Symantec™ Endpoint Protection 及 Symantec Network Access Control 用戶端指南

Symantec

Symantec Endpoint Protection 及 Symantec Network Access Control 用戶端指南

本書所述軟體係按授權許可協議提供，使用時必須遵照授權許可協議條文。

產品版本：12.1.2

文件版本：12.1.2，第 1 版

版權聲明

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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

技術支援

「賽門鐵克技術支援」維護全球的支援中心。「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。「技術支援」小組亦負責編寫線上「知識庫」。「技術支援」小組會與賽門鐵克的其他部門協力合作，以期在極短的時間內回答您的問題。例如，「技術支援」小組會與「產品工程」以及「賽門鐵克安全機制應變中心」合作，提供警示服務及病毒定義檔更新。

賽門鐵克的維護工作，包含下列項目：

- 廣泛的支援選項，讓您在面對任何規模的組織時都能彈性選取正確的服務量
- 電話和網路支援，提供迅速回應和最新資訊
- 升級保證，可傳遞軟體升級
- 全年無休的全球支援
- 進階功能，包括了「專案管理服務」

如需關於賽門鐵克維護服務方案的詳細資訊，您可以造訪我們的網站，網址為：

http://www.symantec.com/zh/tw/support/index.jsp

聯絡技術支援

具有現行維護服務合約的客戶，可以透過下列網址存取「技術支援」資訊：

http://www.symantec.com/zh/tw/support/index.jsp

在聯絡「技術支援」前，請確認是否符合列示於產品文件中的系統要求。另外，您應位於發生問題的電腦前，以防需要重新建立問題。

在聯絡「技術支援」時，請準備好以下資訊：

- 產品版次
- 硬體資訊
- 可用的記憶體、磁碟空間和 NIC 資訊
- 作業系統
- 版本和修正程式等級
- 網路拓樸
- 路由器、閘道和 IP 位址資訊
- 問題說明：
  - 錯誤訊息和日誌檔
  - 在聯絡賽門鐵克前所執行的疑難排解

- 最新的軟體架構變更及網路變更

授權與註冊

如果您的賽門鐵克產品需要註冊或授權碼，請存取我們的技術支援網頁，網址為：

https://licensing.symantec.com/

客戶服務

您可以在下列網址取得客戶服務資訊：

http://www.symantec.com/zh/tw/support/index.jsp

您可以使用「客戶服務」來協助解決一些非技術性問題，例如下面這些問題：

- 產品授權或序列化等相關問題
- 產品註冊更新，如地址或姓名變更
- 一般產品資訊 (功能、可用的語言、當地代理商)
- 產品更新及升級的最新資訊
- 升級保證與維護合約的相關資訊
- 與賽門鐵克採購計畫相關的資訊
- 對賽門鐵克技術支援選項的相關建議
- 非技術性的預售問題
- 與光碟或手冊相關的問題

維護合約資源

如果您要與賽門鐵克聯絡和現有維護合約相關的事項，請聯絡您所在地區的維護合約管理小組，聯絡資訊如下：

國家/地區	銷售熱線	電子郵件
中國大陸	800 810 8826	China-Sales@symantec.com
台灣	0080 1611 391	Taiwan-Sales@symantec.com
中國香港特別行政區	800 963 421	HongKong-Sales@symantec.com

目錄

1

用戶端入門指南

本章包含以下主題：

關於 Symantec Endpoint Protection 用戶端

Symantec Endpoint Protection 用戶端結合了多層防護，可主動保護電腦，不受已知和未知的威脅及網路攻擊入侵。

表 1-1 說明各層防護。

表 1-1 防護類型

防護層	敘述
病毒和間諜軟體防護	「病毒和間諜軟體防護」可對抗種類繁多的威脅，包括間諜軟體、病蟲、特洛伊木馬程式、Rootkit 和廣告軟體。「檔案系統自動防護」會持續檢查所有電腦檔案是否有病毒和安全風險。「Internet 電子郵件自動防護」會掃描使用 POP3 或 SMTP 通訊協定的內送和外寄電子郵件訊息。「Microsoft Outlook 自動防護」會掃描內送和外寄的 Outlook 電子郵件訊息。 請參閱第 48 頁的「管理電腦上的掃描」。
主動型威脅防護	主動型威脅技術包含 SONAR，此工具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。 請參閱第 82 頁的「在用戶端電腦上管理 SONAR」。
網路威脅防護	「網路威脅防護」包含防火牆和入侵預防系統。以規則為基礎的防火牆可防止未經授權的使用者存取您的電腦。入侵預防系統會自動偵測和攔截網路攻擊。 請參閱第 85 頁的「管理防火牆防護」。

管理員負責控制管理伺服器應將哪些類型的防護下載到您的用戶端電腦。用戶端會自動將病毒定義檔、IPS 定義檔和產品更新下載到電腦。使用可攜式電腦的行動使用者可直接從 LiveUpdate 取得病毒定義檔和產品更新。

請參閱第 35 頁的「更新電腦的防護」。

關於 Symantec Network Access Control 用戶端

Symantec Network Access Control 用戶端會在允許電腦連線到公司網路之前，評估電腦是否已受到適當保護並遵從安全性政策。

用戶端會確保您的電腦遵從管理員架構的安全性政策。安全性政策會檢查電腦是否執行最新的安全軟體，如病毒防護和防火牆應用程式。 如果電腦未執行要求的軟體，您必須手動更新軟體，或者用戶端可能會自動更新軟體。在安全軟體為最新之前，電腦可能會遭到攔截而無法存取網路。用戶端會執行定期檢查，確認電腦是否仍遵從安全性政策。

請參閱第 103 頁的「Symantec Network Access Control 的運作方式」。

狀態頁面入門

當您開啟用戶端時，會出現主視窗和**「狀態」**頁面。

表 1-2 顯示可以從左側功能表列執行的主要工作。

表 1-2 用戶端的主視窗

按下此選項	可執行下列工作
狀態	檢視電腦是否受到防護以及電腦的授權是否有效。「狀態」頁面上的色彩和警示圖示會顯示已啟用且正在防護用戶端的技術。 請參閱第 15 頁的「關於狀態頁面上的警示圖示」。 您可以： ■ 在管理員允許的情況下，啟用或停用一或多項防護技術。 請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。 ■ 檢視「病毒和間諜軟體防護」、「主動型威脅防護」和「網路威脅防護」是否有最新的定義檔。 ■ 執行作用中掃描。 請參閱第 20 頁的「立即掃描電腦」。 ■ 檢視威脅清單，瞭解上次病毒和間諜軟體掃描的結果。
掃描威脅	■ 立即執行作用中掃描或完整掃描。 請參閱第 20 頁的「立即掃描電腦」。 ■ 建立在指定時間、開機或需要時執行的新掃描。 請參閱第 59 頁的「排程使用者定義掃描」。 請參閱第 62 頁的「排程執行隨選或開機掃描」。 ■ 如果安裝有 Symantec Network Access Control，執行主機完整性檢查。 請參閱第 105 頁的「執行主機完整性檢查」。
變更設定	架構下列防護技術功能的設定： ■ 啟用和架構「自動防護」設定。 請參閱第 65 頁的「自訂病毒和間諜軟體掃描設定」。 ■ 架構防火牆設定和入侵預防系統設定。 請參閱第 85 頁的「管理防火牆防護」。 ■ 檢視和新增掃描的例外。 請參閱第 71 頁的「排除掃描項目」。 ■ 顯示通知區圖示。 請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。 ■ 架構竄改防護設定。 請參閱第 45 頁的「啟用、停用與架構竄改防護」。 ■ 建立用於將內容和產品更新下載到用戶端的排程。 請參閱第 36 頁的「依排程更新內容」。 請參閱第 33 頁的「管理電腦的防護」。
檢視隔離所	檢視用戶端偵測到和隔離的病毒及安全風險。在隔離所中您可以還原、刪除、清除、匯出和新增檔案。 請參閱第 74 頁的「關於隔離檔案」。

按下此選項	可執行下列工作
檢視日誌	檢視任何用戶端日誌。 請參閱第 40 頁的「檢視日誌」。
LiveUpdate	立即執行 LiveUpdate。LiveUpdate 會從公司網路內的管理伺服器下載最新的內容定義檔和產品更新。 請參閱第 35 頁的「立即更新內容」。

關於受管用戶端和非受管用戶端

您的管理員可以將用戶端安裝成受管用戶端 (由管理員管理的版本) 或非受管用戶端 (單機版)。

表 1-3 受管用戶端與非受管用戶端之間的差別

用戶端類型	敘述
受管用戶端	受管用戶端會與網路中的管理伺服器通訊。管理員會架構防護和預設設定，接著由管理伺服器將設定下載到用戶端。如果管理員對防護做了變更，變更會在極短時間內下載到用戶端。 管理員可利用下列方式變更您與用戶端互動的程度： ■ 管理員完全管理用戶端。 您不需要架構用戶端。所有設定均會鎖定或無法使用，但您可以檢視用戶端在電腦上所執行動作的相關資訊。 ■ 管理員負責管理用戶端，但您可以變更部分用戶端設定和執行某些工作。例如，您可以執行自己的掃描，以及手動擷取用戶端更新和防護更新。 用戶端設定和設定值的可用性會定期變更。例如，如果管理員更新控制用戶端防護的政策，則設定可能會變更。 ■ 管理員負責管理用戶端，但您可以變更所有用戶端設定和執行所有防護工作。
非受管用戶端	非受管用戶端不會與管理伺服器通訊，管理員也不會管理該用戶端。 非受管用戶端可能是下列類型之一： ■ 未連接至網路的單機型電腦，例如家用電腦或筆記型電腦。該電腦必須已使用預設選項設定或管理員預設的選項設定來安裝 Symantec Endpoint Protection。 ■ 連接至企業網路之前即符合安全性需求的遠端電腦。 用戶端在初次安裝時即具有預設設定。在安裝用戶端之後，您可以變更所有用戶端設定以及執行所有防護工作。

表 1-4 說明受管用戶端與非受管用戶端使用者介面之間的差別。

表 1-4 受管用戶端與非受管用戶端在功能區上的差別

功能區	集中受管用戶端	自我管理用戶端
病毒和間諜軟體防護	用戶端會顯示上鎖的掛鎖圖示，而且無法架構的選項會變成灰色。	用戶端既不會顯示上鎖的掛鎖，也不會顯示未上鎖的掛鎖。
主動型威脅防護	用戶端會顯示上鎖的掛鎖圖示，而且無法架構的選項會變成灰色。	用戶端既不會顯示上鎖的掛鎖，也不會顯示未上鎖的掛鎖。
用戶端管理和網路威脅防護設定	管理員控制的設定不會出現。	所有設定均會出現。

請參閱第 15 頁的「檢查用戶端是受管用戶端還是非受管用戶端」。

檢查用戶端是受管用戶端還是非受管用戶端

若要檢查您擁有多少控制權來架構用戶端上的防護，首先必須檢查用戶端是受管或未受管用戶端。在非受管用戶端上，可架構的設定比受管用戶端多。

請參閱第 14 頁的「關於受管用戶端和非受管用戶端」。

檢查用戶端是受管用戶端還是非受管用戶端

1. 在「**狀態**」頁面上按「**說明**」>「**疑難排解**」。
2. 在「**疑難排解**」對話方塊中按「**管理**」。
3. 在「**管理**」面板的「**一般資訊**」之下，查看「**伺服器**」旁的下列資訊：
   - 如果用戶端為受管用戶端，「**伺服器**」欄位會顯示管理伺服器的位址或「**離線**」文字。
     位址可能是 IP 位址、DNS 名稱或 NetBIOS 名稱。例如，DNS 名稱可能是 SEPMServer1。如果用戶端為受管用戶端，但目前未連線至管理伺服器，此欄位會顯示「**離線**」。
   - 如果用戶端為非受管用戶端，「**伺服器**」欄位會顯示「**自我管理**」。
4. 按下「**關閉**」。

關於狀態頁面上的警示圖示

「狀態」頁面最上方會顯示各種警示圖示來表示電腦的防護狀態。

表 1-5 「狀態」頁面的警示圖示

圖示	敘述
	顯示每種防護均啟用。
	警告您用戶端電腦病毒定義檔不是最新的。若要收到最新的病毒定義檔，在管理員允許的情況下，您可以立即執行 LiveUpdate。 Symantec Network Access Control 用戶端電腦可能有下列問題： ■ 用戶端電腦未通過「主機完整性」安全性遵從檢查。若要找出通過檢查所需的項目，請查看「用戶端管理安全」日誌。 ■ 未連線「主機完整性」。 請參閱第 35 頁的「更新電腦的防護」。
	顯示一或多項防護停用，或用戶端的授權已過期。若要啟用防護，請按下**「修正」**或**「全部修正」**。 請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。

如何使用 Symantec Endpoint Protection 保護我的電腦

Symantec Endpoint Protection 用戶端的預設設定可保護您的電腦免受多種類型的惡意軟體入侵。用戶端會自動處理惡意軟體，或是讓您選擇如何處理惡意軟體。

您可以檢查電腦是否受感染，此外，如果想讓電腦更安全或達到更佳效能，可以執行一些額外的工作。

附註：在受管用戶端上，如果您的管理員已將某些選項架構為不可使用，則這些選項不會出現。在未受管用戶端上，大部分選項都會出現。

表 1-6 關於如何保護電腦的常見問題

問題	敘述
如何得知我的電腦受到保護？	在用戶端主控台中，查看**「狀態」**頁面的頂端。警示圖示的色彩和類型會顯示電腦的防護狀態。 如需詳細資訊，請閱讀**「狀態」**窗格或按下**「詳細資料」**。 請參閱第 15 頁的「關於狀態頁面上的警示圖示」。 請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。

問題	敘述
如何判斷我的電腦是否已受到感染？	如果您的電腦受到感染，可能會看到下列任一個訊息： ■ 「自動防護」偵測或手動掃描偵測。 這些訊息描述威脅以及對威脅所採取的動作。您可以選擇其中一個選項來處理威脅。您可以移除、清除、排除、刪除或復原您選取的動作。如果您的管理員允許，您還可以暫停掃描。 請參閱第 25 頁的「回應病毒或風險偵測」。 請參閱第 24 頁的「關於掃描結果」。 請參閱第 21 頁的「暫停和延緩掃描」。 ■ 「下載智慧型掃描」偵測。 此視窗顯示的資訊是關於「下載智慧型掃描」在您嘗試下載時偵測到的惡意和未經證明的檔案。 請參閱第 27 頁的「回應詢問您要允許或攔截嘗試下載的檔案的下載智慧型掃描訊息」。 請參閱第 23 頁的「警示和通知的類型」。
如果我的電腦已受到感染，如何清除病毒？	如果您看到掃描視窗，表示您的管理員已經設定電腦對感染採取的動作。您或許可以選擇一個動作。如果您知道某個檔案受到感染，請按下**「清除」**或**「隔離」**。 若是排程掃描和「自動防護」，請確定主要動作設為**「清除風險」**，且次要動作設為**「隔離風險」**或**「刪除」**。 請參閱第 25 頁的「回應病毒或風險偵測」。 請參閱第 51 頁的「病毒和間諜軟體掃描的運作方式」。 請參閱第 67 頁的「架構在偵測到惡意軟體與安全風險時採取的動作」。

問題	敘述
如何提高電腦的安全性？	根據預設，您的用戶端電腦會受到最大程度的防護。 您的管理員可能修改了某些用戶端的安全性設定，以改善用戶端的效能。您的管理員也可能讓您修改自己電腦的防護。如果您能夠修改這些設定，則可以執行下列工作： ■ 排程定期完整掃描，通常是一天一次或一週一次。 請參閱第 59 頁的「排程使用者定義掃描」。 ■ 應安裝病毒和間諜軟體掃描、「自動防護」、SONAR、入侵預防及「智慧型掃描」，並隨時保持啟用且最新的狀態。 請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。 請參閱第 44 頁的「啟用或停用自動防護」。 在非受管用戶端上，您可以執行下列工作： ■ 使用 LiveUpdate 下載並安裝正確的病毒定義檔。 根據預設，您的用戶端電腦每天會收到兩次最新的病毒定義檔。不過，您可以自行下載最新的定義檔。 請參閱第 35 頁的「立即更新內容」。 ■ 在啟用所有掃描增強功能的情況下，對電腦執行完整掃描。 依預設，您的電腦每週執行一次全面掃描。 但您也可以隨時執行掃描。 請參閱第 59 頁的「排程使用者定義掃描」。 請參閱第 20 頁的「立即掃描電腦」。

問題	敘述
如果掃描導致工作速度變慢，要如何修改掃描設定？	如果掃描讓電腦的速度變慢，請調整下列設定： ■ 減少排程 LiveUpdate 下載最新病毒定義檔的頻率，或排程在您不使用電腦的時間進行。 請參閱第 36 頁的「依排程更新內容」。 ■ 建立在營業時間後或您不使用電腦時執行的排程完整掃描。 請參閱第 59 頁的「排程使用者定義掃描」。 ■ 將您已知為安全的應用程式和檔案排除在掃描範圍之外。 請參閱第 71 頁的「排除掃描項目」。 ■ 限制排程掃描、「自動防護」和「下載智慧型掃描」掃描經常帶有感染之檔案類型的副檔名。例如，指定掃描尋找可執行檔，例如 EXE、COM、BAT 和 VBS。 ■ 在「自動防護」中，停用**「掃描安全風險」**。 請參閱第 65 頁的「自訂病毒和間諜軟體掃描設定」。 **警告：**您可以停用「自動防護」來改善用戶端電腦的效能或進行用戶端疑難排解。不過，賽門鐵克建議您將「自動防護」隨時保持在啟用狀態。 請參閱第 44 頁的「啟用或停用自動防護」。 ■ 停用作用中掃描、完整掃描或自訂掃描中的掃描增強功能選項。 請參閱第 59 頁的「排程使用者定義掃描」。 ■ 停用「下載智慧型掃描」和「智慧型掃描查詢」。 請參閱第 64 頁的「自訂下載智慧型掃描設定」。 請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。 **附註：**如果您的管理員未提供這些設定，您可能無法變更這些設定。
如果防火牆阻止我瀏覽網際網路，該怎麼做？	根據預設，防火牆不會攔截網際網路存取。如果您無法存取網際網路，請聯絡管理員。管理員可能攔截了對特定網站的存取，或是不允許您的電腦使用特定瀏覽器。您不一定有權限修改防火牆規則。 在未受管用戶端上，您可以修改防火牆規則。不過，除非您瞭解防火牆規則攔截的流量是否為惡意，否則不應該變更或新增防火牆規則。 在您修改防火牆規則之前，請先釐清下列問題： ■ 存取網際網路的 Web 應用程式是否合法？ ■ Web 應用程式存取的遠端通訊埠是否正確？HTTP 流量對於 Web 應用程式而言是合法的流量，且 HTTP 流量使用通訊埠 TCP 80 和 443。您可能無法信任來自其他通訊埠的流量。 ■ 應用程式存取的網站 IP 位址是否正確或合法？

問題	敘述
通知區域中出現訊息時要採取什麼動作？	讀取工具列上通知區域中的訊息。 通知會告訴您下列其中一件事： ■ 您的電腦可能遭受攻擊，且用戶端已處理威脅。 ■ 您的電腦收到新的安全性政策。 安全性政策會自動更新。您也可以隨時更新安全性政策。 請參閱第 37 頁的「手動更新用戶端的政策」。 請參閱第 25 頁的「回應病毒或風險偵測」。 請參閱第 29 頁的「回應詢問您是允許還是攔截應用程式的訊息」。 根據威脅的類型而定，您還可以查看其中一個日誌檔中的詳細資訊。 請參閱第 40 頁的「檢視日誌」。

請參閱第 14 頁的「關於受管用戶端和非受管用戶端」。

請參閱第 15 頁的「檢查用戶端是受管用戶端還是非受管用戶端」。

請參閱第 33 頁的「管理電腦的防護」。

立即掃描電腦

您可以隨時手動掃描病毒和安全風險。如果最近安裝了用戶端或收到病毒或安全風險，應該立即掃描電腦。

可以選取單一檔案、一張磁片或甚至整個電腦進行掃描。隨選掃描包括「作用中掃描」與「完整掃描」。您也可以建立隨選執行的自訂掃描。

請參閱第 62 頁的「排程執行隨選或開機掃描」。

請參閱第 35 頁的「更新電腦的防護」。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

立即掃描電腦

◆ 執行下列其中一項動作：

- 在用戶端**「狀態」**頁面的**「病毒和間諜軟體防護」**旁，按下**「選項」>「執行作用中掃描」**。
- 在用戶端的側邊看板中，按下**「掃描威脅」**。
  執行下列其中一項動作：
  - 按下**「執行作用中掃描」**。
  - 按下**「執行完整掃描」**。
  - 在掃描清單中，在任何掃描上按下滑鼠右鍵，然後按下**「立即掃描」**。

隨即會開始掃描。

除非您的管理員停用掃描進度選項，否則您可以檢視掃描進度。若要檢視掃描進度，請按下目前掃描顯示的訊息連結：**「<掃描> 進行中」**。

請參閱第 24 頁的「關於掃描結果」。

您也可以暫停或取消掃描。

請參閱第 21 頁的「暫停和延緩掃描」。

從 Windows 掃描電腦

- 在「我的電腦」或「Windows 檔案總管」視窗中，在需要掃描的檔案、資料夾或磁碟機按下滑鼠右鍵，然後按下**「掃描病毒」**。

  32 位元和 64 位元作業系統支援此功能。

附註：當您執行此類型的掃描時，「智慧型掃描查詢」不會掃描資料夾或磁碟機。 如果您選取要掃描的檔案或檔案群組，「智慧型掃描查詢」會執行。

暫停和延緩掃描

暫停功能可讓您在掃描期間隨時停止掃描，並在稍後繼續進行掃描。您可以暫停您起始的任何掃描。

網路管理員可以決定，您是否可以暫停管理員啟動的掃描。如果無法使用**「暫停掃描」**選項，表示管理員已停用暫停功能。如果您的管理員已啟用「延緩」功能，則您可以將管理員排定的掃描延後一段設好的間隔時間後執行。

掃描繼續時，會從掃描停止處開始。

附註：如果您在用戶端掃描壓縮檔時暫停掃描，用戶端可能要幾分鐘才能回應暫停要求。

請參閱第 48 頁的「管理電腦上的掃描」。

暫停您所啟動的掃描

1. 掃描執行時，請在掃描對話方塊中，按下**「暫停掃描」**。

   掃描會停在目前的階段，而且掃描對話方塊會一直保持開啟，直到重新啟動掃描為止。

2. 在掃描對話方塊中按下**「繼續掃描」**，繼續進行掃描。

暫停或延緩管理員啟動的掃描

1. 管理員啟動的掃描執行時，請在掃描對話方塊中按下「**暫停掃描**」。
2. 在「**排程掃描暫停**」對話方塊中，進行下列任一動作：
   - 若要暫停掃描，請按下「**暫停**」。
   - 若要延緩掃描，請按下「**延緩 1 小時**」或「**延緩 3 小時**」。
     您的管理員會指定您可以延緩掃描的時間長度。暫停的時間到達限制時，便會從頭開始重新掃描。您的管理員會指定在停用此功能之前，您可以延緩排程掃描的次數。
   - 若要繼續掃描不暫停，請按下「**繼續**」。

使用 Symantec Endpoint Protection 支援工具排除電腦問題

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 Endpoint Protection 支援工具排除電腦問題

1. 執行下列其中一項工作：
   - 請參閱知識庫文章 Symantec Diagnostic and Product Advisor。
   - 在用戶端中，按下「**說明**」>「**下載支援工具**」。
2. 按照螢幕上的指示進行。

2

回應警示與通知

本章包含以下主題：

警示和通知的類型

用戶端會在背景執行，防護您的電腦，使您安全無虞，不受惡意活動的威脅。有時候，用戶端必須通知您偵測到的活動，或者提示您提供回應。

表 2-1 顯示您可能會看到和需要回應的訊息類型。

表 2-1 警示和通知的類型

警示	敘述
「<掃描名稱>啟動於」或**「Symantec Endpoint Protection 偵測結果」**對話方塊	如果掃描偵測到病毒或安全性風險，會顯示掃描結果或包含感染詳細資料的**「Symantec Endpoint Protection 偵測結果」**對話方塊。對話方塊也會顯示掃描處理風險時所採取的動作。除了檢視活動和關閉對話方塊，您一般不需要採取任何進一步的動作。然而，若有必要，您也可以採取進一步的行動。 請參閱第 24 頁的「關於掃描結果」。

警示	敘述
其他訊息對話方塊	在下列情況，您會看見彈出式訊息： ■ 用戶端自動更新用戶端軟體。 請參閱第 30 頁的「回應訊息以更新用戶端軟體」。 ■ 用戶端詢問您要允許或攔截應用程式。 請參閱第 29 頁的「回應詢問您是允許還是攔截應用程式的訊息」。 ■ 用戶端的試用版授權已過期。 請參閱第 30 頁的「回應過期的授權訊息」。

通知區圖示訊息	在下列情況，通知區圖示中會出現通知：
	■ 用戶端攔截應用程式。
	例如，您可能會看見以下通知：
	`Traffic has been blocked from this application: (application name)`
	如果用戶端被架構為攔截全部流量，這些通知會經常出現。如果您的用戶端被架構為允許全部流量，這些通知將不會出現。
	請參閱第 29 頁的「回應詢問您是允許還是攔截應用程式的訊息」。
	■ 當用戶端偵測到危害電腦的網路攻擊。
	您可能會看見以下類型的通知：
	`Traffic from IP address 192.168.0.3 is blocked from 2/14/2010 15:37:58 to 2/14/2010 15:47:58. Port Scan attack is logged.`
	■ 安全性遵從檢查失敗。系統可能會攔截出入電腦的流量
	除了讀取訊息外，您不需要執行其他動作。

請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。

關於掃描結果

若是受管用戶端，您的管理員通常會架構每週至少執行一次完整掃描。若是非受管用戶端，當您啟動電腦時，就會執行自動產生的作用中掃描。「自動防護」預設會持續在您的電腦上執行。

掃描執行時，會出現掃描對話方塊，以報告進度和顯示掃描結果。掃描完成時，結果會顯示在清單中。若用戶端未偵測到任何病毒或安全風險，清單將維持空白，且狀態為「已完成」。

如果用戶端在掃描期間偵測到風險，掃描結果對話方塊會顯示含有下列資訊的結果：

- 病毒或安全風險的名稱
- 受感染檔案的名稱
- 用戶端對風險所執行的動作

如果用戶端偵測到病毒或安全風險，您可能需要對受感染的檔案採取動作。

附註：針對受管用戶端，管理員可能會選擇隱藏掃描結果對話方塊。如果用戶端未受管理，您可以顯示或隱藏此對話方塊。

如果您或管理員架構用戶端軟體顯示掃描結果對話方塊，則可以暫停、重新啟動或停止掃描。

請參閱第 14 頁的「關於受管用戶端和非受管用戶端」。

請參閱第 25 頁的「回應病毒或風險偵測」。

請參閱第 21 頁的「暫停和延緩掃描」。

回應病毒或風險偵測

管理員定義掃描、使用者定義掃描或「自動防護」執行時，您可能會看到掃描結果對話方塊。您可以利用掃描結果對話方塊，立即對受影響的檔案採取動作。例如，您可能會決定將已清除病毒的檔案刪除，因為您想要以原始檔案取代該檔案。

如果 Symantec Endpoint Protection 需要終止程序或應用程式，或需要停止服務，**「立即移除風險」**選項便會啟用。對話方塊中的風險要求您採取動作時，您可能無法關閉對話方塊。

您也可以稍後使用「隔離所」、「風險日誌」或「掃描日誌」對檔案執行動作。

在掃描結果對話方塊中回應病毒或風險偵測

1 在掃描結果對話方塊中，選取要對其採取動作的檔案。

2 用滑鼠右鍵按下選擇項目，再選取下列其中一個選項：

清除	移除檔案中的病毒。此選項僅適用於病毒。
排除	將檔案排除在再次掃描的範圍以外。
永久刪除	刪除受感染的檔案和所有的副作用。對於安全風險，請審慎使用此動作。某些情況下，如果刪除安全風險，可能會造成應用程式無法運作。
復原採取的動作	復原採取的動作。
移到隔離所	將受到感染的檔案置入「隔離所」內。若是安全風險，用戶端也會嘗試移除或修復其副作用。在某些情況下，如果用戶端隔離安全風險，可能會造成應用程式無法運作。
屬性	顯示有關病毒或安全風險的資訊。

在某些情況下，可能會無法使用動作。

3 在對話方塊中，按下**「關閉」**。

如果列出的風險要求您執行動作，您可能無法關閉對話方塊。例如，用戶端可能需要終止程序或應用程式，也可能需要停止服務。

如果需要採取動作，會顯示下列其中一個通知：

- **需要移除風險**
  在風險需要終止程序時出現。如果您選擇移除風險，就會回到結果對話方塊。如果也需要重新啟動，對話方塊中的風險列會指出需要重新啟動。
- **需要重新啟動**
  在風險需要重新啟動時出現。
- **需要移除風險並重新啟動**
  在風險需要終止程序且另一個風險需要重新啟動時出現。

4 如果**「立即移除風險」**對話方塊顯示，請按下下列選項之一：

- **立即移除風險(建議)**
  用戶端移除風險。移除風險可能需要重新啟動。對話方塊中的資訊會指明是否需要重新啟動。
- **不要移除風險**

該結果對話方塊會提醒您是否仍需採取動作。不過，在您重新啟動電腦後，**「立即移除風險」**對話方塊會顯示。

5 如果結果對話方塊在步驟 3 中未關閉，請按下**「關閉」**。

如果需要重新啟動，移除或修復會在您重新啟動電腦後才完成。

您可能需要對風險採取動作，但可以選擇稍後再執行動作。

使用下列方式可稍後移除或修復風險：

- 您可以開啟「風險日誌」，在風險上按下滑鼠右鍵，然後執行動作。
- 您可以執行掃描來偵測風險，然後重新開啟結果對話方塊。

在對話方塊中的風險上按下滑鼠右鍵，再選取動作，也可以執行動作。您可以執行的動作取決於已針對掃描偵測出的特定風險類型所架構的動作。

請參閱第 57 頁的「掃描如何回應偵測到的病毒或風險」。

請參閱第 40 頁的「檢視日誌」。

請參閱第 48 頁的「管理電腦上的掃描」。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

回應詢問您要允許或攔截嘗試下載的檔案的下載智慧型掃描訊息

「下載智慧型掃描」通知顯示的資訊是關於在您嘗試下載時偵測到的惡意檔案和未經證明的檔案。

附註：如果針對未證明檔案的動作為**「提示」**時，則無論您是否啟用通知，都將收到偵測訊息。

您或您的管理員可以變更「下載智慧型掃描」對惡意檔案的敏感程度。變更靈敏度等級可能會變更您收到的通知數目。

「下載智慧型掃描」使用「智慧型掃描」。「智慧型掃描」會根據數百萬使用者構成的全球社群評估檔案並決定檔案分級。

「下載智慧型掃描」通知會顯示以下與偵測到的檔案相關的資訊：

- 檔案信譽
  檔案信譽表示檔案的信任度。惡意檔案不受信任。未證明的檔案可能受信任，也可能不受信任。
- 檔案在社群中的常用程度
  檔案的普及率非常重要。不常使用的檔案較可能是威脅。

- 檔案新舊程度
  檔案愈新，賽門鐵克掌握的檔案相關資訊愈少。

此資訊可協助您決定要允許還是攔截檔案。

回應要求您允許或攔截您嘗試下載之檔案的「下載智慧型掃描」偵測

- 在「下載智慧型掃描」偵測訊息中，執行下列動作之一：
  - 按下**「從電腦中移除此檔案」**。
    「下載智慧型掃描」會將此檔案移至「隔離所」。 只會針對未證明的檔案顯示此選項。
  - 按下**「允許此檔案」**。
    您可能會看到權限對話方塊，詢問您是否確定要允許使用此檔案。
    如果您選擇允許使用未被隔離的未證明檔案，則此檔案會自動執行。 如果您選擇允許使用隔離的檔案，則此檔案不會自動執行。 您可以從 Internet 暫存資料夾執行此檔案。
    通常，此資料夾位置為 `\\Documents and Settings\username\Local Settings\Temporary Internet Files`。
    若為非受管用戶端，如果您允許使用某個檔案，用戶端會在此電腦上自動為此檔案建立例外。若為受管用戶端，如果管理員可讓您建立例外，用戶端會在此電腦上自動為此檔案建立例外。

請參閱第 62 頁的「管理電腦上的下載智慧型掃描偵測」。

請參閱第 58 頁的「Symantec Endpoint Protection 如何使用信譽資料進行檔案相關決策」。

請參閱第 48 頁的「管理電腦上的掃描」。

回應出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知

在 Windows 8 用戶端電腦上，用於惡意軟體偵測及其他重要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。不論您目前檢視的是哪一個介面，通知都會警示您 Windows 8 樣式使用者介面或 Windows 8 桌面上發生的事件。您可以在 Windows 桌面上，檢視有關以訊息產生通知之事件的詳細資料。

在受管用戶端上，您的管理員可能會關閉彈出式通知。

回應出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知

1. 在出現於畫面頂端的彈出式通知中，執行下列其中一個工作：
   - 在 Windows 8 樣式使用者介面中，按下該通知。
     桌面便會出現。

- 在桌面上，按下該通知。
  通知便會消失。

2 檢閱出現在桌面上的偵測結果或其他參考用訊息。

  對於不影響Windows 8樣式應用程式的病毒和間諜軟體偵測，您可能需要或想要執行其他矯正動作。對於影響Windows 8樣式應用程式的偵測，您可以執行的唯一額外動作是**「排除」**。

  當您返回Windows 8樣式使用者介面時，可能會在受影響的應用程式上看到一個圖示，表示您必須重新下載應用程式。

請參閱第 77 頁的「如何管理出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知」。

請參閱第 25 頁的「回應病毒或風險偵測」。

回應詢問您是允許還是攔截應用程式的訊息

當電腦上的應用程式嘗試存取網路時，用戶端可能會詢問您要允許或攔截應用程式。您可以選擇攔截您認為不安全的應用程式，防止其存取網路。

此類型的通知顯示原因有：

- 應用程式要求存取您的網路連線。
- 存取您網路連線的應用程式已升級。
- 您的管理員升級了用戶端軟體。

您可能會看見下列訊息，通知您有應用程式嘗試存取您的電腦：

```
IEXPLORE.EXE is attempting to access the network.
Do you want to allow this program to access the network?
```

回應要求您允許或攔截應用程式的訊息

1 另一個選擇是，如果希望下次應用程式嘗試存取網路時不顯示此訊息，請在對話方塊中按下**「記住我的答案，請勿再針對這項應用程式詢問我」**。

2 執行下列其中一項動作：

  - 若要允許應用程式存取網路，請按下**「是」**。
  - 若要阻止應用程式存取網路，請按下**「否」**。

  您可以在「執行中的應用程式」欄位或「應用程式」清單中變更應用程式動作。

請參閱第 97 頁的「建立當應用程式從您的電腦存取網路時的防火牆規則」。

回應過期的授權訊息

用戶端會使用授權來更新掃描的病毒定義檔以及更新用戶端軟體。用戶端可使用試用版授權或已付費授權。如果試用版授權已到期，用戶端就不會再更新任何內容或用戶端軟體。

表 2-2 授權類型

授權類型	敘述

試用版授權	如果試用版授權過期，用戶端的「狀態」面板最上方會變成紅色，並顯示下列訊息：
	
	`Evaluation License has expired.`
	
	`All content download will discontinue on` *`date`*`. Please contact your Administrator to purchase a full Symantec Endpoint Protection License.`
	
	您也可以按**「說明」>「關於」**來檢視到期日。

已付費授權	如果已付費授權過期，用戶端的「狀態」面板最上方會變成黃色，並顯示下列訊息： `Virus and Spyware Protection definitions are out of date.`

不論是哪種授權，您都必須聯絡管理員來更新或續購授權。

請參閱第 23 頁的「警示和通知的類型」。

請參閱第 40 頁的「檢視日誌」。

回應訊息以更新用戶端軟體

如果用戶端軟體已自動更新，您會看見下列通知：

```
Symantec Endpoint Protection has detected that
a newer version of the software is available from
the Symantec Endpoint Protection Manager.
Do you wish to download it now?
```

回應自動更新通知

1 執行下列其中一項動作：

- 若要立刻下載軟體，請按下**「立即下載」**。

- 若要在指定時間後被提醒，請按下**「稍後提醒我」**。

2 如果更新軟體的安裝程序開始後顯示一則訊息，請按下**「確定」**。

3

確保電腦受到防護

本章包含以下主題：

管理電腦的防護

您的電腦預設會受到防護，應該不需要架構用戶端。不過，您可能會因為下列原因而想要監控防護情況：

- 您的電腦執行的是非受管用戶端。
  安裝非受管用戶端之後，只有您可以控制電腦的防護。非受管用戶端預設會受到防護，但您可能需要修改電腦的防護設定。
- 您想啟用或停用一或多項防護技術。
- 您想確認是否有最新的病毒定義檔。
- 您聽說最近出現新病毒或安全威脅，想要執行掃描。

表 3-1 管理電腦防護的程序

步驟	敘述
回應警示或通知	回應出現並要求您輸入資訊的訊息。例如，掃描可能偵測到病毒或安全風險，並且會顯示掃描結果，要求您對偵測到的病毒或安全風險採取動作。 請參閱第 23 頁的「警示和通知的類型」。
檢查防護狀態	定期檢查**「狀態」**頁面，確定所有類型的防護均啟用。 請參閱第 12 頁的「狀態頁面入門」。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。
更新病毒定義檔	檢查電腦是否安裝了最新的病毒定義檔。 ■ 檢查是否有最新的防護更新。您可以在用戶端的**「狀態」**頁面，於每種防護類型底下檢查這些定義檔的日期和編號。 ■ 取得最新的防護更新。 請參閱第 35 頁的「更新電腦的防護」。 在管理員允許的情況下，您可以在受管用戶端上執行這些工作。
掃描電腦	執行掃描來檢查電腦或電子郵件應用程式是否有任何病毒。用戶端預設會在您開啟它時掃描電腦，但您可以隨時掃描電腦。 請參閱第 20 頁的「立即掃描電腦」。
調整防護設定	在大多數情況下，預設設定即能為電腦提供足夠的防護。如有需要，您可以減少或加強下列類型的防護： ■ 排定額外的掃描 請參閱第 48 頁的「管理電腦上的掃描」。 ■ 新增防火牆規則 (僅適用於非受管用戶端) 請參閱第 85 頁的「管理防火牆防護」。
檢視日誌中的偵測或攻擊記錄	查看日誌來確認用戶端是否偵測到病毒或網路攻擊。 請參閱第 40 頁的「檢視日誌」。
更新安全性政策 (僅適用於受管用戶端)	檢查用戶端是否從管理伺服器收到最新的安全性政策。安全性政策包含適用於用戶端的最新防護技術設定。 安全性政策會自動更新。若要確保您有最新的政策，您可以手動更新它，請用滑鼠右鍵按下用戶端通知區圖示，然後按下**「更新政策」**即可。 請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。

請參閱第 14 頁的「關於受管用戶端和非受管用戶端」。

更新電腦的防護

賽門鐵克的產品需要擁有最新的資訊，才能保護您的電腦免受最新的病毒侵入。這些資訊是透過賽門鐵克的 LiveUpdate 提供。

內容更新檔利用最新的威脅防護技術，使賽門鐵克產品保持在最新狀態。您收到的內容更新視您安裝在電腦上的防護而定。例如，LiveUpdate 會下載病毒和間諜軟體防護的病毒定義檔，以及「網路威脅防護」的 IPS 定義檔。

LiveUpdate也可以在需要時，提供已安裝用戶端的改進功能。這些改進的建立通常是用來延伸作業系統或硬體的相容性、調整效能問題，或是修正產品錯誤。

LiveUpdate 會從賽門鐵克 Internet 網站擷取新的內容檔，然後取代舊的內容檔。用戶端電腦可直接從 LiveUpdate 伺服器收到這些改進。受管用戶端電腦也可以自動從公司的管理伺服器收到這些改進更新。您的電腦收到更新的方式取決於您的電腦是受管電腦還是非受管電腦，以及管理員架構更新的方式。

表 3-2 更新電腦內容的方式

工作	敘述
依排程更新內容	依預設，LiveUpdate 會在排程間隔自動執行。 在非受管用戶端上，您可以停用或變更 LiveUpdate 排程。 請參閱第 36 頁的「依排程更新內容」。
立即更新內容	根據您的安全性設定，您可以立即執行 LiveUpdate。 請參閱第 35 頁的「立即更新內容」。

立即更新內容

您可以使用 LiveUpdate 立即更新內容檔。在下列情況下，您應手動執行 LiveUpdate：

- 用戶端軟體是最近安裝的。
- 自上次掃描以來經過了一段長時間。
- 您懷疑有病毒或其他惡意軟體問題。

請參閱第 36 頁的「依排程更新內容」。
請參閱第 35 頁的「更新電腦的防護」。

立即更新防護

- 在用戶端的側邊看板中，按下 **LiveUpdate**。

  LiveUpdate 會連線至賽門鐵克伺服器，並檢查可用的更新，然後自動下載和安裝這些更新。

依排程更新內容

您可以建立排程，以便 LiveUpdate 在排程間隔自動執行。 您可以排程 LiveUpdate 在您未使用電腦的期間執行。

請參閱第 35 頁的「立即更新內容」。

附註：如果使用的是受管用戶端，則您必須在管理員允許的情況下，才能架構 LiveUpdate 依排程執行。如果顯示掛鎖圖示而且選項顯示為灰色，則表示您無法按排程更新內容。

依排程更新防護

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在**「用戶端管理」**旁邊，按下**「架構設定」**。
3. 在**「用戶端管理設定」**對話方塊中，按下 **LiveUpdate**。
4. 在 **LiveUpdate** 標籤上，勾選**「啟用自動更新」**。
5. 在**「頻率及時間」**群組方塊中，選取要每日、每週或每月執行更新。然後，選取要執行更新的天或週、以及一天當中的時刻。

   時間設定取決於您在**「頻率」**群組方塊中選取的內容。其他選項是否可用，還取決於您選取的頻率。
6. 在**「重試時段」**群組方塊中勾選**「持續嘗試」**，然後指定用戶端再次嘗試執行 LiveUpdate 的時間間隔。
7. 在**「隨機選項」**群組方塊中勾選**「隨機設定開始時間為 + 或 -(小時)」**，然後指定小時數或天數。

   此選項會設定更新在排程時間前後開始的時間範圍。
8. 在**「閒置偵測」**群組方塊中，勾選**「延緩排程 LiveUpdate 直到系統閒置。逾期階段作業最終會無條件執行。」**

   您還可架構選項以使 Proxy 伺服器連線至內部 LiveUpdate 伺服器。 若需這些選項的相關資訊，請參閱線上說明。
9. 按下**「確定」**。

手動更新用戶端的政策

如果您認為您沒有最新的用戶端政策，可以手動更新用戶端電腦的政策。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。

從用戶端電腦手動更新政策

1 在用戶端電腦上的用戶端使用者介面中，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」**面板的**「政策設定檔」**下，按下**「更新」**。

如何決定用戶端是否連線和受保護

您可以檢查用戶端上的通知區圖示，判斷用戶端是否連線至管理伺服器以及獲得適當保護。

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。

附註：在受管用戶端上，如果管理員已架構為不能使用，則通知區域圖示不會出現。

表 3-3 Symantec Endpoint Protection 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。此圖示是一個純黃色盾牌。
	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防護電腦。此圖示是一個加上綠點的黃色盾牌。
	用戶端發生次要問題。例如，病毒定義檔可能過期。此圖示是一個黃色盾牌加上含黑色驚嘆號的淡黃點。
	用戶端未執行、發生了重大問題，或至少有一個防護技術停用。例如，「網路威脅防護」可能已停用。此圖示是一個黃色盾牌加上被紅圈包住的白點，白點上還有一條紅線穿越。

表 3-4 會顯示通知區域中所出現的 Symantec Network Access Control 用戶端狀態圖示。

表 3-4 Symantec Network Access Control 用戶端狀態圖示

圖示	敘述
	用戶端執行時未發生問題，且已通過「主機完整性」檢查並更新了安全性政策。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。此圖示是一個純金色鑰匙。
	用戶端執行時未發生問題，且已通過「主機完整性」檢查並更新了安全性政策。該用戶端與伺服器通訊。此圖示是一個加上綠點的金色鑰匙。
	用戶端「主機完整性」檢查失敗或未更新安全性政策。此圖示是一個金色鑰匙加上含白色 x 的紅點。

請參閱第 38 頁的「隱藏及顯示通知區域圖示」。

隱藏及顯示通知區域圖示

如有需要您可以隱藏通知區域圖示。例如，如果在 Windows 工作列上需要更多空間時，可以將它隱藏。

請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。

附註：在受管用戶端上，如果您的管理員限制使用此功能，您便無法隱藏通知區域圖示。

隱藏或顯示通知區域圖示

1. 在主視窗的側邊看板中，按下**「變更設定」**。
2. 在**「變更設定」**頁的**「用戶端管理」**旁，按**「架構設定」**。
3. 在**「用戶端管理設定」**對話方塊**「一般」**標籤下的**「顯示選項」**中，取消勾選或勾選**「在通知區域中顯示賽門鐵克安全性圖示」**。
4. 按下**「確定」**。

關於日誌

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資訊，這些記錄稱為事件。

安全性相關活動包括病毒偵測、電腦狀態，以及進出電腦流量的相關資訊。如果您使用的是受管用戶端，其日誌可以定期上傳至管理伺服器。管理員可以使用日誌的資料，來分析網路的整體安全性狀態。

日誌很重要，可以追蹤電腦活動，以及電腦與其他電腦和網路互動的情形。您可以使用日誌中的資訊來追蹤電腦上病毒、安全風險及攻擊方面的趨勢。

如需日誌的詳細資訊，可按下 F1，檢視該日誌的說明。

表 3-5 用戶端日誌

日誌	敘述
掃描日誌	包含某段時間內，已在您電腦上執行的掃描相關項目。
風險日誌	包含已感染電腦之病毒及安全風險 (如廣告軟體和間諜軟體) 的相關項目。安全風險包含可連至「賽門鐵克安全機制應變中心」網頁的連結，該網頁可提供其他資訊。 請參閱第 75 頁的「從風險日誌或掃描日誌隔離檔案」。
病毒和間諜軟體防護系統日誌	包含電腦上與病毒及安全風險相關的系統活動資訊。這項資訊包含架構變更、錯誤及定義檔資訊。
威脅日誌	包含 SONAR 在您電腦上偵測到的威脅的相關資訊。 SONAR 會偵測任何有可疑行為的檔案。 SONAR 也會偵測系統變更。
主動型威脅防護系統日誌	包含電腦上與 SONAR 相關的系統活動資訊。
流量日誌	包含防火牆流量和入侵預防攻擊的相關事件，日誌包含電腦透過網路進行之連線的相關資訊。 「網路威脅防護」日誌有助於回溯檢查威脅活動的來源，並排除可能的網路攻擊。這些日誌可讓您瞭解您的電腦何時遭到攔截而無法連至網路，並可協助您判斷存取遭攔截的原因。
封包日誌	包含透過電腦通訊埠進出的資料封包相關資訊。 「封包日誌」預設為停用。若為受管用戶端，您無法啟用「封包日誌」。若為非受管用戶端，您可以啟用「封包日誌」。 請參閱第 40 頁的「啟用封包日誌」。
控制日誌	包含應用程式存取的 Windows 登錄機碼、檔案和 DLL，以及您電腦所執行應用程式的相關資訊。
安全日誌	包含可能對您的電腦產生威脅的活動之相關資訊。例如，可能會顯示有關服務阻斷攻擊、通訊埠掃描及可執行檔變更等活動的資訊。
用戶端管理系統日誌	包含電腦上發生之一切作業變更的相關資訊。 變更可能包含下列活動： ■ 服務啟動或停止 ■ 電腦偵測網路應用程式 ■ 已架構軟體
竄改防護日誌	包含嘗試竄改您電腦上賽門鐵克應用程式的事件相關項目。這些項目包含「竄改防護」偵測到或偵測到並阻擋的嘗試事件相關資訊。

日誌	敘述
除錯日誌	包含用於疑難排解之用戶端、掃描及防火牆的相關資訊。管理員可能會要求您啟用或架構日誌，然後匯出。

請參閱第 40 頁的「檢視日誌」。

檢視日誌

您可以檢視電腦上的日誌，查看已發生事件的詳細資料。

附註：如果未安裝**「網路威脅防護」**或**「網路存取控制」**，您就無法檢視「安全日誌」、「系統日誌」或「控制日誌」。

檢視日誌

1. 在主視窗的側邊看板中，按下**「檢視日誌」**。
2. 按下列其中一個項目旁的**「檢視日誌」**：
   - **病毒和間諜軟體防護**
   - **主動型威脅防護**
   - **網路威脅防護**
   - **用戶端管理**
   - **網路存取控制**

   根據您的安裝，一些項目可能不會顯示。
3. 在下拉式清單中，選取您要檢視的日誌。

請參閱第 38 頁的「關於日誌」。

啟用封包日誌

除了「封包日誌」以外，所有「網路威脅防護」日誌及「用戶端管理」日誌都預設會啟用。若為非受管用戶端，您可以啟用和停用「封包日誌」。

若為受管用戶端，管理員可能會讓您啟用或停用「封包日誌」。

請參閱第 38 頁的「關於日誌」。

啟用封包日誌

1. 在用戶端「**狀態**」頁面的「網路威脅防護」右側，按下「**選項**」，然後按下「**變更設定**」。
2. 在「**網路威脅防護設定**」對話方塊中，按下「**日誌**」。
3. 勾選「**啟用封包日誌**」。
4. 按下「**確定**」。

關於在您需要排解疑難問題時啟用和停用防護

通常，您會希望用戶端電腦的防護技術一直都保持啟用。

如果用戶端電腦遇到問題，您可能需要暫時停用所有防護技術或個別防護技術。例如，如果應用程式無法執行或無法正確執行，則不妨停用「網路威脅防護」。如果仍然有這個問題，請在停用所有防護技術後，完整移除用戶端。如果問題仍在，而您知道問題不在於 Symantec Endpoint Protection。

警告：請務必在完成疑難排解工作後，再次啟用任何一種防護，以確保電腦繼續受到保護。

表 3-6 敘述了可能需要停用各防護技術的原因。

表 3-6 停用防護技術的目的

防護技術	停用防護技術的目的
病毒和間諜軟體防護	如果停用這個防護，則只停用「自動防護」。 如果您或管理員架構排程或開機掃描執行，則兩者還是會執行。 您可能會因為下列原因啟用或停用「自動防護」： ■ 「自動防護」可能會阻止您開啟文件。例如，如果開啟包含巨集的Microsoft Word，「自動防護」可能不讓您開啟。如果知道文件安全無虞，可以停用「自動防護」。 ■ 「自動防護」會警告您有疑似病毒活動，但是您知道此活動並非病毒所造成的。例如，您在安裝新的電腦應用程式時，就可能會看到警告。如果您要安裝更多應用程式，但要避免產生警告，可以暫時停用「自動防護」。 ■ 「自動防護」可能干擾 Windows 驅動程式更換。 ■ 「自動防護」可能會減緩用戶端電腦的速度。 **附註：**如果您停用「自動防護」，則即使「下載智慧型掃描」已啟用，也會同時停用「下載智慧型掃描」。SONAR也無法偵測啟發式威脅。對主機檔案及系統變更的SONAR偵測會繼續執行。 請參閱第 44 頁的「啟用或停用自動防護」。 如果「自動防護」導致應用程式發生問題，最好是建立例外，而不要永久停用防護。 請參閱第 71 頁的「排除掃描項目」。
主動型威脅防護	您可能會因為下列原因停用「主動型威脅防護」： ■ 出現太多誤認為是威脅的警告。 ■ 「主動型威脅防護」可能會減緩用戶端電腦的速度。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。
網路威脅防護	您可能會因為下列原因停用「網路威脅防護」： ■ 您安裝了可能導致防火牆加以攔截的應用程式。 ■ 防火牆規則或防火牆設定，因管理員的疏失攔截了某應用程式。 ■ 防火牆或入侵預防系統，導致網路連線相關問題。 ■ 防火牆可能會減緩用戶端電腦的速度。 ■ 您會無法開啟應用程式。 如果不確定「網路威脅防護」是否為問題所在，可能需要停用所有的防護技術。 若為受管用戶端，管理員可能會完全鎖定「網路威脅防護」，讓您無法啟用或停用它。 請參閱第 101 頁的「啟用或停用入侵預防」。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。

防護技術	停用防護技術的目的
竄改防護	通常，您應當保持啟用「竄改防護」。 若是您得到許多誤報偵測，可考慮暫時停用「竄改防護」。例如，有些第三方應用程式可能會進行變更，而在無意間嘗試修改賽門鐵克設定或程序。如果您確定應用程式安全無虞，可以針對該應用程式建立「竄改防護」例外。 請參閱第 45 頁的「啟用、停用與架構竄改防護」。

在用戶端電腦上啟用或停用防護

為進行疑難排解，您可能需要停用「自動防護」、「主動型威脅防護」或「網路威脅防護」。

在用戶端上，任何防護停用時：

- **「狀態」**頁面最上方的狀態列會是紅色的。
- 用戶端圖示會出現常見的禁止符號，即中間有斜線的紅圈。用戶端圖示會在 Windows 桌面右下角的工作列中顯示為完整的盾牌。在某些架構中，圖示不會出現。
  請參閱第 37 頁的「如何決定用戶端是否連線和受保護」。

若為受管用戶端，管理員可以隨時啟用或停用防護技術。如果您停用某個防護，管理員稍後可以再次啟用該防護。管理員也可以鎖定某個防護，讓您無法停用它。

警告：賽門鐵克建議您僅在需要對用戶端電腦進行疑難排解時，才暫時停用「自動防護」。

從狀態頁面啟用防護技術

- 在用戶端**「狀態」**頁面最上方，按下**「修正」**或**「全部修正」**。

從工作列啟用或停用防護技術

- 在 Windows 桌面的通知區域中，用滑鼠右鍵按下用戶端圖示，然後執行下列動作之一：
  - 按下**「啟用 Symantec Endpoint Protection」**。
  - 按下**「停用 Symantec Endpoint Protection」**。

從用戶端內部啟用或停用防護技術

- 在用戶端上，於**「狀態」**頁面的**「<防護類型>防護」**旁，執行下列任一工作：
  - 按下**「選項」>「啟用 <防護類型> 防護」**。
  - 按下**「選項」>「停用所有 <防護類型> 防護功能」**。

啟用或停用防火牆

1 在用戶端「**狀態**」頁面最上方的「**網路威脅防護**」旁邊，按下「**選項**」>「**變更設定**」。

2 在「**防火牆**」標籤上，勾選或取消勾選「**啟用防火牆**」。

3 按下「**確定**」。

請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。

請參閱第 44 頁的「啟用或停用自動防護」。

啟用或停用自動防護

您可以針對檔案和程序、Internet 電子郵件，以及電子郵件群組軟體應用程式，啟用或停用「自動防護」。有任何類型的「自動防護」停用時，病毒和間諜軟體狀態在「狀態」頁面上會以紅色出現。

若為受管用戶端，管理員可能會鎖定「自動防護」，因此您無法自行停用。另外，管理員也可能會指定您可以暫時停用「自動防護」，但指定的時間一過，「自動防護」就會自動再次開啟。

附註：如果您停用「自動防護」，則會同時停用「下載智慧型掃描」，即使「下載智慧型掃描」已啟用也是如此。SONAR 也無法偵測啟發式威脅；但是，SONAR 會繼續偵測主機檔案及系統變更。

警告：賽門鐵克建議，如果需要排除用戶端電腦上的「自動防護」問題，請暫時停用這個功能。

啟動或停用檔案系統的自動防護

◆ 在用戶端的「**狀態**」頁面上，「**病毒和間諜軟體防護**」旁進行下列任一動作：

- 按下「**選項**」>「**啟用病毒和間諜軟體防護**」。
- 按下「**選項**」>「**停用所有病毒和間諜軟體防護功能**」。

啟用或停用電子郵件的「自動防護」

1 在用戶端的側邊看板中，按下「**變更設定**」。

2 在「**病毒和間諜軟體防護**」旁，按下「**架構設定**」。

3 執行下列其中一項動作：

- 在「**Internet 電子郵件自動防護**」標籤，勾選或取消勾選「**啟用 Internet 電子郵件自動防護**」。

- 在「**Outlook 自動防護**」標籤，勾選或取消勾選「**啟用 Microsoft Outlook 自動防護**」。
- 在「**Notes 自動防護**」標籤上，勾選或取消勾選「**啟用 Lotus Notes 自動防護**」。

伺服器作業系統不支援「Internet 電子郵件自動防護」。「Microsoft Outlook 自動防護」會自動安裝在執行 Outlook 的電腦上。

4 按下「**確定**」。

請參閱第 56 頁的「關於自動防護的類型」。

請參閱第 15 頁的「關於狀態頁面上的警示圖示」。

請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。

啟用、停用與架構竄改防護

「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。可防止威脅和安全風險竄改賽門鐵克資源。您可以啟用或停用「竄改防護」。您也可以架構「竄改防護」在偵測到意圖竄改電腦上的賽門鐵克資源時，所要採取的動作。

根據預設，「竄改防護」已設定為「**攔截且不記錄**」。

附註：若為受管用戶端，管理員可能會鎖定「竄改防護」設定。

請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。

啟用或停用竄改防護

1 在用戶端的側邊看板中，按下「**變更設定**」。

2 在「**用戶端管理**」旁，按下「**架構設定**」。

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 按下「**確定**」。

架構竄改防護

1 在用戶端的側邊看板中，按下「**變更設定**」。

2 在「**用戶端管理**」旁，按下「**架構設定**」。

3 在「**竄改防護**」標籤的「**應用程式嘗試竄改或關閉賽門鐵克安全軟體時要執行的動作**」清單方塊中，按下「**只記錄**」、「**攔截且不記錄**」或「**攔截並記錄**」。

4 按下「**確定**」。

4

管理掃描

本章包含以下主題：

- 變更 SONAR 設定

管理電腦上的掃描

根據預設，用戶端會每天執行作用中掃描。在受管用戶端上，如果管理員允許使用這些設定，您就可以自行架構掃描。非受管用戶端包含停用的預設作用中掃描，不過您可以管理自己的掃描。

表 4-1 管理掃描

工作	敘述
了解掃描的運作模式	檢視掃描類型以及病毒和安全性風險的類型。 請參閱第 51 頁的「病毒和間諜軟體掃描的運作方式」。
更新病毒定義檔	確定電腦安裝了最新的病毒定義檔。 請參閱第 35 頁的「更新電腦的防護」。
檢查自動防護是否啟用	「自動防護」預設為啟用。「自動防護」應隨時保持在啟用狀態。如果停用「自動防護」，您還會停用「下載智慧型掃描」並會阻止 SONAR 進行啟發式偵測。 請參閱第 44 頁的「啟用或停用自動防護」。
掃描電腦	定期掃描電腦是否有病毒和安全風險。檢查上次掃描日期，確定掃描定期執行。 請參閱第 20 頁的「立即掃描電腦」。 請參閱第 59 頁的「排程使用者定義掃描」。 掃描執行時，您會看到掃描結果對話方塊。可以使用該掃描結果對話方塊，對掃描偵測到的項目執行一些動作。 請參閱第 25 頁的「回應病毒或風險偵測」。 您可以暫停您開始的掃描。在受管用戶端上，管理員可以決定您能否暫停由管理員啟動的掃描。 請參閱第 21 頁的「暫停和延緩掃描」。

工作	敘述
調整掃描以提高電腦效能	預設情況下，Symantec Endpoint Protection 會在對電腦效能產生最小影響的情況下，提供較高安全性層級。您也可以自訂設定，以進一步提高電腦效能。 對於排程掃描和隨選掃描，可以變更下列選項： ■ 掃描調整 將掃描調整設定為**「最佳應用程式效能」**。 ■ 壓縮檔 變更掃描壓縮檔的層數。 ■ 可復原掃描 可以指定掃描執行的最大時間。掃描會在電腦閒置時復原。 ■ 隨機掃描 可以指定掃描在指定時間間隔內隨機設定開始時間。 此外，您可能還需要停用啟動掃描，或變更排程掃描的排程。 請參閱第 65 頁的「自訂病毒和間諜軟體掃描設定」。 請參閱第 59 頁的「排程使用者定義掃描」。
調整掃描以增強電腦的防護	在大多數情況下，預設掃描設定即可為電腦提供足夠的保護。在某些情況下，您可能希望增強防護。如果增強防護，則可能會影響電腦效能。 對於排程掃描和隨選掃描，可以變更下列選項： ■ 掃描效能 將掃描調整設定為**「最佳掃描效能」**。 ■ 掃描動作 變更偵測到病毒時執行的矯正動作 ■ 掃描持續時間 根據預設，排程掃描將執行到指定時間間隔到期為止，然後在用戶端電腦閒置時復原執行。您可以將掃描持續時間設定為**「到掃描完成」**。 ■ 智慧型掃描查詢 您應確定已啟用「智慧型掃描查詢」。「智慧型掃描查詢」設定與「下載智慧型掃描」設定類似。 ■ 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 65 頁的「自訂病毒和間諜軟體掃描設定」。
指定掃描例外	將安全檔案或程序排除在掃描的範圍以外。 請參閱第 71 頁的「排除掃描項目」。

工作	敘述
將有關偵測的資訊傳送至 Symantec	依據預設，用戶端電腦會將有關偵測的資訊傳送到賽門鐵克安全機制應變中心。您可以關閉傳送，或選擇要傳送哪些種類的資訊。 賽門鐵克建議您永遠啟用傳送功能。此資訊有助於賽門鐵克處理威脅。 請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。
管理隔離的檔案	Symantec Endpoint Protection 會隔離受感染的檔案，並將它們移動到不會感染電腦上其他檔案的位置。 如果無法修復隔離的檔案，您必須決定要如何處理檔案。 您也可以執行下列動作： ■ 如果備份檔案存在，或可從信任的來源取得替換檔案，請刪除隔離的檔案。 ■ 將受到不明感染的檔案保留在「隔離所」中，直到賽門鐵克發佈新的病毒定義檔。 ■ 定期檢查隔離的檔案，以避免累積大量的檔案。當網路上爆發新病毒時，檢查隔離的檔案。 請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。 請參閱第 74 頁的「關於隔離檔案」。

表 4-2 顯示可修改的其他掃描設定，以便能夠提高防護、改善效能或減少誤報情形。

表 4-2 掃描設定

工作	敘述
修改「自動防護」設定以提高電腦效能或增強防護	對於「自動防護」，您可能需要變更下列選項： ■ 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 如果啟用遠端電腦上的「自動防護」，請務必啟用**「只在執行檔案時」**。 ■ 此外，也可以指定「自動防護」信任遠端電腦上的檔案，並使用網路快取。 「自動防護」預設會在檔案從您的電腦寫入遠端電腦時，對其進行掃描。「自動防護」也會在檔案從遠端電腦寫入您的電腦時，對其進行掃描。 網路快取會儲存「自動防護」掃描來自遠端電腦的檔案記錄。如果使用網路快取，「自動防護」就不會重複掃描相同的檔案。 請參閱第 65 頁的「自訂病毒和間諜軟體掃描設定」。
管理 ELAM 偵測	如果您認為用戶端提早啟動反惡意軟體 (ELAM) 偵測會影響電腦的效能，可以啟用或停用 ELAM。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 77 頁的「啟用或停用提早啟動防惡意軟體 (ELAM)」。

工作	敘述
管理「下載智慧型掃描」偵測	「下載智慧型掃描」會檢查您嘗試透過網頁瀏覽器、文字訊息用戶端以及其他入口網站下載的檔案。「下載智慧型掃描」會使用收集檔案信譽相關資訊的「賽門鐵克智慧型掃描」所提供的資訊。「下載智慧型掃描」會使用檔案的信譽等級來允許或攔截檔案，或提示使用者對檔案採取動作。 請參閱第 62 頁的「管理電腦上的下載智慧型掃描偵測」。
管理 SONAR	您可以調整 SONAR 的設定。 請參閱第 82 頁的「在用戶端電腦上管理 SONAR」。

病毒和間諜軟體掃描的運作方式

病毒和間諜軟體掃描身分，並處理或清除電腦上的病毒和安全風險。掃描會使用下列程序排除病毒或風險：

- 掃描引擎會在電腦的檔案和其他元件中，搜尋檔案內是否有病毒的蹤跡。每種病毒都有可辨識的型樣，就是所謂的特徵。安裝於用戶端的是病毒定義檔，其中包含已知病毒特徵，不包括有害的病毒程式碼。掃描引擎會依病毒定義檔比較各檔案或元件。如果發現符合的特徵，表示該檔案已受到感染。
- 掃描引擎會使用定義檔，判斷造成感染的是病毒還是風險。掃描引擎接著會對感染的檔案採取矯正動作。若要矯正受感染的檔案，用戶端會清除、刪除或隔離檔案。
  請參閱第 57 頁的「掃描如何回應偵測到的病毒或風險」。

附註：Symantec Endpoint Protection 不會隔離，也不會清除 Windows 8 樣式應用程式中所偵測到的任何風險。Symantec Endpoint Protection 會刪除該風險。

表 4-3敘述了用戶端會在電腦掃描的元件。

表 4-3 用戶端掃描的電腦元件

元件	敘述
選取的檔案	用戶端會掃描個別檔案。針對大部分的掃描類型，您可以選取要掃描的檔案。 用戶端軟體會使用型樣掃描，在檔案中搜尋是否有病毒的蹤跡。病毒的蹤跡就是所謂的型樣或特徵。每個檔案都會與病毒定義檔中的無害特徵進行比對，當做辨識特定病毒的方式。 如果發現病毒，用戶端預設會嘗試清除檔案中的病毒。如果無法清除檔案，用戶端會隔離該檔案，防止電腦進一步受到感染。 用戶端也會使用型樣掃描，在檔案與 Windows 登錄機碼中搜尋是否有安全風險的跡象。如果發現安全風險，用戶端預設會隔離受感染的檔案，並修復該風險造成的影響。如果用戶端無法隔離檔案，就會記錄該動作。
電腦記憶體	用戶端會搜尋電腦記憶體。任何檔案病毒、開機磁區病毒或巨集病毒都可能常駐在記憶體中。常駐在記憶體中的病毒已自行複製到電腦的記憶體中。病毒可以隱藏在記憶體中，直到發生觸發事件為止。然後，病毒可以散佈到磁碟機中的磁片或硬碟機中。存在於記憶體中的病毒是無法清除的。然而，出現提示時，您可以重新啟動電腦，以移除記憶體中的病毒。
開機磁區	用戶端會檢查電腦的開機磁區是否有開機病毒。將對兩個項目進行檢查：分割區表與主要開機記錄。
軟碟機	透過磁片是常見的病毒散佈方式。當您啟動或關閉電腦時，磁片可能留在磁碟機中。開始掃描時，用戶端會搜尋磁碟機中的磁片開機磁區和分割區表。關閉電腦時，會提示您取出磁片，以防止可能的感染。

關於病毒與安全風險

Symantec Endpoint Protection 可以掃描病毒和安全風險。安全風險包含間諜軟體、廣告軟體、Rootkit 和可使電腦或網路處於風險之中的其他檔案。

病毒和安全風險可透過電子郵件或時傳訊程式感染。您可能會在接受軟體程式的使用者授權許可協議時，不知不覺地下載風險。

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您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。

您可以前往賽門鐵克安全機制應變中心網站，檢視特定風險的相關資訊。

賽門鐵克安全機制應變中心網站提供關於威脅和安全風險的最新資訊。該網站也提供大量的參考資訊，例如，關於病毒與安全風險的白皮書和詳細資訊。

請參閱第 57 頁的「掃描如何回應偵測到的病毒或風險」。

圖 4-1 病毒和安全風險攻擊電腦的方式

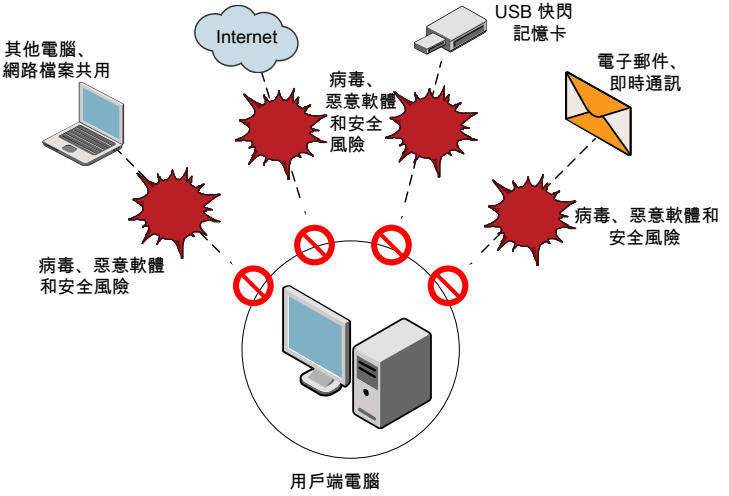

表 4-4 列出可能攻擊電腦的病毒和風險類型。

表 4-4 病毒和安全風險

風險	敘述
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	提供廣告內容的程式。

風險	敘述
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。
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。

關於掃描類型

Symantec Endpoint Protection 包含不同的掃描類型，用於防範不同類型的病毒、威脅和風險。

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。

在非受管電腦上，您應確保每天在電腦上執行一次作用中掃描。如果您懷疑電腦上有非作用中威脅，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。

表 4-5 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。 「自動防護」還會保護您可能傳送或接收的某些電子郵件。 請參閱第 56 頁的「關於自動防護的類型」。
下載智慧型掃描	「下載智慧型掃描」透過以下方法提昇自動防護的安全性：當使用者嘗試從瀏覽器及其他入口網站下載檔案時檢查檔案。 「下載智慧型掃描」會使用「賽門鐵克智慧型掃描」所提供的資訊。「賽門鐵克智慧型掃描」從社群數百萬使用者收集資訊來判斷檔案的安全信譽。「下載智慧型掃描」會使用檔案的信譽等級來允許或攔截檔案，或提示使用者對檔案採取動作。 「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」。如果停用「自動防護」但啟用「下載智慧型掃描」，則「下載智慧型掃描」無法運作。 請參閱第 58 頁的「Symantec Endpoint Protection 如何使用信譽資料進行檔案相關決策」。
管理員掃描和使用者定義的掃描	對於受管用戶端，管理員可建立排程掃描或執行隨選掃描。對於非受管用戶端、或掃描設定解除鎖定的受管用戶端，您可以建立和執行自己的掃描。 管理員掃描或使用者定義的掃描偵測病毒和安全性風險的方法為檢查用戶端電腦上的全部檔案和程序。這些掃描類型也可以檢驗記憶體和載入點。 系統提供以下類型的管理員掃描或使用者定義掃描： ■ 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狀態，除非電腦已架構為重試未執行的掃描，否則不會執行此掃描。您可以排程作用中掃描、完整掃描或自訂掃描。 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資料夾。 ■ 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。 ■ 隨選掃描 隨選掃描是由您手動啟動的掃描。您可以透過**「掃描威脅」**頁面執行隨選掃描。 請參閱第 51 頁的「病毒和間諜軟體掃描的運作方式」。
SONAR	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。 請參閱第 80 頁的「關於 SONAR」。

請參閱第 48 頁的「管理電腦上的掃描」。

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。

如果您的用戶端電腦執行有其他電子郵件安全性產品，例如 Symantec Mail Security，就可能不需要為電子郵件啟用「自動防護」。

「自動防護」只適用於支援的電子郵件用戶端，它不會保護電子郵件伺服器。

附註：如果在開啟電子郵件時偵測到病毒，該電子郵件可能要花數秒鐘才能開啟，讓「自動防護」完成掃描。

表 4-6 自動防護的類型

自動防護的類型	敘述
自動防護	在從電腦讀取檔案或將檔案寫入電腦時，持續掃描檔案 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。 如果您未針對電子郵件執行「自動防護」，用戶端電腦仍會在啟用「自動防護」時受到保護。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。
Internet 電子郵件自動防護	掃描 Internet 電子郵件 (POP3 或 SMTP) 和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。如果您使用 POP3 或 SMTP 搭配 Secure Sockets Layer (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」。64 位元電腦不支援 Internet 電子郵件掃描。 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。

自動防護的類型	敘述
Microsoft Outlook 自動防護	掃描 Microsoft Outlook 電子郵件 (MAPI 與 Internet) 及附件是否存在病毒和安全風險 支援 Microsoft Outlook 98/2000/2002/2003/2007/2010 (MAPI 與 Internet) 當您執行用戶端軟體安裝時，若電腦已安裝 Microsoft Outlook，用戶端軟體會偵測到該電子郵件應用程式。用戶端會自動安裝「Microsoft Outlook 自動防護」。 如果透過 MAPI 或 Microsoft Exchange 用戶端使用 Microsoft Outlook，且已為電子郵件啟用「自動防護」，則會立即下載附件。當您開啟附件時，便會掃描附件。如果您透過慢速連線下載大型附件，會影響電子郵件效能。如果您經常收到大型附件，您可能會想要停用這項功能。 **附註：**請不要在 Microsoft Exchange Server 上安裝「Microsoft Outlook 自動防護」。
Lotus Notes 自動防護	掃描 Lotus Notes 電子郵件和附件是否存在病毒和安全風險 Lotus Notes 4.5 至 8.x 支援此功能。 當您執行用戶端軟體安裝時，若電腦已安裝 Lotus Notes，用戶端軟體會偵測到該電子郵件應用程式。用戶端會自動安裝「Lotus Notes 自動防護」。

掃描如何回應偵測到的病毒或風險

病毒和安全風險感染檔案時，用戶端會以不同的方式回應威脅類型。對於各類威脅，用戶端都會使用第一個動作，如果第一個動作失敗，則會使用第二個動作。

表 4-7　用戶端如何回應病毒和安全風險

威脅類型	動作
病毒	當用戶端偵測到病毒時，用戶端預設會： ■ 首先嘗試從受感染的檔案清除病毒。 ■ 如果用戶端清除檔案，用戶端即完全將風險從您的電腦移除。 ■ 如果用戶端無法清除檔案，就會記錄這個失敗，並將受感染的檔案移到「隔離所」。 請參閱第 74 頁的「關於隔離檔案」。 **附註：**Symantec Endpoint Protection 不會隔離在 Windows 8 樣式應用程式和檔案中偵測到的病毒。Symantec Endpoint Protection 會刪除這個病毒。

威脅類型	動作
安全風險	當用戶端偵測到安全風險時，預設會： ■ 隔離受感染的檔案。 ■ 試著移除或修復安全風險造成的任何變更。 ■ 如果用戶端無法隔離安全風險，就會記錄風險，並讓它保持原狀。 在某些情況下，您可能會在不知情的情況下，安裝了包含安全風險的應用程式，如廣告軟體和間諜軟體。如果賽門鐵克判斷隔離風險不會損害電腦，用戶端就會隔離風險。如果用戶端立即隔離風險，則可能導致電腦不穩定。因此，用戶端會先等候應用程式安裝完成，然後才隔離風險。然後再修復該風險所造成的影響。 **附註：**Symantec Endpoint Protection 不會隔離在 Windows 8 樣式應用程式和檔案中偵測到的安全風險。Symantec Endpoint Protection 會刪除該風險。

對於各掃描類型，您可以變更用戶端處理病毒和安全風險方式的設定。對於各類別的風險和個別安全風險，您可以設定不同的動作。

Symantec Endpoint Protection 如何使用信譽資料進行檔案相關決策

賽門鐵克會從其全球數百萬使用者的社群及全球情報網收集有關檔案的資訊。收集的資訊會形成賽門鐵克承載的信譽資料庫。賽門鐵克產品會利用此資訊保護用戶端電腦，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。用戶端電腦必須要求或查詢信譽資料庫。

賽門鐵克會使用智慧型掃描技術，判斷每個檔案的風險層級或安全性分級。

智慧型掃描可透過檢查檔案的下列特性及其上下文，判斷檔案的安全性分級：

- 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

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。「下載智慧型掃描」根據信譽資訊進行偵測。如果停用智慧型掃描查詢，則「下載智慧型掃描」可以執行，但無法進行偵測。其他防護功能(例如「智慧型掃描查詢」和 SONAR) 也會在進行偵測時使用信譽資訊；然而，這些功能可以使用其他技術進行偵測。

依預設，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。傳送資訊的用戶端愈多，信譽資料庫就會變得愈有用。

您可以停用信譽資訊傳送。然而，賽門鐵克建議您將傳送功能保持啟用。

用戶端電腦也會將其他類型的偵測相關資訊傳送到賽門鐵克安全機制應變中心。

請參閱第 62 頁的「管理電腦上的下載智慧型掃描偵測」。

請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。

排程使用者定義掃描

排程掃描是威脅與安全風險防護的一項重要組成部分。您應該排程至少每週掃描一次，才能確保電腦不受病毒和安全風險威脅。建立新掃描時，掃描會出現在**「掃描威脅」**窗格的掃描清單中。

附註：如果管理員已建立排程掃描，該掃描就會出現在**「掃描威脅」**窗格的掃描清單中。

電腦必須開啟，而且必須載入「Symantec Endpoint Protection 服務」，才能進行排程掃描。「Symantec Endpoint Protection 服務」預設會在開啟電腦時載入。

對於管理型用戶端，管理員可能會覆寫這些設定。

請參閱第 20 頁的「立即掃描電腦」。

請參閱第 48 頁的「管理電腦上的掃描」。

設定排程掃描時，請注意下列重點：

使用者定義的掃描不會要求使用者登入	如果定義掃描的使用者未登入，Symantec Endpoint Protection 仍然會執行掃描。您可以指定用戶端在使用者登出後不執行掃描。
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。如果電腦錯過此掃描並於星期一早上 6 點啟動，則會在早上 6 點執行掃描。下一次掃描會在從星期一早上 6 點算起的一週後執行，而非在下一個星期日的午夜執行。 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。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

排程使用者定義掃描

1. 在用戶端的側邊看板中，按下**「掃描威脅」**。
2. 按下**「建立新掃描」**。
3. 在**「建立新掃描-掃描的項目」**對話方塊中，選取下列其中一種掃描進行排程：

作用中掃描	掃描電腦中最常受病毒和安全風險感染的區域。 您應該每天執行一次作用中掃描。
完整掃描	掃描整部電腦是否有病毒和安全風險。 您可能需要一週或一個月執行一次完整掃描。 完整掃描可能會影響電腦效能。
自訂掃描	掃描電腦上所選取區域是否有病毒和安全風險。

4. 按**「下一步」**。

5 如果選取「**自訂掃描**」，請勾選適當的核取方塊，指定要掃描的位置，然後按「**下一步**」。

符號的敘述如下：

未選取檔案、磁碟機或資料夾。如果該項目是磁碟機或資料夾，其中的資料夾或檔案亦未被選取。

已選取個別檔案或資料夾。

已選取個別資料夾或磁碟機。亦會選取該資料夾或磁碟機內的所有項目。

未選取個別資料夾或磁碟機，但已選取資料夾或磁碟機內的一個或多個項目。

6 在「**建立新掃描 - 掃描選項**」對話方塊中，您可以修改下列任一選項：

檔案類型	變更用戶端要掃描的檔案副檔名。預設設定為掃描所有檔案。
動作	變更發現病毒及安全風險時應採取的第一個和第二個動作。
通知	編寫發現病毒或安全風險時要顯示的訊息。您也可以架構進行矯正動作前要不要收到通知。
進階	變更其他掃描功能，例如顯示掃描結果對話方塊。
掃描加強功能	變更用戶端會掃描的電腦元件。這些選項可用與否，視您在步驟 3 所選取的而定。

7 按「**下一步**」。

8 在「**建立新掃描 - 掃描的時間**」對話方塊按下「**在指定時間**」，然後按下「**下一步**」。

您也可以建立隨選掃描或開機掃描。

請參閱第 62 頁的「排程執行隨選或開機掃描」。

9 在「**建立新掃描 - 排程**」對話方塊的「**掃描排程**」下，指定掃描頻率和掃描時間，然後按「**下一步**」。

10 在「**掃描持續時間**」下，您可以指定必須完成掃描的時間長度。您也可以隨機設定掃描開始時間。

11 在「**錯過掃描排程**」下，可以指定可重試掃描的間隔。

12 在「**建立新掃描 - 掃描名稱**」對話方塊中，輸入掃描的名稱和敘述。

例如，將掃描作業稱為：星期五早上

13 按下「**完成**」。

排程執行隨選或開機掃描

除排程掃描之外，您可以在開機或登入電腦時額外進行自動掃描。通常開機掃描只著重在重要、高風險的資料夾，例如 Windows 資料夾和儲存 Microsoft Word 與 Excel 範本的資料夾。

如果要定期掃描同一組檔案或資料夾，您可以針對這些項目建立隨選掃描。不論何時，您都可以快速確認指定的檔案與資料夾並未受到病毒及安全風險感染。隨選掃描必須以手動方式執行。

如果您建立的開機掃描不只一個，則掃描動作會按照您當初建立的順序依次執行。管理員可能已架構用戶端，因此您無法建立開機掃描。

請參閱第 20 頁的「立即掃描電腦」。

如需各對話方塊上選項的詳細資訊，請按下「**說明**」。

排程執行隨選或開機掃描

1 在用戶端的側邊看板中，按下「**掃描威脅**」。

2 按下「**建立新掃描**」。

3 指定排程掃描的掃描內容和任何掃描選項。

請參閱第 59 頁的「排程使用者定義掃描」。

4 在「**建立新掃描 - 掃描的時間**」對話方塊中，進行下列其中一個動作：

- 按下「**啟動時**」。
- 按下「**隨選**」。

5 按「**下一步**」。

6 在「**建立新掃描 - 掃描名稱**」對話方塊中，輸入掃描的名稱和敘述。

例如，將掃描作業稱為：MyScan1

7 按下「**完成**」。

管理電腦上的下載智慧型掃描偵測

「自動防護」包含一項名為「下載智慧型掃描」的功能，該功能可檢查您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。必須先啟用「自動防護」，「下載智慧型掃描」才能運作。

支援的入口網站包含 Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Windows Live Messenger 和 Yahoo Messenger。

附註：在「風險日誌」中，「下載智慧型掃描」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，您可以使用 Internet Explorer 嘗試下載「下載智慧型掃描」偵測的檔案。如果您接著使用 Firefox 嘗試下載該檔案，則風險詳細資料中的**「下載者」**欄位會將 Internet Explorer 顯示為入口網站。

附註：「自動防護」還可以掃描使用者以電子郵件附件接收的檔案。

表 4-8 管理電腦上的下載智慧型掃描偵測

工作	敘述
了解「下載智慧型掃描」如何使用信譽資料做出關於檔案的決策	「下載智慧型掃描」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。「下載智慧型掃描」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「下載智慧型掃描」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 58 頁的「Symantec Endpoint Protection 如何使用信譽資料進行檔案相關決策」。
回應下載智慧型掃描偵測	當「下載智慧型掃描」執行偵測時，您可能會看到相關通知。對於受管用戶端，您的管理員可以選擇停用「下載智慧型掃描」偵測通知。 啟用通知後，系統將在「下載智慧型掃描」偵測到惡意檔案或未證明的檔案時顯示相關訊息。對於未證明的檔案，您必須選擇是否允許該檔案。 請參閱第 27 頁的「回應詢問您要允許或攔截嘗試下載的檔案的下載智慧型掃描訊息」。
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。 依預設，「下載智慧型掃描」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。信任的網站在 **Windows「控制台」>「信任的 Internet 網站」>「安全性」**標籤上架構。啟用 **「自動信任從內部網路網站下載的任何檔案」**選項後，Symantec Endpoint Protection 將允許使用者從信任的網站下載的任何檔案。 「下載智慧型掃描」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，「下載智慧型掃描」不會將 10.*.*.* 識別為信任網站。此外，「下載智慧型掃描」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。 請參閱第 71 頁的「排除掃描項目」。

工作	敘述
確定已啟用智慧型掃描查詢	「下載智慧型掃描」需要使用信譽資料進行檔案相關決策。 如果停用智慧型掃描查詢，則「下載智慧型掃描」可以執行，但無法進行偵測。 依預設，「智慧型掃描查詢」已啟用。 請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。
自訂下載智慧型掃描設定	您可能因以下原因需要自訂「下載智慧型掃描」設定： ■ 增加或減少「下載智慧型掃描」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。 靈敏度等級愈低，「下載智慧型掃描」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。 靈敏度等級愈高，「下載智慧型掃描」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「下載智慧型掃描」處理惡意檔案或未證明檔案的方式。您可能會想變更對未證明的檔案採取的動作，以避免收到相關偵測通知。 ■ 取得有關「下載智慧型掃描」偵測的警示。 如果「下載智慧型掃描」偵測到其視為惡意的檔案，在相應動作設為**「隔離」**的情況下，它會在用戶端電腦上顯示訊息。您可以復原隔離動作。 如果「下載智慧型掃描」偵測到其視為未證明的檔案，在未證明檔案的相應動作設為**「提示」**或**「隔離」**的情況下，它會在用戶端電腦上顯示訊息。如果將動作設定為**「提示」**，則可以允許或攔截此檔案。如果將動作設定為**「隔離」**，則可以復原隔離動作。 您可以關閉使用者通知，如此您不用在「下載智慧型掃描」偵測到視為未證明的檔案時進行選擇。如果您保持啟用通知，可將未證明檔案的動作設定為**「忽略」**，如此可一律允許這些偵測，且不會通知您。 當啟用通知時，惡意檔案靈敏度的設定會影響您收到的通知數量。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。 請參閱第 64 頁的「自訂下載智慧型掃描設定」。
將有關信譽偵測的資訊傳送給賽門鐵克	依預設，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 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。

自訂下載智慧型掃描設定

您可能需要自訂「下載智慧型掃描」設定，以降低用戶端電腦上的偵測誤報率。您可以變更「下載智慧型掃描」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「下載智慧型掃描」進行偵測時顯示在用戶端電腦上的通知。

請參閱第 62 頁的「管理電腦上的下載智慧型掃描偵測」。

自訂下載智慧型掃描設定

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在**「病毒和間諜軟體防護」**旁，按下**「架構設定」**。
3. 在**「下載智慧型掃描」**標籤上，確定勾選**「啟用下載智慧型掃描以根據檔案信譽偵測下載檔案的潛在風險」**。

   如果停用「自動防護」，則即使「下載智慧型掃描」已啟用，也無法運作。
4. 移動滑動軸以變更惡意檔案靈敏度。

   附註：如果您或您的管理員安裝了基本病毒和間諜軟體防護，則惡意檔案靈敏度將自動設定為等級 1，並且無法變更。

   如果設定為更高等級，則「下載智慧型掃描」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。
5. 您可以勾選或取消勾選下列選項，用做檢查未證明檔案的附加條件：
   - **少於 *x* 個使用者的檔案**
   - **使用者已知時間短於 *x* 天的檔案**
     如果未證明的檔案符合此條件，「下載智慧型掃描」會將這些檔案偵測為惡意檔案。
6. 確定已勾選**「自動信任從內部網路網站下載的任何檔案」**。

   此選項也適用於「智慧型掃描查詢」偵測。
7. 按下**「動作」**。
8. 在**「惡意檔案」**下，指定第一個動作和第二個動作。
9. 在**「未證明的檔案」**下方，指定相應的動作。
10. 按下**「確定」**。
11. 按下**「通知」**，然後指定是否應在「下載智慧型掃描」執行偵測時顯示通知。

    您可以自訂顯示的警告訊息文字。
12. 按下**「確定」**。

自訂病毒和間諜軟體掃描設定

Symantec Endpoint Protection 預設會提供電腦所需的病毒和安全風險防護。如果使用非受管用戶端，您可能需要架構某些掃描設定。

請參閱第 48 頁的「管理電腦上的掃描」。

執行使用者定義的掃描

1 在用戶端的側邊看板中，按下**「掃描威脅」**。

2 在**「掃描威脅」**頁面中，用滑鼠右鍵按下掃描，然後按**「編輯」**。

3 在**「掃描選項」**標籤上，執行下列任一工作：

- 若要變更「智慧型掃描查詢」設定，請按下**「智慧型掃描查詢」**。
  「智慧型掃描查詢」設定與「下載智慧型掃描」設定類似。
  請參閱第 64 頁的「自訂下載智慧型掃描設定」。
- 若要指定減少掃描的檔案類型，請按**「選取的副檔名」**，再按**「副檔名」**。

  附註：使用者定義的掃描一律會掃描配置區檔案的副檔名，除非您在**「進階」**下方停用壓縮檔案選項，或為配置區副檔名建立例外。

- 若要指定用戶端對受感染的檔案採取的第一個動作和第二個動作，請按**「動作」**。
- 若要指定通知選項，請按**「通知」**。
  您可以另外啟用或停用出現在 Windows 8 樣式使用者介面的通知。
  請參閱第 77 頁的「如何管理出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知」。
- 若要架構壓縮檔案、備份和調整的進階選項，請按下**「進階」**。
  您可能需要變更調整選項，以提高用戶端電腦的效能。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

4 按下**「確定」**。

變更全域掃描設定

1 執行下列其中一項動作：

- 在用戶端的邊欄中，按下**「變更設定」**，然後按下「病毒和間諜軟體防護」旁的**「架構設定」**。
- 在用戶端的邊欄中，按下**「掃描威脅」**，然後按下**「檢視全域掃描設定」**。

2 在**「全域設定」**標籤上，在**「掃描選項」**下變更「智慧型掃描」或Bloodhound的設定。

3 若要檢視或建立掃描例外，請按下**「檢視清單」**。檢視或建立例外後，按下**「關閉」**。

4 在**「日誌保留」**或**「網際網路瀏覽器防護」**下，進列所需的所有變更。

5 按下**「確定」**。

自訂自動防護

1 在用戶端的側邊看板中，按下**「變更設定」**。

2 在「病毒和間諜軟體防護」旁，按下**「架構設定」**。

3 在任何「自動防護」標籤上，執行下列工作：

- 若要指定減少掃描的檔案類型，請按**「選取的」**，再按**「副檔名」**。
- 若要指定用戶端對受感染的檔案採取的第一個動作和第二個動作，請按**「動作」**。
- 若要指定通知選項，請按**「通知」**。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

4 在**「自動防護」**標籤上，按下**「進階」**。

您可以變更檔案快取的選項以及「風險追蹤程式」和備份的選項。您可能需要變更這些選項以提高電腦效能。

5 按下**「網路」**以變更在遠端電腦上信任檔案的設定和設定網路快取的設定。

6 按下**「確定」**。

架構在偵測到惡意軟體與安全風險時採取的動作

您可以架構您希望 Symantec Endpoint Protection 用戶端在偵測到惡意軟體或安全風險時採取的動作。您可以架構兩個動作，如果第一個動作失敗，就執行第二個動作。

附註：若您的電腦由管理員所管理，且這些選項顯示一個鎖定圖示，您就無法變更這些選項，因為已被您的管理員鎖定。

對任何類型的掃描，架構動作的方式都相同。每種掃描都有其自己的動作架構。您可以針對不同的掃描，架構不同的動作。

附註：您可以單獨針對「下載智慧型掃描」與 SONAR 架構動作。

請參閱第 65 頁的「自訂病毒和間諜軟體掃描設定」。

請參閱第 64 頁的「自訂下載智慧型掃描設定」。

請參閱第 83 頁的「變更 SONAR 設定」。

如需程序中使用選項的詳細資訊，您可以按下「敘述」。

架構在偵測到惡意軟體與安全風險時採取的動作

1. 在用戶端的側邊欄中，按下**「變更設定」**或**「掃描威脅」**。
2. 執行下列其中一項動作：
   - 在「病毒和間諜軟體防護」旁，按下**「組態設定」**，然後在任何「自動防護」標籤上，按下**「動作」**。
   - 選取掃描，然後以滑鼠右鍵按下並選取**「編輯」**，再按下**「掃描選項」**。
3. 按下**「動作」**。
4. 在**「掃描動作」**對話方塊中，在樹狀結構的**「惡意軟體」**或**「安全風險」**下方，選取類別或子類別。

   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。

   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。
5. 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。

6 從以下選項中選取第一與第二個動作：

清除風險

移除受感染檔案中的病毒。此設定是對病毒執行的第一個預設動作。

附註：這僅適用於作為對病毒執行的第一個動作。此動作不會套用到安全風險。

對病毒執行的第一個動作應一律使用此設定。如果用戶端成功清除檔案中的病毒，您就不需要採取任何其他動作。您的電腦將免於病毒的困擾，而且病毒不再容易散播到電腦的其他區域。

當用戶端清除檔案時，會移除受感染檔案、開機磁區和分割區表中的病毒。這也可以消除病毒散播的能力。用戶端通常可以在病毒對您的電腦造成破壞之前，找出並清除它。用戶端預設會備份檔案。

然而，在某些情況下，清除病毒後的檔案可能會無法使用。因為病毒可能已造成過多的損害。

某些受感染的檔案無法清除。

附註：Symantec Endpoint Protection 不會清除 Windows 8 樣式應用程式和檔案中所偵測到的惡意軟體。Symantec Endpoint Protection 會改為刪除此偵測到的項目。

隔離風險

將受感染的檔案從其原始位置移到「隔離所」。放到「隔離所」後的受感染檔案無法散佈病毒。

若是病毒，將受感染的檔案從其原始位置移到「隔離所」。此設定是對病毒執行的第二個預設動作。

若是安全風險，用戶端會將受感染的檔案從其原始位置移到「隔離所」，並嘗試移除或修復任何副作用。此設定是對安全風險執行的第一個預設動作。

「隔離所」包含所有已執行動作的記錄。您可以使電腦回到用戶端移除風險之前的狀態。

附註：Symantec Endpoint Protection 不會隔離 Windows 8 樣式應用程式和檔案中所偵測到的惡意軟體。Symantec Endpoint Protection 會改為刪除此偵測到的項目。

刪除風險	從電腦硬碟上刪除受感染的檔案。如果用戶端無法刪除檔案，「通知」對話方塊會顯示用戶端已執行動作的相關資訊。此項資訊也會顯示在「事件日誌」中。 只有在您有未受病毒或安全風險感染的備份複本可以取代此檔案時，才能使用此動作。用戶端會永久刪除風險。受感染的檔案無法從「資源回收筒」復原。 **附註：**當您架構對安全風險執行的動作時，請審慎使用此動作。某些情況下，刪除安全風險可能造成應用程式喪失功能。
略過 (只記錄)	保持檔案不變。 如果您對病毒使用此動作，則病毒會留在受感染的檔案中，並可能擴散到電腦的其他區域。「風險記錄」中會置入一個項目，保留受感染檔案的記錄。 您可以使用「略過(只記錄)」作為對惡意軟體和安全風險執行的第二個動作。 當您執行大規模的自動掃描 (如排程掃描) 時，請勿選取此動作。若要檢視掃描結果，之後再採取其他動作，則可能需要使用此動作。其他動作可能是將檔案移到「隔離所」。 若是安全風險，此動作會讓受感染檔案維持不變，並在「風險記錄」中置入項目，以保留該風險的記錄。使用此選項來手動控制用戶端處理安全風險的方法。此設定是對安全風險執行的第二個預設動作。 您的管理員可能會送出自訂訊息，說明應該如何回應。

7 針對您想要設定特定動作的每個類別，重複上述步驟，然後按下**「確定」**。

8 如果您選取安全風險類別，則可以針對該安全風險類別的一個或多個特定實例選取自訂動作。您可以排除掃描某個安全風險。例如，您可能想要排除某個廣告軟體，因為您工作時會用到它。

9 按下**「確定」**。

關於排除掃描項目

例外是指您要排除，不接受掃描的已知安全風險、檔案、副檔名和程序。如果您已掃描電腦，知道有些檔案安全無虞，即可加以排除。在某些情況下，例外可減少掃描時間並提升系統效能。通常您不必建立例外。

對於受管用戶端，您的管理員可能已經建立掃描例外。如果建立的例外與管理員定義的例外發生衝突，會優先採用管理員定義的例外。管理員還可以防止您架構任何或所有類型的例外。

附註：如果電子郵件應用程式將所有電子郵件儲存在單一檔案中，則您應該建立檔案例外，才不會掃描收件匣檔案。依預設，掃描會隔離病毒。如果掃描在收件匣檔案中偵測到病毒，掃描將隔離整個收件匣。如果掃描隔離收件匣，您就無法存取電子郵件。

表 4-9 例外類型

例外類型	敘述
檔案	適用於病毒和間諜軟體掃描 掃描會忽略您選取的檔案。
資料夾	適用於病毒和間諜軟體掃描或SONAR，或同時適用於這兩者 掃描會忽略您選取的資料夾。
已知風險	適用於病毒和間諜軟體掃描 掃描會忽略您選取的所有已知風險。
副檔名	適用於病毒和間諜軟體掃描 掃描會忽略帶有指定副檔名的全部檔案。
Web 網域	適用於病毒和間諜軟體掃描 「下載智慧型掃描」會忽略指定的信任 Web 網域。
應用程式	適用於病毒和間諜軟體掃描，以及 SONAR 掃描會忽略、記錄、隔離或終止您在此指定的應用程式。
DNS 或主機檔案變更	適用於 SONAR 當特定應用程式嘗試變更DNS設定或變更主機檔案時，掃描會忽略、記錄或攔截應用程式，並且提示使用者。

請參閱第 71 頁的「排除掃描項目」。

排除掃描項目

例外是您要從掃描中排除的已知安全風險、檔案、資料夾、檔案副檔名、Web網域或應用程式。如果您已掃描電腦，知道有些檔案安全無虞，即可加以排除。在某些情況下，例外可減少掃描時間並提升系統效能。您也可以針對嘗試變更DNS或主機檔案的應用程式建立例外。通常您不必建立例外。

對於受管用戶端，您的管理員可能已經建立掃描例外。如果建立的例外與管理員定義的例外發生衝突，會優先採用管理員定義的例外。

SONAR 不支援檔案例外。使用應用程式例外將檔案從 SONAR 中排除。

附註：在 Windows Server 2008 的 Server Core 安裝上，對話方塊的外觀可能會與這些步驟中說明的對話方塊不同。

從安全風險掃描中排除項目

1 在用戶端的側邊看板中，按下**「變更設定」**。

2 在**「例外」**旁，按下**「架構設定」**。

3 在**「例外」**對話方塊的**「使用者定義例外」**下，按下**「新增」>「安全風險例外」**。

4 選取下列任一例外類型：

- **已知風險**
- **檔案**
- **資料夾**
- **副檔名**
- **Web 網域**

5 執行下列其中一項動作：

- 對於已知風險，勾選您要從掃描中排除的安全風險。
  若要記錄偵測到或忽略安全風險時的事件，請勾選**「偵測到安全風險時記錄」**。
- 對於檔案或資料夾，選取您要排除的檔案或資料夾，或輸入檔案或資料夾名稱。
  選取掃描類型(**「全部掃描」**、**「自動防護」**或**「排程和隨選」**)，然後按下**「確定」**。
- 對於副檔名，輸入您要排除的副檔名。
  文字方塊中只能輸入一個副檔名。若輸入多個副檔名，用戶端會將該輸入項目視為一個副檔名。
- 對於網域，輸入您要從「下載智慧型掃描」和SONAR偵測中排除的網站或 IP 位址。

6 按下**「確定」**。

將資料夾從 SONAR 中排除

1 在用戶端的側邊看板中，按下**「變更設定」**。

2 在**「例外」**旁，按下**「架構設定」**。

3 在**「例外」**對話方塊的**「使用者定義例外」**下，按下**「新增」>「SONAR 例外」>「資料夾」**。

4 選取您要排除的資料夾，勾選或取消勾選「**包括子資料夾**」，然後按下「**確定**」。

5 按下「**關閉**」。

變更所有掃描處理應用程式的方式

1 在用戶端的側邊看板中，按下「**變更設定**」。

2 在「**例外**」旁，按下「**架構設定**」。

3 在「**例外**」對話方塊的「**使用者定義例外**」下，按下「**新增**」>「**應用程式例外**」。

4 選取應用程式的檔名

5 在「**動作**」下拉式方塊中，選取「**忽略**」、「**只記錄**」、「**隔離**」、「**終止**」或「**移除**」。

6 按下「**確定**」。

7 按下「**關閉**」。

請參閱第 48 頁的「管理電腦上的掃描」。

請參閱第 70 頁的「關於排除掃描項目」。

管理用戶端電腦上的隔離檔案

依預設，Symantec Endpoint Protection 會嘗試在偵測到受感染的檔案時清除檔案中的病毒。如果無法清除此檔案，則掃描作業會將此檔案放置在電腦上的「隔離所」中。對於安全風險，掃描作業會將受感染的檔案移至「隔離所」，並修復安全風險的任何副作用。「下載智慧型掃描」和 SONAR 也可以隔離檔案。

請參閱第 74 頁的「關於隔離檔案」。

表 4-10 管理用戶端電腦上的隔離檔案

工作	敘述
將隔離的檔案還原至原始位置	有時候，乾淨的檔案並沒有可供還原的位置。例如，受感染的附件可能是從電子郵件中移除，而並被送至「隔離所」。您必須釋放該檔案並指定一個位置。
手動隔離項目	透過將檔案新增到「隔離所」，或者藉由從病毒和間諜軟體日誌或 SONAR 日誌中選取檔案，可以手動隔離檔案。 請參閱第 75 頁的「從風險日誌或掃描日誌隔離檔案」。

工作	敘述
從隔離所永久刪除檔案	您可以從「隔離所」手動刪除不再需要的檔案。您也可以設定自動刪除檔案的時間週期。 **附註：**您的管理員可以指定該項目可保留在「隔離所」中最大天數。在時間限制之後，便會自動從「隔離所」中刪除該項目。
在接收新的定義檔後，重新掃描「隔離所」中的檔案	更新定義時，可能會自動掃描、清除或還原「隔離所」中的檔案。對於部分檔案，會出現「修復精靈」。按照螢幕上的指示完成重新掃描和修復。 您還可以手動重新掃描「隔離所」中受病毒感染的檔案。
匯出隔離所資訊	將「隔離所」的內容匯出為逗號分隔 (.csv) 檔案或 Microsoft Access 資料庫 (.mdb) 檔案。
將隔離所中受感染的檔案傳送至「賽門鐵克安全機制應變中心」	重新掃描「隔離所」中的項目後，您可能希望將仍受感染的檔案傳送至「賽門鐵克安全機制應變中心」，以便進行進一步分析。 請參閱第 75 頁的「將可能感染病毒的檔案以手動方式傳送至「賽門鐵克安全機制應變中心」進行分析」。
清除備份項目	在嘗試清除或修復項目時，用戶端依預設會備份受感染的項目。在用戶端成功清除病毒之後，您應該手動清除「隔離所」中的項目，這是因為備份仍然受感染。
自動從隔離所刪除檔案	您可以將用戶端設定為在經過指定的時間間隔後，自動移除隔離所中的項目。您也可以指定，在儲存項目的資料夾達到特定大小時，用戶端便移除項目。此架構可防止您因忘記從這些區域中手動移除檔案而造成檔案堆積。 請參閱第 76 頁的「自動從隔離所刪除檔案」。

關於隔離檔案

當用戶端將受感染的檔案移到「隔離所」時，病毒或風險就無法感染電腦或網路中其他電腦上的檔案。然而，「隔離所」動作不會清除病毒風險。病毒風險會停留在電腦上，直到用戶端清除風險或刪除檔案為止。您雖然無法存取此檔案，但可以從「隔離所」移除此檔案。

當您以新病毒定義更新您的電腦時，用戶端會自動檢查隔離所。您可以重新掃描隔離所中的項目。最新的定義可能會清除或修復先前隔離的檔案。

大多數病毒都可以隔離。開機型病毒存放在電腦的開機磁區或分割區表，因此這些項目無法被移動至「隔離所」。有時候，用戶端會偵測到不明病毒，無法以目前的病毒定義集加以排除。如果您認為某個檔案已經遭受感染，但是掃描無法偵測到任何感染狀況，就應手動隔離該檔案。

附註：您用戶端的作業系統語言可能無法轉譯風險名稱中的某些字元。如果作業系統無法解譯字元，那些字元會在通知中顯示為問號。例如，某些Unicode編碼的風險名稱可能包含全形字元。在執行用戶端的英文作業系統電腦上，這些字元會顯示為問號。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

從風險日誌或掃描日誌隔離檔案

根據威脅偵測的預設動作，在偵測到威脅時，用戶端不一定能夠執行您選取的動作。您可以稍後再使用「風險日誌」或「掃描日誌」來隔離檔案。

請參閱第 74 頁的「關於隔離檔案」。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

從風險日誌或掃描日誌隔離檔案

1. 在用戶端中，按下**「檢視日誌」**。
2. 在**「病毒和間諜軟體防護」**旁，按下**「檢視日誌」**，然後選取**「風險日誌」**或**「掃描日誌」**。
3. 選取要隔離的檔案，然後按下**「隔離」**。
4. 按下**「確定」**，然後再按下**「關閉」**。

將可能感染病毒的檔案以手動方式傳送至「賽門鐵克安全機制應變中心」進行分析

當您將受感染的項目從隔離清單送出至「賽門鐵克安全機制應變中心」時，「賽門鐵克安全機制應變中心」可分析此項目以確保其不受感染。「賽門鐵克安全機制應變中心」還會使用此資料防範新威脅或威脅變種。

附註：如果管理員停用這些傳送類型，傳送選項將無法使用。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

從「隔離所」將檔案傳送到賽門鐵克安全機制應變中心

1. 在用戶端的側邊看板中，按下**「檢視隔離所」**。
2. 從隔離項目清單中選取檔案。
3. 按下**「傳送」**。
4. 遵照精靈中畫面上的指示，收集必要資訊並傳送檔案以供分析。

自動從隔離所刪除檔案

您可以設定軟體，在經過一段指定的時間之後，自動從「隔離所」清單移除項目。您也可以指定，在儲存項目的資料夾達到特定大小時，用戶端便移除項目。此架構可防止您因忘記從這些區域中手動移除檔案而造成檔案堆積。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

從「隔離所」自動刪除檔案

1. 在用戶端的側邊看板中，按下**「檢視隔離所」**。
2. 按下**「清除選項」**。
3. 在**「清除選項」**對話方塊中，選取下列其中一個標籤：
   - **隔離項目**
   - **備份項目**
   - **修復項目**
4. 勾選或取消勾選**「儲存的時間長度超過」**，以允許或禁止用戶端在架構的時間超過之後刪除檔案。
5. 如果您勾選**「儲存的時間長度超過」**核取方塊，請輸入時間，或按下箭頭輸入時間。
6. 從下拉式清單中選取時間單位。預設值為 30 天。
7. 如果您勾選**「資料夾總大小超過」**核取方塊，則輸入允許的資料夾大小上限，以 MB 為單位。預設值為 50 MB。

   如果您兩個核取方塊都勾選，則會先刪除早於所設定時間的全部檔案。如果資料夾大小仍然超過您設定的限制，則用戶端會個別刪除最舊的檔案。用戶端會刪除最舊的檔案，直到資料夾大小不超過限制為止。
8. 針對其他標籤的任何項目，重複步驟 4 至 7。
9. 按下**「確定」**。

啟用或停用提早啟動防惡意軟體 (ELAM)

提早啟動防惡意軟體 (ELAM) 可在您的電腦啟動時，以及第三方驅動程式初始化之前，為您的電腦提供保護。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。

Symantec Endpoint Protection 提供的提早啟動防惡意軟體驅動程式可搭配 Microsoft 提早啟動防惡意軟體驅動程式使用，以提供防護。Microsoft Windows 8 支援這些設定。

附註：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。

對於需要矯正的某些 ELAM 偵測，您可能需要執行 Power Eraser。Power Eraser 是 Symantec Endpoint Protection 支援工具的一部分。

啟用或停用提早啟動防惡意軟體

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在**「病毒和間諜軟體防護」**旁，按下**「架構設定」**。
3. 在**「提早啟動防惡意軟體」**標籤上，勾選或取消勾選**「啟用賽門鐵克提早啟動防惡意軟體」**。

   必須啟用 Windows 提早啟動防惡意軟體驅動程式，這個選項才能生效。
4. 如果您要僅記錄偵測，請在**「當 Symantec Endpoint Protection 偵測到潛在的惡意驅動程式時」**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 48 頁的「管理電腦上的掃描」。

請參閱第 22 頁的「使用 Symantec Endpoint Protection 支援工具排除電腦問題」。

請參閱第 71 頁的「排除掃描項目」。

如何管理出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知

依預設，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。

您可以執行下列動作以管理彈出式通知：

- 在用戶端的**「用戶端管理設定」**頁面上，修改 Windows 8 樣式使用者介面通知的全域設定。
- 在 Windows 8 中，變更作業系統的通知設定。
  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。如需詳細資訊，請參閱 Windows 8 使用者說明文件。

在受管用戶端上，您的管理員可能會控制您是否可在 Windows 8 中看到彈出式通知。

請參閱第 28 頁的「回應出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知」。

關於將偵測相關資訊傳送至賽門鐵克安全機制應變中心

您可以將電腦架構為自動將偵測相關資訊傳送至賽門鐵克安全機制應變中心進行分析。

賽門鐵克安全機制應變中心和全球情報網會使用此項傳送資訊，以針對新的與發展中的安全性威脅快速做出回應。您傳送的資料會提升賽門鐵克回應威脅與自訂防護的能力。賽門鐵克建議您永遠允許進行此類資料傳送。

請參閱第 11 頁的「關於 Symantec Endpoint Protection 用戶端」。

您可以選擇傳送下列任何類型的資料：

- 檔案信譽
  依據檔案信譽偵測到的檔案相關資訊。有關這些檔案的資訊會匯入「賽門鐵克智慧型掃描」信譽資料庫，以協助您的電腦防範新的和新興風險。
- 防毒偵測
  有關病毒和間諜軟體掃描偵測的資訊。
- 防毒進階啟發式偵測
  由 Bloodhound 及其他病毒和間諜軟體掃描啟發式技術偵測到的潛在威脅的相關資訊。
  這些偵測是無訊息偵測，不會顯示在「風險日誌」中。有關這些偵測的資訊用於進行統計分析。
- SONAR 偵測
  SONAR 偵測到的威脅的相關資訊，包括高/低風險偵測、系統變更事件和受信任應用程式出現的可疑行為。
- SONAR 啟發式
  SONAR 啟發式偵測是無訊息偵測，不會顯示在「風險日誌」中。此資訊用於進行統計分析。

您也可以從隔離所中手動將樣本傳送到賽門鐵克安全機制應變中心，或透過賽門鐵克網站傳送。 若要透過賽門鐵克網站傳送檔案，請聯絡賽門鐵克技術支援。

請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。

請參閱第 58 頁的「Symantec Endpoint Protection 如何使用信譽資料進行檔案相關決策」。

將有關偵測的資訊傳送到賽門鐵克安全機制應變中心

Symantec Endpoint Protection 可以藉由監控進出電腦的資訊以及攔截攻擊嘗試，保護您的電腦。

您可以允許電腦將偵測到的威脅資訊傳送至「賽門鐵克安全機制應變中心」。「賽門鐵克安全機制應變中心」使用此資訊保護您的用戶端電腦，使其免受新威脅、目標威脅和變種威脅的危害。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。賽門鐵克建議您傳送盡可能多的偵測資訊。

您也可以透過「隔離」頁面向「賽門鐵克安全機制應變中心」手動傳送範例。「隔離」頁面也可供您決定向「賽門鐵克安全機制應變中心」傳送項目的方式。

架構傳送至賽門鐵克安全機制應變中心

1. 選取**「變更設定」**>**「用戶端管理」**。
2. 在**「遞送」**標籤上，勾選**「允許此電腦自動向賽門鐵克轉送選取的匿名安全資訊」**。 使用這個選項，Symantec Endpoint Protection 可傳送電腦中發現的威脅之相關資訊。

   賽門鐵克建議您保持此選項的啟用狀態。
3. 選取要送出的資訊類型。

   關於這些選項的更多資訊，請按下**「說明」**。
4. 啟用**「允許智慧型掃描查詢以偵測威脅」**，以允許 Symantec Endpoint Protection 使用賽門鐵克信譽資料庫來進行威脅相關決策。
5. 按下**「確定」**。

請參閱第 73 頁的「管理用戶端電腦上的隔離檔案」。

請參閱第 78 頁的「關於將偵測相關資訊傳送至賽門鐵克安全機制應變中心」。

關於用戶端和 Windows 資訊安全中心

如果您在 Windows XP (已安裝 Service Pack 2 或 Service Pack 3) 上使用 Windows 資訊安全中心 (WSC)，則可以在 WSC 中查看 Symantec Endpoint Protection 的狀態。

表 4-11 顯示 WSC 中的防護狀態報告。

表 4-11 WSC 防護狀態報告

賽門鐵克產品狀況	防護狀態
尚未安裝 Symantec Endpoint Protection	找不到 (紅色)
已安裝 Symantec Endpoint Protection，並啟用全面防護	啟動 (綠色)
已安裝 Symantec Endpoint Protection，但病毒和安全風險定義不是最新的	過期 (紅色)
已安裝 Symantec Endpoint Protection，但未啟用檔案系統的「自動防護」。	關閉 (紅色)
已安裝 Symantec Endpoint Protection，但未啟用檔案系統的「自動防護」，而且病毒和安全風險定義不是最新的	關閉 (紅色)
已安裝 Symantec Endpoint Protection，但 ccSvcHst 已手動關閉	關閉 (紅色)

表 4-12 顯示 WSC 中報告的 Symantec Endpoint Protection 防火牆狀態。

表 4-12 WSC 防火牆狀態報告

賽門鐵克產品狀況	防火牆狀態
未安裝 Symantec Firewall	找不到 (紅色)
已安裝並啟用 Symantec Firewall	啟動 (綠色)
已安裝 Symantec Firewall，但未啟用	關閉 (紅色)
尚未安裝或啟動 Symantec Firewall，但有安裝並啟動第三方的防火牆	啟動 (綠色)

附註：在 Symantec Endpoint Protection 中，預設會停用「Windows 防火牆」。

如果啟用一個以上的防火牆，WSC 會報告已安裝並啟用多個防火牆。

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、入侵預防和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，並且對電腦進行主動型本機監視。SONAR 也會偵測您應監視的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。

附註：SONAR 不會將程式碼插入 Symantec Endpoint Protection 12.1 或以前版本用戶端上的應用程式中。如果使用 Symantec Endpoint Protection Manager 12.1.2 來管理用戶端，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。

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。

請參閱第 82 頁的「在用戶端電腦上管理 SONAR」。

請參閱第 71 頁的「排除掃描項目」。

在用戶端電腦上管理 SONAR

您可以將 SONAR 作為「主動型威脅防護」的一部分進行管理。在受管用戶端上，管理員可能會鎖定部分設定。

表 4-13 在用戶端電腦上管理 SONAR

工作	敘述
確定 SONAR 已啟用	為了在用戶端電腦上提供最佳防護，應啟用 SONAR。依預設，SONAR 為啟用狀態。 您可以透過啟用「主動型威脅防護」來啟用 SONAR。 請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。
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 (信譽查詢)，SONAR 將只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。 請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。
變更 SONAR 設定	您可以啟用或停用 SONAR。您也可以變更對 SONAR 偵測到的某些威脅類型的偵測動作。您可能希望變更偵測動作以減少偵測誤報率。 請參閱第 83 頁的「變更 SONAR 設定」。
為已知安全的應用程式建立例外	SONAR 可能會偵測您希望在電腦上執行的檔案或應用程式。您可以在**「例外」>「變更設定」**頁面上，針對檔案、資料夾或應用程式建立SONAR例外。您也可以從「隔離所」建立例外。 請參閱第 71 頁的「排除掃描項目」。
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。您可以針對該應用程式建立檔案或應用程式例外。 請參閱第 71 頁的「排除掃描項目」。
將有關 SONAR 偵測的資訊傳送到「賽門鐵克安全機制應變中心」	賽門鐵克建議您將有關偵測的資訊傳送至「賽門鐵克安全機制應變中心」。此資訊有助於賽門鐵克處理威脅。遞送預設為啟用。 請參閱第 79 頁的「將有關偵測的資訊傳送到賽門鐵克安全機制應變中心」。

請參閱第 48 頁的「管理電腦上的掃描」。

請參閱第 54 頁的「關於掃描類型」。

變更 SONAR 設定

您可能希望變更 SONAR 動作，以降低誤報偵測率。您還可以變更針對 SONAR 啟發式偵測的通知。

請參閱第 82 頁的「在用戶端電腦上管理 SONAR」。

附註：在受管用戶端上，管理員可能會鎖定這些設定。

變更 SONAR 設定

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在**「主動型威脅防護」**旁，按下**「架構設定」**。
3. 在 **SONAR** 標籤上，變更高風險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. 此外，也可以選擇變更通知設定。
5. 在**「可疑行為偵測」**標籤上，變更高風險偵測或低風險偵測的動作。當受信任檔案與可疑行為有關聯時，SONAR 將執行這些偵測。
6. 在**「系統變更事件」**標籤上，變更偵測到DNS伺服器設定或主機檔案發生變更時的掃描動作。
7. 按下**「確定」**。

5

管理防火牆和入侵預防

本章包含以下主題：

管理防火牆防護

根據預設，Symantec Endpoint Protection 用戶端會提供電腦所需的適當防火牆防護等級。

不過，您的管理員可能變更了某些預設防火牆規則和設定。如果您的管理員授予了您修改防火牆防護的權限，您就可以修改防火牆規則或防火牆設定。

表 5-1 說明您可以執行的保護電腦的防火牆工作。所有這些工作都是選擇性的工作，並且可以任何順序執行。

表 5-1 管理防火牆防護

工作	敘述
讀取防火牆的運作方式	瞭解防火牆如何保護電腦不受網路攻擊威脅。 請參閱第 87 頁的「防火牆的運作方式」。
新增及自訂防火牆規則	您可以新增防火牆規則或編輯現有的防火牆規則。例如，您可以攔截不想在電腦上執行的應用程式，例如廣告軟體應用程式。 請參閱第 87 頁的「管理防火牆規則」。 您也可以架構防火牆規則來允許或防止應用程式存取網路。 請參閱第 97 頁的「建立當應用程式從您的電腦存取網路時的防火牆規則」。
架構防火牆設定	除建立防火牆規則外，您還可以啟用及架構防火牆設定，以進一步增強防火牆防護。 請參閱第 93 頁的「啟用或停用防火牆設定」。
檢視防火牆日誌	您可以定期檢查電腦上的防火牆防護狀態，以確定以下事項： ■ 您所建立的防火牆規則是否正常運作。 ■ 用戶端是否攔截任何網路攻擊。 ■ 用戶端是否攔截您希望執行的任何應用程式。 您可以使用「流量日誌」和「封包日誌」來檢查防火牆防護狀態。根據預設，「封包日誌」在受管用戶端上為停用。 請參閱第 38 頁的「關於日誌」。 請參閱第 40 頁的「啟用封包日誌」。
允許或攔截應用程式和某些類型的流量	為了額外的安全性，您可以在下列情況下攔截網路流量以防存取您的電腦。 ■ 當電腦的螢幕保護程式開啟時，您可以攔截流量。 ■ 當防火牆沒有執行時，您可以攔截流量。 ■ 您可以在任何時候攔截全部流量。 請參閱第 98 頁的「架構用戶端在螢幕保護程式處於作用中或防火牆未執行時攔截流量」。 ■ 您可以允許、攔截或顯示訊息以允許還是攔截應用程式存取網路。這些應用程式已經在電腦上執行。 請參閱第 96 頁的「允許或攔截應用程式存取網路」。 請參閱第 97 頁的「建立當應用程式從您的電腦存取網路時的防火牆規則」。
啟動或停用防火牆。	您可以暫時停用「網路威脅防護」以進行疑難排解。例如，您可能需要停用防火牆以便能夠開啟某個應用程式。 請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。

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片段，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。

封包包含以下資訊：

- 傳送端電腦
- 設定的接收端
- 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 85 頁的「管理防火牆防護」。

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 用戶端包含預設防火牆規則，可保護您的電腦。不過，如果您的管理員允許，或者您的用戶端未受管理，則可以為其他防護修改防火牆規則。

表 5-2 說明管理防火牆規則所需瞭解的相關內容。

表 5-2 管理防火牆規則

主旨	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。 ■ 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 90 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。 ■ 用戶端會使用狀態式檢測，因此您不需建立額外的規則。 請參閱第 91 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。 請參閱第 88 頁的「防火牆規則的組成要素」。
新增防火牆規則	您可以執行下列工作來管理防火牆規則： ■ Symantec Endpoint Protection 會與預設防火牆規則一起安裝，但是您可以新增自己的規則。 請參閱第 91 頁的「新增防火牆規則」。 ■ 您可以自訂預設規則，或是藉由變更任何防火牆規則條件所建立的規則。 ■ 匯出和匯入防火牆規則 增加防火牆規則的另一種方法，是從其他防火牆政策中匯出現有的防火牆規則。接著您可以匯入防火牆規則和設定，這樣一來就不需要重新加以建立。 請參閱第 93 頁的「匯出和匯入防火牆規則」。 ■ 複製並貼上防火牆規則
啟用或停用防火牆規則	防火牆規則會自動啟用。不過，您可能需要暫時停用防火牆規則來測試規則。防火牆不會檢查停用的規則。 請參閱第 92 頁的「啟用和停用防火牆規則」。

防火牆規則的組成要素

防火牆規則會控制用戶端保護電腦的方式，以攔阻惡意網路流量。當一台電腦嘗試與另一台電腦連線時，防火牆會根據防火牆規則比對連線類型。防火牆會自動根據這類規則，檢查所有入埠及離埠的流量封包。防火牆可根據規則，允許或攔截封包。

您可以使用應用程式、主機及通訊協定這類觸發條件，來定義防火牆規則。例如，一條可辨別與目的位址有關之通訊協定的規則。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。若目前封包有任何觸發條件為假，防火牆就不會套用該項規則。

一旦觸發某項防火牆規則，便不會評估其他防火牆規則。如果未觸發任何規則，系統將自動攔截該資料包，且不記錄該事件。

防火牆規則描述允許或攔截網路連線的條件。例如，某項規則可能允許每日上午 9 時至下午 5 時之間，在 IP 位址 192.58.74.0 和遠端通訊埠 80 之間進行的網路通訊。

表 5-3 說明用於定義防火牆規則的準則。

表 5-3 防火牆規則條件

條件	敘述
觸發條件	防火牆規則觸發條件如下： ■ 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，則防火牆會允許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，描述允許進行通訊的特定網路通訊協定和主機。 ■ 主機 本機主機一定是本機用戶端電腦，而遠端主機一定是位在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。在定義主機觸發條件時，您可以指定位於所述網路連線遠端的主機。 ■ 通訊協定 通訊協定觸發條件會根據所述的流量，識別產生作用的一項或多項網路通訊協定。 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。 ■ 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。 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。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 True，防火牆即不會套用規則。
條件	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。條件參數是選用項目，如果未經定義，則不會有任何作用。您可以設定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。防火牆接收封包時，防火牆不會評估非作用中規則。
動作	允許或攔截，記錄或不記錄。 動作參數會指定防火牆成功比對到規則時所採取的動作。如果規則是針對接收的封包選取的規則，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。

請參閱第 91 頁的「防火牆如何使用狀態式檢測」。
請參閱第 91 頁的「新增防火牆規則」。
請參閱第 87 頁的「管理防火牆規則」。

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。

建立規則資料庫的最佳方法，包括下列規則順序：

第一　攔截所有流量的規則。

第二　允許所有流量的規則。

第三　允許或攔截特定電腦的規則。

第四　允許或攔截特定應用程式、網路服務，以及通訊埠的規則。

表 5-4 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 5-4　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 92 頁的「變更防火牆規則的順序」。

請參閱第 87 頁的「防火牆的運作方式」。

請參閱第 100 頁的「入侵預防的運作方式」。

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。

請參閱第 87 頁的「防火牆的運作方式」。

請參閱第 87 頁的「管理防火牆規則」。

新增防火牆規則

新增防火牆規則時，您必須決定規則有何功能。例如，您可能想要允許來自特定來源的全部流量，或攔截來自某個網站的 UDP 封包。

建立防火牆規則時，將自動啟用規則。

新增防火牆規則

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在**「網路威脅防護」**旁，按下**「選項」>「架構防火牆規則」**。
3. 在**「架構防火牆規則」**對話方塊中，按下**「新增」**。
4. 在**「一般」**標籤上輸入規則的名稱，然後按下**「攔截此流量」**或**「允許此流量」**。
5. 若要定義規則的觸發條件，請按下各個標籤並依需要進行架構。
6. 若要定義規則有效或無效的期間，請在**「排程」**標籤上按下**「啟用排程」**，然後設定排程。

7 當您完成變更時，按下**「確定」**。

8 按下**「確定」**。

請參閱第 88 頁的「防火牆規則的組成要素」。

請參閱第 92 頁的「啟用和停用防火牆規則」。

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。

當您變更順序時，它只會影響目前所選位置的順序。

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。

變更防火牆規則的順序

1 在用戶端的側邊看板中，按下**「狀態」**。

2 在**「網路威脅防護」**旁，按下**「選項」>「架構防火牆規則」**。

3 在**「架構防火牆規則」**對話方塊中，選取您要移動的規則。

4 執行下列其中一項動作：

- 若要讓防火牆處理上一則規則之前處理此規則，請按向上箭頭。
- 若要讓防火牆處理下一則規則之後處理此規則，請按向下箭頭。

5 當您移動規則完畢時，按下**「確定」**。

請參閱第 90 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。

啟用和停用防火牆規則

您必須啟用規則，好讓防火牆處理這些規則。新增防火牆規則時，規則會自動啟用。

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。

啟用與停用防火牆規則

1 在用戶端的側邊看板中，按下**「狀態」**。

2 在**「網路威脅防護」**旁，按下**「選項」>「架構防火牆規則」**。

3 在**「架構防火牆規則」**對話方塊的**「規則名稱」**欄中，在要啟用或停用的規則旁勾選或取消勾選核取方塊。

4 按下**「確定」**。

請參閱第 91 頁的「新增防火牆規則」。

匯出和匯入防火牆規則

您可以和另一個用戶端共用規則，即可不必重新建立規則。您可以從另一部電腦匯出規則，然後匯入至您的電腦。匯入規則時，這些規則會新增至防火牆規則清單的末端。即使匯入的規則與現有規則完全相同，匯入的規則也不會覆寫現有規則。

匯出的規則和匯入的規則會儲存在 .sar 檔案中。

匯出防火牆規則

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在「網路威脅防護」旁，按下**「選項」>「架構防火牆規則」**。
3. 在**「架構防火牆規則」**對話方塊中，選取想要匯出的規則。
4. 在規則上按滑鼠右鍵，然後按下**「匯出選取的規則」**。
5. 在**「匯出」**對話方塊中，輸入檔案名稱，然後按下**「儲存」**。
6. 按下**「確定」**。

匯入防火牆規則

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在「網路威脅防護」旁，按下**「選項」>「架構防火牆規則」**。
3. 在**「架構防火牆規則」**對話方塊中，在防火牆規則清單上按滑鼠右鍵，然後按下**「匯入規則」**。
4. 在**「匯入」**對話方塊中，找出包含想要匯入規則的 .sar 檔案。
5. 按下**「開啟」**。
6. 按下**「確定」**。

請參閱第 91 頁的「新增防火牆規則」。

啟用或停用防火牆設定

您可以啟用用戶端的防火牆設定來防護電腦，避免特定類型的網路攻擊。某些設定會取代您需要另外新增的防火牆規則。

附註：管理員不一定會允許您架構部分設定。

表 5-5 描述您可架構的防火牆設定類型以進一步自訂防火牆防護。

表 5-5 防火牆設定

類別	敘述
重要網路服務的內建規則	Symantec Endpoint Protection 提供了內建規則，供某些重要網路服務進行一般交換。有了內建規則，您無須建立明確允許這些服務的防火牆規則。處理期間，這些內建規則會在防火牆規則之前評估，如此符合作用中內建規則的封包即獲得允許。您可以定義 DHCP、DNS 和 WINS 服務的內建規則。
流量和隱藏網頁瀏覽	您可以啟用各種流量設定和隱藏網頁瀏覽設定，保護用戶端不受特定類型的網路攻擊。您可以啟用流量設定，偵測和攔截透過驅動程式、NetBIOS 和 Token Ring 進行通訊的流量。您可以架構設定，以偵測使用較隱形攻擊的流量。您也可以控制不符合任何防火牆規則的 IP 流量行為。
網路檔案和列印共用	您可以允許用戶端在區域網路上共用本身的檔案或瀏覽共用的檔案與印表機。若要防範網路攻擊，您可以停用網路檔案與印表機共用。 請參閱第 94 頁的「啟動網路檔案和印表機共用」。
攔截攻擊電腦	當 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。然後，用戶端會在一段時間內自動攔截所有進出攻擊電腦 IP 位址的全部流量。 單一位置會攔截攻擊電腦的 IP 位址。

啟用或停用防火牆設定

1. 在用戶端中，按下**「變更設定」**。
2. 在**「網路威脅防護」**旁，按下**「架構設定」**。
3. 在**「防火牆」**標籤上，勾選要啟用的設定。

   如需關於設定的詳細資訊，請按下**「說明」**。
4. 按下**「確定」**。

請參閱第 87 頁的「管理防火牆規則」。

啟動網路檔案和印表機共用

您可以允許用戶端在區域網路上共用本身的檔案或瀏覽共用的檔案與印表機。若要防範網路攻擊，您可以停用網路檔案與印表機共用。

表 5-6 啟用網路檔案與列印共用的方式

工作	敘述
在**「Microsoft Windows 網路」**標籤上自動啟用網路檔案與印表機共用設定。	如果有防火牆規則攔截此流量，防火牆規則的優先順序將高於此設定。 自動啟用網路檔案與列印共用

工作	敘述
藉由新增防火牆規則，手動啟用網路檔案與印表機共用。	如果您需要更高的彈性 (相較於設定所提供者)，則可以新增防火牆規則。例如，當您建立規則時，可以指定特定主機而非所有主機。防火牆規則允許存取通訊埠來瀏覽和共用檔案及印表機。 您可以建立一套防火牆規則，讓用戶端得以共用其檔案。然後建立第二套防火牆規則，讓用戶端得以瀏覽其他檔案與印表機。 手動允許用戶端瀏覽檔案與印表機 手動允許其他電腦瀏覽用戶端上的檔案

自動啟用網路檔案與列印共用

1 在用戶端的側邊看板中，按下**「變更設定」**。

2 在**「網路威脅防護」**旁，按下**「架構設定」**。

3 在**「設定」**下的**「Microsoft Windows 網路」**標籤上，按下拉式功能表並選取這些設定適用的配接卡。

4 若要瀏覽網路上的其他電腦和印表機，請按下**「瀏覽網路上的檔案和印表機」**。

5 若要讓其他電腦瀏覽您的電腦上的檔案，請按下**「與網路上的其他人共用我的檔案和印表機」**。

6 按下**「確定」**。

手動允許用戶端瀏覽檔案與印表機

1 在用戶端的側邊看板中，按下**「狀態」**。

2 在**「網路威脅防護」**旁，按下**「選項」**>**「架構防火牆規則」**。

3 在**「架構防火牆規則」**對話方塊中，按下**「新增」**。

4 在**「一般」**標籤上輸入規則名稱，並按下**「允許此流量」**。

5 在**「通訊埠和通訊協定」**標籤的**「通訊協定」**下拉式清單中，按下 **TCP**。

6 在**「遠端通訊埠」**下拉式清單中，輸入：

88, 135, 139, 445

7 按下**「確定」**。

8 在**「架構防火牆規則」**對話方塊中，按下**「新增」**。

9 在**「一般」**標籤上輸入規則名稱，並按下**「允許此流量」**。

10 在**「通訊埠和通訊協定」**標籤的**「通訊協定」**下拉式清單中，按下 **UDP**。

11 在「**遠端通訊埠**」下拉式清單中，輸入：

88

12 在「**本機通訊埠**」下拉式清單中，輸入：

137, 138

13 按下「**確定**」。

手動允許其他電腦瀏覽用戶端上的檔案

1 在用戶端的側邊看板中，按下「**狀態**」。

2 在「**網路威脅防護**」旁，按下「**選項**」>「**架構防火牆規則**」。

3 在「**架構防火牆規則**」對話方塊中，按下「**新增**」。

4 在「**一般**」標籤上輸入規則名稱，並按下「**允許此流量**」。

5 在「**通訊埠和通訊協定**」標籤的「**通訊協定**」下拉式清單中，按下 **TCP**。

6 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「**架構防火牆規則**」對話方塊中，按下「**新增**」。

9 在「**一般**」標籤上輸入規則名稱，並按下「**允許此流量**」。

10 在「**通訊埠和通訊協定**」標籤的「**通訊協定**」下拉式清單中，按下 **UDP**。

11 在「**本機通訊埠**」下拉式清單中，輸入：

88, 137, 138

12 按下「**確定**」。

請參閱第 93 頁的「啟用或停用防火牆設定」。

允許或攔截應用程式存取網路

您可以指定應用程式在嘗試從您的電腦存取網路或嘗試存取您的電腦時，用戶端對應用程式採取的動作。例如，您可以攔截 Internet Explorer 從您的電腦存取任何網站。

表 5-7 說明用戶端對網路流量執行的動作。

表 5-7 應用程式存取用戶端或網路時，防火牆採取的動作

動作	敘述
允許	允許入埠流量存取用戶端電腦，以及允許離埠流量存取網路。 如果用戶端接收流量，圖示的左下角會顯示一個小藍點。如果用戶端傳送流量，小藍點會顯示在圖示的右下角。
攔截	阻止入埠流量及離埠流量存取網路或網際網路連線。
詢問	詢問您下次嘗試執行應用程式時，是否要應用程式存取網路。
終止	停止程序。

允許或攔截應用程式存取網路

1 在用戶端的側邊看板中，按下**「狀態」**。

2 在**「網路威脅防護」**旁，按下**「選項」>「檢視網路活動」**。

3 在**「網路活動」**對話方塊的應用程式或服務上按下滑鼠右鍵，然後按下您希望用戶端對該應用程式採取的動作。

4 按下**「關閉」**。

如果您按下**「允許」**、**「攔截」**或**「詢問」**，則您可以僅針對該應用程式建立防火牆規則。

請參閱第 97 頁的「建立當應用程式從您的電腦存取網路時的防火牆規則」。

建立當應用程式從您的電腦存取網路時的防火牆規則

您可以建立防火牆規則，指定在您的電腦上執行的應用程式是否可以存取網路。用戶端可以允許或攔截應用程式，或者先詢問您是否允許或攔截應用程式。例如，您可以將用戶端架構成攔截任何網站，使其無法出現在您的 Web 瀏覽器中。

您也可以指定何時及如何允許或攔截應用程式的條件。例如，您可以指定某個電玩遊戲只能在特定時段存取網路。這些規則稱為以應用程式為基礎的防火牆規則。

附註：如果防火牆規則和以應用程式為基礎的防火牆規則發生衝突，則會優先採用防火牆規則。例如，可攔截凌晨 1:00 至上午 8:00 之間所有流量的防火牆規則，會覆寫可允許 iexplore.exe 隨時執行的應用程式規則。

「網路活動」對話方塊中顯示的應用程式，是自用戶端服務啟動以來即在執行的應用程式和服務。

請參閱第 96 頁的「允許或攔截應用程式存取網路」。

建立當應用程式從您的電腦存取網路時的防火牆規則

1. 在用戶端的側邊看板中，按下「**狀態**」。
2. 在「**網路威脅防護**」旁，按下「**選項**」>「**檢視應用程式設定**」。
3. 或者，在「**檢視應用程式設定**」對話方塊中，您可以透過在應用程式上按下滑鼠右鍵，然後按下「**允許**」、「**詢問**」或「**攔截**」，變更動作。
4. 按下「**架構**」。
5. 在「**架構應用程式設定**」對話方塊中，架構此應用程式的限制。

   如需詳細資訊，請將滑鼠移至文字欄位和選項上，或按下「**說明**」。

   如果動作已在步驟 3 中設定為「**允許**」，您架構的所有設定都是此規則的限制。如果您按下「**攔截**」，則您架構的設定就是此規則的例外。
6. 按下「**確定**」。

   您可以透過按下「**移除**」或「**全部移除**」，移除您對應用程式所設的條件。在移除限制時，也會消除用戶端針對應用程式採取的動作。當應用程式或服務嘗試再度連線至網路時，系統會再次詢問您是要允許或攔截應用程式。
7. 按下「**確定**」。

請參閱第 91 頁的「新增防火牆規則」。

架構用戶端在螢幕保護程式處於作用中或防火牆未執行時攔截流量

您可以架構您的電腦在下列情況下攔截入埠流量以及離埠流量：

當您電腦的螢幕保護程式啟動時。	您可以架構讓電腦在啟動螢幕保護程式時，攔截「網路上的芳鄰」的所有入埠及離埠流量。一旦關閉螢幕保護程式時，您的電腦就會返回先前指定的安全層級。 在螢幕保護程式啟動時攔截流量
當防火牆停止執行時。	在電腦啟動後，防火牆服務啟動前，或在防火牆服務停止、電腦關閉之後的這段時間，電腦皆不受保護。這段時間是安全上的漏洞，可能會允許未經授權的通訊。 在防火牆停止執行時攔截流量
當您在任何時候想要攔截所有入埠及離埠流量時。	您可能會在破壞性病毒攻擊您公司的網路或子網路時攔截所有流量。在一般情況下您不會攔截所有流量。 **附註：**管理員可能已經架構不提供這個選項。您無法攔截非受管用戶端上的通訊。 在任何時候攔截全部流量

停用「網路威脅防護」後即可允許全部流量。

請參閱第 43 頁的「在用戶端電腦上啟用或停用防護」。

在螢幕保護程式啟動時攔截流量

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在「網路威脅防護」旁，按下**「架構設定」**。
3. 在**「Microsoft Windows 網路」**標籤的**「螢幕保護程式模式」**下，按下**「執行螢幕保護程式時，攔截 Microsoft Windows 網路流量」**。
4. 按下**「確定」**。

在防火牆停止執行時攔截流量

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在「網路威脅防護」旁，按下**「架構設定」**。
3. 在**「防火牆」**標籤的**「流量設定」**下，按下**「在防火牆啟動之前及防火牆停止之後攔截所有流量」**。
4. 選擇性按下**「允許初始 DHCP 和 NetBIOS 流量」**。
5. 按下**「確定」**。

在任何時候攔截全部流量

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在**「網路威脅防護」**旁，按下**「選項」>「檢視網路活動」**。
3. 按下**「工具」>「攔截全部流量」**。
4. 若要確認，請按下**「是」**。
5. 若要返回用戶端先前使用的防火牆設定，請取消勾選**「工具」>「攔截全部流量」**。

請參閱第 93 頁的「啟用或停用防火牆設定」。

管理入侵預防

您可將入侵預防當作「網路威脅防護」的一部分來管理。

表 5-8　管理入侵預防

動作	敘述
了解入侵預防	了解入侵預防如何偵測和攔截網路及瀏覽器攻擊。 請參閱第 100 頁的「入侵預防的運作方式」。

動作	敘述
下載最新的 IPS 特徵	依預設，會將最新特徵下載到用戶端。不過，您可能會想要立即手動下載特徵。 請參閱第 35 頁的「更新電腦的防護」。
啟用或停用網路入侵預防或瀏覽器入侵預防	當需要進行疑難排解，或用戶端電腦偵測到過多誤報結果時，您可以停用入侵預防。通常情況下，不應停用入侵預防。 您可以啟用或停用下列入侵預防類型： ■ 網路入侵預防 ■ 瀏覽器入侵預防 請參閱第 101 頁的「啟用或停用入侵預防」。 您也可以在啟用或停用「網路威脅防護」時，啟用或停用入侵預防。 請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。
架構入侵預防通知	您可以架構 Symantec Endpoint Protection 在偵測到入侵時顯示通知。 請參閱第 102 頁的「架構入侵預防通知」。

入侵預防的運作方式

入侵預防是「網路威脅防護」的一部分。

入侵預防會自動偵測和攔截網路攻擊和瀏覽器上的攻擊。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程序層的攻擊。

入侵預防提供兩種類型的防護。

表 5-9 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。 您無法在用戶端上建立自訂特徵。但您可以匯入您或管理員在 Symantec Endpoint Protection Manager 中建立的自訂特徵。

類型	敘述
瀏覽器入侵預防	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，但可以重新啟用它。 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。 請參閱下列知識庫文章，以取得瀏覽器入侵預防保護的最新資訊：支援瀏覽器入侵預防的瀏覽器版本。

請參閱第 99 頁的「管理入侵預防」。

啟用或停用入侵預防

一般來說，當您停用電腦上的入侵預防設定時，電腦的安全性會降低。但是，您可能需要停用這些設定以避免誤報或對電腦進行疑難排解。

Symantec Endpoint Protection 將入侵嘗試和事件記錄在「安全日誌」中。如果管理員進行相應架構，Symantec Endpoint Protection 也可以將入侵事件記錄在「封包日誌」中。

請參閱第 99 頁的「管理入侵預防」。

請參閱第 40 頁的「檢視日誌」。

您可以啟用或停用下列兩種類型的入侵預防：

- 網路入侵預防
- 瀏覽器入侵預防

附註：管理員可能已經架構不提供這些選項。

請參閱第 41 頁的「關於在您需要排解疑難問題時啟用和停用防護」。

啟用或停用入侵預防設定

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 在**「網路威脅防護」**旁，按下**「架構設定」**。
3. 在**「入侵預防」**標籤上，勾選或取消勾選下列其中一項設定：
   - **啟用網路入侵預防**
   - **啟用瀏覽器入侵預防**

如需設定的詳細資訊，請按下**「說明」**。

4 按下**「確定」**。

架構入侵預防通知

您可以架構在用戶端偵測到電腦出現網路攻擊時，或在用戶端攔截某應用程式存取您的電腦時，出現通知。您可以設定這些通知出現的時間長度，以及通知出現時是否發出音訊。您必須啟用入侵預防系統，入侵預防通知才會出現。

如果電腦上已啟用「入侵預防」，則 Windows 用戶端和 Mac 用戶端都會觸發這些通知。

附註：管理員可能已經架構不提供這些選項。

請參閱第 99 頁的「管理入侵預防」。

架構 Windows 用戶端上的入侵預防通知

1 在用戶端的側邊看板中，按下**「變更設定」**。

2 在「網路威脅防護」旁，按下**「架構設定」**。

3 在**「網路威脅防護設定」**對話方塊中，按下**「通知」**。

4 勾選**「顯示入侵預防通知」**。

5 若要架構在通知出現時發出嗶聲，請勾選**「通知使用者時使用音效」**。

6 按下**「確定」**。

架構 Mac 用戶端上的入侵預防通知

1 在 Symantec QuickMenu 上，按下 **Symantec Endpoint Protection >「開啟入侵預防偏好設定」**。

2 按下鎖定圖示以進行變更，或防止進一步變更。

您必須提供管理員名稱和密碼，才能鎖定或解除鎖定「入侵預防」偏好。

3 按下**「顯示入侵預防通知」**。

如有需要，按下**「通知使用者時使用音效」**。

6

管理 Symantec Network Access Control

本章包含以下主題：

Symantec Network Access Control 的運作方式

對於嘗試連線至網路的電腦，Symantec Network Access Control 用戶端會驗證和強制執行政策遵從。此程序會在電腦連線至網路前開始進行，並且在整個連線期間持續運作。「主機完整性政策」是所有的評估和動作基準的安全性政策。「主機完整性」也稱為「安全性遵從」。

表 6-1 說明 Network Access Control 用來在用戶端電腦上強制執行政策遵從的程序。

表 6-1 Symantec Network Access Control 如何運作

動作	敘述
用戶端會持續評估遵從狀況	開啟用戶端電腦。用戶端執行「主機完整性」檢查，比較電腦的架構和從管理伺服器下載的「主機完整性政策」。 「主機完整性」檢查會評估您的電腦是否遵從「主機完整性」政策關於防毒軟體、修正程式、修補程式和其他安全性需求。例如，政策會檢查最近更新病毒定義檔的狀況，並檢查套用至作業系統的最新修正程式有哪些。 請參閱第 105 頁的「執行主機完整性檢查」。
Symantec Enforcer 會驗證用戶端電腦，然後授予電腦網路存取權限，或者攔截並隔離非遵從電腦。	如果電腦符合全部的政策需求，則表示通過「主機完整性」檢查。Enforcer 會將完整的網路存取權限授予通過「主機完整性」檢查的電腦。 如果電腦未符合政策需求，則「主機完整性」檢查會失敗。「主機完整性」檢查失敗時，用戶端或 Symantec Enforcer 會攔截或隔離電腦，直到電腦已修補為止。被隔離的電腦網路存取權限會受到限制，甚至無法存取網路。 請參閱第 104 頁的「用戶端如何與 Enforcer 搭配使用」。
管理員可能已經設定政策，因此，即使在不符合特定要求的狀況下，「主機完整性」檢查仍然會通過。	每次「主機完整性」檢查通過時，用戶端會顯示通知。 請參閱第 23 頁的「警示和通知的類型」。
用戶端會矯正非遵從電腦	如果未通過「主機完整性」檢查，用戶端會安裝或要求您安裝所需的軟體。在矯正電腦之後，電腦會再次嘗試存取網路。如果電腦完全遵從，則網路會授予電腦網路存取權限。 請參閱第 105 頁的「矯正電腦」。
用戶端會主動監控遵從狀況	用戶端會主動監控全部用戶端電腦的遵從狀態。一旦電腦的遵從狀態變更，電腦的網路存取權限也會變更。

您可以在安全日誌中檢視有關「主機完整性」檢查結果的詳細資訊。

請參閱第 40 頁的「檢視日誌」。

請參閱第 109 頁的「檢視 Symantec Network Access Control 日誌」。

用戶端如何與 Enforcer 搭配使用

用戶端會與 Symantec Enforcer 互動。Enforcer 可確保全部電腦連線至 Enforcer 防護的網路時，都執行用戶端軟體，並具有正確的安全性政策。

請參閱第 103 頁的「Symantec Network Access Control 的運作方式」。

Enforcer 必須先驗證使用者或用戶端電腦，之後才允許用戶端電腦存取網路。Symantec Network Access Control 可與多種類型的 Enforcer 搭配，以驗證用戶端電腦。Symantec Enforcer 是一項網路硬體裝置，可在允許電腦存取網路之前，先驗證主機完整性的結果和用戶端電腦的識別。

授予用戶端存取網路之前，Enforcer 會先檢查下列資訊：

- 電腦所執行的用戶端軟體版本。
- 用戶端具有唯一識別碼 (UID)。
- 用戶端已更新最新的主機完整性政策。
- 用戶端電腦已通過主機完整性檢查。

請參閱第 106 頁的「架構用戶端進行 802.1x 驗證」。

執行主機完整性檢查

管理員會架構用戶端執行「主機完整性」檢查的頻率。您可能需要立即執行「主機完整性」檢查，而非等候下次檢查進行。例如，未通過的「主機完整性」檢查過程中，可能發現您需要更新電腦上的病毒防護特徵。用戶端可允許您選擇立即或稍後下載所需軟體。如果您立即下載軟體，則必須再次執行「主機完整性」檢查，以確認您已使用正確的軟體。您可以等候下次排程的「主機完整性」檢查執行，也可以立即執行檢查。

執行主機完整性檢查

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在 **Network Access Control** 旁，按下**「選項」>「檢查遵從」**。
3. 按下**「確定」**。

   如果您先前已經受攔截而無法存取網路，在電腦經過更新且符合安全性政策之後，您應該已重新取得網路存取權限。

請參閱第 103 頁的「Symantec Network Access Control 的運作方式」。

矯正電腦

如果用戶端發現「主機完整性政策」要求不符合，用戶端會以下列其中一種方式回應：

- 用戶端會自動下載軟體更新。
- 用戶端會提示您下載所需的軟體更新。

矯正電腦

- 在 Symantec Endpoint Protection 對話方塊中，執行下列其中一個動作：

- 若要檢視電腦不符合的安全要求，請按「**詳細資訊**」。
- 若要立即安裝軟體，請按「**立即還原**」
  在開始安裝之後，您有可能無法選擇取消安裝。
- 若要延後進行軟體安裝，請按「**稍後提醒我**」，然後在下拉式清單中選擇時間間隔。
  管理員能夠架構您延後安裝的次數上限。

架構用戶端進行 802.1x 驗證

如果公司網路使用 LAN Enforcer 進行驗證，用戶端電腦必須經過架構才能執行 802.1x驗證。您或管理員都可以架構用戶端。您的管理員不一定會授予您架構 802.1x 驗證的權限。

802.1x 驗證程序包含下列步驟：

- 未驗證的用戶端或第三方請求者，會將使用者資訊和遵從資訊傳送至受管 802.1x 網路交換器。
- 網路交換器會將資訊轉送至 LAN Enforcer。LAN Enforcer 會將使用者資訊傳送至驗證伺服器進行驗證。RADIUS 伺服器是驗證伺服器。
- 如果用戶端未通過使用者層級驗證，或者未遵從主機完整性政策，則 Enforcer 可能會攔截網路存取。Enforcer 會將非遵從用戶端電腦放置在隔離網路中，電腦可以在這裡獲得矯正。
- 在用戶端矯正電腦，使電腦符合遵從之後，802.1x 通訊協定會重新驗證電腦，並且授予電腦存取網路的權限。

若要搭配使用 LAN Enforcer，用戶端可以使用第三方請求者或內建請求者。

表 6-2 說明可以針對 802.1x 驗證架構的選項類型。

表 6-2 802.1x 驗證選項

選項	敘述
第三方請求者	使用第三方 802.1x 請求者。 LAN Enforcer 可和 RADIUS 伺服器和第三方 802.1x 請求者一起搭配使用，以執行使用者驗證。 802.1x 請求者會提示您輸入使用者資訊， 而 LAN Enforcer 會將該使用者資訊傳遞至 RADIUS 伺服器，以進行使用者層級驗證。用戶端會將用戶端設定檔和主機完整性狀態傳送至 Enforcer，以便 Enforcer 驗證電腦。 **附註：**如果您要將 Symantec Network Access Control 用戶端和第三方請求者一起搭配使用，就必須安裝 Symantec Endpoint Protection 用戶端的「網路威脅防護」模組。

選項	敘述
透明模式	將用戶端當作 802.1x 請求者使用。 如果管理員不要使用 RADIUS 伺服器執行使用者驗證，您可以使用這個方法。LAN Enforcer 會在透明模式中執行，並成為虛擬 RADIUS 伺服器。 透明模式表示請求者不會提示您使用者資訊。在透明模式中，用戶端會作為 802.1x 請求者。用戶端會以用戶端設定檔和主機完整性狀態，回應交換器的 EAP 挑戰。然後交換器會將資訊轉送至作為虛擬 RADIUS 伺服器執行的 LAN Enforcer。LAN Enforcer 會驗證來自交換器的主機完整性和用戶端設定檔資訊，並且可以視需要允許、攔截或動態指派 VLAN。 **附註：**若要將用戶端當作 802.1x 請求者使用，您需要移除或停用用戶端電腦上的第三方 802.1x 請求者。
內建請求者	使用用戶端電腦的內建 802.1x 請求者。 內建驗證通訊協定包括智慧卡、PEAP 或 TLS。在您啟用 802.1x 驗證之後，您必須指定要使用的驗證通訊協定。

警告：架構用戶端使用 802.1x 驗證之前，請聯絡管理員。您必須瞭解公司網路是否使用 RADIUS 伺服器作為驗證伺服器。如果 802.1x 驗證的架構不正確，可能會造成網路連線中斷。

架構用戶端使用第三方請求者

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在「網路存取控制」旁，按下**「選項」>「變更設定」>「802.1x 設定」**。
3. 在**「網路存取控制設定」**對話方塊中，按下**「啟用 802.1x 驗證」**。
4. 按下**「確定」**。

   您也必須設定防火牆規則，允許第三方 802.1x 請求者驅動程式存取網路。

   請參閱第 91 頁的「新增防火牆規則」。

   您可以架構用戶端使用內建請求者。請將用戶端同時設為使用 802.1x 驗證和 802.1x 請求者。

架構用戶端使用透明模式或內建請求者

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 在「網路存取控制」旁，按下**「選項」>「變更設定」>「802.1x 設定」**。
3. 在**「網路存取控制設定」**對話方塊中，按下**「啟用 802.1x 驗證」**。
4. 按下**「將用戶端當作 802.1x 請求者使用」**。
5. 執行下列其中一項動作：

- 若要選取透明模式，請勾選**「使用 Symantec 透明模式」**。
- 若要架構內建請求者，請按下**「允許您選擇驗證通訊協定」**。
  然後您需要選擇網路連線的驗證通訊協定。

6 按下**「確定」**。

選擇驗證通訊協定

1 在用戶端電腦上，按下**「開始」>「設定」>「網路連線」**，然後按下**「區域連線」**。

附註：若為執行 Windows XP 的電腦，則會寫入這些步驟。 程序可能會有所不同。

---

2 在**「區域連線狀態」**對話方塊中，按下**「內容」**。

3 在**「區域連線內容」**對話方塊中，按下**「驗證」**標籤。

4 在**「驗證」**標籤上，按下**「EAP類型」**下拉式清單，然後選取其中一項驗證通訊協定。

請確定已勾選**此網路的「啟用 802.1x 驗證」**核取方塊。

5 按下**「確定」**。

6 按下**「關閉」**。

請參閱第 103 頁的「Symantec Network Access Control 的運作方式」。

重新驗證電腦

如果您的電腦先前已通過「主機完整性」檢查，但是Enforcer會攔截電腦，您可能需要重新驗證電腦。在一般狀況下，您應該不需要重新驗證電腦。

發生下列其中一項事件時，Enforcer 可能會攔截電腦：

- 由於您輸入的使用者名稱或密碼不正確，使得用戶端電腦使用者驗證無法通過。
- 用戶端電腦位於錯誤的 VLAN。
- 用戶端電腦沒有網路連線。網路連線中斷的原因，通常是因為用戶端電腦和LAN Enforcer 之間的交換器未驗證您的使用者名稱和密碼。
- 您已登入已驗證前一位使用者的用戶端電腦。
- 用戶端電腦未通過遵從檢查。

只有在您或管理員以內建請求者架構電腦之後，您才能夠重新驗證電腦。

附註：管理員可能尚未架構用戶端顯示**「重新驗證」**指令。

重新驗證電腦

1. 在通知區域圖示上按下滑鼠右鍵。
2. 按下**「重新驗證...」**。
3. 在**「重新驗證」**對話方塊中，輸入您的使用者名稱和密碼。
4. 按下**「確定」**。

請參閱第 103 頁的「Symantec Network Access Control 的運作方式」。

檢視 Symantec Network Access Control 日誌

Symantec Network Access Control 用戶端會使用下列日誌，監控其作業的各個細項以及「主機完整性」檢查結果：

安全性	記錄「主機完整性」檢查的結果和狀態。
系統	記錄用戶端的全部作業變更，例如連線至管理伺服器，以及更新用戶端安全性政策。

如果您使用受管用戶端，這兩份日誌都會定期上傳至伺服器。管理員會使用日誌的內容，分析網路的整體安全性狀態。

您可以匯出這些日誌的日誌資料。

檢視 Symantec Network Access Control 日誌

1. 在用戶端的側邊看板中，按下**「狀態」**。
2. 若要檢視安全日誌，請在**「網路存取控制」**旁按下**「選項」>「檢視日誌」**。
3. 在「安全日誌」中，選取最上方的日誌項目。

   左下角會顯示「主機完整性」檢查結果。如果已經安裝用戶端，就會通過預先定義的防火牆需求。如果沒有安裝用戶端，預先定義的防火牆需求則失敗，但會報告為通過。
4. 若要檢視系統日誌，請在**「安全日誌 - Symantec Network Access Control 日誌」**對話方塊中，按下**「檢視」>「系統日誌」**。
5. 按下**「檔案」>「結束」**。

   請參閱第 38 頁的「關於日誌」。

索引

十劃

十一劃

十二劃

十三劃

十四劃

十六劃

十七劃

十八劃

二十劃

二十三劃