。
  請參閱第 648 頁的「備份資料庫和日誌」。

- 如果您停用某個遠端複製夥伴以升級至最新版的管理伺服器，則必須重新新增遠端複製夥伴。
  請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。
  請參閱第 119 頁的「升級至新版本」。

請參閱第 206 頁的「連線至遠端複製網站上的目錄伺服器」。

什麼是網站以及遠端複製如何運作？

網站和遠端複製夥伴

網站是 Symantec Endpoint Protection Manager 資料庫，有一或多個 Symantec Endpoint Protection Manager 附加至該資料庫。遠端複製功能可以在不同網站的資料庫之間複製資料，以便讓兩個資料庫包含相同的資訊。如果其中一個資料庫發生故障，您可以使用第二個網站上的資料庫中的資訊來管理每個網站。

遠端複製夥伴是第二個網站或遠端據點內的個別管理伺服器。一個網站可視其需要有不限數目的遠端複製夥伴。每個夥伴都會連線到主網站或本機網站，也就是您登入的網站。所有設定為夥伴的網站都可以視為位於相同網站陣列。

任何與您共同進行資料遠端複製的網站，都是遠端複製夥伴或網站夥伴。遠端複製夥伴和網站夥伴都會使用多部管理伺服器，但它們使用的資料庫以及通訊方式則不相同：

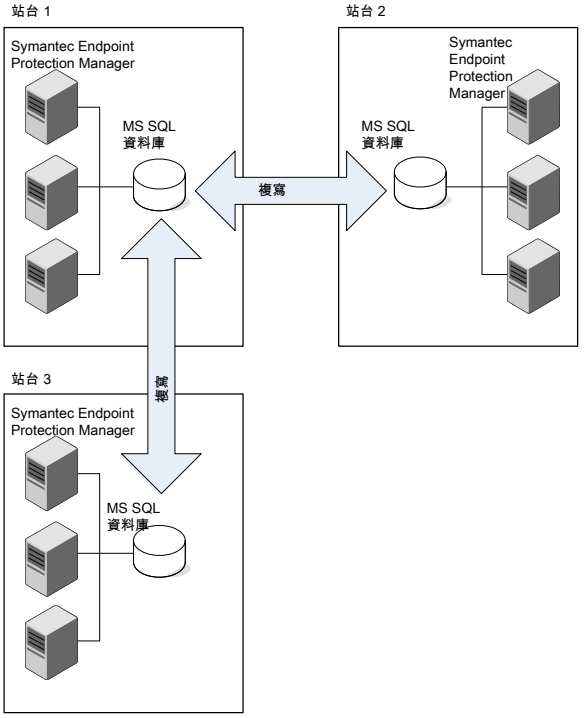
- 遠端複製夥伴可以使用內嵌資料庫或 Microsoft SQL Server 資料庫。 管理伺服器不會共用資料庫。 所有的遠端複製夥伴會共用公共的授權碼。
  如果您使用的是內嵌資料庫，則只能連線一個 Symantec Endpoint Protection Manager。
  如果您使用的是 Microsoft SQL Server 資料庫，則可以連接共用一個資料庫的多個管理伺服器。 只有其中一個管理伺服器需要設為遠端複製夥伴。
- 網站夥伴會共用單一 Microsoft SQL Server 資料庫。

遠端複製如何運作？

您在任何夥伴上執行的變更都會複製到所有其他夥伴上。 例如，您可能會想要在主要辦公室設定一個網站 (網站 1) 和第二個網站 (網站 2)。 網站 2 是網站 1 的夥伴。透過遠端複製排程，網站 1 和網站 2 上的資料庫會進行協調。如果在網站 1 進行了變更，在執行遠端複製之後，該變更會自動顯示在網站 2。 如果在網站 2 進行了變更，在執行遠端複製之後，該變更會自動顯示在網站 1。您也可以安裝第三個網站 (網站 3)，它可從網站 1 或網站 2 遠端複製資料。

在遠端複製進行之後，網站 1 上的資料庫及網站 2 上的資料庫會彼此相同。 只有伺服器的電腦識別資訊會不同。

圖 38-1　　主網站與兩個遠端據點之間進行遠端複製的方式



如需遠端複製頻率的詳細資訊，請參閱下列文章：SEPM 遠端複製設定的原理

請參閱第 640 頁的「決定是否要設定多個網站和遠端複製」。

請參閱第 641 頁的「判斷需要的網站數量」。

請參閱第 639 頁的「如何解決遠端複製期間網站之間的資料衝突」。

判斷遠端複製伺服器的大小

遠端複製夥伴需要比單一管理伺服器安裝更大的資料庫。遠端複製伺服器的大小需求增加包括下列因素：

- 受管用戶端數目
- 資料庫中保留的用戶端安裝套件大小
- 保留的日誌檔數目
- 資料庫維護設定
- 日誌大小與到期時間範圍
- 定義檔更新大小

- 資料庫備份資訊需求

一般來說，遠端複製伺服器的硬碟需求應該是原始 Symantec Endpoint Protection Manager 用於初始遠端複製之硬碟空間的至少三倍。

請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。

遠端複製考量和最佳實務準則

Symantec Endpoint Protection 規模設定及擴充性最佳實務白皮書

如何解決遠端複製期間網站之間的資料衝突

遠端複製會將資料傳輸或轉送到另一台管理伺服器。網站可以有多個遠端複製夥伴，而在其中一個夥伴上做出的任何變更都會遠端複製到所有網站。

會複製哪些資料？

遠端複製網站並不會互相覆寫，而是會比較每個網站的內容；如果某個網站有一套或一份其餘網站所沒有的內容，就會共用該內容。如果所有 LiveUpdate 內容和用戶端套件都相符，就不會交換任何內容。

遠端複製夥伴會複製下列資料：

- 政策和群組 (必要，雙向)
- LiveUpdate 內容和用戶端安裝套件 (如果您指定了這些選項) (選擇性，雙向)
- 日誌 (選擇性，雙向或單向)

如果在一個網站上升級管理伺服器，則必須在所有網站上升級管理伺服器版本。如果資料庫結構綱要版本不相符，就不會進行遠端複製。

表 38-2說明管理伺服器如何在管理員變更網站陣列中網站上的設定時解決衝突。

表 38-2　　管理伺服器解決網站間衝突的方式

衝突類型	範例	解決方法
兩項差異無法共存。	網站 1 和網站 2 的管理員都架構同一個防火牆政策設定。在網站 1 上，該設定為啟用。在網站 2 上，該設定為停用。	管理伺服器只會保留最近所做的變更。 例如，如果您先在網站 1 進行變更，然後在網站 2 進行變更，則會保留網站 2 的變更。
為兩個網站建立了相同的變數。	網站 1 和網站 2 的管理員都新增相同名稱的群組。	管理伺服器會保留這兩項變更，並在最近建立的變數後加上波浪號和數字 1 (~1)。 例如，兩個群組都命名為 Sales 時，最近命名的 Sales 群組會變成 Sales ~1。

衝突類型	範例	解決方法
資料可以合併，沒有衝突。	網站1的管理員新增了兩項防火牆政策，而網站2的管理員新增了五項防火牆政策。	管理伺服器會合併變更。 例如，管理伺服器會在雙方網站上顯示所有七項防火牆政策。

決定是否要設定多個網站和遠端複製

安裝第二個網站之前，您應先決定多個網站和遠端複製是否是適合您網路的選擇。設定一個以上的網站可能會增加不必要的複雜性。多個網站可能會導致某些工作 (例如檢視用戶端日誌和報告) 更加困難。一般來說，您應只安裝一個網站。

設定多個網站和遠端複製的主要目的如下：

- 如果網路的 WAN 連結速度很慢。
  多個網站會提供第二部管理伺服器，供位於多個地理區域的用戶端在本機上連線。例如，假設公司在德國和美國都設有幾個大型的辦公室。如果德國和美國之間的連線速度很慢，則該公司應分別在德國和美國各建立一個網站。德國用戶端可以連線至德國網站，而美國用戶端可以連線至美國網站。這樣的分配方式可減少必須透過慢速 WAN 連結通訊的用戶端數目。
- 為了提供資料庫備援。
  遠端複製可確保在其中一個資料中心損毀或遺去的情況下，其他資料中心有備份的資料庫。

在某些情況下，您應使用群組更新提供者 (GUP)，而非多個網站和遠端複製。當您有為數眾多的用戶端，或是用戶端分散在多個地理位置時，請使用 GUP。

附註：您不應設定超過五個遠端複製的網站。

表 38-3　決定要使用一個以上的網站搭配遠端複製、使用 GUP，或是都不使用

問題	答	使用多個網站搭配遠端複製或使用 GUP
您是否有超過 45,000 個用戶端？	是。 您是否有多個位置，或連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度很慢？	是。 ■ 若 WAN 連結速度很慢，請考慮使用遠端複製。 ■ 若有多個位置，請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。
	否。 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用遠端複製。
		否。您不需要遠端複製或 GUP。

問題	答	使用多個網站搭配遠端複製或使用 GUP
您的 WAN 連結速度是否很慢？	是。 您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。請考慮使用遠端複製。
		否。請考慮使用 GUP。
	否。 您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。請考慮使用遠端複製。
		否。您不需要遠端複製或 GUP。
您是否有多個位置，而每個位置都有超過 1,000 個用戶端？	是。 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。
	否 您連線到包含超過 1,000 個用戶端的位置的 WAN 連結速度是否很慢？	是。請考慮使用 GUP。
		否。您不需要遠端複製或 GUP。

何時將遠端複製與 Symantec Endpoint Protection Manager 搭配使用

請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。

請參閱第 635 頁的「設定網站和遠端複製」。

請參閱第 641 頁的「判斷需要的網站數量」。

判斷需要的網站數量

大多數中小組織只需要單一網站集中管理網路安全性。由於每個網站只有一個資料庫，因此所有資料都在中央位置上。

甚至位於單一地理位置的大型組織，通常也只需要一個網站。但是對於過於複雜無法集中管理的組織，您應該使用具有多個網站的分散式管理架構。

對於下列任何因素，您都應該考慮使用多個網站：

- 大量用戶端。
- 地理位置數量，以及不同位置之間的通訊連結類型。
- 功能部門或管理群組數量。
- 資料中心數量。最佳實務準則是針對各個資料中心設定一個 Symantec Endpoint Protection 網站。
- 要更新內容的頻率。
- 需要保留的用戶端日誌資料量、保留資料的時間長度，以及應該儲存資料的位置。

- 多個具有幾千個用戶端的實體位置之間的 WAN 連結速度很慢。 如果您設定具有自己的管理伺服器的第二個網站，可以將用戶端與伺服器之間透過該緩慢連結的流量減至最少。 用戶端較少時，應該使用「群組更新提供者」。
  請參閱第 184 頁的「使用群組更新提供者將內容散佈至用戶端」。
- 任何其他獨特的企業管理和 IT 安全性管理考量事項。

請使用下列規模指引決定安裝網站的數量：

- 儘可能安裝較少的網站，最多不超過 20 個網站。 遠端複製網站的數量應維持在五個以下。
- 最多將 10 個管理伺服器連線到一個資料庫。
- 將多達 18,000 個用戶端 (適用於 14.x) 或 50,000 個用戶端 (適用於 12.1.x) 連線至管理伺服器。

新增網站後，您應該透過遠端複製功能在多個網站間遠端複製網站資訊。 遠端複製是在資料庫之間共用資訊的程序，可確保內容一致。

表 38-4　　多網站設計

網站設計	敘述
已派送	每個網站都會針對群組和政策執行雙向遠端複製，但不會針對日誌和內容執行遠端複製。若要檢視網站報告，您可以使用主控台連線至遠端據點中的管理伺服器。 如果您不需要即時存取遠端據點資料，則可以使用此設計。
集中式記錄設計	所有日誌都從其他網站轉送到中央網站上。 如果您需要集中式報告，則使用此設計。
高可用性	每個網站都有多個管理伺服器安裝和資料庫叢集。 若要處理其他用戶端，您需要新增多個管理伺服器而不是新增多個網站。您可以使用管理伺服器清單，將用戶端電腦架構為在主要管理伺服器變成無法使用時自動切換到替代管理伺服器。 使用此設計可提供備援、容錯移轉和災難復原功能。 **附註：**當您將遠端複製與內嵌資料庫搭配使用時，賽門鐵克建議您不要新增負載平衡，因為可能導致資料不一致和遺失。 請參閱第 629 頁的「設定容錯移轉和負載平衡」。

如需是否要設定遠端複製的詳細資訊，請參閱下列文章：何時將遠端複製與 Symantec Endpoint Protection Manager 搭配使用

請參閱第 637 頁的「什麼是網站以及遠端複製如何運作？」。

請參閱第 635 頁的「設定網站和遠端複製」。

請參閱第 640 頁的「決定是否要設定多個網站和遠端複製」。

如何安裝第二個網站用於遠端複製

安裝用於遠端複製的第二個網站的程序分兩個階段：

- 安裝第二個 Symantec Endpoint Protection Manager 和資料庫以透過已安裝的 Symantec Endpoint Protection Manager 和資料庫進行遠端複製。
- 登入第二個 Symantec Endpoint Protection Manager 並變更要遠端複製的排程和項目 (選擇性)。
  變更遠端複製頻率和內容

安裝第二個網站用於遠端複製

安裝第二個網站用於遠端複製

1. 安裝第二個 Symantec Endpoint Protection Manager。

   請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

   「管理伺服器組態精靈」會在安裝管理伺服器後自動啟動。
2. 在**「管理伺服器組態精靈」**中，按下**「新安裝的自訂組態 (多於 500 個用戶端，或自訂設定)」**，然後按**「下一步」**。
3. 按下**「安裝其他網站」**，然後按**「下一步」**。
4. 在下一個面板中，輸入以下資訊，然後按**「下一步」**：
   - **遠端複製伺服器**
     已安裝之管理伺服器的名稱或 IP 位址以及遠端複製此管理伺服器所使用的名稱或 IP 位址。
   - **系統管理員名稱**和**密碼**。
     依據預設，系統管理員的使用者名稱為 `admin`。您必須使用系統管理員帳戶，而不是使用限制的管理員帳戶或網域管理員帳戶。
   - 勾選**「在本機網站和此夥伴網站之間遠端複製用戶端套件和 LiveUpdate 內容」**(選擇性)。
     如果您現在不勾選此選項，可以稍後勾選。
5. 如果出現有關接受憑證的警告訊息，請按下**「是」**。
6. 在「網站資訊」窗格中，接受或變更預設值，然後按**「下一步」**。
7. 在「資料庫選擇」窗格中，按下**「預設內嵌資料庫」**或**「Microsoft SQL Server 資料庫」**，然後按**「下一步」**。

   賽門鐵克建議您遠端複製的網站使用相同類型的資料庫，但這並非是必需的。

   根據選擇的資料庫完成安裝。

8 在「**執行 LiveUpdate**」窗格中，按「**下一步**」。

或者，也可以新增夥伴資訊。

9 或者，接受資料收集功能，然後按「**下一步**」。

隨即建立資料庫。此步驟需要一些時間。

Symantec Endpoint Protection Manager 隨即啟動。

變更遠端複製頻率和內容

依據預設，已排程為在安裝第二個網站和管理伺服器之後自動執行遠端複製。在安裝第二個管理伺服器的過程中，根據預設排程執行遠端複製。但是，您可能需要根據遠端複製所需時間來變更頻率。您可以在本機網站或新網站上變更頻率，但賽門鐵克建議您首先在新網站上架構遠端複製。下次當兩個網站遠端複製時，這些網站上的排程相同。具有較小 ID 號碼的網站會起始排程遠端複製。無論哪個網站架構為新的遠端複製夥伴，都將始終由來自新網站所指向的本機網站的資料庫覆寫其資料庫。

兩個網站會自動共用群組和政策。可以根據可用磁碟空間量選擇是否遠端複製日誌、用戶端安裝套件或 LiveUpdate 內容。

遠端複製所需時間，取決於資料庫大小及網站間的網路連線。 首先，測試一個遠端複製週期，查看其花費的時間。 您應該根據該段時間來排程遠端複製，並確定管理伺服器複製資料的時間不會重疊。用戶端套件和 LiveUpdate 內容可包含大量資料。用戶端套件中的資料最大可達 5 GB。 用戶端安裝套件可能需要多達 500 MB 的磁碟空間。如果您計劃遠端複製日誌，務必確定您有充足的磁碟空間可以儲存所有遠端複製夥伴伺服器上的其他日誌。

在初次的完整資料庫遠端複製完成後，如果只遠端複製政策、用戶端和群組，而不遠端複製日誌，則後續的遠端複製規模會相當小。確保管理伺服器具有足夠的可用磁碟空間來根據頻率及內容進行遠端複製。

變更遠端複製頻率和排程

1 在主控台中，按下「**管理員**」>「**伺服器**」。

2 在「**伺服器**」>「**本機網站**」下，展開「**遠端複製夥伴**」，然後選取您要遠端複製的網站。

3 在「**工作**」下方，按下「**編輯遠端複製夥伴屬性**」。

4 選擇您要遠端複製的內容。

5 若要變更排程，請執行下列其中一項工作：

- 勾選「**自動遠端複製**」讓管理伺服器選擇何時遠端複製資料。
  此選項可在兩個網站之間約每 2 小時定期進行自動遠端複製。
- 勾選「**按排程遠端複製**」以設定自訂排程。

6 按下「**確定**」。

遠端複製考量和最佳實務準則

請參閱第 645 頁的「立即遠端複製資料」。

請參閱第 635 頁的「設定網站和遠端複製」。

請參閱第 637 頁的「什麼是網站以及遠端複製如何運作？」。

請參閱第 640 頁的「決定是否要設定多個網站和遠端複製」。

請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

立即遠端複製資料

遠端複製通常會在您設定其他網站時根據預設排程進行。您可能希望立即進行遠端複製。具有較小 ID 號碼的網站會起始排程遠端複製。

如果在多部伺服器上使用了 Microsoft SQL Server 資料庫，則只能從該網站上的第一部伺服器開始遠端複製。

請參閱第 635 頁的「設定網站和遠端複製」。

請參閱第 643 頁的「如何安裝第二個網站用於遠端複製」。

隨時遠端複製資料

1. 在主控台中，按下**「管理員」**>**「伺服器」**。
2. 在**「伺服器」**>**「本機網站」**下，展開**「遠端複製夥伴」**並選取網站。
3. 在**「工作」**下方，按下**「立即遠端複製」**。
4. 按下**「是」**。
5. 按下**「確定」**。

刪除網站

在 Symantec Endpoint Protection Manager 中刪除遠端複製夥伴會中斷夥伴關係，但不會解除安裝管理伺服器軟體或刪除第二個網站。

如果移除遠端據點中的管理伺服器，您需要手動從所有網站中刪除它。將軟體從某個管理伺服器主控台中解除安裝，並不會使圖示從其他主控台上的**「伺服器」**窗格中消失。

請參閱第 129 頁的「在升級前後停用遠端複製和還原遠端複製」。

刪除網站

1. 在主控台中，按下**「管理員」**>**「伺服器」**>**「本機網站」**，展開**「遠端複製夥伴」**，於遠端複製夥伴上按下滑鼠右鍵，然後按下**「刪除遠端複製夥伴」**。
2. 在**「遠端據點」**下的網站上按下滑鼠右鍵，然後按下**「刪除遠端據點」**。
3. 按下**「是」**。

請參閱第 635 頁的「設定網站和遠端複製」。

39

準備進行災難復原

本章包含以下主題：

災難復原最佳實務準則

若要準備在發生硬體故障或資料庫損毀後復原，您應該備份安裝 Symantec Endpoint Protection Manager 後所收集的資訊。

準備進行災難復原

執行災難復原

準備進行災難復原

表 39-1 準備災難復原時的重要工作

步驟	敘述
步驟 1：備份資料庫	定期備份資料庫 (最好每週備份一次)。 依據預設，資料庫備份資料夾會儲存到以下預設位置： `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup` 備份檔案命名為 *date_timestamp*.zip。 請參閱第 648 頁的「備份資料庫和日誌」。
步驟 2：備份災難復原檔案	復原檔案包括加密密碼、金鑰庫檔案網域 ID、憑證檔案、授權檔及通訊埠編號。依據預設，此檔案位於以下目錄中： `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip` 復原檔案僅儲存預設網域 ID。如果您有多個網域，則復原檔案不會儲存該資訊。如果需要執行災難復原，您必須再次新增網域。 請參閱第 264 頁的「新增網域」。
步驟 3：更新或備份伺服器憑證 (選擇性)	如果將自我簽署憑證更新為不同的憑證類型，則管理伺服器會建立新的復原檔案。由於復原檔案具有時間戳記，因此您可以分辨出哪一個檔案是最新的檔案。 請參閱第 612 頁的「更新或還原伺服器憑證」。 請參閱第 649 頁的「備份伺服器憑證」。
步驟 4：將管理伺服器的 IP 位址和主機名稱儲存到文字檔 (選擇性)	如果您發生嚴重的硬體錯誤，必須使用原始管理伺服器的 IP 位址和主機名稱來重新安裝管理伺服器。 請將 IP 位址和主機名稱新增至文字檔，例如：`Backup.txt`。
步驟 5：在離站的安全位置儲存備份資料	將您在先前步驟中所備份的檔案複製到另一台電腦

執行災難復原

表 39-2 列出在發生硬體故障或資料庫損毀時復原 Symantec Endpoint Protection 環境的步驟。

在執行這些步驟之前，請確保您已建立備份和復原檔案。

表 39-2 執行災難復原的程序

步驟	動作
步驟 1：使用災難復原檔案重新安裝 Symantec Endpoint Protection Manager。	藉由重新安裝管理伺服器，您可以復原初始安裝後儲存的檔案。 請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。 如果您在不同的電腦上重新安裝 Symantec Endpoint Protection Manager，而且沒有使用災難復原檔案，則必須產生新的伺服器憑證。 請參閱第 651 頁的「產生新的伺服器憑證」。
步驟 2：還原資料庫。	無論有沒有資料庫備份，您都可以還原資料庫。 請參閱第 652 頁的「還原資料庫」。
步驟 3：重新啟用聯邦資訊處理標準 (FIPS) 140-2 法規遵循。(選擇性)	如果您使用遵從 FIPS 的 Symantec Endpoint Protection 版本並且啟用遵從 FIPS，那麼在復原 Symantec Endpoint Protection Manager 之後，您必須重新啟用遵從 FIPS。 此設定未儲存在災難復原檔案中。

請參閱第 85 頁的「備份您的授權檔」。

請參閱第 617 頁的「匯出和匯入伺服器設定」。

請參閱：Symantec Endpoint Protection 12.1 災難復原最佳實務準則。

備份資料庫和日誌

賽門鐵克建議您，至少每週備份一次資料庫。您應將備份檔案儲存於另一部電腦內。

依據預設，備份檔案儲存在下列資料夾中：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup`。

備份會放入 .zip 檔案中。根據預設，備份資料庫檔案命名為 *date_timestamp*.zip，即備份執行日期。

附註：避免將備份檔案儲存於產品安裝目錄內。否則移除產品時將一併移除備份檔案。

日誌資料不會備份，除非架構 Symantec Endpoint Protection Manager 來加以備份。如果不備份日誌，則備份期間只會儲存日誌架構選項。您可以使用備份還原資料庫，但資料庫的日誌在還原之後將不會有任何資料。

您可以保留多達 10 個版本的網站備份。如果選擇保留多個版本，請確定有足夠的磁碟空間可存放所有資料。

您可以在備份期間和備份之後，於「系統日誌」以及備份資料夾查看狀態。

您可以立即備份資料庫，也可以排程自動備份。您可以備份內嵌資料庫或架構為 Symantec Endpoint Protection Manager 資料庫的 Microsoft SQL Server 資料庫。

請參閱第 621 頁的「排程自動資料庫備份」。

請參閱第 646 頁的「災難復原最佳實務準則」。

備份資料庫和日誌

1. 在執行 Symantec Endpoint Protection Manager 之電腦的**「開始」**功能表上，按下**「所有程式」> Symantec Endpoint Protection Manager >「Symantec Endpoint Protection Manager 工具」>「資料庫備份及還原」**。
2. 在**「資料庫備份與還原」**對話方塊中，按下**「備份」**。
3. 在**「備份資料庫」**對話方塊中，選擇性勾選**「備份日誌」**，然後按下**「是」**。
4. 按下**「確定」**。
5. 資料庫備份完畢後，按**「結束」**。
6. 複製備份的資料庫檔案至另一部電腦。

從主控台內備份資料庫和日誌

1. 在主控台中，按下**「管理員」>「伺服器」**。
2. 在**「伺服器」**下方，按下**「本機網站 (我的網站)」>「本地主機」**。
3. 在**「工作」**下方，按下**「立即備份資料庫」**。
4. 在**「備份資料庫」**對話方塊中，選擇性勾選**「備份日誌」**，然後按下**「是」**。
5. 按下**「確定」**。
6. 按下**「關閉」**。

備份伺服器憑證

您應該備份私密金鑰與憑證，以便在管理伺服器上的電腦遭到毀損時使用。

初始安裝期間，會備份 JKS 金鑰儲存檔案。此外也會備份名為 `server_timestamp.xml` 的檔案。JKS 金鑰儲存檔案包含伺服器的私密和公開金鑰組以及自我簽署憑證。

備份伺服器憑證

1. 在主控台中，按下**「管理員」**，再按下**「伺服器」**。
2. 在**「伺服器」**下方，按下要備份其伺服器憑證的管理伺服器。
3. 在**「工作」**下方，按下**「管理伺服器憑證」**，然後按**「下一步」**。
4. 在**「管理伺服器憑證」**面板中，按下**「備份伺服器憑證」**，然後按**「下一步」**。

5 在「**備份伺服器憑證**」面板中，按下「**瀏覽**」以指定備份資料夾，然後按下「**開啟**」。

請注意，管理伺服器憑證會備份到相同的資料夾中。

6 在「**備份伺服器憑證**」面板中，按下「**下一步**」。

7 按下「**完成**」。

請參閱第 608 頁的「關於伺服器憑證」。

請參閱第 651 頁的「產生新的伺服器憑證」。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

重新安裝或重新架構 Symantec Endpoint Protection Manager

如果需要重新安裝或重新架構管理伺服器，您可以使用災難復原檔案匯入所有設定。 您可以將軟體重新安裝在同一台電腦的同一個安裝目錄中。Symantec Endpoint Protection Manager 會在安裝期間建立復原檔案。您也可以使用這個程序重新架構現有站台，或安裝其他用於複寫的站台。

請參閱第 646 頁的「災難復原最佳實務準則」。

重新安裝管理伺服器

1 移除現有管理伺服器。

2 從安裝檔案安裝伺服器。

請參閱第 36 頁的「安裝 Symantec Endpoint Protection Manager」。

3 在「**歡迎使用**」面板中，確保勾選「**使用還原檔案還原與之前已部署用戶端的通訊**」選項，再按「**下一步**」。

依據預設，復原檔案位於：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup`。復原檔案會將您的用戶端重新連線至 Symantec Endpoint Protection Manager。

4 遵照每個面板的指示進行。 預設設定適用於大多數情況。 如果重新安裝的伺服器連線至現有資料庫，則要將資料庫設定變更為現有資料庫的設定。

必要時，也可還原資料庫。 不過，如果 Symantec Endpoint Protection Manager 資料庫位於另一部電腦或未受影響，則不需要還原資料庫。

請參閱第 652 頁的「還原資料庫」。

重新架構管理伺服器

1 若要重新架構管理伺服器，請按下**「開始」>「所有程式」> Symantec Endpoint Protection Manager >「Symantec Endpoint Protection Manager 工具」>「管理伺服器架構精靈」**。

2 選取下列其中一個選項：

- 若要在現有的站台上重新架構管理伺服器，請按下**「重新架構管理伺服器」**。
- 若要重新架構管理伺服器透過現有的站台複寫資料，請按下**「重新架構管理伺服器透過不同站台複寫」**。
  此選項會將本機安裝的管理伺服器重新架構為建立新站台並透過網路中的其他現有站台複寫資料。 此外，如果您擁有兩個非複寫站台，使用此選項可將其中一個轉換為透過第二個站台複寫的站台。

附註：如果保留**「使用還原檔案還原與之前已部署用戶端的通訊」**為勾選狀態，安裝會繼續。 但是，會忽略還原檔案中的預設網域 ID，並使用複寫夥伴的網域 ID。 完成重新組態之後，現有用戶端可能會因為網域 ID 發生變更而無法連線。

---

3 遵照每個面板的指示進行。

請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。

產生新的伺服器憑證

如果伺服器的 IP 位址或主機名稱發生變更，或私密金鑰遭受破壞，請為 Symantec Endpoint Protection Manager 產生新的伺服器憑證。

依據預設，用戶端伺服器通訊取決於伺服器憑證驗證。如果產生新的伺服器憑證，則此驗證失敗且通訊中斷。開始執行此程序之前，請遵循更新憑證的最佳實務準則。

請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。

產生新的伺服器憑證

1 在主控台中，按下**「管理員」**，再按下**「伺服器」**。

2 在**「伺服器」**下方，按下管理伺服器。

3 在**「工作」**下方，按下**「管理伺服器憑證」**，然後按**「下一步」**。

4 在**「管理伺服器憑證」**面板中，按下**「產生新的伺服器憑證」**。確保已勾選**「產生新的金鑰」**，然後按**「下一步」**。

「產生新的金鑰」會產生具有新金鑰組 (公開和私密金鑰) 的新憑證。如果取消勾選此選項，新憑證會使用與之前相同的金鑰組，這樣一來會在金鑰組遭受破壞時降低 Symantec Endpoint Protection Manager 伺服器安全性設定檔。

5 按下「**是**」，然後按「**下一步**」。

6 您必須重新啟動下列服務以使用新的憑證：

- Symantec Endpoint Protection Manager 服務
- Symantec Endpoint Protection Manager Webserver 服務。
- Symantec Endpoint Protection Manager API 服務

請參閱第 128 頁的「停止及啟動管理伺服器服務」。

請參閱第 661 頁的「停止和啟動 Apache Web 伺服器」。

下次您登入 Symantec Endpoint Protection Manager 時，系統會要求您信任新的憑證。

請參閱第 258 頁的「關於接受 Symantec Endpoint Protection Manager 的自我簽署伺服器憑證」。

請參閱第 40 頁的「登入 Symantec Endpoint Protection Manager 主控台」。

還原資料庫

如果資料庫損毀或需要執行災難復原，您可以還原資料庫。若要還原資料庫，您必須先備份資料庫。

請參閱第 648 頁的「備份資料庫和日誌」。

您必須使用備份資料庫所用的相同 Symantec Endpoint Protection Manager 版本還原資料庫。您可以在本來安裝資料庫的同一部電腦或是不同的電腦上還原資料庫。

還原資料庫可能需要數分鐘的時間才能完成。

使用資料庫備份還原資料庫

1 停止管理伺服器服務。

請參閱第 128 頁的「停止及啟動管理伺服器服務」。

2 在「**開始**」功能表上，按下「**所有程式**」**> Symantec Endpoint Protection Manager >** 「**Symantec Endpoint Protection Manager 工具**」**>**「**資料庫備份及還原**」。

3 在「**資料庫備份及還原**」對話方塊中，按下「**還原**」。

4 按下「**是**」確認還原資料庫。

5 在「**還原網站**」對話方塊中，選取備份的資料庫檔案，然後按下「**確定**」。

尋找備份資料庫時製作的備份資料庫檔案複本。備份的資料庫檔案會預設命名為 *date_timestamp*.zip。

6 按下「**確定**」。

7 按下「**結束**」。

8 重新啟動管理伺服器服務。

不使用資料庫備份還原資料庫

在下列情況下，您可能需要不使用資料庫備份還原資料庫：

- 您嘗試過並且無法重設管理員密碼。
  請參閱第 255 頁的「Symantec Endpoint Protection Manager 密碼遺失後重設」。
- 內嵌的資料庫服務不會啟動。
- 您未進行資料庫備份，而資料庫已損毀。

不使用資料庫備份還原資料庫

1. 備份政策檔。

   您在重新安裝資料庫之後匯入了匯出的政策檔。

   請參閱第 277 頁的「匯出和匯入個別 Endpoint Protection 政策」。

2. 如果您有多個網域，請建立名為 SEPBackup.txt 的文字檔案，並新增任何網域 ID。(選擇性)

   若要儲存管理伺服器資訊，請將管理伺服器的 IP 位址和主機名稱新增至該檔案。

3. 停止管理伺服器服務。

   請參閱第 128 頁的「停止及啟動管理伺服器服務」。

4. 使用「管理伺服器組態精靈」和復原檔案來重新架構管理伺服器。

   請參閱第 650 頁的「重新安裝或重新架構 Symantec Endpoint Protection Manager」。

5. 在重新架構的 Symantec Endpoint Protection Manager 上，於以下檔案中：

   SEPM_Install/tomcat/etc/conf.properties

   SEPM_Install 的預設值為 C:/Program files (x86)/Symantec/Symantec Endpoint Protection Manager。

   變更：

   `scm.agent.groupcreation=false` 變更為 `scm.agent.groupcreation=true`

   此編輯可自動建立用戶端群組。否則，用戶端會在登入時重新出現在預設群組中。

用戶端可與 Symantec Endpoint Protection Manager 通訊，但只有在其下次登入後才會重新出現在主控台中。

部分 9

Symantec Endpoint Protection Manager 疑難排解

40

安裝與通訊問題疑難排解

本章包含以下主題：

- 疑難排解 Symantec Endpoint Protection
- 使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解
- 找出安裝的失敗點
- Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解
- Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題疑難排解
- 用戶端與伺服器通訊檔案

疑難排解 Symantec Endpoint Protection

表 40-1 顯示了在安裝和使用 Symantec Endpoint Protection 時可能會遇到的最常見問題。

表 40-1 您可以解決的常見問題

工作	敘述
解決安裝問題	您可以下載並執行 Symantec Diagnostic Tool (SymDiag) 來驗證電腦是否已做好安裝準備。此工具是透過管理伺服器和用戶端上的「說明」，由 Symantec 支援網站提供。 請參閱第 656 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。 請參閱第 657 頁的「找出安裝的失敗點」。

工作	敘述
處理病毒疫情 (爆發)	您可以防止威脅攻擊網路上的電腦。 請參閱第 347 頁的「阻止和處理病毒和間諜軟體對用戶端電腦的攻擊」。 請參閱第 348 頁的「移除病毒和安全風險」。 如果確實有威脅在攻擊用戶端電腦，您可以識別威脅並做出回應。 網路上的病毒移除和疑難排解。
內容更新問題疑難排解	如果 Symantec Endpoint Protection Manager 或用戶端未正確更新最新病毒定義檔，請參閱下列文章： 疑難排解 Endpoint Protection Manager 的 LiveUpdate 和定義檔問題 Symantec Endpoint Protection：LiveUpdate 疑難排解流程圖
解決通訊問題	Symantec Endpoint Protection 的所有元件之間的通訊通道都必須處於開啟狀態。這些通道包括下列項目：伺服器到用戶端、伺服器到資料庫以及伺服器和用戶端到內容傳送元件 (如 LiveUpdate) 之間的通道。 請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。 請參閱第 664 頁的「Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題疑難排解」。 群組更新提供者的最佳實務準則和疑難排解
執行災難復原	發生資料庫損毀或硬體故障時，如果您有資料庫備份檔案，則可以還原資料庫的最新快照。 請參閱第 646 頁的「災難復原最佳實務準則」。
減少資料庫空間	如果資料庫變得太大，您可以挪出資料庫中更多的可用空間。 請參閱第 618 頁的「維護資料庫」。
報告問題疑難排解	您可以解決各種報告和日誌問題。 請參閱第 668 頁的「報告問題疑難排解」。
疑難排解複寫問題	Symantec Endpoint Protection 的複寫疑難排解流程圖

請參閱第 718 頁的「Symantec Endpoint Protection 隨附的工具有哪些？」。

使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解

您可以下載公用程式來診斷安裝與使用 Symantec Endpoint Protection Manager 或 Symantec Endpoint Protection 用戶端遇到的常見問題。

支援工具可幫助您解決下列問題：

- 迅速和準確地識別已知的問題。
- 當工具識別問題後，工具會將您重新導向到相應資源以讓您自行解決問題。
- 如果問題未解決，工具會讓您輕鬆將資料提交給技術支援以進行進一步診斷。

使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解

1 執行下列其中一項工作：

- 請參閱：下載 Symantec Diagnostic Tool (SymDiag) 以偵測賽門鐵克產品問題
- 在 Symantec Endpoint Protection Manager 或用戶端中，按下**「說明」>「下載 Symantec Diagnostic Tool」**

2 按照畫面上的指示進行操作。

找出安裝的失敗點

Windows Installer 和「推送部署精靈」會建立日誌檔，這些日誌檔可用於確認安裝是否成功。日誌檔會列出成功安裝的元件，並提供安裝套件的各種詳細資訊。您可使用日誌檔來協助辨識會造成安裝失敗的元件或動作。如果您無法判斷安裝失敗的原因，就必須保留日誌檔。如果需要，請將這個檔案提供給賽門鐵克技術支援。

附註：每次執行安裝封裝時，日誌檔都會被覆寫。

找出安裝的失敗點

1 使用文字編輯器，開啟安裝程式所產生的日誌檔。

2 若要尋找失敗，請搜尋以下項目：

```
Value 3
```

在此項目所在那一行前面的動作，最有可能是造成失敗的動作。在這個項目後面出現的各行，是因安裝不成功而傳回的安裝元件。

請參閱第 100 頁的「選擇使用用戶端部署精靈安裝用戶端的方法」。

Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解

如果用戶端與伺服器之間的通訊出現問題，您應該先檢查確定網路沒有任何問題。您也應該檢查網路連線，若仍無法解決問題，才電洽「賽門鐵克技術支援」。

您可以透過多種方式，檢查用戶端與管理伺服器之間的通訊。

表 40-2 檢查管理伺服器與用戶端之間的連線

檢查的項目	解決方案
查看用戶端是否連線到管理伺服器	可下載並檢視用戶端上的問題疑難排解檔案，確認通訊設定。 請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。 請參閱第 659 頁的「在用戶端電腦上檢查與管理伺服器的連線」。 請參閱第 659 頁的「在用戶端上使用疑難排解檔案調查防護問題 在用戶端上」。
測試用戶端與管理伺服器之間的連線	您可以執行幾項工作來檢查用戶端與管理伺服器之間的連線。 ■ 請參閱第 660 頁的「啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器」。 ■ 從用戶端電腦測試與管理伺服器的連線。 請參閱第 661 頁的「使用 ping 指令測試與管理伺服器的連線」。 ■ 在用戶端電腦上使用網頁瀏覽器連線到管理伺服器。 請參閱第 661 頁的「使用瀏覽器測試與 Symantec Endpoint Protection 用戶端上的 Symantec Endpoint Protection Manager 的連線」。
檢查管理伺服器是否使用正確的伺服器憑證	如果您重新安裝了 Symantec Endpoint Protection Manager，請檢查是否已套用正確的伺服器憑證。如果管理伺服器使用不同的伺服器憑證，伺服器仍可下載內容，但用戶端會無法讀取內容。如果管理伺服器使用了錯誤的伺服器憑證，您必須加以更新。 請參閱第 612 頁的「更新或還原伺服器憑證」。 請參閱第 609 頁的「更新伺服器憑證和維護用戶端伺服器連線的最佳實務準則」。 您可以透過檢查下列項目，驗證管理伺服器是否使用錯誤的伺服器憑證： ■ 用戶端沒有在工作列中顯示綠點，表示它未與管理伺服器通訊。 請參閱第 138 頁的「檢查用戶端是否已連線至管理伺服器且受保護」。 ■ 用戶端未從管理伺服器接收政策更新。 ■ 管理伺服器顯示它未與用戶端連線。 請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。
檢查網路是否有問題	您應該檢查下列項目，以確認網路沒有任何問題： ■ 可先測試用戶端與管理伺服器之間的連線。如果用戶端電腦無法測試與管理伺服器的連線，或者無法以 Telnet 連線到管理伺服器，您應該確認用戶端的 DNS 服務是否正常。 ■ 檢查用戶端的路由路徑。 ■ 檢查管理伺服器是否存在網路問題。 ■ 檢查 Symantec Endpoint Protection 防火牆 (或任何第三方防火牆) 是否造成任何網路問題。

檢查的項目	解決方案
檢查用戶端上的除錯日誌	您可以使用用戶端上的除錯日誌，判斷用戶端是否有通訊問題。 請參閱第 662 頁的「檢查用戶端電腦上的除錯日誌」。 請參閱第 662 頁的「檢查管理伺服器上的收件匣日誌」。
復原失去的用戶端通訊	用戶端若失去與管理伺服器之間的通訊，可使用工具復原通訊檔案。 請參閱第 663 頁的「使用 SylinkDrop 工具還原用戶端伺服器通訊設定」。

如果 Symantec Endpoint Protection Manager 顯示記錄錯誤或 HTTP 錯誤碼，請參閱以下文章：Symantec Endpoint Protection Manager 通訊疑難排解。

在用戶端電腦上檢查與管理伺服器的連線

如果您具有受管用戶端，您可以檢查與管理伺服器的連線。如果您沒有連線到管理伺服器，您可以要求用戶端連線。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

在用戶端電腦上檢查與管理伺服器的連線

1. 在「**狀態**」頁面上，按下「**說明**」>「**疑難排解**」。
2. 在「**疑難排解**」對話方塊中，按「**連線狀態**」。
3. 在「**連線狀態**」窗格中，您可以看到最後嘗試的連線和最後成功的連線。
4. 若要重新建立與管理伺服器的連線，請按下「**立即連線**」。

在用戶端上使用疑難排解檔案調查防護問題 在用戶端上

若要檢查用戶端問題，您可以查看用戶端電腦上的 `Troubleshooting.txt` 檔案。`Troubleshooting.txt` 檔案的資訊包括政策、病毒定義檔以及其他用戶端相關資料。

賽門鐵克技術支援可能會要求您以電子郵件方式寄送 `Troubleshooting.txt` 檔案。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

從用戶端匯出疑難排解檔案

1. 在用戶端電腦中開啟用戶端。
2. 在用戶端中按「**說明**」>「**疑難排解**」。
3. 在「**管理**」窗格的「**疑難排解資料**」底下按「**匯出**」。

4 在「**另存新檔**」對話方塊中，接受預設的疑難排解檔案名稱或輸入新的檔案名稱，然後再按「**儲存**」。

您可以將檔案儲存在桌面或指定資料夾。

5 利用文字編輯器，開啟 `Troubleshooting.txt` 查看內容。

啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器

您可以檢視管理伺服器上的 Apache HTTP 伺服器存取日誌，檢查用戶端是否連線到管理伺服器。如果用戶端有連線，表示用戶端的連線問題可能不是網路方面的問題。網路問題包括防火牆攔截存取或網路之間無法連線。

您必須先啟用 Apache HTTP 伺服器存取日誌才能檢視日誌。

附註：請在檢視完畢後停用日誌，因為日誌會佔用不必要的 CPU 資源和硬碟空間。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

附註：*SEPM_Install* 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

啟用 Apache HTTP 伺服器存取日誌

1 在文字編輯器中，開啟檔案 *`SEPM_Install`*`\apache\conf\httpd.conf`。

2 在 `httpd.conf` 檔案中，移除以下文字字串中的井字號 (#)，然後儲存檔案：

```
#CustomLog "logs/access.log" combined
```

3 停止並重新啟動 Symantec Endpoint Protection Manager 服務和 Apache HTTP 伺服器：

請參閱第 128 頁的「停止及啟動管理伺服器服務」。

請參閱第 661 頁的「停止和啟動 Apache Web 伺服器」。

檢視 Apache HTTP 伺服器存取日誌

1 在管理伺服器上，開啟檔案 *`SEPM_Install`*`\apache\logs\access.log`。

2 尋找用戶端電腦的 IP 位址或主機名稱，這表示用戶端已連線到 Apache HTTP 伺服器。

3 停用 Apache HTTP 伺服器存取日誌。

停止和啟動 Apache Web 伺服器

當您安裝 Symantec Endpoint Protection Manager 時，它會安裝 Apache Web 伺服器。 Apache Web 伺服器會執行成為自動服務。 您可能需要停止並重新啟動 Web 伺服器，才能啟用 Apache HTTP 伺服器存取日誌。

請參閱第 660 頁的「啟用並檢視存取日誌，以檢查用戶端是否連線到管理伺服器」。

停止 Apache Web 伺服器

- 從指令提示處輸入：

```
net stop semwebsrv
```

啟動 Apache Web 伺服器

- 從指令提示處輸入：

```
net start semwebsrv
```

使用 ping 指令測試與管理伺服器的連線

您可以嘗試從用戶端電腦使用 ping 指令，測試管理伺服器的連線。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

使用 ping 指令測試與管理伺服器的連線

1. 在用戶端上，開啟命令提示字元。
2. 輸入 ping 指令。例如：

   ping *name*

   其中 *name* 是管理伺服器的電腦名稱。您可以使用伺服器 IP 位址取代電腦名稱。在這兩種狀況下，指令應該都會傳回正確的伺服器 IP 位址。

   如果 ping 指令未傳回正確位址，請確認用戶端的 DNS 服務並檢查其路由路徑。

使用瀏覽器測試與 Symantec Endpoint Protection 用戶端上的 Symantec Endpoint Protection Manager 的連線

您可以在用戶端電腦上使用網頁瀏覽器測試管理伺服器與用戶端之間的連線。 此方法有助於判斷問題是出於連線或網路，還是用戶端本身。

您也可以使用下列方法檢查管理伺服器與用戶端電腦的之間連線：

- 查看 Symantec Endpoint Protection 用戶端狀態圖示是否顯示綠點。
  請參閱第 140 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。
- 檢查 Symantec Endpoint Protection 用戶端的連線狀態。
  請參閱第 659 頁的「在用戶端電腦上檢查與管理伺服器的連線」。

使用瀏覽器測試與 Symantec Endpoint Protection 用戶端上的 Symantec Endpoint Protection Manager 的連線

1. 在用戶端電腦上開啟網頁瀏覽器，例如 Internet Explorer。
2. 在瀏覽器指令行中，輸入下列指令：

   http://*SEPMServer*:8014/secars/secars.dll?hello,secars

   其中 *SEPMServer* 是管理伺服器的 DNS 名稱、NetBIOS 名稱或 IP 位址。

   IP 位址包括 IPv4 和 IPv6。您必須用方括弧括住 IPv6 位址：**http://[*SEPMServer*]:*通訊埠編號***
3. 當網頁出現時，尋找是否有下列其中一種結果：
   - 如果出現 **OK** 一字，表示用戶端電腦已連線到管理伺服器。請檢查用戶端本身是否有問題。
   - 如果未出現 **OK** 一字，表示用戶端電腦未連線到管理伺服器。 請檢查用戶端的網路連線以及用戶端電腦上是否正在執行網路服務。確認用戶端的 DNS 服務並檢查其路由路徑。

     請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

檢查用戶端電腦上的除錯日誌

您可以檢查用戶端上的除錯日誌。如果用戶端與管理伺服器之間的通訊出現問題，日誌會顯示連線問題的狀態訊息。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

您可以使用下列方法檢查除錯日誌：

- 在用戶端的「說明及支援」功能表中，按下「疑難排解」對話方塊中的**「編輯除錯日誌設定」**，然後輸入日誌的名稱。您可以接著按下**「檢視日誌」**。
- 您可以使用 Windows 登錄在用戶端上開啟除錯功能。
  您可以在下列位置找到 Windows 登錄機碼：
  HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

檢查管理伺服器上的收件匣日誌

您可以使用 Windows 登錄機碼，產生管理伺服器收件匣活動的日誌。修改 Windows 登錄機碼時，管理伺服器會產生日誌 (ersecreg.log 及 exsecars.log)。您可以檢視這些日誌，以解決用戶端與伺服器通訊的問題。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

請參閱第 662 頁的「檢查用戶端電腦上的除錯日誌」。

檢查管理伺服器上的收件匣日誌

1 在管理伺服器 HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM 下，將 DebugLevel 值設定為 3。

收件匣會出現在管理伺服器電腦上的下列預設位置：*SEPM_Install*\data\inbox\log

SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

2 使用「記事本」開啟日誌。

使用 SylinkDrop 工具還原用戶端伺服器通訊設定

Sylink.xml 檔案包含用戶端與 Symantec Endpoint Protection Manager 伺服器之間的通訊設定。如果用戶端失去與管理伺服器之間的通訊，則必須使用新的 Sylink.xml 檔案來取代舊的 Sylink.xml 檔案。SylinkDrop 工具會自動使用新的 Sylink.xml 檔案來取代用戶端電腦上的 Sylink.xml 檔案。

附註：您也可以重新部署用戶端安裝套件，藉此取代 Sylink.xml 檔案。請將此方法用於大量電腦、您實際上無法輕易存取的電腦或需要管理存取的電腦。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

執行 SylinkDrop 工具時，亦會執行下列工作：

- 將用戶端移轉/移動至新的網域或管理伺服器。
- 將無法在管理伺服器上修正的通訊損壞還原至用戶端。
- 將用戶端從一台伺服器移至另一台非遠端複製夥伴的伺服器。
- 將用戶端從一個網域移至另一個網域。
- 將非受管用戶端轉換為受管用戶端。

您可以使用工具來撰寫程序檔，以便修改大量的用戶端通訊設定。

請參閱第 108 頁的「關於受管和非受管用戶端」。

請參閱第 657 頁的「Symantec Endpoint Protection Manager 與 Symantec Endpoint Protection 用戶端之間的連線問題疑難排解」。

使用適用於 Windows 的 SylinkDrop 工具還原用戶端伺服器通訊設定

1 在主控台中，將連線至管理伺服器的群組通訊檔案匯出至您要用戶端電腦進行連線的伺服器。通訊檔案為 Sylink.xml 檔案。

請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

2 將通訊檔案複製到用戶端電腦。

您可以將檔案儲存到網路位置、透過電子郵件傳送給用戶端電腦的使用者，或是複製到抽取式媒體。

3 執行下列其中一項工作：

- 在來自 MySymantec 的完整產品安裝檔案中，找出 `Tools\SylinkDrop\SylinkDrop.exe`。
  請參閱 MySymantec 入門指南。
- 在執行管理伺服器的電腦上，找出 `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\`*`Version.Number`*`\Bin\SylinkDrop.exe`

您可以遠端執行工具，或是先儲存該工具，然後再於用戶端電腦執行該工具。如需指令行選項的相關資訊，請在 `\Tools\SylinkDrop` 資料夾中按下讀我檔。

4 在 **Sylink Drop** 對話方塊中，按下**「瀏覽」**找出您在步驟 2 中部署至用戶端電腦的 .xml 檔案。

5 按下**「更新 Sylink」**。

6 您看見確認對話方塊時，請按下**「確定」**。

7 在 **Sylink Drop** 對話方塊中，按下**「結束」**。

Symantec Endpoint Protection Manager 與主控台或資料庫之間的通訊問題疑難排解

如果 Symantec Endpoint Protection Manager 主控台或資料庫發生連線問題，您可能會看到下列其中一種症狀：

- 管理伺服器服務 (semsrv) 停止。
- 管理伺服器服務未處於啟動狀態。
- 「首頁」、「監視器」和「報告」頁面顯示 HTTP 錯誤。
- 「首頁」、「監視器」和「報告」頁面空白。
- 「首頁」、「監視器」和「報告」頁面顯示持續載入中的進度列，而未顯示任何內容。

上述所有問題在 Windows 事件日誌中均會顯示 Java -1 錯誤。 若要找出 Java -1 錯誤的確切原因，請查看 scm-server 日誌。 scm-server 日誌預設位於下列位置：

SEPM_Install\tomcat\logs\scm-server-0.log

SEPM_Install 的預設值為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager。

表 40-3 檢查與主控台或資料庫的連線

檢查的項目	敘述
測試資料庫與管理伺服器之間的連線。	您可以檢查管理伺服器與資料庫之間的通訊是否正常。 請參閱第 665 頁的「檢查與資料庫的連線」。
檢查管理伺服器的堆疊大小是否正確。	如果您無法登入管理伺服器的遠端主控台，則可能需要增加 Java 堆疊大小。 您也可能會在 scm-server 日誌中看到記憶體不足的訊息。 如需預設堆疊大小的詳細資訊，請參閱：決定安裝 Symantec Endpoint Protection Manager 期間所選取網路大小的預設設定
檢查管理伺服器是否未執行多個版本的 PHP。	您可以檢查管理伺服器是否執行多個使用不同版本 PHP 的軟體套件。 PHP 會檢查全域架構檔 (php.ini)。 如果有多個架構檔，您必須強制每個產品使用其本身的解譯器。 當每個產品使用其正確版本的 PHP 時，管理伺服器就能恢復正常運作。
檢視系統需求。	您可以檢查用戶端和管理伺服器是否在符合最低或建議系統需求的情況下執行。 如需最新系統需求，請參閱：所有端點防護版本的版本說明、新修正和系統需求

檢查與資料庫的連線

管理伺服器和資料庫可能無法正常進行通訊。請先檢查資料庫是否執行，然後測試伺服器與資料庫之間的連線。

如果管理伺服器執行內嵌 Sybase 資料庫，請執行下列步驟：

- 檢查 Symantec 內嵌資料庫服務是否執行，而且 dbsrv9.exe 程序是否接聽 TCP 通訊埠 2638。
- 測試 ODBC 連線。

如果管理伺服器執行遠端 SQL 資料庫，請執行下列動作：

- 檢查您在安裝和架構 Symantec Endpoint Protection Manager 時是否指定了具名實例。
- 檢查 SQL Server 是否執行而且正確架構。
- 檢查管理伺服器與 SQL 資料庫之間的網路連線是否正確。
- 測試 ODBC 連線。

檢查與內嵌資料庫的通訊

1. 在管理伺服器上，按下**「開始」>「控制台」>「系統管理工具」**。
2. 在**「系統管理工具」**對話方塊中，連按兩下**「資料來源 (ODBC)」**。
3. 在**「ODBC 資料來源管理員」**對話方塊中，按下**「系統 DSN」**。
4. 在**「系統 DSN」**標籤上，連按兩下 **SymantecEndpointSecurityDSN**。
5. 在 **ODBC** 標籤上，確定「資料來源名稱」下拉式清單是 SymantecEndpointSecurityDSN，然後輸入選用說明。
6. 按下**「登入」**。
7. 在**「登入」**標籤的**「使用者 ID」**文字方塊中，輸入 dba。
8. 在**「密碼」**文字方塊中，輸入資料庫的密碼。

   密碼是您在安裝管理伺服器時，為資料庫輸入的密碼。
9. 按下**「資料庫」**。
10. 在**「資料庫」**標籤的**「伺服器名稱」**文字方塊中，輸入：

    \\servername\instancename

    如果使用的是 Symantec Endpoint Protection Manager 英文版，請輸入預設值 sem5。否則，請將「伺服器名稱」文字方塊保留空白。
11. 在 **ODBC** 標籤上，按下**「測試連線」**並確認是否成功。
12. 按下**「確定」**。
13. 按下**「確定」**。

檢查與 SQL 資料庫的通訊

1. 在管理伺服器上，按下**「開始」>「控制台」>「系統管理工具」**。
2. 在**「系統管理工具」**對話方塊中，連按兩下**「資料來源 (ODBC)」**。
3. 在**「ODBC 資料來源管理員」**對話方塊中，按下**「系統 DSN」**。
4. 在**「系統 DSN」**標籤上，連按兩下 **SymantecEndpointSecurityDSN**。
5. 在**「伺服器」**下拉式清單中，檢查是否已選取正確的伺服器和實例。
6. 按**「下一步」**。
7. 在「登入 ID」中，輸入 sa。
8. 在**「密碼」**文字方塊中，輸入資料庫的密碼。

   密碼是您在安裝管理伺服器時，為資料庫輸入的密碼。
9. 按**「下一步」**，確定為預設資料庫選取 sem5。
10. 按**「下一步」**。

11 按下「**完成**」。

12 按下「**測試資料來源**」，然後查看結果是否如下：

```
TESTS COMPLETED SUCCESSFULLY!
```

用戶端與伺服器通訊檔案

用戶端與伺服器之間的通訊設定，以及其他用戶端設定，是儲存在用戶端電腦的檔案中。

表 40-4 用戶端檔案

檔案名稱	敘述
SerDef.dat	依照位置儲存通訊設定的加密檔案。每當使用者變更位置時，用戶端就會讀取 SerDef.dat 檔案並套用新位置所對應之適當的通訊設定。
sylink.xml	儲存全域通訊設定。此檔案僅供內部使用，且不應加以編輯，其包含 Symantec Endpoint Protection Manager 的設定。如果您編輯此檔案，大部分設定會在下一次用戶端連線到管理伺服器時，遭到管理伺服器的設定所覆寫。
SerState.dat	儲存使用者介面相關資訊的加密檔案，這些資訊包括用戶端畫面大小、是否顯示防網路和主機侵入的用戶端主控台，以及是否顯示 Windows 服務等。用戶端啟動時，會讀取此檔案並傳回與其停止前相同的使用者介面狀態。

41

報告問題疑難排解

本章包含以下主題：

- 報告問題疑難排解
- 變更檢視報告和日誌的逾時參數
- 在停用回送位址時存取報告頁面

報告問題疑難排解

使用報告時，請務必注意下列資訊：

- 報告與日誌的時間戳記 (含用戶端掃描時間) 會以使用者的本地時間為準。 報告資料庫所包含的事件則是以格林威治標準時間 (GMT) 為準。 當您建立報告時，GMT 值會轉換成您檢視報告所在電腦的當地時間。
- 若受管型用戶端與管理伺服器的時區不同，而且您使用**「設定特定日期」**過濾選項，則可能會發生無法預期的結果，而且可能影響用戶端與管理伺服器的資料與時間準確性。
- 如果您在伺服器上變更時區，請登出主控台後重新登入，以便在日誌和報告中看到正確的時間。
- 在某些情況下，報告資料不會與安全產品中所出現的事件一一對應。 發生不對應的情況是因為報告軟體會彙總安全性事件。
- 您可以將 SSL 與報告功能搭配使用，以增加安全性。 SSL 可確保用戶端和伺服器之間的機密性和資料的完整性，並可在兩者之間進行驗證。
  請參閱文章：在 Symantec Endpoint Protection Manager 與其用戶端之間啟用 SSL 通訊
- 報告中的風險類別資訊是從「賽門鐵克安全機制應變中心」網站取得的。 在 Symantec Endpoint Protection Manager 主控台能擷取此項資訊之前，您產生的任何報告在風險類別欄位中都會顯示為「不明」。
- 您產生的報告可提供網路中受威脅電腦的精準狀況。這些報告基於日誌資料，而非Windows登錄資料。

- 如果在執行含大量資料的報告時，出現資料庫錯誤，您可能要變更資料庫逾時參數。
請參閱第 669 頁的「 變更檢視報告和日誌的逾時參數」。
- 如果出現 CGI 或終止程序錯誤，您可能要變更其他逾時參數。
如需詳細資訊，請參閱下列文章中的下列文件：查詢大量資料時，SEPM Reporting 不回應或顯示逾時錯誤訊息。
- 如果您在電腦上停用回送位址，則不會顯示報告頁面。
請參閱第 670 頁的「在停用回送位址時存取報告頁面」。

變更檢視報告和日誌的逾時參數

如果檢視含有大量資料的報告或日誌時資料庫發生錯誤，您可以進行下列變更：

- 變更資料庫連線逾時時間
- 變更資料庫指令逾時時間

這些報告預設值如下：

- 連線逾時時間為 300 秒 (5 分鐘)
- 指令逾時時間為 300 秒 (5 分鐘)

變更 Reporter.php 中的資料庫逾時值

1 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources

2 以諸如「記事本」的純文字編輯器來開啟 Reporter.php 檔案。

3 找到 **$CommandTimeout** 和 **$ConnectionTimeout** 行，並增加值 (以秒為單位)。如果其中一行不存在，請建立它。例如，若要將逾時期間增加到 10 分鐘，請將此行變更為以下值：

```
$CommandTimeout = 600;

$ConnectionTimeout = 600;
```

在下列字元之前新增這些新行：`?>`

4 儲存並關閉 Reporter.php 檔案。

附註：如果您指定零值，或使欄位留白，則會使用預設設定。

如果收到 CGI 或終止程序錯誤，您可能要變更下列參數：

- Php.ini 檔案中的 max_execution_time 參數

- httpd.conf 檔案中的 Apache 逾時參數 FcgidIOTimeout、FcgidBusyTimeout 和 FcgidIdleTimeout

變更 Php.ini 中的 max_execution_time 參數

1. 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：

   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php
2. 在 Php.ini 檔案上按下滑鼠右鍵，再按下**「內容」**。
3. 在**「一般」**標籤上，取消勾選**「唯讀」**。
4. 按下**「確定」**。
5. 以諸如「記事本」的純文字編輯器來開啟 Php.ini 檔案。
6. 找到 **max_execution_time** 項目並增加值 (以秒為單位)。 例如，若要將逾時時間增加到 10 分鐘，請將此行變更為以下值：

   max_execution_time=600
7. 儲存並關閉 Php.ini 檔案。
8. 在 Php.ini 檔案上按下滑鼠右鍵，再按下**「內容」**。
9. 在**「一般」**標籤上，勾選**「唯讀」**。
10. 按下**「確定」**。

變更 httpd.conf 中的 Apache 逾時參數

1. 瀏覽至 Symantec Endpoint Protection Manager 伺服器的下列預設資料夾：

   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf
2. 以諸如「記事本」的純文字編輯器來開啟 httpd.conf 檔案。
3. 找到下面這幾行並增加值 (以秒為單位)：
   - FcgidIOTimeout 1800
   - FcgidBusyTimeout 1800
   - FcgidIdleTimeout 1800
4. 儲存並關閉 httpd.conf 檔案。

在停用回送位址時存取報告頁面

如果您在電腦上停用回送位址，則報告頁面不會顯示。如果您嘗試登入 Symantec Endpoint Protection Manager 主控台，或嘗試存取報告功能，您會看見下列錯誤訊息：

無法與報告元件進行通訊

「首頁」、**「監視器」**以及**「報告」**頁面空白；**「政策」**、**「用戶端」**以及**「管理員」**頁面的外觀和功能正常。

若要使**「報告」**元件在已停用回送位址時顯示，必須將文字 localhost 與電腦的 IP 位址相關聯。您可以編輯 Windows 主機檔案，使本機主機與 IP 位址相關聯。

請參閱第 548 頁的「從獨立式網頁瀏覽器登入報告」。

在執行 Windows 的電腦上使本機主機與 IP 位址相關聯

1. 將目錄變更至主機檔案的位置。

   主機檔案預設位於 *%SystemRoot%*\system32\drivers\etc

2. 使用編輯器開啟 hosts 檔案。

3. 將下列一行新增至主機檔案：

   IPAddress **localhost #***以登入報告功能*

   其中 *IPAddress* 需取代為您電腦的 IP 位址。您可以在井字符號 (#) 後加上任何需要的註解。例如，您可以鍵入下列一行：

   192.168.1.100 localhost # 此項目是我的主控台電腦的 IPv4 位址

   2001:db8:85a3::8a2e:370:7334 localhost # 此項目是我的主控台電腦的 IPv6 位址

4. 儲存並關閉檔案。

42

使用 Power Eraser 針對持續性的嚴重威脅進行疑難排解

本章包含以下主題：

從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項

Power Eraser 提供主動掃描和分析，以協助解決嚴重感染的 Windows 電腦的問題。由於 Power Eraser 分析是主動的，因此它有時會標記您可能需要的關鍵檔案。Power Eraser 產生的誤報數可能超過病毒和間諜軟體所掃描到的誤報數。

警告：您應只在緊急的狀況下才執行 Power Eraser，例如當電腦出現不穩定或存在持續性問題時。通常情況下，在單一電腦或一小組電腦上執行 Power Eraser。您不應同時執行其他應用程式。在某些情況下，定期掃描事件會警示您執行 Power Eraser 分析。

從 Symantec Endpoint Protection Manager 使用強力清除器與在本機使用 SymDiag 工具執行強力清除器的差異

您可以從 Windows 用戶端上的管理主控台遠端執行 Power Eraser。Symantec Endpoint Protection 不包括直接從用戶端啟動 Power Eraser 的選項。但是，用戶端電腦上的使用者可以下載 SymDiag 工具並從該工具執行強力清除器。

- 如果使用 SymDiag 工具，則強力清除器偵測到的項目不會出現在 Symantec Endpoint Protection Manager 日誌中。
- 當您從主控台執行強力清除器時，強力清除器不會檢查使用者特定載入點、註冊和資料夾，但是 SymDiag 工具卻會。

附註：請確保您不會同時從主控台執行強力清除器，又在本機使用 SymDiag 工具執行強力清除器。否則，可能會對電腦效能產生負面的影響。

Power Eraser 耗用大量的電腦資源。如果您在某台電腦上多次執行 Power Eraser，則 Power Eraser 檔案也會耗用該電腦上的大量空間。在每次分析期間，Power Eraser 都會將偵測資訊儲存在存放於 Symantec Endpoint Protection 應用程式資料夾中的檔案。用戶端清除日誌時會清除這些檔案。

Power Eraser 與病毒和間諜軟體掃描有何不同

Power Eraser 與定期掃描的差異體現在以下方面：

- 與完整掃描不同的是，Power Eraser 不會掃描電腦上的每個檔案。Power Eraser 會檢查載入點和載入點磁碟位置，以及執行中的程序和已安裝的服務。
- Power Eraser 偵測不會出現在「隔離」中。
- Power Eraser 優先於病毒和間諜軟體掃描。當您執行 Power Eraser 時，Symantec Endpoint Protection 會取消進行中的所有病毒和間諜軟體掃描。
- Power Eraser 不會自動矯正偵測。您必須檢閱掃描日誌或風險日誌中的偵測清單，並從日誌中選取動作。您可以選擇移除偵測或將偵測標示為安全 (略過)。您也可以還原 (復原) 已移除的偵測。

Power Eraser 可以在正常模式或 Rootkit 模式下執行。Rootkit 模式需要在掃描啟動之前重新啟動。此外，如果您選擇移除任何 Power Eraser 偵測，則必須重新啟動電腦才能完成矯正。

需要執行 Power Eraser 時所執行的高階步驟概觀

從主控台執行 Power Eraser 時，請執行兩個高階步驟：

- 在一台電腦或一小組電腦上啟動 Power Eraser 分析。Power Eraser 不會自動矯正任何偵測，因為可能會發生誤報。
- 使用風險日誌或掃描日誌檢閱 Power Eraser 偵測，並手動要求 Power Eraser 移除任何您判斷為威脅的偵測。您也可以認可您要忽略的偵測並略過。

檢閱工作流程，以取得有關如何從主控台執行 Power Eraser 以及如何確保您正確架構主控台設定的詳細資料。

請參閱第 675 頁的「需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作」。

影響 Power Eraser 之 Symantec Endpoint Protection Manager 政策設定的概觀

以下是影響 Power Eraser 的政策設定：

- 使用者互動的掃描設定
  當您讓使用者取消任何病毒和間諜軟體掃描時，也就是讓他們取消任何 Power Eraser 分析。但是，使用者無法暫停或延緩 Power Eraser。
  請參閱第 414 頁的「允許使用者在 Windows 電腦上檢視掃描進度並與掃描互動」。
- 例外政策
  Power Eraser 遵守下列病毒和間諜軟體例外：檔案、資料夾、已知風險、應用程式和信任的 Web 網域。Power Eraser 不遵守副檔名例外。
  請參閱第 472 頁的「建立病毒和間諜軟體掃描的例外」。
- 日誌保留設定
  只要日誌中出現偵測，便可以對 Power Eraser 偵測採取動作。經過病毒和間諜軟體防護政策中指定的時間之後，日誌將被清除。根據預設，有 14 天的日誌事件可用。您可以修改日誌保留設定，也可以在事件到期之後，執行另一個掃描並重新填入日誌。
  請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。
- 重新啟動選項
  當您選擇在 Rootkit 偵測模式下執行 Power Eraser 時，可以專門針對 Rootkit 分析架構重新啟動設定。管理員必須具有重新啟動權限。在選擇移除 Power Eraser 偵測之後，電腦會使用群組重新啟動設定。Power Eraser 不會使用 Rootkit 重新啟動設定來重新啟動和完成矯正。
  請參閱第 107 頁的「從 Symantec Endpoint Protection Manager 重新啟動用戶端電腦」。
- 信譽查詢
  Power Eraser 在掃描檔案並做出有關檔案的決策時，會使用雲端中的 Symantec Insight 伺服器。如果停用信譽查詢，或用戶端電腦無法連線至 Insight 伺服器，則 Power Eraser 無法使用 Symantec Insight。若沒有 Symantec Insight，Power Eraser 所進行的偵測會變少，同時它進行的偵測較可能是誤報。如果已啟用**「允許進行智慧型掃描查詢以偵測威脅」**選項，會啟用信譽查詢。此選項預設為啟用。
  請參閱第 383 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。
- 傳送
  如果已啟用**「防毒偵測」**選項，Symantec Endpoint Protection 會將 Power Eraser 偵測的相關資訊傳送給賽門鐵克。此選項預設為啟用。
  請參閱第 418 頁的「瞭解伺服器資料收集和用戶端提交及其對網路安全的重要性」。

請參閱第 656 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。

需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作

在風險日誌顯示修復失敗並建議執行 Power Eraser 時，一般您需要執行 Power Eraser 分析。當電腦變得不穩定且似乎有無法移除的惡意軟體或病毒時，您可能也需要執行 Power Eraser。

警告：請謹慎使用 Power Eraser。該分析是積極的，但容易誤報。

請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。

您僅可在 Windows 用戶端電腦上從 Symantec Endpoint Protection Manager 執行 Power Eraser。

附註：Power Eraser 在以下其中一種模式下執行：不具有 Rootkit 偵測或具有 Rootkit 偵測。Rootkit 偵測分析需要重新啟動。管理員必須擁有重新啟動權限，才能在具有 Rootkit 偵測的模式下執行 Power Eraser。

表 42-1 需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作

工作	敘述
設定管理員權限以執行 Power Eraser	若要在用戶端電腦上執行 Power Eraser，管理員必須擁有下列指令存取權限： ■ **「啟動 Power Eraser 分析」** ■ **重新啟動用戶端電腦** (在具有 Rootkit 偵測的模式下執行 Power Eraser 時需要) 請參閱第 242 頁的「新增管理員帳戶和設定存取權限」。
設定日誌存留政策	日誌存留設定將影響事件供您執行 Power Eraser 矯正和還原動作所花費的時間。如果您需要更多時間考慮上述動作，您可以修改日誌存留設定。或者，您可以再次執行 Power Eraser 以重新填入日誌。 日誌存留設定屬於病毒和間諜軟體防護政策中的其他選項。 請參閱第 410 頁的「在 Windows 電腦上修改日誌處理及通知設定」。

工作	敘述
確保您的用戶端具有 Internet 連線	您的用戶端電腦需要 Internet 存取，以便 Power Eraser 可以使用 Symantec Insight 信譽資料來做出有關潛在威脅的決策。 間歇或不存在的 Internet 存取表示 Power Eraser 無法使用 Symantec Insight。如果不使用 Symantec Insight，Power Eraser 進行偵測的次數會變少，且產生的偵測更容易是誤報。
在用戶端電腦上從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析	選擇是在正常模式還是 Rootkit 模式下執行 Power Eraser。 您可以從 Symantec Endpoint Protection Manager 中的幾個地方發出 Power Eraser 指令： ■ **用戶端頁面** ■ 電腦狀態日誌 ■ 風險日誌 **附註：**用戶端電腦上的使用者無法在用戶端使用者介面上直接執行 Power Eraser。強力清除器可做為 SymDiag 工具的一部分使用。不過，如果用戶端使用者執行該工具，所產生的包括 Power Eraser 偵測的日誌不會傳送至 Symantec Endpoint Protection Manager。 請參閱第 678 頁的「從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析」。 您可以在電腦狀態日誌中檢視指令的狀態。您可以篩選該日誌，以僅顯示 Power Eraser 指令，從而便於檢視。 在您執行 Power Eraser 後，您可以在掃描日誌或風險日誌中檢視結果。掃描日誌顯示掃描結果是否處於擱置中。
在用戶端電腦上取消 Power Eraser 指令或動作	若要取消 Power Eraser 指令，請使用電腦狀態日誌。 **附註：**重新啟動提示出現在用戶端電腦上後，您就無法取消在 Rootkit 模式下執行的 Power Eraser。重新啟動後，如果病毒和間諜軟體防護政策讓使用者取消掃描，則僅電腦使用者可以取消 Power Eraser。 如果取消 Power Eraser 指令，您也可以取消與所有 Power Eraser 分析相關聯的任何擱置中的動作，包括所有矯正或復原動作。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

工作	敘述
從日誌中檢視 Power Eraser 偵測	您可以從 Symantec Endpoint Protection Manager 的下列日誌中檢視 Power Eraser 偵測： ■ 掃描日誌 掃描日誌有一個可僅顯示 Power Eraser 結果的**「掃描類型」**篩選器。該檢視也表示掃描結果是否處於擱置中。您可以在篩選檢視中選取**「偵測」**，以顯示**「Power Eraser 偵測」**檢視。 ■ 風險日誌 風險日誌針對 Power Eraser 偵測提供類似的篩選器。不過，風險日誌不會顯示掃描結果是否處於擱置中。 ■ 電腦狀態日誌 電腦狀態日誌可能在**「受感染」**欄中包含報告圖示。事件詳細資料圖示將連結到一個報告，該報告顯示目前無法矯正的所有威脅。該報告包含只記錄偵測和未解析的偵測。該報告可能建議在相同電腦上執行 Power Eraser。 Power Eraser 圖示將連結到一個報告，該報告顯示需要管理員動作的電腦上的所有 Power Eraser 偵測。 這些圖示也會出現在**「用戶端」**頁面的**「健康狀態」**欄中。 請參閱第 563 頁的「檢視日誌」。
檢查建議您在用戶端電腦上執行 Power Eraser 的通知	根據預設，管理員會在定期掃描無法修復感染時收到一條通知：建議使用 Power Eraser。您可以在**「監視器」>「通知」**頁面上檢查**「建議使用 Power Eraser」**通知。 請參閱第 575 頁的「檢視和認可通知」。
在**「指令狀態」**頁面上檢視 Power Eraser 偵測	可以在**「指令狀態」**頁面上存取有關 Power Eraser 偵測的報告。 事件詳細資料圖示將出現在**「完成狀態」**欄中。該圖示將連結到一個報告，該報告顯示**「啟動 Power Eraser 分析」**指令和任何其他掃描指令所執行的偵測的相關資訊。 指令狀態詳細資料選項提供有關特定掃描的資訊。可以按下事件詳細資料圖示，以取得有關特定用戶端電腦的資訊。 請參閱第 217 頁的「在用戶端電腦上從主控台執行指令」。

工作	敘述
從「用戶端」標籤中檢視 Power Eraser 偵測	您可以從**「用戶端」**頁面的**「用戶端」**標籤存取有關 Power Eraser 偵測的報告。 如果資訊可用，報告圖示將出現在**「健康狀態」**欄中。事件詳細資料圖示將連結到一個報告，該報告顯示目前無法矯正的所有威脅。該報告包含所有 Power Eraser 偵測。 Power Eraser 圖示將連結到一個報告，該報告顯示需要管理員動作的電腦上的所有 Power Eraser 偵測。 這些圖示也出現在電腦狀態日誌中。 請參閱第 212 頁的「檢視用戶端電腦的防護狀態」。
從 Symantec Endpoint Protection Manager 中的掃描日誌或風險日誌矯正或還原 Power Eraser 偵測	不同於其他 Symantec Endpoint Protection 掃描，Power Eraser 不會自動矯正偵測到的威脅。Power Eraser 分析是積極的，但可能會偵測到許多誤報。在您決定偵測需要矯正後，您必須手動啟動矯正。 也可以復原 (還原) 已矯正的 Power Eraser 偵測。 請參閱第 680 頁的「回應 Power Eraser 偵測」。

從 Symantec Endpoint Protection Manager 啟動 Power Eraser 分析

您可以執行 Power Eraser 來分析和偵測單一電腦或一小組電腦上的持續性威脅。

請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。

在 Power Eraser 偵測到潛在風險之後，您可以檢視風險並判斷哪些風險是威脅。 Power Eraser 不會自動矯正風險。 您必須手動執行 Power Eraser 以矯正您判斷為威脅的風險。 您也可以對特定威脅或其他防護功能偵測到的威脅執行 Power Eraser。 Power Eraser 在與偵測關聯的電腦上執行。

請參閱第 675 頁的「需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作」。

請參閱第 680 頁的「回應 Power Eraser 偵測」。

附註：在 Rootkit 模式下執行 Power Eraser，且用戶端電腦上顯示重新啟動選項訊息時，管理員或使用者無法取消 Power Eraser。 在重新啟動之後，如果病毒和間諜軟體防護政策讓使用者取消掃描，則使用者可以取消 Power Eraser。

從 Symantec Endpoint Protection Manager 中的「用戶端」頁面啟動 Power Eraser 分析

1 在「**用戶端**」頁面的「**用戶端**」標籤上，選取您要分析的電腦。

如果您選取多台電腦，可能會對網路的效能產生負面影響。

2 在「**工作**」下，按下「**對電腦執行指令**」，然後按下「**啟動 Power Eraser 分析**」。

3 在「**選擇 Power Eraser**」對話方塊中，選取是否希望 Power Eraser 在 Rootkit 模式下執行。 對於 Rootkit 模式，您可以設定重新啟動選項。 您必須擁有管理員權限，才能設定重新啟動選項並執行 Rootkit 掃描。

4 按下「**確定**」。

Power Eraser 即會在選取電腦上執行。 您可以在「**監視器**」頁面的「**指令狀態**」標籤上取消此指令。

從 Symantec Endpoint Protection Manager 中的電腦狀態日誌啟動 Power Eraser 分析

1 在主控台的側邊看板中，按下「**監視器**」，然後選取「**日誌**」標籤。

2 在「**日誌類型**」清單方塊中，選取「**電腦狀態**」日誌，然後按下「**檢視日誌**」。

3 選取要在其上執行 Power Eraser 的電腦，然後從「**指令**」下拉式方塊中選取「**啟動 Power Eraser 分析**」。

如果您選取多台電腦，可能會對網路的效能產生負面影響。

4 按下「**開始**」。

5 在「**選擇 Power Eraser**」對話方塊中，選取是否希望 Power Eraser 在 Rootkit 模式下執行。 對於 Rootkit 模式，您可以設定重新啟動選項。 您必須擁有管理員權限，才能設定重新啟動選項並執行 Rootkit 掃描。

6 按下「**確定**」。

Power Eraser 即會在選取的電腦上執行。 您可以在「**指令狀態**」標籤上取消此指令。

從 Symantec Endpoint Protection Manager 中的風險日誌啟動 Power Eraser 分析

1 在主控台的側邊看板中，按下「**監視器**」，然後選取「**日誌**」標籤。

2 在「**日誌類型**」清單方塊中，選取「**風險**」日誌，然後按下「**檢視日誌**」

3 選取要對其執行 Power Eraser 的風險。 在「**事件動作**」欄中，您可能會看到執行 Power Eraser 的警示。

您可以對日誌中的任何風險執行 Power Eraser。

4 從「**動作**」下拉式清單或「**動作**」欄中，選取「**啟動 Power Eraser 分析**」。

5 按下「**開始**」。

6 在「**選擇 Power Eraser**」對話方塊中，選取是否希望 Power Eraser 在 Rootkit 模式下執行。對於 Rootkit 模式，您可以設定重新啟動選項。您必須擁有管理員權限，才能設定重新啟動選項並執行 Rootkit 掃描。

7 按下「**確定**」。

Power Eraser 即會在受所選風險感染的電腦上執行。您可以在「**指令狀態**」標籤上取消此指令。

回應 Power Eraser 偵測

Power Eraser 不會在掃描期間矯正任何偵測，因為它的主動偵測功能容易發生誤報情況。在檢閱過偵測之後，您必須針對日誌中偵測到的事件要求矯正，然後決定予以矯正還是忽略。如果您選擇矯正，Power Eraser 會移除與偵測關聯的檔案。但在日誌被清除之前，您可以還原已移除的檔案。

日誌保留政策決定 Power Eraser 事件的存留時間長度。依預設，事件會保留 14 天。

請參閱第 675 頁的「需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作」。

請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。

回應 Power Eraser 偵測

1 確認 Power Eraser 分析已完成。

- 電腦狀態日誌包含用於指示掃描已完成的圖示。
- 掃描日誌會顯示 Power Eraser 是否已完成分析。

2 在風險日誌或「**掃描日誌**」>「**檢視偵測**」頁面中，選取要套用動作的一或多個偵測。

- 在標示為「**發現潛在風險 (擱置管理員動作)**」的特定風險旁邊，按下「**動作**」欄中的加號圖示。
- 選取標示為「**發現潛在風險 (擱置管理員動作)**」的多個風險，然後從「**動作**」下拉式功能表中選取動作。

3 選擇下列其中一個動作：

- **刪除 Power Eraser 偵測到的風險**
  將風險從電腦中移除以矯正該風險。Power Eraser 會儲存一份可供還原的安全備份檔案。
- **忽略 Power Eraser 偵測到的風險**
  確認您已檢閱偵測，但不想要矯正風險。

附註：此動作只會在管理主控台日誌中將事件動作變更為「由管理員略過」。此認可不會更新用戶端上對應的事件動作。用戶端日誌檢視會繼續將事件動作顯示為「等待分析中」。

4 如果已從**「動作」**下拉式功能表中選取動作，請按下**「套用」**。

如果您選取了**「忽略 Power Eraser 偵測到的風險」**，偵測現在會顯示為**「發現潛在風險 (略過)」**。

您可以透過選取**「還原 Power Eraser 刪除的風險」**動作，將標示為**「發現潛在風險 (已移除)」**的已移除偵測還原。

表 42-2 Power Eraser 偵測狀態摘要

偵測狀態	敘述
擱置管理員動作	Power Eraser 將風險偵測為潛在威脅。您應檢閱風險並決定 Power Eraser 是否應矯正風險，或認可該風險並予以忽略。
已還原	管理員已還原管理員要求 Power Eraser 矯正風險時所移動的所有檔案。
已刪除	管理員要求 Power Eraser 矯正並刪除風險。當 Power Eraser 刪除風險時，它會刪除與風險關聯的檔案，同時建立可供還原的安全備份複本。當日後判斷並非風險時，您可能會想要將已刪除的風險還原。在日誌事件被清除之前，您可以還原檔案。
由管理員略過	管理員要求 Power Eraser 略過風險。

附錄 A

用戶端功能比較表

本附錄包含以下主題：

針對 Windows 用戶端 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能相依性

需要同時啟用部分政策功能，才能提供對 Windows 用戶端電腦的完整防護。

警告：賽門鐵克建議您不要停用「智慧型掃描查詢」。

表 A-1 防護功能的相依性

功能	交互操作性指示
下載防護	下載防護功能為自動防護的一部分，可使 Symantec Endpoint Protection 能夠追蹤 URL。有幾種政策功能需要追蹤 URL。 如果您安裝的 Symantec Endpoint Protection 沒有下載防護功能，則「下載鑑識」的功能會有所限制。瀏覽器入侵預防和 SONAR 需要下載防護功能。 **「自動信任從內部網路網站下載的任何檔案」**選項也需要下載防護功能。

功能	交互操作性指示
下載鑑識	「下載鑑識」具有下列相依性： ■ 必須啟用「自動防護」 如果您停用「自動防護」，即使「下載鑑識」已啟用，仍將無法運作。 ■ 必須啟用智慧型掃描查詢 賽門鐵克建議您讓「智慧型掃描查詢」選項保持啟用狀態。 如果您停用該選項，會完全停用「下載鑑識」。 **附註：**如果沒有安裝基本的「下載防護」，「下載鑑識」會在層級 1 的用戶端上執行。系統不會套用您在此政策中設定的任何層級。同樣地，使用者也無法調整敏感程度。 即使您停用「下載鑑識」，**「自動信任從內部網路網站下載的任何檔案」**選項仍會繼續運作。 如果您停用「下載鑑識」，則會停用入口網站偵測。這意味著自動防護以及排程掃描和隨選掃描會將所有檔案評估為非入口網站檔案，並使用由賽門鐵克決定的敏感程度。 請參閱第 380 頁的「管理「下載鑑識」偵測」。
智慧型掃描查詢 (12.1.x 用戶端) 和雲端防護	「智慧型掃描查詢」會使用雲端中的 Symantec Insight 信譽資料庫，針對從支援的入口網站下載的檔案進行決策。 從14 開始： ■ 在標準和內嵌式/VDI 用戶端上執行自動防護、排程掃描和隨選掃描的過程中，「智慧型掃描查詢」功能會自動執行。標準和內嵌式/VDI 用戶端支援啟用雲端的內容。 ■ 可以在您所具備的任何 12.1.x 用戶端的掃描設定中啟用或停用「智慧型掃描查詢」，但無法再為「智慧型掃描查詢」架構特定的敏感程度。舊版「智慧型掃描查詢」現可使用下載鑑識政策中設定的敏感程度。 請參閱第 355 頁的「Windows 用戶端如何從雲端接收定義檔」。 雲端掃描和 12.1.x 智慧型掃描查詢具有下列功能相依性： ■ 必須啟用「智慧型掃描查詢」。否則，雲端掃描和「智慧型掃描查詢」無法運作。 ■ 必須啟用「下載鑑識」，才能將檔案標示為入口網站檔案。 ■ 如果「下載鑑識」已停用，則雲端掃描和「智慧型掃描查詢」會繼續運作。它們所使用的敏感程度由賽門鐵克自動設定，僅用於偵測大多數惡意檔案。 **附註：**(僅限 12.1.x 用戶端) 雲端查詢不會套用至用戶端電腦上資料夾或磁碟機的按右鍵掃描。但是，雲端查詢會套用至所選入口網站檔案的按右鍵掃描中。

功能	交互操作性指示
SONAR	SONAR 具有下列相依性： ■ 必須安裝下載防護。 ■ 必須啟用「自動防護」。 如果已停用「自動防護」，則 SONAR 會失去部分偵測功能，並顯示未於用戶端上正常運作。 然而，即使已停用「自動防護」，SONAR 仍然可以偵測啟發式威脅。 ■ 必須啟用「智慧型掃描查詢」。 如果沒有使用「智慧型掃描查詢」，則 SONAR 可以執行，但無法進行偵測。 在極少見的情況下，SONAR 可以在沒有使用「智慧型掃描查詢」的情況下進行偵測。 如果 Symantec Endpoint Protection 先前已快取了有關特定檔案的信譽資訊，則 SONAR 可能會使用快取的資訊。 請參閱第 425 頁的「管理 SONAR」。
瀏覽器入侵預防	必須安裝下載防護。可啟用或停用「下載鑑識」。
信任的 Web 網域例外	只有在已安裝「下載防護」時才會套用例外。
自訂 IPS 特徵	使用防火牆。 請參閱第 334 頁的「管理自訂入侵預防特徵」。
Power Eraser	使用「智慧型掃描查詢」。 Power Eraser 使用信譽資訊檢查檔案。Power Eraser 具有無法修改的預設信譽靈敏度設定。如果您停用「**允許進行智慧型掃描查詢以偵測威脅**」選項，Power Eraser 就無法使用 Symantec Insight 提供的信譽資訊。在沒有「智慧型掃描」的情況下，Power Eraser 會減少偵測次數，而且偵測較可能產生誤報的情況。 **附註：**Power Eraser 會使用自己的信譽臨界值，這些臨界值無法在 Symantec Endpoint Protection Manager 中架構。Power Eraser 不使用「下載鑑識」設定。 請參閱第 672 頁的「從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 之前所應瞭解的事項」。
記憶體攻擊緩和	必須安裝入侵預防。可啟用或停用入侵預防。

請參閱第 101 頁的「選擇要在用戶端上安裝哪些安全性功能」。

根據平台 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能

- 管理功能 (依平台分類)
- 依據平台的自動升級差異
- 病毒和間諜軟體防護政策設定 (依平台分類)
- 防火牆、入侵預防和記憶體攻擊緩和設定 (依平台分類)
- LiveUpdate 政策設定 (依平台分類)
- 整合政策設定 (依平台分類)
- 例外政策設定 (依平台分類)
- 依據平台的「**裝置控制**」差異

請參閱第 99 頁的「如何選擇用戶端安裝類型」。

請參閱第 682 頁的「針對 Windows 用戶端 (12.1.x 至 14.x) 的 Symantec Endpoint Protection 功能相依性」。

用戶端防護功能 (依平台分類)

表 A-2 列出 Windows 用戶端、Mac 用戶端和 Linux 用戶端上提供的防護功能。

表 A-2 用戶端防護功能 (依平台分類)

用戶端功能	Windows	Mac	Linux
病毒和間諜軟體防護	是	是	是
防網路和主機刺探利用 ■ 網路威脅防護 (入侵預防和防火牆) ■ 記憶體攻擊緩和 (在 14 版中推出時稱為「防一般攻擊程式」)	是	■ 防火牆 (自 14.2 起) ■ 入侵預防 (自 12.1.4 起) 適用於 Mac 的入侵預防不支援自訂特徵。	否
主動型威脅防護 ■ 應用程式與裝置控制 ■ SONAR	是	僅限裝置控制 (自 14 版起)	否
主機完整性	是	否	否
其他防護 ■ 系統鎖定 ■ 竄改防護	是	否	否

請參閱第 432 頁的「關於應用程式控制、系統鎖定和裝置控制」。

請參閱第 522 頁的「主機完整性的運作方式」。

管理功能 (依平台分類)

表 A-3 列出 Windows 用戶端、Mac 用戶端和 Linux 用戶端上提供的管理功能。

表 A-3 管理功能 (依平台分類)

管理功能	Windows	Mac	Linux
從 Symantec Endpoint Protection Manager 遠端部署用戶端 ■ 網路連結與電子郵件 ■ 遠端推送 ■ 儲存套件	是	是	是 (僅限「**網路連結與電子郵件**」、「**儲存套件**」)
從管理伺服器在用戶端上執行指令	■ 掃描 ■ 更新內容 ■ 更新內容和掃描 ■ 啟動 Power Eraser 分析 (自 12.1.5 起) ■ 重新啟動用戶端電腦 ■ 啟用自動防護 ■ 啟用網路威脅防護 ■ 停用網路威脅防護 ■ 啟用下載鑑識 ■ 停用下載鑑識 ■ 收集檔案指紋清單 (自 12.1.6 起) ■ 從隔離所刪除** ■ 取消全部掃描**	■ 掃描 ■ 更新內容 ■ 更新內容和掃描 ■ 重新啟動用戶端電腦(僅限硬式重新啟動) ■ 啟用自動防護 ■ 啟用網路威脅防護 (自 12.1.4 起) ■ 停用網路威脅防護 (自 12.1.4 起)	■ 掃描 ■ 更新內容 ■ 更新內容和掃描 ■ 啟用自動防護
啟用探索到的應用程式和網路應用程式監控	是	否	否
建立位置和設定安全政策 (依位置套用)	是	是	否 您可以透過指令行來檢視用戶端的位置，但是用戶端不會根據特定的準則自動切換位置。
設定用戶端的重新啟動選項	是	否	否

管理功能	Windows	Mac	Linux
快速報告和排程報告	■ 稽核 ■ 應用程式與裝置控制 ■ 合規性 ■ 電腦狀態 ■ 欺敵 (14.0.1) ■ 防網路和主機剌探利用 ■ 風險 ■ 掃描 ■ 系統	■ 電腦狀態 ■ 防網路和主機剌探利用 ■ 風險 ■ 掃描	■ 稽核 ■ 電腦狀態 ■ 風險 ■ 掃描 ■ 系統
針對用戶端電腦上維護的日誌設定大小和保留選項	■ 系統 ■ 安全性和風險 ■ 安全性 ■ 流量 ■ 封包 ■ 控制	■ 系統 ■ 安全性和風險 ■ 安全性	■ 系統 ■ 安全性和風險
使用密碼保護用戶端	是	解除安裝用戶端 (14.0.1)	否
執行 SylinkDrop 工具以將用戶端移至其他管理伺服器	是	是	否
使用「**通訊更新套件部署**」選項重新部署用戶端套件，以將用戶端移至其他管理伺服器	是	是	否
架構用戶端向賽門鐵克提交匿名安全資訊	是	(12.1.4 及更新版本) 傳送設定僅控制防毒偵測資訊。 您可以在用戶端上手動停用或啟用入侵預防傳送。 如何在 Symantec Endpoint Protection for Mac 用戶端上停用 IPS 資料傳送	否
架構用戶端以安全提交匿名系統和使用資訊	是	否	否
管理管理伺服器與用戶端之間的外部通訊	是	僅限 LiveUpdate	否

管理功能	Windows	Mac	Linux
管理用戶端通訊設定	■ 管理伺服器清單 ■ 通訊模式 (推送或提取) ■ 設定活動訊號間隔時間 ■ 上傳探索到的應用程式 ■ 立即上傳重大事件 ■ 設定下載隨機化 ■ 設定重新連線喜好設定	■ 管理伺服器清單 ■ 通訊模式 (推送或提取) ■ 設定活動訊號間隔時間 ■ 設定下載隨機化 ■ 設定重新連線喜好設定	■ 管理伺服器清單 ■ 通訊模式 (推送或提取) ■ 設定活動訊號間隔時間
將用戶端架構為使用私用伺服器 (12.1.6) ■ 用於智慧型掃描查詢和提交的 Endpoint Detection and Response 伺服器 ■ 用於智慧型掃描查詢的私用 Insight 伺服器	是	否	否
使用「自動升級」來自動升級 Symantec Endpoint Protection 用戶端	是	是 (14)	否
自動解除安裝現有的第三方安全軟體	是	否	否
自動解除安裝有問題的 Symantec Endpoint Protection 用戶端	是 (14)	否	否
Symantec Endpoint Protection Manager 登入的驗證	■ Symantec Endpoint Protection Manager 驗證 ■ 雙因素驗證 (14.2) ■ RSA SecurID 驗證 ■ 目錄驗證 ■ 智慧卡 (PIV/CAC) 驗證 (14.2)	不適用	不適用

**您只能在 Symantec Endpoint Protection Manager 中檢視日誌時執行這些指令。

請參閱第 215 頁的「什麼是可對用戶端電腦執行的指令？」。

請參閱第 675 頁的「需要從 Symantec Endpoint Protection Manager 主控台執行 Power Eraser 時要執行的工作」。

請參閱第 284 頁的「監控在用戶端電腦執行的應用程式與服務」。

請參閱第 137 頁的「管理用戶端伺服器連線」。

請參閱第 147 頁的「使用「通訊更新套件部署」還原用戶端伺服器通訊」。

依據平台的自動升級差異

表 A-4 列出 Windows 用戶端與 Mac 用戶端之間的自動升級功能上的差異。

表 A-4 依據平台的自動升級差異

功能	Windows	Mac
差量套件	標準用戶端和暗網用戶端會接收 Symantec Endpoint Protection Manager 產生的差量升級套件。內嵌式用戶端則接收完整安裝套件來進行升級。	Mac用戶端一律接收完整安裝套件，以進行升級。
組態選項	包括自訂安裝資料夾，以及解除安裝現有安全軟體的選項。	僅適用於重新啟動和升級。您無法自訂安裝資料夾。安裝記錄一律寫入 `/tmp/sepinstall.log`。
「用戶端安裝設定」中升級完成之後的重新啟動選項	包括不要重新啟動 Windows 用戶端電腦的選項。	請勿包括不要重新啟動的選項。升級完成後，Mac用戶端電腦一律重新啟動。
「使用套件升級用戶端」精靈	您可以修改 Windows 用戶端上的功能集。	您無法修改 Mac 用戶端上的功能集。
從舊版升級	您可依據支援的升級路徑，從任何更早版本升級至 Symantec Endpoint Protection 的最新版本。	不支援從 12.1.6.x 版或更早版本進行升級。例如，您無法使用自動升級從 12.1.6.4 升級至 14。

請參閱第 132 頁的「使用自動升級來升級用戶端軟體」。

請參閱第 122 頁的「最新版本 Symantec Endpoint Protection 14.x 支援的升級路徑」。

請參閱第 99 頁的「如何選擇用戶端安裝類型」。

病毒和間諜軟體防護政策設定 (依平台分類)

表 A-5 列出 Windows 用戶端、Mac 用戶端和 Linux 用戶端所提供設定之間的差異。

表 A-5 病毒和間諜軟體防護政策設定 (依平台分類)

政策設定	Windows	Mac	Linux
管理員定義掃描	■ 排程掃描 (作用中、完整、自訂) ■ 隨選掃描 ■ 觸發掃描 ■ 開機掃描 ■ 重試錯過的排程掃描 ■ 隨機設定排程掃描	■ 排程掃描 (自訂) ■ 隨選掃描 ■ 重試錯過的排程掃描	■ 排程掃描 (自訂) ■ 隨選掃描 ■ 重試錯過的排程掃描
自動防護	■ 啟用自動防護 ■ 掃描所有檔案 ■ 只掃描選取的副檔名 ■ 檢查檔案內容來判斷檔案類型 ■ 掃描安全風險 ■ 掃描遠端電腦上的檔案 (14) ■ 存取、修改或備份檔案時掃描 ■ 掃描磁片是否存在開機病毒，含有選項可刪除開機病毒或僅記錄它 ■ 一律刪除新建立的受感染檔案或安全風險 ■ 保留檔案時間 ■ 針對掃描速度或應用程式速度調整掃描效能 ■ 包裝的惡意軟體的模擬器 (14)	■ 啟用自動防護 ■ 自動修復受感染的檔案 ■ 隔離無法修復的檔案 ■ 掃描壓縮檔 ■ 掃描所有檔案 ■ 僅掃描選取的資料夾 ■ 掃描除所選資料夾外的所有位置 ■ 掃描安全風險 在掛載的目前用戶端上掃描： ■ 資料磁碟 ■ 所有其他磁碟和裝置 在掛載的舊版用戶端上掃描 (12.1.3 及更早版本)： ■ 音樂或視訊磁碟 ■ iPod 播放器 ■ 在掃描期間顯示進度	■ 啟用自動防護 ■ 掃描所有檔案 ■ 只掃描選取的副檔名 ■ 掃描抽取式媒體 ■ 掃描安全風險 ■ 掃描遠端電腦上的檔案 ■ 在存取或修改檔案時進行掃描 ■ 在壓縮檔內掃描
電子郵件掃描	■ Microsoft Outlook 自動防護 ■ Internet 電子郵件自動防護 (14.2 RU1 中已移除) ■ Lotus Notes 自動防護 (14.2 RU1 中已移除)	否	否

政策設定	Windows	Mac	Linux
要掃描的內容	■ 其他位置 ■ 記憶體 ■ 選取的資料夾 ■ 選取的副檔名 ■ 儲存體移轉位置 ■ 壓縮檔內的檔案 ■ 安全風險	■ 全部或選取的資料夾 ■ 硬碟和抽取式磁碟機 ■ 壓縮檔內的檔案	■ 所有檔案 ■ 全部或選取的資料夾 ■ 選取的副檔名 ■ 壓縮檔內的檔案 ■ 安全風險
使用者定義的掃描 (用戶端)	■ 作用中掃描 ■ 完整掃描 ■ 自訂掃描個別資料夾、檔案和副檔名	■ 完整掃描 ■ 自訂掃描個別資料夾和檔案	■ 完整掃描 ■ 自訂掃描個別資料夾和檔案
定義偵測的矯正動作	■ 清除 (僅適用於惡意軟體) ■ 隔離 ■ 刪除 ■ 略過 (只記錄) 這些動作適用於賽門鐵克定期更新的惡意軟體和安全風險類別。	■ 修復受感染的檔案 ■ 隔離無法修復的檔案	■ 清除 (僅適用於惡意軟體) ■ 隔離 ■ 刪除 ■ 略過 (只記錄)
設定掃描執行時要採取的動作	■ 停止掃描 ■ 暫停掃描 ■ 延緩掃描 ■ 僅在電腦閒置時掃描	(12.1.4) ■ 停止掃描 ■ 暫停掃描 ■ 開始前延緩掃描 ■ 延緩進行中掃描 (僅透過 12.1.6x) ■ 僅在電腦閒置時掃描	否
下載鑑識	是	否	否
智慧型掃描查詢用於偵測威脅	是	否	否
Bloodhound	是	否	否
SONAR	是 遠端電腦掃描 (14) 可疑行為偵測 (14)	否	否
提早啟動防惡意軟體驅動程式	Windows 8 及更新版本，以及 Windows Server 2012 及更新版本	否	否

政策設定	Windows	Mac	Linux
Power Eraser	是 (12.1.5)	否	否
Endpoint Detection and Response 啟用	是 (12.1.6)	否	否
共用智慧型掃描快取	是 已啟用 vShield (12.1.6 及更早版本)	否	否
虛擬影像例外	是	否	否

請參閱第 347 頁的「阻止和處理病毒和間諜軟體對用戶端電腦的攻擊」。

請參閱第 581 頁的「在虛擬基礎架構中使用 Symantec Endpoint Protection」。

防火牆、入侵預防和記憶體攻擊緩和設定 (依平台分類)

表 A-6顯示適用於 Windows 用戶端和 Mac 用戶端的設定中存在的差異。

表 A-6　　入侵預防政策設定 (依平台分類)

政策設定	Windows	Mac (12.1.4)
入侵預防特徵的例外	是 **附註：**「瀏覽器防護」特徵不支援自訂例外。	是
顯示或隱藏使用者通知	是	是
啟用或停用排除的主機	是	是
自訂 IPS 特徵	是	否
啟用或停用網路入侵預防	是	是
LiveUpdate 更新 IPS 內容	是	是
管理伺服器更新 IPS 內容	是	否 **
用戶端套件包含 IPS	是	是
網路入侵預防	是	是
瀏覽器入侵預防	是 ■ 只記錄模式 (12.1.6)	否
排除的主機 (網路入侵預防)	是	是

**您可以將隨 Symantec Endpoint Protection Manager 安裝的 Apache Web 伺服器設定為 LiveUpdate 內容的反向代理。 請參閱：

使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

請參閱第 325 頁的「管理入侵預防」。

表 A-7 記憶體攻擊緩和政策設定 (依平台分類)

政策設定	Windows	Mac (12.1.4)
記憶體攻擊緩和 防一般攻擊程式 (14 MPx)	是 (14) ■ 微調誤報 (14.0.1) ■ 自訂應用程式 (僅限 14.1、雲端)	否

請參閱第 339 頁的「使用記憶體攻擊緩和政策強化 Windows 用戶端防範記憶體竄改攻擊」。

LiveUpdate 政策設定 (依平台分類)

表 A-8 顯示可用於 Windows 用戶端、Mac 用戶端和 Linux 用戶端的 LiveUpdate 設定中存在的差異。

表 A-8 LiveUpdate 政策設定 (依平台分類)

政策設定	Windows	Mac	Linux
使用預設管理伺服器	是	否 **	否 **
使用 LiveUpdate 伺服器 (內部或外部)	是	是	是
使用群組更新提供者	是	否	否
啟用第三方內容管理	是	否	否
啟用/停用定義	是	是	否
減少大小定義 (12.1.6)	是	否	否
執行智慧型更新小幫手 (Intelligent Updater) 以更新內容	■ 病毒和間諜軟體定義檔 ■ SONAR (12.1.3 及更新版本) ■ IPS 定義檔 (12.1.3 及更新版本)	病毒和間諜軟體定義檔	病毒和間諜軟體定義檔

政策設定	Windows	Mac	Linux
LiveUpdate 代理架構	是	是，但它不在 LiveUpdate 政策中架構。若要架構此設定，請按下**「用戶端」>「政策」**，然後按下**「外部通訊設定」**。	是
LiveUpdate 排程設定	■ 頻率 ■ 重試時段 ■ 下載隨機化 ■ 電腦閒置時執行 ■ 用於略過 LiveUpdate 的選項	■ 頻率 ■ 下載隨機化	■ 頻率 ■ 重試時段 ■ 下載隨機化
使用標準 HTTP 標頭 (12.1.6 和更早版本)	是，依據預設	是，依據預設	是，依據預設
用戶端安全修補程式	是 (14)	否	否
應用程式控制內容	是 (14.2)	否	否

** 您可以將隨 Symantec Endpoint Protection Manager 安裝的 Apache Web 伺服器設定為 LiveUpdate 內容的反向代理。請參閱：

使 Mac 和 Linux 用戶端能夠透過將 Apache Web 伺服器用作反向代理來下載 LiveUpdate 內容

請參閱第 99 頁的「如何選擇用戶端安裝類型」。

請參閱第 152 頁的「如何更新用戶端上的內容和定義檔」。

請參閱第 191 頁的「使用智慧型更新小幫手 (Intelligent Updater) 檔案更新 Symantec Endpoint Protection 用戶端上的內容」。

整合政策設定 (依平台分類)

表 A-10 顯示整合政策設定。

表 A-9　　整合政策設定 (依平台分類)

政策設定	Windows	Mac	Linux
Web Security Services (WSS) 流量重新導向 (WTR)	是	是 (14.2)	否
本機代理服務 (自 14.2 起，包含到 WTR 中)	是	否 Mac 會忽略此設定。	否

請參閱第 486 頁的「架構 WSS 流量重新導向」。

例外政策設定 (依平台分類)

表 A-10 顯示例外政策設定。

表 A-10 例外政策設定 (依平台分類)

政策設定	Windows	Mac	Linux
伺服器型例外	■ 應用程式 ■ 要監控的應用程式 ■ 副檔名 ■ 檔案 ■ 資料夾 ■ 已知風險 ■ 信任的 Web 網域 ■ 竄改防護例外 ■ DNS 或主機檔案變更例外 ■ 憑證 (14.0.1)	■ 檔案或資料夾的安全風險例外	■ 資料夾 ■ 副檔名
用戶端限制 (控制一般使用者可以在用戶端電腦上新增哪些限制)	是	否	否

請參閱第 468 頁的「管理 Symantec Endpoint Protection 中的例外」。

依據平台的「裝置控制」差異

表 A-11 列出 Mac 及 Windows 在**「裝置控制」**功能上的差異。

應用程式控制僅會在 Windows 電腦上執行。

表 A-11 依據平台的「裝置控制」差異

Windows	Mac
裝置控制僅依據類別 ID (GUID) 和裝置 ID 運作。	裝置控制在檔案系統層級上運作。磁碟區層級的工作 (例如，可透過指令行或磁碟公用程式執行的工作)未受影響。
裝置控制對具有星形字元或星號 (*) 的類別 ID 或裝置 ID 執行萬用字元比對。	裝置控制執行規則運算式 (regexp) 比對，且限於執行下列特定作業： ■ . (點) ■ \ (反斜線) ■ `[set]`、`[^Set]` (字集) ■ * (星形字元或星號) ■ + (加號)

Windows	Mac
依預設，硬體裝置清單包括多種常見裝置類型。	您只能從五個裝置類型中進行選擇： ■ Thunderbolt ■ CD/DVD ■ USB ■ FireWire ■ 安全數位 (SD) 卡 您無法使用硬體裝置清單。
您可透過類別 ID 或裝置 ID 將其他自訂裝置新增到硬體裝置清單。	您無法新增其他自訂裝置。
要攔截 (或從攔截排除) 的裝置僅可從硬體裝置清單中取得。此清單包括預設常見裝置類型，也包括您可能已新增的自訂裝置。	要攔截 (或從攔截排除) 的裝置可從上述裝置類型中選取。廠商、型號和序號可保留為空白，或由規則運算式 (regexp) 查詢定義。您可使用規則運算式來定義一系列類似裝置，例如不同廠商、型號、序號範圍等。
您可一次新增多個裝置類型。	您一次僅可以新增一個裝置類型。
要採取的行動是攔截，或從攔截排除 (允許)。	要採取的行動是攔截，或使用掛載權限從攔截排除 (允許)。 下列掛載權限受支援： ■ 唯讀 ■ 讀取和寫入 ■ 讀取和執行 ■ 讀取、寫入和執行
您可以自訂裝置控制的用戶端通知。	您無法自訂裝置控制的用戶端通知。

請參閱第 463 頁的「管理裝置控制」。

附錄 B

使用第三方工具自訂和部署 Windows 用戶端安裝

本附錄包含以下主題：

使用第三方工具安裝 Windows 用戶端軟體

您可以使用第三方工具安裝用戶端，而不使用隨管理伺服器一起安裝的工具。如果您使用的是大型網路，則可能使用這些選項來安裝賽門鐵克用戶端軟體比較有利。

您可以藉由使用各種不同的第三方產品安裝用戶端。這些產品包括 Microsoft Active Directory、Tivoli、Microsoft Systems Management Server (SMS) 和 Novell ZENworks。Symantec Endpoint Protection 支援 Novell ZENworks、Microsoft Active Directory 和 Microsoft SMS。

您也可以在使用 **Symantec Software Management Solution powered by Altiris** 管理的環境中部署 Symantec Endpoint Protection。您可以使用下列其中一項政策，從一個 Software Management Solution 套件部署 Symantec Endpoint Protection：

- **「受管軟體傳送」**政策
- **「快速傳送」**政策

如需詳細資訊，請參閱 Software Management Solution 套件產品說明，或者請參閱：

Symantec Software Management Solution 產品登陸頁面

表 B-1　　安裝用戶端的第三方工具

工具	敘述
Windows Installer 指令行工具	賽門鐵克用戶端軟體安裝套件屬於 Windows Installer (MSI) 檔案，您可以使用標準的 Windows Installer 選項來架構。您可以使用支援 MSI 部署的環境管理工具 (如 Active Directory 或 Tivoli)，在您的網路上安裝用戶端。您可以架構「Windows 資訊安全中心」與非受管用戶端互動的方式。 請參閱第 699 頁的「關於用戶端安裝功能和屬性」。 請參閱第 699 頁的「關於架構 MSI 指令字串」。 請參閱第 699 頁的「關於架構 Setaid.ini」。 請參閱第 701 頁的「Symantec Endpoint Protection 指令行用戶端功能」。 請參閱第 700 頁的「Symantec Endpoint Protection 指令行用戶端安裝屬性」。 請參閱第 702 頁的「Windows Installer 參數」。 請參閱第 705 頁的「安裝 Windows 用戶端的指令行範例」。 請參閱第 704 頁的「Windows 資訊安全中心屬性」。
Microsoft SMS 2003	您可以使用 Microsoft Systems Management Server 安裝用戶端。 請參閱第 706 頁的「使用 Microsoft SCCM/SMS 安裝 Windows 用戶端」。
Windows Active Directory	如果用戶端電腦是 Windows Active Directory 網域的成員，您就可以使用 Windows Active Directory 群組原則物件。用戶端電腦同樣必須使用支援的 Windows 作業系統。 請參閱第 707 頁的「使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端」。 請參閱第 710 頁的「使用 Active Directory 群組原則物件移除用戶端軟體」。
虛擬化軟體	您可以在虛擬環境中安裝用戶端。 請參閱第 68 頁的「支援的虛擬安裝和虛擬化產品」。

請參閱第 114 頁的「匯出用戶端安裝套件」。

關於用戶端安裝功能和屬性

安裝功能和屬性是出現在文字檔和指令行中的字串。 在所有用戶端軟體安裝期間，都會處理一些文字檔和指令行。 安裝功能會控制要安裝的元件。 安裝屬性則控制安裝之後要啟用或停用哪些子元件。 安裝功能和屬性僅適用於 Symantec Endpoint Protection 用戶端軟體，也適用於 Windows 作業系統。 安裝功能和屬性不適用於 Symantec Endpoint Protection Manager 安裝。

安裝功能和屬性的指定方式有兩種：作為 Setaid.ini 檔案中的資料行，和作為 Windows Installer (MSI) 指令中的值。 MSI 指令可以於 Windows Installer 字串中指定，也可以於 Setaid.ini 中指定，以執行自訂部署。 進行所有受管型用戶端軟體的安裝時，一律會處理 Windows Installer 指令和 Setaid.ini。 如果指定不同的值，則一律優先採用 Setaid.ini 中的值。

關於架構 MSI 指令字串

Symantec Endpoint Protection 安裝軟體使用 Windows Installer (MSI) 3.1 或更新的套件進行安裝和部署。如果您使用指令行部署套件，您可以自訂安裝。您可以使用標準的 Windows Installer 參數，以及賽門鐵克特定功能與內容。

使用 Windows Installer 需要更高的權限。如果您嘗試在沒有提高權限的情況下安裝，安裝可能會失敗而無預先通知。

如需 Symantec 安裝指令及參數的最新清單，請參閱文章：Symantec Endpoint Protection MSI 指令行參考。

附註：不支援 Windows Installer 廣告功能。Setaid.ini 指定的功能和屬性的優先順序高於 MSI 指定的功能和屬性。MSI 指令的功能和屬性名稱區分大小寫。

請參閱第 699 頁的「關於架構 Setaid.ini」。

關於架構 Setaid.ini

Setaid.ini 會出現在所有安裝套件中，並且控制許多方面的安裝內容，例如要安裝哪些功能。Setaid.ini 一律優先於用於啟動安裝的 MSI 指令字串中可能出現的任何設定。Setaid.ini 與 setup.exe 出現在相同的目錄中。如果匯出至單一 .exe 檔案，則無法架構 Setaid.ini。但是，當您從主控台匯出 Symantec Endpoint Protection 用戶端安裝檔案時，會自動架構該檔案。

以下幾行顯示了一些您可以在 Setaid.ini 中架構的選項。

```
[CUSTOM_SMC_CONFIG]
InstallationLogDir=
DestinationDirectory=

[FEATURE_SELECTION]
Core=1
```

```
SAVMain=1
 Download=1
 OutlookSnapin=1
 Pop3Smtp=0
 NotesSnapin=0

PTPMain=1
 DCMain=1
 TruScan=1
```

附註：這些功能會縮排以顯示階層。不過，在 Setaid.ini 檔案中時不會縮排。Setaid.ini 中的功能名稱區分大小寫。

功能值設為 1，則會安裝此功能。功能值設為 0，則不安裝此功能。 您必須指定並安裝父功能，才能順利安裝用戶端功能。

請注意下列額外的 setaid.ini 設定，這些設定會對應至 MSI 屬性，以進行 Symantec Endpoint Protection 用戶端安裝：

- DestinationDirectory 對應至 PRODUCTINSTALLDIR
- KeepPreviousSetting 對應至 MIGRATESETTINGS
- AddProgramIntoStartMenu 對應至 ADDSTARTMENUICON

請參閱第 701 頁的「Symantec Endpoint Protection 指令行用戶端功能」。

請參閱第 700 頁的「Symantec Endpoint Protection 指令行用戶端安裝屬性」。

請參閱第 702 頁的「Windows Installer 參數」。

Symantec Endpoint Protection 指令行用戶端安裝屬性

這些安裝屬性是搭配 MSI 指令行安裝使用的。

表 B-2 Symantec Endpoint Protection 用戶端安裝屬性

屬性	敘述
RUNLIVEUPDATE=*val*	決定安裝程序是否執行 LiveUpdate，其中 *val* 是以下其中一個值： ■ 1: 安裝期間執行 LiveUpdate (預設)。 ■ 0: 安裝期間不執行 LiveUpdate。 依預設，群組中全部的 Symantec Endpoint Protection 用戶端都會收到所有內容和產品更新的最新版本。如果用戶端架構為從管理伺服器接收更新，則用戶端只會接收伺服器所下載的更新。如果 LiveUpdate 內容政策允許所有更新，但管理伺服器未下載所有更新，用戶端只會接收伺服器所下載的內容。
ENABLEAUTOPROTECT=*val*	決定安裝完成後是否啟用「檔案系統自動防護」，其中 *val* 是以下任一個值： ■ 1: 安裝後啟用「自動防護」(預設)。 ■ 0: 安裝後停用「自動防護」。
CACHE_INSTALLER=*val*	決定是否在用戶端上快取安裝檔案，其中 *val* 是下列任一個值： ■ 1：快取安裝檔案 (預設)。 ■ 0：不快取安裝檔案。
MIGRATESETTINGS=*val*	決定升級方案中保留設定的狀態，其中 *val* 是下列任一個值： ■ 0：不保留設定或日誌。 ■ 1：保留所有設定和日誌。 ■ 2：僅保留 Sylink.xml 和日誌。
ADDSTARTMENUICON=*val*	決定是否將程式新增到「開始功能表」資料夾，其中 *val* 是下列任一值： ■ 0：不將程式新增到「開始功能表」資料夾。 ■ 1：將程式新增到「開始功能表」資料夾 (預設)。

Symantec Endpoint Protection 指令行用戶端功能

您可以在 Setaid.ini 檔案和 MSI 指令中指定安裝的防護功能。功能多半都有父與子的關係。如果您需要安裝具有父系功能的子系功能，必須也安裝父系功能。例如，如果您指定安裝「防火牆」功能，但是未指定安裝 NTPMain，就不會安裝防火牆。

表 B-3 Symantec Endpoint Protection 用戶端功能

功能	敘述	必選的父系功能
Core	安裝用於用戶端與 Symantec Endpoint Protection Manager 之間通訊的檔案。這是必要的功能。	無
SAVMain	安裝病毒、間諜軟體和基本下載防護。子功能會安裝其他防護。	Core
下載	安裝下載檔案的完整防護。包含「下載鑑識」提供的完整功能性信譽掃描。	SAVMain
NotesSnapin	安裝「Lotus Notes 自動防護」電子郵件功能。 僅適用於低於 14.2 RU1 的版本。	SAVMain
OutlookSnapin	安裝「Microsoft Exchange 自動防護」電子郵件功能。	SAVMain
Pop3Smtp	安裝 POP3 和 SMTP 郵件的防護。僅適用於 32 位元系統。 僅適用於低於 14.2 RU1 的版本。	SAVMain
PTPMain	安裝「主動型威脅防護」元件。	Core
TruScan	安裝 SONAR 掃描功能。	PTPMain
DCMain	安裝「應用程式控制與裝置控制」功能。	PTPMain
NTPMain	安裝「防網路和主機刺探利用」元件。	Core
ITPMain	安裝「網路入侵預防和瀏覽器入侵預防」功能。	NTPMain
防火牆	安裝防火牆功能。	NTPMain
LANG1033	安裝英文資源。	Core

Windows Installer 參數

Symantec Endpoint Protection 用戶端安裝套件會使用標準的 Windows Installer 參數和一組用來進行指令行安裝及部署的延伸檔案。

如需使用標準 Windows Installer 參數的詳細資訊，請參閱 Windows Installer 說明文件。您也可以從指令行執行 msiexec.exe，取得完整的參數清單。

表 B-4 Windows Installer 參數

參數	敘述
Sep.msi (32 位元) Sep64.msi (64 位元)	Symantec Endpoint Protection 用戶端的安裝檔案。如果檔案名稱包含空格，在與 /I 和 /x 一起使用時，請在檔案名稱兩邊加上引號。 必要項
Msiexec	Windows Installer 執行檔。 必要項
/I "*.msi 檔案名稱*"	安裝指定的檔案。如果檔名包含空格，請在檔名兩邊加上引號。如果檔案和您執行的 Msiexec 位於不同的目錄，請指定路徑名稱。如果路徑名稱包含空格，請在路徑名稱兩邊加上引號。例如，`msiexec.exe /I "C:\path to\Sep.msi"` 必要項
/qn	無訊息安裝。 **附註：**使用無訊息部署時，安裝後必須重新啟動加裝到 Symantec Endpoint Protection 的應用程式，如 Microsoft Outlook。
/x "*.msi 檔案名稱*"	解除安裝指定的元件。 選擇性
/qb	顯示安裝進度的基本使用者介面安裝。 選擇性
/l*v *logfilename*	建立詳細的日誌檔，其中 *logfilename* 是您要建立的日誌檔名稱。 選擇性
PRODUCTINSTALLDIR=*path*	在目標電腦上指定一個自訂路徑，其中 *path* 是指定的目標目錄。如果路徑包含空格，請在路徑兩邊加上引號。 **附註：**32 位元電腦的預設目錄為 C:\Program Files\Symantec\Symantec Endpoint Protection。64 位元電腦的預設目錄為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection。 選擇性

參數	敘述
SYMREBOOT=*value*	控制安裝完成後重新啟動電腦，其中 *value* 是一個有效引數。 有效引數如下： ■ Force：要求電腦重新啟動。解除安裝時需要。 ■ Suppress：大部分情況下都不重新啟動。 ■ ReallySuppress：安裝程序完全不重新啟動，甚至是無訊息安裝。 選擇性 **附註：**以無訊息模式解除安裝 Symantec Endpoint Protection 用戶端時，使用 ReallySuppress 防止重新啟動。
ADDLOCAL= *feature*	選取要安裝的自訂功能，其中 *feature* 是一個指定的元件或元件清單。如果沒有使用這個屬性，預設會安裝所有適用的功能，並且安裝只偵測電子郵件程式的自動防護電子郵件用戶端。 若要增加用戶端安裝的全部適當功能，請依照 ADDLOCAL=ALL 使用 ALL 指令。 請參閱第 701 頁的「Symantec Endpoint Protection 指令行用戶端功能」。 **附註：**指定要安裝的新功能時，您必須在已安裝功能名稱中，加上要保留的。如果未指定需要保留的功能，Windows Installer 便會將功能移除。指定現有的功能，就不會覆寫已安裝的功能。若要解除安裝現有的功能，請使用 REMOVE 指令。 選擇性
REMOVE=*feature*	解除安裝先前安裝的程式，或已安裝程式中的特定功能，其中 *feature* 是以下任一項目： ■ *Feature*：從目標電腦解除安裝功能或功能清單。 ■ ALL：解除安裝程式及所有已安裝的功能。如果沒有指定某個功能，那麼預設是 ALL。 選擇性

Windows 資訊安全中心屬性

Symantec Endpoint Protection 用戶端安裝期間，您可以自訂 Windows 資訊安全中心 (WSC) 屬性。這些屬性只適用於非受管用戶端。Symantec Endpoint Protection Manager 控制受管型用戶端的這些屬性。

附註：這些屬性僅適用於 Windows XP Service Pack 3。不適用於執行 Windows Vista 或 Windows 7 或更新版本的用戶端，WSCAVUPTODATE 屬性除外。

「Windows 資訊安全中心」已在 Windows 7 及 Windows 8 中分別重新命名為「行動作業中心」與「重要訊息中心」，在 Windows 10 中則為「安全性與維護」。

表 B-5 Windows 資訊安全中心屬性

屬性	敘述
WSCCONTROL=*val*	控制 WSC，其中 *val* 是以下其中一個值： ■ 0: 不控制 (預設)。 ■ 1: 在第一次偵測到時，停用一次。 ■ 2: 永遠停用。 ■ 3: 若是停用，請還原。
WSCAVALERT=*val*	架構 WSC 的防毒警示，其中 *val* 是以下其中一個值： ■ 0: 啟用。 ■ 1: 停用 (預設)。 ■ 2: 不控制。
WSCFWALERT=*val*	架構 WSC 的防火牆警示，其中 *val* 是以下其中一個值： ■ 0: 啟用。 ■ 1: 停用 (預設)。 ■ 2: 不控制。
WSCAVUPTODATE=*val*	架構防毒定義的 WSC 過期時間，其中 *val* 是以下其中一個值： 1 - 90：天數 (預設為 30)。
DISABLEDEFENDER=*val*	決定安裝期間是否停用 Windows Defender，其中 *val* 是以下其中一個值： ■ 1: 停用 Windows Defender (預設)。 ■ 0: 不停用 Windows Defender。

安裝 Windows 用戶端的指令行範例

表 B-6 指令行範例

工作	指令行
以無訊息模式，使用預設設定將所有 Symantec Endpoint Protection 用戶端元件安裝至目錄 C:\SFN。 抑制電腦重新啟動，然後建立詳細的日誌檔。	`msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log`
以無訊息模式安裝含「病毒和間諜軟體防護」以及入侵預防和防火牆的 Symantec Endpoint Protection 用戶端。 強制電腦重新啟動，然後建立詳細日誌檔。	`msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3Smtp,ITPMain,Firewall SYMREBOOT=Force /qn /l*v c:\temp\msi.log`

使用 Microsoft SCCM/SMS 安裝 Windows 用戶端

您可以使用 Microsoft System Center Configuration Manager (SCCM) 來安裝 Symantec 用戶端軟體。我們假定使用 SCCM 的系統管理員先前已使用 SCCM 安裝軟體。因此，我們假定您不需要使用 SCCM 安裝 Symantec 用戶端軟體的相關詳細資訊。

附註：此主題也適用於 Microsoft Systems Management Server (SMS)。

附註：本附註適用於 SMS 2.0 及更早版本：如果使用 SMS，需要在**「宣告的程式監視器」**中停用用戶端的**「在工具列上顯示所有系統動作的狀態圖示」**功能。在某些情況下，Setup.exe 也許需要更新「宣告的程式監視器」所使用的某個共用檔案。如果檔案在使用中，那麼安裝就會失敗。

賽門鐵克建議 SCCM/SMS 套件啟動 Setup.exe，而非直接啟動 MSI。此方法可啟用安裝程式記錄。使用 SCCM/SMS 中的自訂套件建立功能而非套件精靈功能建立自訂套件。

警告：您應該使用從 Symantec Endpoint Protection Manager 中匯出的受管用戶端安裝套件。如果您使用產品下載或安裝檔案的用戶端安裝套件，則可以部署非受管用戶端。以預設設定安裝非受管用戶端，且用戶端不會與管理伺服器進行通訊。

請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

表 B-7 使用 Microsoft System Center Configuration Manager / Systems Management Server 安裝用戶端的程序

步驟	敘述
步驟 1	從包含軟體和政策的 Symantec Endpoint Protection Manager 中匯出受管用戶端安裝套件，以便安裝到用戶端電腦。依預設，受管用戶端安裝套件包含名為 Sylink.xml 的檔案，該檔案可識別管理用戶端的伺服器。
步驟 2	建立來源目錄，並將 Symantec 用戶端安裝套件複製到該來源目錄。例如，您可以建立來源目錄並複製從 Symantec Endpoint Protection Manager 中匯出的 Setup.exe 檔案。
步驟 3	在 SCCM/SMS 中，建立自訂套件，命名套件，然後將來源目錄指明為套件的一部分。
步驟 4	架構套件的**「程式」**對話方塊，來指定啟動安裝程序的可執行檔，可能的話，也指定具有參數的 MSI。
步驟 5	使用**「宣告」**功能將軟體派送到特定**「集合」**。

如需使用 SCCM/SMS 的詳細資訊，請參閱適合您版本的 Microsoft 說明文件。

使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端

您可以使用 Windows Active Directory 群組原則物件來安裝 Windows 用戶端。此程序假設您已安裝此軟體，並且使用 Windows Active Directory 來安裝具有 Active Directory 群組原則物件的用戶端軟體。

Symantec 用戶端安裝使用標準 Windows Installer (MSI) 檔案。因此，您可以使用 MSI 屬性自訂用戶端安裝。

請參閱第 699 頁的「關於架構 MSI 指令字串」。

您應該確認您的 DNS 伺服器設定正確無誤，然後再進行部署。設定必須正確無誤，因為 Active Directory 仰賴 DNS 伺服器進行電腦通訊。若要測試設定，您可以連線偵測 Windows Active Directory 電腦，然後反向連線偵測。請使用完整的網域名稱。僅使用電腦名稱將無法呼叫新的 DNS 搜尋。格式如下：

```
ping computername.fullyqualifieddomainname.com
```

警告：您應該使用從 Symantec Endpoint Protection Manager 中匯出的受管用戶端安裝套件。如果您使用產品下載或安裝檔案的用戶端安裝套件，則可以部署非受管用戶端。以預設設定安裝非受管用戶端，且用戶端不會與管理伺服器進行通訊。

請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

表 B-8 使用 Active Directory 群組原則物件安裝用戶端軟體的步驟

步驟	動作
步驟 1	透過**「獨立檔案 (.MSI 必需)」**.選項匯出受管用戶端安裝套件。 請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。
步驟 2	佈置安裝檔案的資料夾。例如，將受管用戶端安裝套件複製到您已在其上設定正確權限以允許存取的共用資料夾中。
步驟 3	建立 GPO 軟體派送。 您還應該在正式部署之前，在少數電腦上進行 GPO 安裝測試。如果您未正確架構 DNS，GPO 安裝可能要花一小時或更長時間。 請參閱第 708 頁的「建立 GPO 軟體派送」。
步驟 4	將電腦新增到組織單位。 請參閱第 709 頁的「將電腦新增到組織單位以安裝軟體」。

請參閱第 710 頁的「使用 Active Directory 群組原則物件移除用戶端軟體」。

建立 GPO 軟體派送

如果您在環境中使用 Microsoft Active Directory，則您可以使用 GPO 部署 Symantec Endpoint Protection 用戶端套件至 Windows 電腦。您可建立軟體派送，然後架構軟體套件的 GPO 系統管理範本。

此程序假設您已安裝 Microsoft 的「群組原則管理主控台」，並加裝 Service Pack 1 或更新版本。Windows 介面可能會根據您使用的 Windows 版本而略微不同。

此程序也假設您在 Computers 群組或其他群組中有電腦需要安裝用戶端軟體。您可以選擇性地將這些電腦拖曳到建立的新群組。

請參閱第 707 頁的「使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端」。

建立 GPO 軟體散佈

1. 在 Windows 工作列上，按下**「開始」>「所有程式」>「系統管理工具」>「群組原則管理」**。
2. 在**「Active Directory 使用者和電腦」**視窗的主控台樹狀結構中，在網域上按下滑鼠右鍵，然後按下**「Active Directory 使用者和電腦」**。
3. 在**「Active Directory 使用者和電腦」**視窗中，選取合適網域下的目標組織單位 (OU)。

   您也可以建立新 OU 以供測試或其他用途。如需有關如何建立新 OU 的詳細資訊，請參閱 Microsoft 的 Active Directory 說明文件。
4. 在**「群組原則管理」**視窗的主控台樹狀結構中，在您剛選擇或建立的組織單位上按下滑鼠右鍵，然後按下**「在這裡建立及連結 GPO」**。

   您可能需要重新整理網域，才能看到新建的 OU。
5. 在**「新增 GPO」**對話方塊的「名稱」方塊中，輸入 GPO 的名稱，然後按下**「確定」**。
6. 在右窗格您剛建立的 GPO 上按下滑鼠右鍵，然後按下**「編輯」**。
7. 在**「群組政策物件編輯器」**視窗的左窗格，展開**「電腦設定」**下方的**「軟體設定」**。
8. 在**「軟體安裝」**上按下滑鼠右鍵，再按**「新增」>「套件」**。
9. 在**「開啟」**對話方塊中，輸入指向並包含 MSI 套件的通用命名慣例 (UNC) 路徑。

   使用以下範例所示的格式：

   ***伺服器名稱**SharedDir*\Sep.msi**
10. 按下**「開啟」**。
11. 在**「部署軟體」**對話方塊中，按下**「已指派」**，然後按下**「確定」**。

    如果您選取「軟體安裝」，套件會出現在「群組政策物件編輯器」視窗的右窗格。

架構軟體套件的系統管理範本

1. 在**「群組政策物件編輯器」**視窗的主控台樹狀結構中，顯示並啟用下列設定：

- **「電腦組態」>「系統管理範本」>「系統」>「登入」>「永遠在電腦啟動及登入時等待網路啟動」**
- **「電腦組態」>「系統管理範本」>「系統」>「群組政策」>「軟體安裝政策處理」**
- **「使用者組態」>「系統管理範本」>「Windows 元件」>「Windows Installer」>「永遠以較高的權限安裝」**

附註：如果您啟用了用戶端電腦上的使用者帳戶控制 (UAC)，您也必須啟用**「電腦組態」>「系統管理範本」>「Windows 元件」>「Windows Installer」>「永遠以較高的權限安裝」**，來安裝具有 GPO 的 Symantec 用戶端軟體。設定這些選項，才能讓所有 Windows 使用者安裝 Symantec 用戶端軟體。

---

2 關閉「群組政策物件編輯器」視窗。

3 在**「群組原則管理」**視窗的左窗格中，於剛編輯的 GPO 上按下滑鼠右鍵，然後按下**「強制」**。

4 在右窗格的**「安全性過濾」**下方，按下**「新增」**。

5 在對話方塊的**「輸入要選取的物件名稱」**下方，輸入**「網域電腦」**，然後按下**「確定」**。

將電腦新增到組織單位以安裝軟體

您可以將電腦新增到由 GPO 安裝 Symantec Endpoint Protection 的組織單位。電腦重新啟動時，用戶端軟體安裝程序就會開始。使用者登入電腦時，用戶端軟體安裝程序即告完成。不過，群組政策更新並非即時，因此，需要時間來傳播此政策。下列程序包含您可以在用戶端電腦上執行的指令，以便依照需求更新政策。

請參閱第 707 頁的「使用 Active Directory 群組原則物件 (GPO) 安裝 Windows 用戶端」。

新增電腦到組織單位以安裝軟體

1 在 Windows 工作列上，按下**「開始」>「所有程式」>「系統管理工具」>「Active Directory 使用者和電腦」**。

2 在**「Active Directory 使用者和電腦」**視窗的主控台樹狀結構中，找出一或多部電腦，將其新增到您針對 GPO 安裝所選擇的組織單位。

電腦會先出現在**「電腦」**組織單位中。

3 將電腦拖放到為安裝而選擇或建立的組織單位中。

4 關閉**「Active Directory 使用者和電腦」**視窗。

在用戶端電腦上隨選更新 GPO

1 若要快速將變更套用至用戶端電腦，請在用戶端電腦上開啟指令提示。

2 輸入 **gpupdate**，然後按 **Enter** 鍵。

完成時，「指令提示」視窗會顯示訊息，讓您知道已成功完成政策更新。如果顯示了錯誤訊息，請依照螢幕上的指示取得更多資訊。

3 關閉「指令提示」視窗。

複製 Sylink.xml 檔案以製作受管安裝套件

安裝 Symantec Endpoint Protection Manager 時會為每一個用戶端群組建立 Sylink.xml 檔案。Symantec Endpoint Protection 用戶端會讀取這個檔案的內容，以瞭解哪一部管理伺服器管理用戶端。如果您從取自賽門鐵克的安裝檔案安裝用戶端，則安裝的是非受管用戶端。不過，您可以在安裝之前將 Sylink.xml 檔複製到此資料夾，以安裝受管用戶端。

附註：使用 Symantec Endpoint Protection Manager 主控台匯出的套件是受管套件，並且已經包含 Sylink.xml 檔案。若要匯出可以用「群組政策物件」部署的新受管套件，請使用用戶端部署精靈。按下**「儲存套件」**，然後在系統提示時勾選**「獨立檔案」(.MSI 需要此項)**。

請參閱第 44 頁的「使用儲存套件安裝 Symantec Endpoint Protection 用戶端」。

將 Sylink.xml 檔案複製到產品安裝檔案以製作受管安裝套件

1 在 Symantec Endpoint Protection Manager 中，從正確的用戶端群組匯出 Sylink.xml 檔並將它複製到電腦。

附註：匯出 Sylink.xml 檔之前，應該透過管理主控台建立至少一個新群組。如果未建立，用戶端會出現在預設群組中。

請參閱第 203 頁的「新增群組」。

請參閱第 148 頁的「手動匯出用戶端伺服器通訊檔案 (Sylink.xml)」。

2 將安裝資料夾從您下載的安裝檔案複製到電腦上的資料夾。資料夾 `SEP` 包含 32 位元用戶端，而資料夾 `SEPx64` 包含 64 位元用戶端。

您可以對先前匯出為個別檔案的非受管用戶端套件使用安裝資料夾。

3 將 Sylink.xml 複製到安裝資料夾。在系統提示時取代現有的 Sylink.xml 檔。

使用 Active Directory 群組原則物件移除用戶端軟體

您可以使用 Active Directory 移除已安裝的用戶端軟體。

請參閱第 111 頁的「移除適用於 Windows 的 Symantec Endpoint Protection 用戶端」。

使用 Active Directory 群組原則物件移除用戶端軟體

1. 在 Windows 工作列上，按下**「開始」>「所有程式」>「系統管理工具」>「群組原則管理」**。

   您使用的 Windows 版本可能會在**「開始」**功能表中顯示**「程式集」**，而非**「所有程式」**。

2. 在**「群組原則管理」**視窗的主控台樹狀結構中，展開網域，展開**「電腦設定」**，展開**「軟體設定」**，在**「軟體安裝」**上按下滑鼠右鍵，然後按下**「內容」**。

3. 在**「進階」**標籤上，勾選**「如果這個群組原則物件不再適用於管理領域，就解除這個應用程式安裝」**，然後按下**「確定」**。

4. 在右窗格的軟體封裝上按下滑鼠右鍵，然後按下**「移除」**。

5. 在**「移除軟體」**對話方塊中，勾選**「立刻移除使用者及電腦軟體」**，然後按下**「確定」**。

6. 關閉**「群組原則物件編輯器」**視窗，然後關閉**「群組原則管理」**視窗。

   重新啟動用戶端電腦時，就會移除軟體。

附錄 C

Windows 用戶端的指令行選項

本附錄包含以下主題：

- Endpoint Protection 用戶端服務的 Windows 指令 smc
- smc.exe 指令錯誤碼

Endpoint Protection 用戶端服務的 Windows 指令 smc

您可以使用 smc (或 smc.exe) 指令行介面執行 Windows 用戶端服務。您可以在遠端執行用戶端的程序檔中使用 smc 指令。例如，您可能需要停止用戶端才能在多個用戶端上安裝應用程式。然後，您可以使用程序檔一次停止和重新啟動所有用戶端。

除了 smc -start 參數之外，用戶端服務必須執行，才能使用指令行參數。指令行參數不區分大小寫。對於某些參數，您可能需要密碼 。用戶端不支援 UNC 路徑。

請參閱第 716 頁的「使用 smc 指令行介面執行 Windows 指令」。

請參閱第 717 頁的「smc.exe 指令錯誤碼」。

表 C-1 smc 參數

參數	敘述	套用到
smc -start *	啟動用戶端服務。 傳回 0、-1	所有支援的版本
smc -stop *†	停止用戶端服務，並從記憶體卸載。 傳回 0、-1	所有支援的版本

參數	敘述	套用到
`smc -checkinstallation`	檢查 smc 用戶端服務是否已安裝。 傳回 0、-3	所有支援的版本
`smc -checkrunning`	檢查 smc 用戶端服務是否正在執行。 傳回 0、-4	所有支援的版本
`smc -cloudmanaged` *path_to_sep_setup.exe*	將雲端管理裝置移至另一個雲端網域或租用戶。 將受 Symantec Endpoint Protection Manager 管理的用戶端電腦移至受雲端主控台管理。 對於目的地雲端網域/租用戶，需要 `sep_setup.exe` 安裝檔案。您可從雲端主控台下載此檔案。	自 14.2 RU1 起
`smc -enable -ntp` `smc -disable -ntp` †	啟用/停用 Symantec Endpoint Protection 防火牆與入侵預防系統。	所有支援的版本 自 14.2 RU1 起 `-disable` 的密碼需求
`smc -enable -mem` * `smc -disable -mem` *	啟用/停用 Symantec Endpoint Protection 記憶體攻擊緩和系統。	自 14 MP1 版起
`smc -dismissgui`	關閉用戶端使用者介面。 用戶端仍會執行並繼續保護用戶端電腦。 傳回 0	所有支援的版本
`smc -exportconfig` *†	將用戶端的架構檔匯出至 .xml 檔案。架構檔包含管理伺服器上的所有設定，例如政策、群組、日誌設定、安全設定以及使用者介面設定。 您必須指定路徑名稱和檔案名稱。例如，您可以輸入下列指令： `smc -exportconfig C:\My Documents\MyCompanyprofile.xml` 傳回 0、-1、-5、-6	所有支援的版本

參數	敘述	套用到

`smc -exportlog`	將日誌的全部內容匯出為 `.txt` 檔案。
	若要匯出日誌，請使用下列語法：
	`smc -exportlog log_type0 -1 output_file`
	其中：
	`log_type` 如下：
	■ 0 = 系統日誌
	■ 1 = 安全日誌
	■ 2 = 流量日誌
	■ 3 = 封包日誌
	■ 4 = 控制日誌
	例如，您可以輸入下列語法：
	`smc -exportlog 2 0 -1 c:\temp\TrafficLog`
	其中：
	`0` 是檔案的開頭
	`-1` 是檔案的結尾
	您僅可以匯出「控制日誌」、「封包日誌」、「安全日誌」、「系統日誌」和「流量日誌」。
	`output_file` 是您指派給匯出檔案的路徑名稱和檔案名稱。
	傳回 0、-2、-5
		所有支援的版本

`smc -exportadvrule` *†	將用戶端的防火牆規則匯出為 .xml 檔案。匯出的規則只能夠匯入至處於用戶端控制模式或混合模式的非受管用戶端或受管用戶端。處於伺服器控制模式的受管用戶端會忽略這些規則。 您必須指定路徑名稱和檔案名稱。例如，您可以輸入下列指令： `smc -exportadvrule C:\myrules.xml` 傳回 0、-1、-5、-6 匯入架構檔和防火牆規則時，請注意遵守下列規則： ■ 您無法直接從對應網路磁碟機匯入架構檔或防火牆規則檔案。	所有支援的版本

參數	敘述	套用到
`smc -importadvrule` *†	將防火牆規則匯入用戶端。您匯入的規則會覆寫任何現有的規則。您可以匯入下列項目： ■ 透過 `smc -exportadvrule` 匯出的 .xml 格式規則 ■ 透過用戶端使用者介面匯出的 .sar 格式規則 只有用戶端為非受管用戶端，或是受管用戶端處於用戶端控制模式或混合模式時，才能匯入防火牆規則。處於伺服器控制模式的受管用戶端會忽略這些規則。 若要匯入防火牆規則，請匯入 .xml 或 .sar 檔案。例如，您可以輸入下列指令： `smc -importadvrule C:\myrules.xml` 匯入規則之後，系統日誌會新增項目。 傳回 0、-1、-5、-6 若要附加規則而不是覆寫規則，請從用戶端使用者介面中使用**「匯入規則」**。 請參閱第 221 頁的「防止和允許使用者變更用戶端的使用者介面」。	所有支援的版本
`smc -importconfig` *†	以匯入的架構檔取代用戶端目前架構檔的內容，並更新用戶端的政策。用戶端必須執行才能匯入架構檔的內容。 您必須指定路徑名稱和檔案名稱。例如，您可以輸入下列指令： `smc -importconfig C:\My Documents\MyCompanyprofile.xml`。 傳回 0、-1、-5、-6	所有支援的版本
`smc -importsylink` †	匯入用戶端通訊檔案 (sylink.exe)。	所有支援的版本
`smc -enable -wss` `smc -disable -wss`	啟用或停用 WSS 流量重新導向。	自 14.0.1 MP1 版
`smc -p [password ]`†	與要求密碼的指令搭配使用，其中 [password] 就是所需的密碼。例如： `smc -p [password] -importconfig`	所有支援的版本

參數	敘述	套用到
smc -report	建立包含用戶端上發生之當機和邏輯錯誤的傾印檔案 (.dmp)。此檔案會自動傳送給賽門鐵克技術支援。請聯絡技術支援來尋求協助診斷錯誤。 您可以在以下位置找到傾印檔案： *SEP_Install*\Data\LocalDumps 其中 *SEP_Install* 是安裝資料夾。依據預設，此為 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection*version*。	自 14 版起
smc -runhi	執行主機完整性檢查。 傳回 0	所有支援的版本
smc -showgui	顯示用戶端使用者介面。 傳回 0	所有支援的版本
smc -updateconfig	起始用戶端伺服器通訊，確保用戶端的組態檔是最新的。 如果用戶端組態檔已過時，updateconfig 會下載最新的組態檔，並取代現有的組態檔，也就是 serdef.dat。 傳回 0	所有支援的版本

* 如果符合下列條件，則只有管理員群組的成員可以使用的參數：

- 用戶端執行 Windows /Vista 或 Windows Server 2008，且使用者為 Windows 管理員群組的成員。
  如果用戶端執行 Windows Vista，且啟用「使用者帳戶控制」，使用者會自動同時成為管理員群組和使用者群組的成員。

† 需要密碼的參數。您可以使用密碼保護 Symantec Endpoint Protection Manager 中的用戶端。

使用 smc 指令行介面執行 Windows 指令

1. 在用戶端電腦上，按下**「開始」>「執行」**，然後鍵入 **cmd**。
2. 在 MS-DOS 提示中，執行下列其中一項工作：
   - 如果此參數不需要密碼，請鍵入：
     smc *-parameter*
     其中 *parameter* 是參數。
   - 如果此參數需要密碼，請輸入下列內容：
     - **smc -p *password -parameter***

例如：`smc -p password -exportconfig c:\profile.xml`

附註：您必須在指令之前輸入 `smc` 服務的安裝路徑。例如，在安裝 Symantec Endpoint Protection 到預設位置的 64 位元 Windows 系統上，請輸入：

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe
```

請參閱第 223 頁的「用密碼保護 Symantec Endpoint Protection 用戶端」。

smc.exe 指令錯誤碼

表 C-2 顯示當必要參數無效或遺失時 `smc.exe` 指令傳回的錯誤碼。

表 C-2 `smc.exe` 指令錯誤碼

錯誤碼	說明
0	指令成功。
-1	Windows 管理員群組或 Windows 進階使用者群組中，無此使用者。若用戶端執行 Windows Vista，則 Windows 管理員群組成員中無此使用者。
-2	無效的參數。 您鍵入的參數可能錯誤，或者在參數後方附加了不正確的參數。
-3	未安裝 `smc` 用戶端服務。
-4	並未執行 `smc` 用戶端服務。
-5	無效的輸入檔。 例如，`importconfig`、`exportconfig`、`updateconfig`、`importadv`、`exportadvrule` 與 `exportlog` 參數需要正確的路徑名稱與檔案名稱。
-6	輸入檔不存在。 例如，`importconfig`、`updateconfig` 和 `importadvrule` 參數需要正確的路徑名稱、組態檔名稱 (.xml) 或防火牆規則檔案名稱 (.sar)。

請參閱第 712 頁的「Endpoint Protection 用戶端服務的 Windows 指令 `smc`」。

附錄 D

Symantec Endpoint Protection 工具

本附錄包含以下主題：

Symantec Endpoint Protection 隨附的工具有哪些？

本文說明了 Symantec Endpoint Protection 隨附的工具以及這些工具的用途。

位於 MySymantec 上安裝檔案中的工具

與 Symantec Endpoint Protection Manager 一起安裝的工具

位於 MySymantec 上安裝檔案中的工具

下列工具和說明文件位於從 MySymantec 下載之 Symantec Endpoint Protection 安裝檔案的 /Tools 資料夾中。

- ApacheReverseProxy (12.1.4 及更新版本)
- CentralQ (12.1.6 及更早版本)
- CleanWipe
- ContentDistributionMonitor (SEPMMonitor)
- 欺敵 (14.0.1)
- DeviceInfo (14)、DevViewer
- Integration (WebServicesDocumentation)
- ITAnalytics
- JAWS

- LiveUpdate Administrator (12.1.4 及更早版本)
- 無支援 > MoveClient
- 無支援 > Qextract
- 無支援 > SEPprep (12.1.6 及更早版本)
- OfflineImageScanner (12.1.6 及更早版本)
- PushDeploymentWizard
- SylinkDrop
- SymDiag (SymHelp)
- 虛擬化
- WebServicesDocumentation (Integration)

所有 Symantec Endpoint Protection 版本的產品指南

ApacheReverseProxy (12.1.4 及更新版本)

此工具可在 Symantec Endpoint Protection Manager 中設定 Apache Webserver，以允許 Mac 用戶端和 Linux 用戶端透過 Web 伺服器下載 LiveUpdate 內容。Apache Web 伺服器與 Symantec Endpoint Protection Manager 搭配運作，可在每次發佈新內容時，針對 Mac 和 Linux 用戶端本機下載和快取 LiveUpdate 內容。

此工具適用於用戶端數目較少的網路。

CentralQ (12.1.6 及更早版本)

Symantec Endpoint Protection 可自動將包含受感染檔案及相關副作用的隔離封裝，從本機隔離所轉送到中央隔離所。使用「中央隔離所」可以更方便地收集蒐證資訊。此工具可讓您從受感染電腦擷取範例，而無須直接存取該電腦。

在下列情況下使用 Symantec Endpoint Protection 環境中的隔離所伺服器：

- 從 Symantec Endpoint Protection 用戶端擷取可疑威脅範例。
- 將這些範例自動傳送至安全機制應變中心。
- 下載專門針對僅傳送至隔離所伺服器之可疑威脅的快速發布定義檔。這些定義檔不會推送至產生威脅的 Symantec Endpoint Protection 用戶端。
  快速發布病毒定義檔

如需詳細資訊，請參閱：在 Symantec Endpoint Protection 環境中使用隔離所伺服器的最佳實務準則

CleanWipe

CleanWipe 會解除安裝 Symantec Endpoint Protection 產品。只有在嘗試 Windows 控制台等其他解除安裝方法失敗的情況下，才應使用 CleanWipe 作為最後方法。

解除安裝 Symantec Endpoint Protection

也可以在下列位置 (64 位元) 找到此工具：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

ContentDistributionMonitor (SEPMMonitor)

ContentDistributionMonitor 工具可協助您管理和監控您環境中的多個群組更新提供者 (GUP)。此工具以圖形方式顯示 GUP 的運作狀態和內容派送狀態。

在 12.1.6 及更早版本中，`ContentDistributionMonitor` 命名為 `SEPMMonitor`。在 12.1.5 及更早版本中，`ContentDistributionMonitor` 位於 `NoSupport` 資料夾。

請參閱：Symantec Endpoint Protection 內容派送監控工具

欺敵 (14.0.1)

欺敵可用於偵測端點中使用「欺敵」的對抗活動。此方法的基礎假設為攻擊者已違反網路的主要防禦並在環境中執行偵察。攻擊者會尋找重要資產，例如網域控制器或資料庫憑證。

DeviceInfo (14)、DevViewer

DeviceInfo (適用於 Mac；自 14 版起) 和 DevViewer (適用於 Windows) 可獲取特定裝置的裝置廠商、型號或序號。新增此資訊至**「硬體裝置」**清單。然後，可以將裝置 ID 新增至裝置控制政策，以允許或攔截用戶端電腦上的裝置。

請參閱第 467 頁的「新增硬體裝置至硬體裝置清單中」。

在 Endpoint Protection 中攔截或允許裝置

Integration (WebServicesDocumentation)

自 14 版起，Integration 資料夾已重新命名為 `WebServicesDocumentation`。

WebServicesDocumentation (Integration)

ITAnalytics

IT Analytics 軟體透過讓您建立自訂報告和自訂查詢，來擴充 Symantec Endpoint Protection 提供的內建報告功能。它提供 Symantec Endpoint Protection Manager 資料庫內包含之資料的多維分析和圖形報告功能。此功能可讓您不需要具備資料庫或第三方報告工具的進階知識，就能夠自行瀏覽資料。

JAWS

JAWS 螢幕閱讀器程式和一組程序檔可讓您更易於讀取 Symantec Endpoint Protection 功能表和對話方塊。JAWS 是一項輔助技術，可遵循Section 508 產品存取性。

LiveUpdate Administrator (12.1.4 及更早版本)

Symantec LiveUpdate Administrator 是不同於 Symantec Endpoint Protection 的獨立式 Web 應用程式。LiveUpdate Administrator 會鏡像公用 LiveUpdate 伺服器的內容，然後在內部透過內建 Web 伺服器將該內容提供給賽門鐵克產品。

LiveUpdate Administrator 是 Symantec Endpoint Protection 的選擇性元件，更新 Symantec Endpoint Protection 用戶端時不需要 LiveUpdate Administrator。依據預設，Symantec Endpoint Protection Manager 使用 LiveUpdate 技術而非 LiveUpdate Administrator，以從 Symantec 公用 LiveUpdate 伺服器直接下載內容。

在某些情況下，您可能需要使用 LiveUpdate Administrator。例如，如果 Symantec Endpoint Protection Manager 無法下載內容，您可能需要將內容下載至大量非 Windows 用戶端或用戶端。因此，您可以安裝 LiveUpdate Administrator 伺服器，然後將 Symantec Endpoint Protection Manager 架構為從該伺服器進行下載。

使用 LiveUpdate Administrator 的時機

若要下載 LiveUpdate Administrator 和說明文件，請參閱：下載 LiveUpdate Administrator (LUA)

LiveUpdate Administrator 2.3.x 版本說明

無支援 > MoveClient

`MoveClient` 是 Visual Basic 程序檔，會根據用戶端的主機名稱、使用者名稱、IP 位址或作業系統，將用戶端從一個 Symantec Endpoint Protection Manager 群組移至另一個群組。也可以將用戶端從使用者模式切換為電腦模式，反之亦然。

請參閱第 218 頁的「在使用者模式和電腦模式之間切換 Windows 用戶端」。

無支援 > Qextract

`Qextract` 可從用戶端的本機隔離所解壓縮和還原檔案。如果用戶端隔離了某個檔案，而您認為其為誤報，就可能需要此工具。

無支援 > SEPprep (12.1.6 及更早版本)

SEPprep 是一款不受支援的工具，會自動解除安裝競爭者的防毒產品。如果您要從 Norton 移轉到 Symantec Endpoint Protection，則 SEPprep 還會解除安裝 Symantec Norton™ 產品。

您可以將 SEPprep 封裝在會解除安裝競爭者產品的程序檔中，然後自動且無訊息地啟動 Symantec Endpoint Protection 安裝程式。

請使用「用戶端部署精靈」而非 SEPprep 解除安裝競爭者的產品。在精靈的**「用戶端安裝設定」**標籤中，按下**「自動解除安裝現有的協力廠商安全軟體」**。

請參閱第 104 頁的「架構用戶端套件來解除安裝現有安全軟體」。

使用 SEPprep 解除安裝協力廠商安全軟體

如需「用戶端部署精靈」解除安裝的產品清單，請參閱：

Endpoint Protection 12.1 的協力廠商安全軟體移除

SEPprep 不會解除安裝任何賽門鐵克產品。但是，自版本 14 起，CleanWipe 將內建於「用戶端部署精靈」中，用來移除其他賽門鐵克產品，包括 Symantec Endpoint Protection 用戶端。

OfflineImageScanner (12.1.6 及更早版本)

此工具可掃描和偵測離線 VMware 虛擬磁碟 (.vmdk 檔案) 中的威脅。

關於 Symantec Offline Image Scanner 工具

PushDeploymentWizard

可使用推動部署精靈將 Symantec Endpoint Protection 用戶端安裝套件部署至目標電腦。推動部署精靈與 Symantec Endpoint Protection Manager 中的用戶端部署精靈相同。通常，您可以使用它來部署至較小的電腦或遠端電腦群組。

如需詳細資訊，請參閱 Symantec Endpoint Protection 中的推動部署精靈概觀

SEPIntegrationComponent (12.1.5 及更早版本)

Symantec Endpoint Integration Component (SEPIC) 將 Symantec Endpoint Protection 與使用單一網頁式 Symantec Management Console 的其他 Symantec Management Platform 解決方案合併。您可以使用 SEPIC 清查電腦、更新修補程式、傳送軟體和部署新電腦。您也可以備份和還原系統及資料、管理 DLP 代理程式，以及管理 Symantec Endpoint Protection 用戶端。

SylinkDrop

Sylink.xml 檔案包含 Windows 用戶端或 Mac 用戶端與 Symantec Endpoint Protection Manager 之間的通訊設定。如果用戶端失去與 Symantec Endpoint Protection Manager 之間的通訊，請使用 SylinkDrop 工具自動將用戶端電腦上的現有 Sylink.xml 檔案取代為新的 Sylink.xml 檔案。

取代 Sylink.xml 檔案需執行下列工作：

- 將非受管用戶端轉換為受管用戶端。
- 將用戶端移轉/移動至新的網域或管理伺服器。
- 將無法在管理伺服器上修正的通訊損壞還原至用戶端。
- 將用戶端從一台伺服器移至另一台非遠端複製夥伴的伺服器。
- 將用戶端從一個網域移至另一個網域。

您也可以將此工具僅用於 Windows 用戶端；該工具位於下列位置 (64 位元)：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools`

請參閱第 663 頁的「使用 SylinkDrop 工具還原用戶端伺服器通訊設定」。

SymDiag (SymHelp)

自 14 版起，SymHelp 工具已重新命名為 Symantec Diagnostic (SymDiag)。

SymDiag 是一款多產品診斷工具，可識別常見問答集、收集支援協助式疑難排解所需的資料、提供其他客戶自助和支援資源的連結。SymDiag 也可以針對一些賽門鐵克產品以及 Threat Analysis Scan 提供授權和維護狀態，這有助於找到潛在的惡意軟體。

虛擬化

此虛擬化工具可改善虛擬桌面基礎架構 (VDI) 環境中所安裝用戶端的掃描效能。

- **SecurityVirtualAppliance (12.1.6 及更早版本)**
  賽門鐵克安全性虛擬硬體裝置包含 VMware vShield 基礎架構之具 vShield 功能的共用智慧型掃描快取。
  我需要採取什麼動作來安裝安全性虛擬硬體裝置？
  安裝 Symantec Endpoint Protection 安全性虛擬硬體裝置

- **SharedInsightCache**
  共用智慧型掃描快取工具使用戶端不必掃描 Symantec Endpoint Protection 用戶端已判斷為未感染病毒的檔案，因而改善了虛擬化環境中的掃描效能。如果用戶端掃描某個檔案中是否存在威脅並判斷其未感染病毒，則用戶端會將有關該檔案的資訊傳送至共用智慧型掃描快取。
  此後，當其他用戶端嘗試掃描同一個檔案時，該用戶端可以查詢共用智慧型掃描快取以判斷該檔案是否未感染病毒。如果該檔案未感染病毒，該用戶端不會掃描該特定檔案。如果該檔案感染了病毒，則用戶端會掃描該檔案中的病毒，並將相應結果傳送到共用智慧型掃描快取。
  共用智慧型掃描快取是一種獨立於用戶端執行的 Web 服務。不過，必須架構 Symantec Endpoint Protection 以指定共用智慧型掃描快取的位置，以便用戶端能夠與其通訊。共用智慧型掃描快取透過 HTTP 或 HTTPS 與用戶端通訊。在掃描完成之前，會維持與用戶端的 HTTP 連線。
  安裝和架構 SEP 共用智慧型掃描快取

- **虛擬影像例外**
  若要在 VDI 環境中提高效能和安全性，常見的做法是視需要利用基礎影像建立虛擬機器階段作業。賽門鐵克虛擬影像例外工具可讓 Symantec Endpoint Protection 用戶端略過基礎影像檔威脅掃描，這會降低磁碟 I/O 的資源負載。它還會改善 VDI 環境中的 CPU 掃描程序效能。
  關於賽門鐵克虛擬影像例外工具

WebServicesDocumentation (Integration)

在 12.1.6 及更早版本中，此工具位於 \Tools\Integration 資料夾中。

Symantec Endpoint Protection 包含一組 Web 服務形式的公用 API，可為遠端監控與管理 (RMM) 應用程式提供支援。Web 服務提供有關用戶端和管理伺服器的功能。對 Symantec Endpoint Protection Web 服務的所有呼叫都將透過 OAuth 進行驗證，並且僅允許授權的 Symantec Endpoint Protection 管理員存取。開發人員使用這些 API 將其公司的第三方網路安全解決方案與 Symantec Endpoint Protection 管理伺服器和用戶端進行整合。

針對遠端管理和遠端監控提供支援。遠端管理透過 Web 服務形式的公用 API 提供，可讓您將協力廠商解決方案或自訂主控台與基本用戶端和管理伺服器功能整合。遠端監控透過公開支援的登錄機碼和 Windows 事件記錄提供。

適用於遠端管理的 Web 服務可執行下列工作：

- 除了將授權狀態報告至 Windows 事件日誌外，還會依 Web 服務呼叫報告管理伺服器上的授權狀態和內容狀態。
- 將指令核發給用戶端，例如更新、更新並掃描，以及重新啟動。
- 管理傳送至用戶端的政策。可以從另一部管理伺服器匯入政策，也可以將政策指派至另一部管理伺服器上的群組或位置。

與 Symantec Endpoint Protection Manager 一起安裝的工具

下列工具將與 Symantec Endpoint Protection Manager 一起安裝到以下預設位置：`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools`。

- CleanWipe
- CollectLog
- 資料庫驗證程式
- SetSQLServerTLSEncryption (14)
- SylinkDrop
- Symantec Endpoint Protection Manager API 參考 (14)

CollectLog

CollectLog.cmd 將 Symantec Endpoint Protection Manager 日誌放置在壓縮的 .zip 檔案中。將該 .zip 檔案傳送給 Symantec 支援或其他管理員以進行疑難排解。

可以在下列位置 (64 位元) 找到此工具：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

資料庫驗證程式

可使用 dbvalidator.bat 來協助支援部門診斷 Symantec Endpoint Protection Manager 執行之資料庫所存在的問題。

可以在下列位置 (64 位元) 找到此工具：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

SetSQLServerTLSEncryption (14)

依據預設，Symantec Endpoint Protection Manager 透過加密通道與 Microsoft SQL Server 進行通訊。此工具可讓您停用或啟用管理伺服器和 Microsoft SQL Server 通訊之間的 TLS 加密。從 14 版開始，此工具可用於架構為使用 Microsoft SQL Server 資料庫的管理伺服器安裝。

此工具隨 Symantec Endpoint Protection Manager 一起安裝在下列位置 (64 位元)：C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

Symantec Endpoint Protection Manager API 參考 (14)

Symantec Endpoint Protection Manager 包含一組連線至 Endpoint Detection and Response (EDR) 並從中執行 Symantec Endpoint Protection Manager 作業的 REST API。如果您無法存取 Symantec Endpoint Protection Manager，請使用 API。說明文件位於下列位置：

- 位於下列位址的 Symantec Endpoint Protection Manager 伺服器上，其中 *SEPM-IP* 是 Symantec Endpoint Protection Manager 伺服器的 IP 位址：
  https://*SEPM-IP*:8446/sepm/restapidocs.html
  IP 位址包括 IPv4 和 IPv6。您必須用方括弧括住 IPv6 位址：**http://[*SEPMServer*]:*通訊埠編號***
- 所有 Symantec Endpoint Protection 版本的產品指南

附錄 E

虛擬影像例外工具的指令行選項

本附錄包含以下主題：

- vietool

vietool

vietool – 執行虛擬影像例外工具

大綱

vietool.exe *volume*: --generate|clear|verify|hash [options ...]

敘述

vietool 指令透過新增屬性標示指定磁碟區上的基礎影像檔。

選項

--generate

對指定磁碟區上的所有檔案執行虛擬影像例外工具。不能將此選項與 --clear 搭配使用。

例如：vietool c: --generate

--verify

確認已針對指定磁碟區上的所有檔案設定虛擬影像例外。不能將此選項與 --clear 搭配使用。

例如：vietool c: --verify

--clear

移除指定磁碟區上的所有檔案的虛擬影像例外。

例如：vietool.exe c: --clear

刪除特定檔案：vietool.exe c:\Users\Administrator\target.file --clear

您可以使用完整路徑代替磁碟區識別元，清除單個檔案或資料夾內容的虛擬影像例外。每個指令行只允許有一個檔案名稱、資料夾名稱或磁碟區識別元。不能將此指令與 --generate、--verify 或 --hash 搭配使用。

執行 --clear 指令後，必須重新啟動用戶端。

--hash

針對指定磁碟區上的所有檔案產生雜湊值。

虛擬影像例外工具會使用雜湊將本機檔案排除在以後的掃描外。用戶端會分別計算檔案雜湊，以傳送到共用智慧型掃描快取來儲存掃描結果。不能將此選項與 --clear 搭配使用。

例如：vietool.exe c: --generate --hash

--volume arg

指定該工具掃描的磁碟區。

使用 --clear 選項時，此選項可以是一個檔案。您必須指定磁碟區，磁碟區可以使用磁碟區旗標進行指定，也可以單獨進行指定。例如，使用旗標指定 vietool.exe --volume c: --generate，或單獨指定 vietool.exe c: --generate。

--verbose

將最大量的程式執行資訊輸出到主控台。

--stop

在該工具遇到第一個錯誤時停止。否則，該工具會將錯誤資訊寫入主控台，然後繼續。

--help

顯示此說明訊息。

索引

M

N

P

R

S

T

W

二劃

三劃

四劃

五劃

六劃

七劃

十劃

十一劃

十二劃

十三劃

十四劃