Symantec™ Endpoint Protection 14.2 Windows 用戶端指南

Symantec

Windows 適用的 Symantec Endpoint Protection 用戶端指南

產品版本：14.2

文件版本：1

此文件上次更新的日期： 六月 21, 2018

法律聲明

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

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

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。

聯絡支援之前，請參閱：https://support.symantec.com/zh_TW/article.TECH236428.html

若要聯絡 Symantec 支援，請參閱：

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

目錄

1

Symantec Endpoint Protection 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	說明
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 26 頁的「管理電腦上的掃描」。

防護層	說明
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 59 頁的「管理電腦上的 SONAR」。
防網路和主機侵入	此防護包括防火牆、入侵預防系統和記憶體攻擊緩和。 ■ 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。 ■ 記憶體攻擊緩和會阻止對您的 Windows 電腦上常用應用程式的攻擊。 請參閱第 63 頁的「管理防火牆防護」。 請參閱第 77 頁的「架構入侵預防」。 請參閱第 78 頁的「防止攻擊易受攻擊的應用程式」。

您的管理員負責控制管理伺服器將哪些類型的防護下載到您的用戶端電腦。用戶端也會將病毒定義檔、IPS 定義檔和產品更新下載到您的電腦。如果您在旅途中攜帶可攜式電腦，則可直接從 LiveUpdate 取得病毒定義檔和產品更新。

請參閱第 15 頁的「使用 LiveUpdate 更新用戶端內容」。

如何保護我的電腦？

Symantec Endpoint Protection 用戶端的預設設定可保護您的電腦免受多種安全威脅的入侵。用戶端會自動處理威脅，或是讓您選擇如何處理威脅。

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 1-2　關於如何保護電腦的常見問題

問題	說明
如何得知我的電腦受到保護？	Symantec Endpoint Protection 用戶端會顯示您電腦的防護狀態。 安裝所有防護功能並進行更新，您的電腦便受到最嚴密的保護。 請參閱第 12 頁的「如何判定用戶端電腦是否已使用「狀態」頁面圖示進行防護」。 請參閱第 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。

問題	說明
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類型的訊息： ■ 自動防護掃描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。 請參閱第 19 頁的「回應病毒或風險偵測」。 請參閱第 19 頁的「關於掃描結果」。 請參閱第 14 頁的「暫停和延緩掃描」。 ■ 「下載鑑識」偵測。 這些訊息描述「下載鑑識」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 21 頁的「回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息」。 請參閱第 17 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 19 頁的「回應病毒或風險偵測」。 請參閱第 29 頁的「病毒和間諜軟體掃描的運作方式」。 請參閱第 47 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	說明
如何提高電腦的安全性？	根據預設，受管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設定，以改善用戶端的效能。 如果您的管理員讓您修改自己電腦的防護設定，便可執行下列工作： ■ 排程定期完整掃描，通常是一天一次或一週一次。 請參閱第 39 頁的「在用戶端上排程使用者定義的掃描」。 ■ 安裝病毒和間諜軟體掃描、自動防護、SONAR、防火牆、入侵預防、記憶體攻擊緩和及下載鑑識，並隨時保持啟用且最新的狀態。 請參閱第 84 頁的「在用戶端電腦上啟用防護」。 請參閱第 54 頁的「啟用自動防護」。 請參閱第 78 頁的「防止攻擊易受攻擊的應用程式」。 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和安全內容。 安全機制應變中心會每天發佈病毒定義檔多次，並定期或視需要發佈其他安全內容。根據預設，Symantec Endpoint Protection 用戶端排程為每四小時執行 LiveUpdate 一次。您也可以隨時啟動 LiveUpdate。 請參閱第 15 頁的「使用 LiveUpdate 更新用戶端內容」。 ■ 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 39 頁的「在用戶端上排程使用者定義的掃描」。 請參閱第 13 頁的「立即掃描用戶端電腦」。
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： ■ 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 39 頁的「在用戶端上排程使用者定義的掃描」。 ■ 排除您已知為安全的應用程式和檔案。 請參閱第 51 頁的「排除掃描項目」。 ■ 關閉掃描壓縮檔，或減少要在壓縮檔內展開已壓縮檔案的層數。 請參閱第 46 頁的「自訂病毒和間諜軟體掃描設定」。 ■ 針對使用者定義的掃描停用掃描增強功能選項。 請參閱第 39 頁的「在用戶端上排程使用者定義的掃描」。 **附註：**如果您的管理員已鎖定這些設定，您可能無法變更這些設定。

問題	說明
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存取特定瀏覽器。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？ 請參閱第 69 頁的「在用戶端上新增防火牆規則」。
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。 請參閱第 19 頁的「回應病毒或風險偵測」。 請參閱第 23 頁的「回應詢問您是允許還是攔截應用程式的訊息」。 ■ 您的電腦自動收到新的安全性政策。 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 88 頁的「檢視日誌」。

請參閱第 84 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 80 頁的「管理用戶端」。

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。

附註：在受管型用戶端上，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 1-3 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。
	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。

請參閱第 84 頁的「隱藏和顯示 Symantec Endpoint Protection 用戶端上的通知區域圖示」。

如何判定用戶端電腦是否已使用「狀態」頁面圖示進行防護

開啟 Symantec Endpoint Protection 用戶端時，「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。如果您必須採取進一步的動作，則與圖示一起顯示的文字會提供更多資訊。

表 1-4 「狀態」頁面的警示圖示

圖示	敘述
	顯示每種防護均啟用。
	警告您用戶端電腦上的病毒定義檔或安全性內容已過期。若要接收最新的病毒定義檔或安全性內容，您可以在管理員允許的情況下立即執行 LiveUpdate。 此狀態可能也指示 Symantec Endpoint Protection 需要重新啟動。 具有作用中主機完整性政策的 Symantec Endpoint Protection 用戶端電腦也可能具有下列問題： ■ 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。 ■ 用戶端電腦無法下載主機完整性內容。 請參閱第 15 頁的「使用 LiveUpdate 更新用戶端內容」。

圖示	敘述
	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 84 頁的「在用戶端電腦上啟用防護」。

立即掃描用戶端電腦

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。

可以選取從單一檔案、USB 磁碟機，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。

您可以透過下列其中一種方式立即掃描電腦：

- 從「掃描威脅」頁面立即掃描 Windows 電腦
- 從「狀態」頁面立即掃描 Windows 電腦
- 從 Windows 立即掃描電腦

從「掃描威脅」頁面立即掃描 Windows 電腦

◆ 在用戶端的側邊看板中，按下**「掃描威脅」**。

- 按下**「執行作用中掃描」**以掃描最常感染的區域。
- 按下**「執行完整掃描」**以掃描整個電腦。
- 按下**「執行主機完整性掃描」**以檢查是否遵從安全性政策。

  附註：「執行主機完整性掃描」僅在用戶端已啟用主機完整性政策的情況下顯示。

- 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」**。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

您也可以暫停或取消掃描。

從「狀態」頁面立即掃描 Windows 電腦

◆ 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」**。

從 Windows 立即掃描電腦

- 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。

請參閱第 19 頁的「關於掃描結果」。

請參閱第 14 頁的「暫停和延緩掃描」。

請參閱第 42 頁的「排程執行隨選或開機掃描」。

請參閱第 15 頁的「使用 LiveUpdate 更新用戶端內容」。

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 26 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 LiveUpdate 更新用戶端內容

賽門鐵克產品需要擁有最新的資訊，才能保護您的電腦免受新發現威脅的侵害。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。

從 14 開始，用戶端也可以存取雲端中的完整內容集。在連線至雲端的標準或內嵌式/VDI 用戶端上執行的掃描可取得雲端中的完整定義檔集。

請參閱第 38 頁的「Windows 用戶端如何從雲端接收定義檔」。

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。 只要經過架構，這些更新可以透過管理伺服器提供給受管用戶端。

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。 受管用戶端電腦通常都是從其管理伺服器接收內容更新。受管或非受管用戶端電腦均可以直接從 LiveUpdate 伺服器接收此內容。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 1-5　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。您也可以修改排程，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。 在受管用戶端上，您只能將 LiveUpdate 架構為依排程執行，或是修改已由管理員啟用的現有排程。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或修改現有排程。在非受管用戶端上，您可以停用或變更 LiveUpdate 排程。 請參閱第 16 頁的「使用 LiveUpdate 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。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。 **附註：**僅當管理員將設定架構為允許受管用戶端手動執行 LiveUpdate 時，受管用戶端才能這麼做。 請參閱第 16 頁的「使用 LiveUpdate 立即更新內容」。

使用 LiveUpdate 依排程更新內容

1 在用戶端的側邊列中，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**「頻率和時間」**群組方塊中，視需要修改更新的頻率。

6 選擇性地啟用和架構隨機化選項和閒置偵測設定。

這些選項可改善 LiveUpdate 更新用戶端所需的時間量。

7 按下**「確定」**。

使用 LiveUpdate 立即更新內容

◆ 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。

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	說明
掃描結果對話方塊	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。 如果掃描仍在進行中，對話方塊可能會顯示一個名稱，例如，**「*已於日期時間*開始的*掃描名稱*」**。如果掃描完成，對話方塊可能會顯示**「Symantec Endpoint Protection 偵測結果」**之類的名稱。 請參閱第 19 頁的「關於掃描結果」。
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 24 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 23 頁的「回應詢問您是允許還是攔截應用程式的訊息」。 ■ 用戶端的試用授權已過期。 請參閱第 23 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：
	
	`Traffic has been blocked from this application:`
	`Application name`
	
	如果用戶端架構為攔截全部流量，則這些通知會頻繁出現，並且通常不要求您執行任何動作。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 23 頁的「回應詢問您是允許還是攔截應用程式的訊息」。
	■ 用戶端終止應用程式：
	`Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection will terminate <application name> application`
	請參閱第 78 頁的「防止攻擊易受攻擊的應用程式」。
	■ 用戶端偵測到危害電腦的網路攻擊：
	
	`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.`
	
	除了讀取訊息外，您不需要執行其他動作。
	■ 安全性遵從檢查失敗。系統可能會攔截出入電腦的流量:
	安全性遵從掃描失敗。
	請參閱第 61 頁的「矯正電腦以通過主機完整性檢查」。

請參閱第 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。

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，當您開啟電腦時，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 82 頁的「關於受管用戶端和非受管用戶端」。

請參閱第 19 頁的「回應病毒或風險偵測」。

請參閱第 14 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。

您可能需要對風險採取動作，但可以選擇稍後再執行動作。您可以稍後透過下列方式使用「隔離所」、「風險日誌」或「掃描日誌」對檔案執行動作：

- 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先前針對掃描偵測出的特定風險類型所架構的動作。

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，並嘗試移除或修復感染所造成的任何副作用。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感染所造成的副作用。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。
  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。
- **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」**。

請參閱第 36 頁的「掃描如何回應偵測到的病毒或風險」。

請參閱第 88 頁的「檢視日誌」。

請參閱第 26 頁的「管理電腦上的掃描」。

請參閱第 53 頁的「管理電腦上的隔離檔案」。

回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息

「下載鑑識」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「下載鑑識」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。

「下載鑑識」使用賽門鐵克的智慧型掃描技術，該技術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。

「下載鑑識」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「下載鑑識」偵測

◆ 在「下載鑑識」偵測訊息中，執行下列動作之一：

- 按下**「從電腦中移除此檔案」**。
  「下載鑑識」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 *Drive*:\Users*username*\AppData\Local\Microsoft\Windows\Temporary Internet Files、*Drive*:\Users*username*\AppData\Local\Microsoft\Windows\INetCache 或 *Drive*:\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。 若為受管型用戶端，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 43 頁的「管理電腦上的下載鑑識偵測」。

請參閱第 37 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。

請參閱第 26 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 55 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 19 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」**。

   在非受管電腦和部分受管電腦上，您也可以透過「狀態」頁面變更對應用程式採取的動作。在「防網路和主機侵入」旁，按下**「選項」**，然後按下**「檢視網路活動」**，或按下**「檢視應用程式設定」**。

請參閱第 75 頁的「允許或攔截已在用戶端上執行的應用程式」。

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。用戶端可使用試用授權或已付費授權。如果試用授權已到期，用戶端就不會再更新任何內容。

表 2-2 授權類型

授權類型	說明

試用授權	如果試用授權過期，用戶端的「狀態」窗格最上方會變成紅色，並顯示下列訊息：
	
	`Trial License has expired.`
	`Click Details for more information.`
	
	當您按下**「詳細資料」**時，會出現訊息，指出內容下載於特定日期中止，並要求聯絡您的管理員以購買付費授權。「狀態」窗格也可能會顯示一些指出內容已過期的文字。
	
	您也可以透過用戶端介面檢視授權到期日。按下**「說明」>「關於」**。

已付費授權	如果已付費授權過期，您應該不會在用戶端的「狀態」窗格中看到任何與過期狀態相關的訊息。已付費授權到期日不會顯示在**「說明」>「關於」**下。 內容會持續更新，例如病毒和間諜軟體定義檔。

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 17 頁的「警示和通知的類型」。

請參閱第 88 頁的「檢視日誌」。

回應訊息以更新用戶端軟體

如果有用戶端軟體更新可供下載，您可能會看到下列通知：

```
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?
```

用戶端軟體更新也可能會在背景中以無訊息方式安裝。安裝完成時，可能會出現訊息，通知您必須重新啟動電腦。

回應更新通知

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. 如果出現訊息通知您升級已完成，請按照螢幕上的指示重新啟動。當您重新啟動電腦後，安裝即完成。

3

管理掃描

本章包含以下主題：

- 變更 SONAR 設定
- 透過主機完整性掃描檢查電腦安全性遵從
- 啟用竄改防護

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。

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 38 頁的「Windows 用戶端如何從雲端接收定義檔」。

表 3-1 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 29 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 15 頁的「使用 LiveUpdate 更新用戶端內容」。
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「下載鑑識」並會阻止 SONAR 進行啟發式偵測。 請參閱第 54 頁的「啟用自動防護」。

工作	敘述
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 13 頁的「立即掃描用戶端電腦」。 請參閱第 39 頁的「在用戶端上排程使用者定義的掃描」。 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 19 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 14 頁的「暫停和延緩掃描」。 在受管用戶端上，管理員可能會從管理主控台起始 Power Eraser 掃描。Power Eraser 是一種強大的掃描，可以偵測嚴重的威脅，並且有時需要重新啟動才能完成。管理員可手動處理用於偵測的矯正。 您無法直接從用戶端執行 Power Eraser，但是，Power Eraser 可做為 SymDiag 支援工具的一部分使用。如果直接在用戶端上下載 SymHelp 工具並執行 Power Eraser 掃描，則不會將日誌傳送到管理主控台。管理員從管理主控台執行 Power Eraser 時，您應該確認沒有使用 SymHelp 工具在本機執行 Power Eraser；否則，可能會對電腦效能產生不良影響。
調整掃描以提高電腦效能	依預設，Symantec Endpoint Protection 會在對電腦效能影響最小的情況下，提供較高層級的安全性。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 46 頁的「自訂病毒和間諜軟體掃描設定」。 請參閱第 39 頁的「在用戶端上排程使用者定義的掃描」。

工作	敘述
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」**。 ■ 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 46 頁的「自訂病毒和間諜軟體掃描設定」。
調整掃描以減少誤報	將安全檔案或程序排除在掃描的範圍以外。 請參閱第 51 頁的「排除掃描項目」。
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 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。
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。如果已隔離檔案無法修復，則用戶端最終會將其移除。您也可以對此檔案採取其他動作。 請參閱第 53 頁的「管理電腦上的隔離檔案」。

表 3-2 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 3-2 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 46 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。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 55 頁的「啟用或停用提早啟動防惡意軟體 (ELAM)」。
管理「下載鑑識」偵測	「下載鑑識」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。「下載鑑識」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。「下載鑑識」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 43 頁的「管理電腦上的下載鑑識偵測」。
管理 SONAR	您可以調整 SONAR 的設定。 請參閱第 59 頁的「管理電腦上的 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：

- 掃描引擎會在電腦上的檔案和其他元件中，搜尋病毒、特洛伊木馬程式、病蟲和其他威脅 (例如安全風險)。每種威脅都有可辨識的型樣，就是所謂的特徵。用戶端會使用包含大量已知特徵資訊的定義檔。掃描引擎會將每個檔案或元件與定義檔進行比較。如果掃描引擎發現符合的特徵，表示該檔案已受到感染或帶有惡意。
- 掃描引擎使用定義檔來判斷威脅所屬的種類。掃描引擎會對威脅採取矯正動作。掃描引擎會清除、刪除或隔離被偵測為威脅的項目。掃描引擎也會修復威脅所造成的任何副作用。它所採取的動作，取決於偵測到的威脅類型。
  請參閱第 36 頁的「掃描如何回應偵測到的病毒或風險」。

- 從 14 開始，在連線至雲端的標準或內嵌式/VDI 用戶端上，掃描可存取雲端中的完整定義檔集。
  請參閱第 38 頁的「Windows 用戶端如何從雲端接收定義檔」。

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 3-3敘述了用戶端會在電腦掃描的元件。

表 3-3 用戶端掃描的電腦元件

元件	敘述
選取的檔案	用戶端會根據您選取的掃描類型或管理員排程的掃描類型，來掃描個別檔案。您也可以在 Windows 中掃描個別檔案或資料夾。針對大部分的掃描類型，您可以選取要掃描的檔案。
電腦記憶體	用戶端會掃描電腦的記憶體。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，病毒會散佈到硬碟機中。掃描無法清除存在於記憶體中的病毒。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。
卸除式媒體	利用卸除式媒體 (例如 USB 磁碟機) 傳播，是某些威脅的常見傳播方式。用戶端不會在您插入卸除式媒體時自動掃描該媒體，但您可以在 Windows 中透過對媒體按下滑鼠右鍵來對其進行掃描。

請參閱第 13 頁的「立即掃描用戶端電腦」。

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。

圖 3-1 病毒和安全風險攻擊電腦的方式

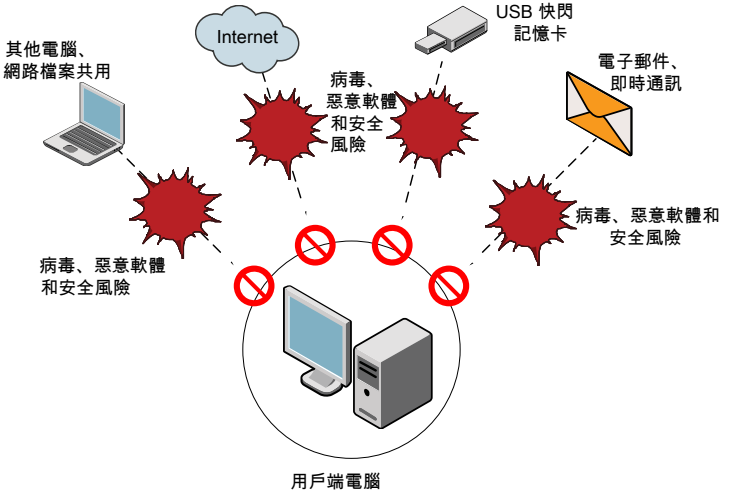

表 3-4 列出可能攻擊電腦的病毒和風險類型。

表 3-4 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	提供廣告內容的程式。
Cookie	Web 伺服器傳送到網頁瀏覽器來用於識別電腦或使用者的訊息

風險	說明
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。
勒索軟體	一種惡意軟體類別，會破壞文件並使其無法使用，但電腦使用者仍可存取電腦。
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。

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 36 頁的「掃描如何回應偵測到的病毒或風險」。

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。

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 38 頁的「Windows 用戶端如何從雲端接收定義檔」。

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 3-5 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。 自 14 版起，在連線至雲端的標準和內嵌式/VDI 用戶端上，自動防護也會使用雲端定義檔。 請參閱第 34 頁的「關於自動防護的類型」。
下載鑑識	「下載鑑識」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。 「下載鑑識」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。「下載鑑識」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。 「下載鑑識」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「下載鑑識」，則「下載鑑識」無法運作。 請參閱第 37 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。在非受管用戶端或掃描設定已解除鎖定的受管用戶端上，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。 從 14 版開始，在連線至雲端的標準和內嵌式/VDI 用戶端上，這些掃描會使用雲端定義檔。 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。 如果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 29 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 58 頁的「關於 SONAR」。

請參閱第 26 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。

「自動防護」只適用於支援的電子郵件用戶端，它不會保護郵件伺服器。

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 3-6 自動防護的類型

自動防護的類型	敘述
檔案系統自動防護	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。 自動防護會掃描所有檔案，甚至包括電子郵件附件。如果您未針對電子郵件啟用自動防護，用戶端電腦仍會在啟用檔案系統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.
Microsoft Outlook 自動防護	下載內送的 Microsoft Outlook 電子郵件附件，並在您讀取郵件並開啟附件時掃描是否有病毒和安全風險。 Microsoft Outlook 自動防護支援 Microsoft Outlook 98 到 Outlook 2016 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。 安裝期間，如果您的管理員將 Microsoft Outlook 自動防護包含在套件中，而且電腦上已安裝 Microsoft Outlook，Symantec Endpoint Protection 會安裝 Microsoft Outlook 自動防護。 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。

自動防護的類型	敘述
Lotus Notes 自動防護	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。 安裝期間，如果您的管理員將 Lotus Notes 自動防護包含在套件中，而且電腦上已安裝 Lotus Notes，Symantec Endpoint Protection 會安裝 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 3-7　　用戶端如何回應病毒和安全風險

威脅類型	動作
病毒	根據預設，當用戶端偵測到病毒時會採取下列動作： ■ 用戶端會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 53 頁的「管理電腦上的隔離檔案」。 **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。
安全風險	根據預設，當用戶端偵測到安全風險時會採取下列動作： ■ 用戶端會隔離受感染的檔案。 ■ 用戶端會嘗試移除或修復安全風險所造成的任何變更。 ■ 如果用戶端無法隔離安全風險，就會記錄該風險，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，不小心安裝了包含安全風險的應用程式，如廣告軟體和間諜軟體。當偵測到此類安全風險時，用戶端會採取下列動作： ■ 如果隔離風險的動作不會對電腦造成傷害或讓電腦處於不穩定的狀態，用戶端會立即這麼做。 ■ 否則，用戶端會先等候應用程式安裝完成，然後才隔離風險，接著再修復風險所造成的影響。 **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 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。

您可以變更智慧型掃描查詢設定。移至**「變更設定」>「用戶端管理」>「傳送」**。

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。

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 43 頁的「管理電腦上的下載鑑識偵測」。

請參閱第 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。

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。

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。

您的用戶端類型必須支援啟用雲端的內容。

您可以在**「說明」>「疑難排解」>「安裝設定」**中查看用戶端類型。

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。

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，智慧型威脅雲端服務還可減少 15% 的掃描時間。

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。

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靈敏度等級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靈敏度等級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。

雲端查詢動作範例

智慧型威脅雲端服務保護用戶端的方式範例：

- 使用 Internet Explorer 以嘗試下載檔案。下載鑑識使用雲端中的 Symantec Insight 提供之靈敏度等級和信譽資訊，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。
- 如果您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靈敏度等級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 43 頁的「管理電腦上的下載鑑識偵測」。
- 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。

- 傳送
  賽門鐵克建議您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。賽門鐵克會盡量嘗試讓資料匿名，以防止傳輸個人識別資訊。
  請參閱第 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。

在用戶端上排程使用者定義的掃描

Symantec Endpoint Protection 用戶端上的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 13 頁的「立即掃描用戶端電腦」。

請參閱第 26 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。

您也可以建立隨選掃描或開機掃描。

請參閱第 42 頁的「排程執行隨選或開機掃描」。

排程使用者定義掃描

1 在用戶端的側邊列中，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。

掃描增強功能 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**」。

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 13 頁的「立即掃描用戶端電腦」。

排程執行隨選或開機掃描

1 在用戶端的側邊列中，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 39 頁的「在用戶端上排程使用者定義的掃描」。

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，輸入掃描的名稱和說明。

例如，將掃描作業稱為：MyScan1

7 按下「**完成**」。

管理電腦上的下載鑑識偵測

「自動防護」包含「下載鑑識」，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」，「下載鑑識」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，您可以使用 Internet Explorer 嘗試下載「下載鑑識」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 3-8 管理電腦上的下載鑑識偵測

工作	敘述
了解「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」會根據與檔案信譽有關的證據，判斷下載的檔案是否存在風險。「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 37 頁的「Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策」。
確定已啟用智慧型掃描查詢	「下載鑑識」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「下載鑑識」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 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。
回應下載鑑識偵測	當「下載鑑識」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「下載鑑識」偵測通知。 啟用通知後，系統將在「下載鑑識」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 21 頁的「回應詢問您要允許或攔截嘗試下載的檔案的下載鑑識訊息」。

工作	敘述
為特定檔案或 Web 網域建立例外	您可以為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。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 用戶端將允許使用者從信任的網站下載的任何檔案。 「下載鑑識」只會辨識您或管理員明確架構的受信任網站。 請參閱第 51 頁的「排除掃描項目」。
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。 靈敏度等級愈低，「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。 靈敏度等級愈高，「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。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「下載鑑識」偵測的警示。 如果「下載鑑識」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「下載鑑識」偵測到其視為未證明的檔案，它會在用戶端電腦上顯示訊息。只有在您將未證明檔案的動作設定為**「提示」**或**「隔離」**的情況下，此訊息才會出現。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「下載鑑識」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」**，以一律允許這些偵測，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 45 頁的「自訂下載智慧型掃描設定」。
控制要將哪些信譽偵測相關資訊傳送給賽門鐵克	根據預設，所有受管用戶端都會將有關信譽偵測的資訊傳送給賽門鐵克。 賽門鐵克建議您持續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 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。

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。

附註：必須先啟用「自動防護」，「下載智慧型掃描」才能運作。如果停用「自動防護」，則即使「下載智慧型掃描」已啟用，「下載智慧型掃描」也無法運作。

請參閱第 43 頁的「管理電腦上的下載鑑識偵測」。

自訂下載智慧型掃描設定

1. 在用戶端的側邊列中，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：如果僅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，並且無法變更設定。

   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：
   - **使用者數量不超過: *x* 個的檔案**，其中 *x* 預設為 5。您可以從下拉式清單中選取其他值。
   - **使用者已知不超過: *x* 天的檔案**，其中 *x* 預設為 2。您可以輸入任何值
     如果未證明的檔案符合此條件，下載鑑識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」**。
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。

您可以自訂使用者定義的掃描、全域掃描設定，以及自動防護。

- 執行使用者定義的掃描
- 變更全域掃描設定
- 自訂自動防護

請參閱第 26 頁的「管理電腦上的掃描」。

執行使用者定義的掃描

1 在用戶端的側邊列中，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：

- 若要指定減少掃描的檔案類型，請按下「**選取的副檔名**」，然後按下「**副檔名**」。

  附註：使用者定義的掃描一律會掃描配置區檔案，除非您在「**進階掃描選項**」下方為排程掃描停用壓縮檔案選項，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 55 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**」。
  您可以變更調整選項，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. 在用戶端的側邊看板中，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」**。
2. 在**「全域設定」**標籤上，在**「掃描選項」**下變更智慧型掃描或 Bloodhound 啟發式病毒偵測的設定。
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. 在用戶端的側邊列中，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 46 頁的「自訂病毒和間諜軟體掃描設定」。

請參閱第 45 頁的「自訂下載智慧型掃描設定」。

請參閱第 60 頁的「變更 SONAR 設定」。

如需各對話方塊上選項的詳細資訊，請按下**「說明」**。

架構在偵測到惡意軟體與安全風險時採取的動作

1. 在用戶端的側邊看板中，按下**「變更設定」**。
2. 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」**。
3. 按下**「動作」**。
4. 在**「掃描動作」**對話方塊中，選取**「惡意軟體」**或**「安全風險」**類別。

   您還可以選取子類別。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. 針對類別或子類別，選取下列選項中的第一個和第二個動作：

清除風險	移除受感染檔案中的病毒。此設定是對**「惡意軟體」**類別執行的第一個預設動作。 **附註：**此設定僅適用於作為**「惡意軟體」**類別的第一個動作。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。您的電腦將免於偵測到病毒的困擾，而且病毒不再容易散播到電腦的其他區域。 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。

- 若是惡意軟體，此動作會將受感染的檔案從其原始位置移到「隔離所」。此設定是對惡意軟體執行的第二個預設動作。
- 若是安全風險，此動作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」**對話方塊會顯示已採取之動作的相關資訊。此項資訊也會顯示在事件日誌中。

此設定是對安全風險執行的第二個預設動作。

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)

維持檔案不變，並在風險記錄中置入項目，以記錄該風險。使用此選項來手動控制用戶端處理惡意軟體或安全風險的方法。

附註：惡意軟體可能會擴散到電腦的其他部分或網路上的其他電腦，直到您採取進一步的動作。

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」。

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

例外是您要從掃描中排除的檔案和其他項目。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。

表 3-9　　例外類型

例外類型	說明
檔案	適用於排程掃描和手動掃描、自動防護、SONAR 和應用程式控制。 掃描會忽略您選取的檔案。
資料夾	適用於排程掃描和手動掃描、自動防護、SONAR 和應用程式控制。 掃描會忽略您選取的資料夾。
已知風險	適用於排程掃描和手動掃描、自動防護以及 SONAR。 掃描會忽略您選取的所有已知風險。
副檔名	適用於排程掃描和手動掃描以及自動防護。 掃描會忽略帶有指定副檔名的全部檔案。
Web 網域	適用於下載鑑識。 「下載智慧型掃描」會忽略指定的信任 Web 網域。
應用程式	適用於排程掃描和手動掃描、自動防護、SONAR 以及下載鑑識。 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。

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。

請參閱第 51 頁的「排除掃描項目」。

排除掃描項目

您可以將已知為安全的應用程式和檔案項目排除在掃描範圍之外。您也可以排除某些項目以改善電腦的效能。

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。

您可以將項目排除在安全風險掃描之外、將資料夾排除在SONAR掃描之外，以及將應用程式排除在所有掃描之外。

- 從安全風險掃描中排除項目
- 將資料夾從 SONAR 中排除
- 排除會變更 DNS 或主機檔案的應用程式
- 變更所有掃描處理應用程式的方式

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. 在用戶端的側邊列中，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」**。
     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。

- 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，輸入您要從下載鑑識和 SONAR 偵測中排除的網域名稱或 IP 位址。您可以指定 URL，但是例外狀況僅使用 URL 的網域名稱部分。如果指定了 URL，則您可以使用 HTTP 或 HTTPS (不區分大小寫) 預先擱置 URL，但是例外狀況適用於兩者，即 HTTP 和 HTTPS。此例外允許您從網域中的任何位置下載檔案。
  針對「下載鑑識」，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**「網際網路選項」>「安全性」>「自動偵測內部網路」**選項所搜尋到的網站，

6 按下**「確定」**。

將資料夾從 SONAR 中排除

1 在用戶端的側邊列中，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」**。

排除會變更 DNS 或主機檔案的應用程式

1 在用戶端的側邊列中，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**「DNS 或主機檔案變更例外」>「應用程式」**
4 選取您要排除的應用程式，然後按下**「確定」**。

變更所有掃描處理應用程式的方式

1 在用戶端的側邊列中，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 26 頁的「管理電腦上的掃描」。

請參閱第 50 頁的「關於排除掃描項目」。

管理電腦上的隔離檔案

關於隔離的檔案

依據預設，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。當用戶端將受感染的檔案移到隔離所時，它會加密該檔案。由於檔案已加密，因此您無法存取隔離的檔案。隔離所中的檔案無法感染電腦或網路中其他電腦上的檔案。但是，隔離動作不會清除風險。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。

以新的病毒定義檔更新電腦之後，用戶端會自動重新掃描隔離所。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。開機病毒存在於電腦的開機磁區或分割表中，因此這些項目無法移至隔離所。有時候，用戶端會偵測到不明病毒，無法以目前的病毒定義檔集加以排除。
- 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。
- 下載鑑識和 SONAR 也可以隔離檔案。

請參閱第 36 頁的「掃描如何回應偵測到的病毒或風險」。

管理隔離所中的檔案

由於隔離所會處理您電腦上受感染的檔案，您可以將這些檔案保留在隔離所中。但是，有一些動作您可能需要對隔離所中的檔案執行。例如，如果檔案錯誤遭到隔離，可以從隔離所還原該檔案。或者，如果您需要節省電腦空間，可以減少隔離所自動刪除其內容前的時間。

管理隔離所中的檔案

1 在用戶端的側邊列中，按下「**檢視隔離所**」。

2 在「**檢視隔離所**」視窗中，選取隔離項目清單中的檔案。

3 按下以下其中一個選項，並按照畫面上的指示操作。

請參閱第 26 頁的「管理電腦上的掃描」。

啟用自動防護

對於檔案和程序、Internet 電子郵件和電子郵件群組軟體應用程式，您應該使自動防護保持啟用狀態。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。

針對檔案系統啟用自動防護

- 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」**。

針對電子郵件啟用自動防護

1. 在用戶端的側邊列中，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」**標籤上，勾選**「啟用 Internet 電子郵件自動防護」**。
   - 在**「Outlook 自動防護」**標籤上，勾選**「啟用 Microsoft Outlook 自動防護」**。
   - 在**「Notes 自動防護」**標籤上，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 34 頁的「關於自動防護的類型」。

請參閱第 12 頁的「如何判定用戶端電腦是否已使用「狀態」頁面圖示進行防護」。

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用戶端啟動前攻擊系統。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 和更新版本以及 Windows Server 2012 和更新版本支援這些設定。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。

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 是賽門鐵克說明工具的一部分。您可以透過 Symantec Endpoint Protection 用戶端的**「說明」**按鈕取得賽門鐵克說明工具。

啟用或停用提早啟動防惡意軟體

1. 在用戶端的側邊列中，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，核取或取消核取**「啟用賽門鐵克提早啟動防惡意軟體」**。
4. 如果您要僅記錄偵測，請在**「偵測到潛在的惡意驅動程式」**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 26 頁的「管理電腦上的掃描」。

請參閱第 86 頁的「使用 Symantec Diagnostic Tool (SymDiag) 對電腦問題進行疑難排解」。

請參閱第 51 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 22 頁的「回應出現在 Windows 8 電腦上的 Symantec Endpoint Protection 彈出式通知」。

瞭解向賽門鐵克傳送資訊可改善電腦防護功能

依據預設，用戶端會定期向賽門鐵克傳送匿名偵測、網路及組態資訊。賽門鐵克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可提升賽門鐵克回應威脅的能力。賽門鐵克建議您傳送盡可能多的資訊。

賽門鐵克會竭盡所能匿名化用戶端傳送的任何資訊。

用戶端向賽門鐵克傳送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。您可以僅停用網路資訊傳送，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。

修改向賽門鐵克傳送資訊

1. 選取「**變更設定**」>「**用戶端管理**」。
2. 在「**傳送**」標籤上，勾選「**將匿名資料傳送給賽門鐵克，以獲得增強的威脅防護情報**」。
   此選項可讓 Symantec Endpoint Protection 傳送在您電腦中發現的威脅之相關資訊，以及網路和組態的相關資訊。

   賽門鐵克建議您保持此選項為啟用狀態。
3. 如果想選擇要傳送的資訊類型，請選取「**更多選項**」。
4. 按下「**確定**」。

您也可以將檔案從隔離所手動傳送至賽門鐵克。

請參閱第 53 頁的「管理電腦上的隔離檔案」。

如需隱私權的詳細資訊，請參閱下列文件：

隱私權聲明

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 3-10 顯示 WSC 中的防護狀態報告。

表 3-10 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	開啟 (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 3-11 顯示 WSC 中報告的 Symantec Endpoint Protection 防火牆狀態。

表 3-11 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	開啟 (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、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。

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 59 頁的「管理電腦上的 SONAR」。

請參閱第 51 頁的「排除掃描項目」。

管理電腦上的 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 3-12 管理電腦上的 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 84 頁的「在用戶端電腦上啟用防護」。
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 45 頁的「自訂下載智慧型掃描設定」。
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 60 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 51 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 51 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 56 頁的「瞭解向賽門鐵克傳送資訊可改善電腦防護功能」。

請參閱第 26 頁的「管理電腦上的掃描」。

請參閱第 32 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。

附註：在受管型用戶端上，管理員可能會鎖定這些設定。

變更 SONAR 設定

1. 在用戶端的側邊列中，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。

   您也可以變更通知設定，以及 SONAR 是否在遠端電腦 (網路磁碟機) 上進行偵測。
4. 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。

   您僅可以在 SONAR 停用時，啟用或停用**「可疑行為偵測」**。
5. 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。
6. 按下**「確定」**。

請參閱第 59 頁的「管理電腦上的 SONAR」。

透過主機完整性掃描檢查電腦安全性遵從

主機完整性掃描可確認在電腦連線至網路之前該電腦是否符合某些安全性需求。例如，主機完整性檢查可以確認作業系統是否有最新的安全修正程式。如果您的電腦不符合安全性需求，則用戶端會矯正您的電腦，以確保其可以通過主機完整性檢查。若要矯正，檢查會自動下載並安裝必要的軟體。您的管理員可能會傳送讓您矯正電腦的訊息。

主機完整性檢查將在您啟動電腦時執行，並且會在網路連線結束之前一直執行。您也可以手動執行主機完整性檢查。

即使特定需求未能通過，您的管理員也可以將主機完整性檢查架構為通過。您可以在用戶端安全日誌中檢視主機完整性檢查的結果。

透過主機完整性掃描檢查電腦安全性遵從

1 在用戶端的側邊看板中，按下**「掃描威脅」**。

2 在**「掃描威脅」**對話方塊中，按下**「執行主機完整性掃描」**。

3 按下**「確定」**。

如果遵從失敗阻止了您對網路的存取，則應該在更新電腦以符合遵從需求時重新獲得存取權。

掃描結果將會出現在安全日誌中。

請參閱第 61 頁的「矯正電腦以通過主機完整性檢查」。

請參閱第 88 頁的「檢視日誌」。

矯正電腦以通過主機完整性檢查

如果用戶端未能符合主機完整性政策需求，則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性需求，請按下**「詳細資料」**。
- 若要立即安裝軟體，請按下**「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。

請參閱第 60 頁的「透過主機完整性掃描檢查電腦安全性遵從」。

啟用竄改防護

「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。

啟用竄改防護

1 在用戶端的側邊列中，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，確保已勾選**「防護賽門鐵克安全軟體不受竄改或關閉」**。

4 在**「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」**。

5 按下**「確定」**。

4

管理防火牆、入侵預防和應用程式強化

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 4-1 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 4-1 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 64 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 65 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 75 頁的「允許或攔截已在用戶端上執行的應用程式」。
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 71 頁的「啟用防火牆設定」。
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 87 頁的「關於日誌」。 請參閱第 88 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 75 頁的「當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量」。 ■ 您可以自動地允許或攔截網路存取，也可以由電腦上所執行的應用程式來要求您這麼做。您也可以架構 請參閱第 74 頁的「允許或攔截應用程式存取網路」。 請參閱第 75 頁的「允許或攔截已在用戶端上執行的應用程式」。
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 84 頁的「在用戶端電腦上啟用防護」。

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 63 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 4-2 說明管理防火牆規則所需瞭解的相關內容。

表 4-2 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： ■ 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 67 頁的「關於防火牆規則、防火牆設定和入侵預防處理順序」。 ■ 用戶端使用狀態式檢測，可保持追蹤網路連線的狀態 請參閱第 68 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 66 頁的「用戶端上防火牆規則的元素」。
新增防火牆規則	您可以執行下列工作來管理防火牆規則： ■ 將您自己的規則新增至 Symantec Endpoint Protection 預設安裝的規則 請參閱第 69 頁的「在用戶端上新增防火牆規則」。 ■ 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 70 頁的「在用戶端上匯出或匯入防火牆規則」。 ■ 複製並貼上防火牆規則

用戶端上防火牆規則的元素

當一台電腦嘗試連線到另一台電腦時，Symantec Endpoint Protection 防火牆會將連線類型與防火牆規則進行比較。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。

一旦封包觸發防火牆規則，防火牆便不會再進一步評估防火牆規則。如果封包未觸發任何規則，防火牆會自動攔劫封包，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 4-3 說明用於定義防火牆規則的準則。

表 4-3 防火牆規則準則

條件	敘述
觸發條件	■ 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，說明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準則，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，規則指定的流量便可存取網路。 如果防火牆攔截流量，規則指定的流量則無法存取網路。

請參閱第 68 頁的「防火牆如何使用狀態式檢測」。

請參閱第 69 頁的「在用戶端上新增防火牆規則」。

請參閱第 65 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 4-4 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 4-4　　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 64 頁的「防火牆的運作方式」。

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。

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 64 頁的「防火牆的運作方式」。

請參閱第 65 頁的「管理防火牆規則」。

在用戶端上新增防火牆規則

在 Symantec Endpoint Protection 用戶端上新增或變更防火牆規則時，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。

附註：您可以在非受管用戶端 (若管理員授予對受管用戶端的用戶端控制權) 上新增或變更防火牆規則。

新增防火牆規則

1. 在用戶端的側邊列中，按下**「狀態」**。
2. 在**「防網路和主機侵入」**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」**以開啟空白規則。

   附註：對於受管用戶端，此動作會啟動規則建立精靈。以下步驟說明了架構空白規則。

4. 在空白規則的**「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，請按下各個標籤並視需要進行架構。
   - **一般**
   - **主機**
   - **通訊埠和通訊協定**

- **應用程式**
- **排程**

例如，您可能要選取此規則套用到的網路配接器、此規則套用到的主機、規則處於作用中或非作用中狀態的時段，或記錄封包流量。

附註：寫入封包日誌時請務必小心，因為可能會記錄大量資料。

請參閱第 66 頁的「用戶端上防火牆規則的元素」。

6 按下「**確定**」。

規則會自動啟用。您必須啟用規則，以便防火牆處理這些規則。

7 若要變更規則順序，請按下向上或向下箭頭。

8 按下「**確定**」。

在用戶端上匯出或匯入防火牆規則

您可以和另一個 Symantec Endpoint Protection 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。

在用戶端上匯出防火牆規則

1 在用戶端的側邊列中，按下「**狀態**」。

2 在「**防網路和主機侵入**」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**」。

在用戶端上匯入防火牆規則

1 在用戶端的側邊列中，按下「**狀態**」。

2 在「**防網路和主機侵入**」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下滑鼠右鍵，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 格式檔案。

5 按下「**開啟**」。

6 按下「**確定**」。

請參閱第 69 頁的「在用戶端上新增防火牆規則」。

啟用防火牆設定

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 4-5 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 4-5　　防火牆設定

類別	說明
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。 請參閱第 72 頁的「在已安裝 Symantec Endpoint Protection 用戶端的情況下啟用網路檔案和印表機共用」。
攻擊偵測和攔截	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。
入埠流量控制	您可以架構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。 ■ 當防火牆停止執行時。 ■ 當您在任何時候想要攔截所有入埠及離埠流量時。 請參閱第 75 頁的「當螢幕保護程式處於作用中狀態或防火牆未執行時攔截流量」。

啟用防火牆設定

1 在用戶端中，按下**「變更設定」**。

2 在**「防網路和主機侵入」**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 65 頁的「管理防火牆規則」。

請參閱第 69 頁的「在用戶端上新增防火牆規則」。

在已安裝 Symantec Endpoint Protection 用戶端的情況下啟用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 4-6 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。 請參閱第 72 頁的「自動啟用網路檔案和印表機共用與瀏覽」。
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。 請參閱第 73 頁的「手動啟用網路檔案和印表機共用與瀏覽」。 請參閱第 73 頁的「手動允許其他電腦瀏覽用戶端電腦上的檔案」。

自動啟用網路檔案和印表機共用與瀏覽

1 在用戶端的側邊列中，按下**「狀態」**。

2 在**「防網路和主機侵入」**旁，按下**「選項」>「變更設定」**。

3 在**「Microsoft Windows 網路」**標籤上，按下以下其中一個設定：

- 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」**。

- 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」**。

4 按下**「確定」**。

手動啟用網路檔案和印表機共用與瀏覽

1 在用戶端的側邊列中，按下**「狀態」**。

2 在**「防網路和主機侵入」**旁，按下**「選項」>「變更設定」>「架構防火牆規則」**。

附註：僅當您的管理員使此設定可用或者您正在執行非受管用戶端時，才可查看此設定。

---

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，輸入以下內容：

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，輸入以下內容：

88

12 在**「本機通訊埠」**下拉式清單中，輸入以下內容：

137, 138

13 按下**「確定」**。

手動允許其他電腦瀏覽用戶端電腦上的檔案

1 在用戶端的側邊列中，按下**「狀態」**。

2 在**「防網路和主機侵入」**旁，按下**「架構設定」**

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，輸入以下內容：

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，輸入以下內容：

88, 137, 138

12 按下「**確定**」。

請參閱第 71 頁的「啟用防火牆設定」。

允許或攔截應用程式存取網路

您可以將 Symantec Endpoint Protection 架構為允許或攔截應用程式，或架構為先詢問您要允許應用程式還是攔截應用程式。此動作會建立防火牆規則，該規則指定電腦上的執行中應用程式是否可以存取網路。這些規則稱為以應用程式為基礎的防火牆規則。例如，您可以攔截 Internet Explorer 從您的電腦存取任何網站。

表 4-7 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 在用戶端的側邊列中，按下「**狀態**」。

2 在「**防網路和主機刺探利用**」旁，按下「**選項**」>「**檢視網路活動**」。

3 在「**網路活動**」對話方塊中的執行應用程式或服務上按下滑鼠右鍵，然後選取您希望用戶端對該應用程式採取的動作。

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

請參閱第 75 頁的「允許或攔截已在用戶端上執行的應用程式」。

4 按下「**關閉**」。

允許或攔截已在用戶端上執行的應用程式

您可以針對已在用戶端電腦上執行之應用程式的允許或攔截時間和方式架構條件。例如，您可以指定某個電玩遊戲應用程式只能在特定時段存取網路。應用程式型防火牆規則也稱為應用程式設定。

請參閱第 74 頁的「允許或攔截應用程式存取網路」。

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。

允許或攔截已在用戶端上執行的應用程式

1. 在用戶端的側邊列中，按下**「狀態」**。
2. 在**「防網路和主機侵入」**旁，按下**「選項」>「檢視應用程式設定」**。
3. 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」**來變更動作。
4. 若要變更應用程式型規則的其他選項，請按下**「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或例外。

   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。

   若需這些設定的詳細資訊，請按下**「說明」**。
6. 按下**「確定」**，接受架構變更。
7. 若要移除您對應用程式加諸的規則，請按下應用程式名稱，然後按下**「移除」**。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。

   若要移除所有應用程式型防火牆規則，請按下**「全部移除」**。
8. 按下**「確定」**，關閉**「檢視應用程式設定」**對話方塊。

請參閱第 69 頁的「在用戶端上新增防火牆規則」。

當螢幕保護程式處於作用中狀態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派的安全層級。 請參閱第 76 頁的「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。 請參閱第 76 頁的「在防火牆停止執行時攔截流量」。
當您想要隨時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。 請參閱第 76 頁的「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 84 頁的「在用戶端電腦上啟用防護」。

在螢幕保護程式啟動時攔截流量

1. 在用戶端的側邊列中，按下**「變更設定」**。
2. 在**「防網路和主機侵入」**旁，按下**「架構設定」**。
3. 在**「Microsoft Windows 網路」**標籤上，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. 在用戶端的側邊列中，按下**「變更設定」**。
2. 在**「防網路和主機侵入」**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」**。

   如果您停用**「允許初始 DHCP 和 NetBIOS 流量」**，啟用網路連線的初始流量會遭到攔截。
4. 按下**「確定」**。

在任何時候攔截全部流量

1. 在用戶端的側邊列中，按下**「狀態」**。
2. 在**「防網路和主機侵入」**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 71 頁的「啟用防火牆設定」。

架構入侵預防

依據預設，入侵預防會在您的電腦上執行。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)。

附註：入侵預防和防火牆是網路威脅防護的一部分。「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。

若要管理入侵預防：

1. 確定已下載最新的 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 15 頁的「使用 LiveUpdate 更新用戶端內容」。

2. 將入侵預防保持啟用狀態。

   您應該將入侵預防隨時保持在啟用狀態。Symantec Endpoint Protection 會在安全日誌中記錄入侵嘗試和事件。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 88 頁的「檢視日誌」。

   請參閱第 88 頁的「啟用封包日誌」。

3. 如果您認為偵測為誤報，請通知您的管理員。

   請勿將非預期的事件視為誤報。

   回應 Symantec Endpoint Protection 中可疑 IPS 誤報的最佳實務準則

附註：管理員可能已經架構不提供這些選項。

啟用入侵預防

入侵預防包含兩種類型：

- 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。

- 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。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。

您也可以啟用或停用當用戶端偵測到網路攻擊時的通知。

請參閱：啟用入侵預防通知

啟用入侵預防

1 在用戶端的側邊列中，按下**「變更設定」**。

2 在**「防網路和主機侵入」**旁，按下**「架構設定」**。

3 在**「入侵預防」**標籤上，確定勾選下列選項：

- **啟用網路入侵預防**
- **啟用瀏覽器入侵預防**
  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。 您應該只暫時使用此組態，因為它會降低電腦的防護。例如，當您對遭攔截的流量進行疑難排解時，您會架構只記錄模式。 在檢閱安全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。

4 按下**「確定」**。

啟用入侵預防通知

1 在用戶端的側邊列中，按下**「變更設定」**。

2 在「防網路和主機侵入」旁，按下**「架構設定」**。

3 在**「通知」**標籤上，確定已勾選**「顯示入侵預防和記憶體攻擊緩和通知」**。

4 按下**「確定」**。

防止攻擊易受攻擊的應用程式

記憶體攻擊緩和 (MEM) 會阻止對 Windows 電腦上所執行常用應用程式的攻擊。當用戶端偵測到侵入嘗試時，會顯示下列其中一則或兩則訊息。

- `Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected`
  用戶端會攔截侵入，而不終止應用程式。
- `Symantec Endpoint Protection will terminate your application`
  用戶端會終止應用程式，使其無法執行。

如果應用程式保持終止，請執行以下步驟：

1. 通知您的管理員。

2. 判斷實際侵入攻擊了應用程式，還是偵測為誤報。

   - 如果侵入攻擊了應用程式，請檢查是否存在修正版本或更新版本的受感染應用程式可修正目前弱點。當您或您的管理員安裝修正應用程式後，請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應用程式。
   - 如果偵測為誤報，請暫時停用記憶體攻擊緩和。通知您的管理員或賽門鐵克安全機制應變中心有關錯誤偵測的資訊。使記憶體攻擊緩和處於停用狀態，直到賽門鐵克解決問題為止。然後，重新啟用記憶體攻擊緩和。

判斷偵測是否為誤報

1 在安全日誌中，確認記憶體攻擊緩和確實已終止應用程式。

例如，您可能會看到下列事件：`Attack: Blocked Structured Exception Handler Overwrite attack against C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe`

請參閱第 88 頁的「檢視日誌」。

2 停用記憶體攻擊緩和。

3 重新執行應用程式。

   - 如果應用程式正常執行，則偵測為誤報。
   - 如果應用程式行為異常，例如開啟另一個應用程式，則偵測為檢出。

在受管用戶端上，您的管理員可能會防止您停用記憶體攻擊緩和。

停用並重新啟用記憶體攻擊緩和

1 在**「防網路和主機侵入」**旁的**「狀態」**頁面上，按下**「選項」**。

2 在下拉式功能表中，執行下列其中一項工作：

   - 按下**「停用記憶體攻擊緩和」**或**「啟用記憶體攻擊緩和」**。
   - 按下**「變更設定」**>**「記憶體攻擊緩和」**標籤，然後勾選或取消勾選**「啟用記憶體攻擊緩和」**。

5

管理用戶端

本章包含以下主題：

管理用戶端

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修改防護情況：

- 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。
  請參閱第 82 頁的「關於受管用戶端和非受管用戶端」。
  請參閱第 84 頁的「檢查用戶端是受管用戶端還是非受管用戶端」。
- 您想啟用或停用一或多項防護技術。
  請參閱第 84 頁的「在用戶端電腦上啟用防護」。
- 您想確認是否有最新的病毒定義檔和安全性內容。
- 您聽說最近出現新病毒或安全威脅，想要執行掃描。

表 5-1 架構用戶端的工作

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 17 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 84 頁的「在用戶端電腦上啟用防護」。 請參閱第 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。
更新病毒定義檔及安全性內容	檢查電腦是否具有最新的病毒定義檔及安全性內容。 ■ 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 15 頁的「使用 LiveUpdate 更新用戶端內容」。 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 13 頁的「立即掃描用戶端電腦」。
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 26 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 63 頁的「管理防火牆防護」。
執行遵從檢查	檢查電腦是否符合公司的安全政策。 請參閱第 60 頁的「透過主機完整性掃描檢查電腦安全性遵從」。
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 88 頁的「檢視日誌」。

步驟	敘述
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。 請參閱第 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。 安全政策會自動更新。然而，若要確保擁有最新政策，您可以手動加以更新。 請參閱第 82 頁的「更新用戶端政策」。

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。

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。

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。

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. 在用戶端中按**「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。

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 5-2 受管用戶端與非受管用戶端之間的差別

用戶端類型	說明
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。管理伺服器會通知用戶端，並且用戶端會下載設定。根據管理伺服器的通訊設定，如果管理員對防護進行變更，則用戶端將立即下載此變更。 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。 ■ 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。 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。
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： ■ 未連線至網路的獨立式電腦，例如家用電腦或筆記型電腦。該電腦會使用預設選項設定或管理員預設的設定來安裝 Symantec Endpoint Protection 用戶端。 ■ 連線至公司網路之前即符合安全性需求的遠端電腦。然而，非受管用戶端不支援主機完整性。 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 5-3 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 5-3 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	非受管用戶端
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。
用戶端管理和防網路和主機侵入設定	管理員控制的設定不會出現。	所有設定均會出現。

請參閱第 84 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 82 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**」。

隱藏和顯示 Symantec Endpoint Protection 用戶端上的通知區域圖示

您可以視需要隱藏 Symantec Endpoint Protection 通知區域圖示 (亦稱為系統匣圖示)。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 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。

隱藏或顯示用戶端上的通知區域圖示

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。

---

1. 在用戶端中，按下「**變更設定**」。
2. 在「**變更設定**」頁面上，按下「**用戶端管理**」旁的「**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**」。

在用戶端電腦上啟用防護

您應將電腦上所有類型的防護始終保持啟用狀態，尤其是「自動防護」。

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 11 頁的「Symantec Endpoint Protection 用戶端狀態圖示」。

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。

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」**。

從工作列啟用防護技術

◆ 在 Windows 桌面的通知區域中，以滑鼠右鍵按下用戶端圖示，然後按下**「啟用 Symantec Endpoint Protection」**。

從用戶端內部啟用防護技術

◆ 在用戶端的**「狀態」**頁面上，按下**「*防護類型* 防護」**旁的**「選項」>「啟用 *防護類型* 防護」**。

啟用防火牆

1 在用戶端**「狀態」**頁面最上方的**「防網路和主機侵入」**旁邊，按下**「選項」>「變更設定」**。

2 在**「防火牆」**標籤上，核取**「啟用防火牆」**。

3 按下**「確定」**。

請參閱第 54 頁的「啟用自動防護」。

6

疑難排解用戶端

本章包含以下主題：

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 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。

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 6-1 用戶端日誌

日誌	敘述
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。
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。
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。 在受管用戶端上，除非管理員允許，否則您無法啟用封包日誌。 若為非受管用戶端，則您可以啟用封包日誌。 請參閱第 88 頁的「啟用封包日誌」。
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 53 頁的「管理電腦上的隔離檔案」。
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。
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。 安全日誌也會顯示主機完整性檢查的結果。
系統日誌	■ 病毒和間諜軟體防護：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。 ■ 主動型威脅防護：包含電腦上與 SONAR 相關的系統活動資訊。 ■ 用戶端管理：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

日誌	敘述
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。
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。
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。 在啟用風險追蹤程式的情況下，防網路和主機侵入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。 如需詳細資訊，請參閱：什麼是風險追蹤程式？

請參閱第 88 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。

檢視日誌

1. 在用戶端的側邊看板中，按下**「檢視日誌」**。
2. 按下**「檢視日誌」**按鈕，並在下拉式功能表中選擇您要檢視的日誌。

   根據您的安裝，一些防護技術可能不會顯示。

請參閱第 87 頁的「關於日誌」。

啟用封包日誌

除了封包日誌以外，所有防網路和主機侵入日誌及用戶端管理日誌都預設為啟用。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 87 頁的「關於日誌」。

啟用封包日誌

1. 在用戶端之**「狀態」**頁面的**「防網路和主機侵入」**旁，按下**「選項」**，再按下**「變更設定」**。
2. 按下**「日誌」**。
3. 勾選**「啟用封包日誌」**。
4. 按下**「確定」**。

索引

七劃

八劃

九劃

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