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

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

文件版本 11.00.00.00.00

版權聲明

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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

目錄

部分 2 Symantec Endpoint Protection

第 4 章 介紹 Symantec Endpoint Protection

第 5 章 Symantec Endpoint Protection 用戶端基礎

第 6 章 管理防毒和防間諜軟體防護

第 7 章 管理主動型威脅防護

第 8 章 管理網路威脅防護

部分 3 Symantec Network Access Control

第 9 章 Symantec Network Access Control 基礎

部分 4 監控與記錄

第 10 章 使用和管理日誌

索引

部分 1

簡介

1

Symantec 用戶端簡介

本章包含以下主題：

關於用戶端

賽門鐵克提供兩種端點安全產品，可搭配使用或單獨使用：Symantec Endpoint Protection 和 Symantec Network Access Control。您或您的管理員已在您的電腦上安裝一種或兩種 Symantec 用戶端軟體產品。如果是您的管理員安裝用戶端，則由您的管理員決定用戶端上啟用的產品。

附註：如果您或您的管理員在您的電腦上安裝其中一個產品，產品名稱會出現在標題列。當兩種防護都啟用時，Symantec Endpoint Protection 會出現在標題列。

Symantec Endpoint Protection 保護您的電腦不受網際網路威脅和安全風險的入侵。它可以執行下列動作：

- 掃描您電腦上的病毒、已知威脅和安全風險。
- 監控通訊埠上的已知攻擊特徵。
- 監控您電腦上程式的可疑行為。

請參閱第 31 頁的「關於 Symantec Endpoint Protection」。

Symantec Network Access Control 可確定您電腦的安全設定符合網路政策。安全設定可以包括軟體、軟體架構設定、特徵檔案、修正程式或其他元素。

請參閱第 113 頁的「關於 Symantec Network Access Control」。

關於受管用戶端和非受管用戶端

Symantec 產品的管理員能夠將用戶端安裝成非受管用戶端或受管理員管理的用戶端。非受管用戶端表示管理員無法控制 Symantec 用戶端中的設定和動作。在非受管用戶端中，您可以控制用戶端的全部設定和動作。

在受管理環境中，管理員會從 Symantec Endpoint Protection Manager 遠端監控、架構和更新用戶端。這個管理伺服器可供管理員決定您控制用戶端設定和動作的控制數量。用戶端會檢查管理伺服器，以判斷是否有新的政策資訊或更新可供使用。

在受管理環境中，您可能無法檢視或存取每一個用戶端元件。用戶端中可見的元件和可用的動作，視管理員授予電腦的存取權限程度而定。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。

在全部的環境中，用戶端都會提示資訊和問題。您必須回應這些提示。

請參閱第 17 頁的「關於用戶端互動」。

關於通知區域圖示

用戶端在您桌面右下角有一個通知區域圖示。對這個圖示按下滑鼠右鍵，可顯示常用命令。

附註：在受管用戶端上，如果您的管理員已架構它為不能使用，則此圖示不會顯示。

表 1-1 描述通知區域圖示可用的命令。

表 1-1 通知區域圖示命令

選項	敘述
開啟 Symantec Endpoint Protection 開啟 Symantec Network Access Control	開啟主視窗
更新政策	從伺服器擷取最新安全性政策 **附註**：此命令僅限受管用戶端使用。
重新驗證	重新驗證用戶端電腦。 **附註**：此命令僅限當您的管理員架構用戶端為內建的 802.1x 請求者時使用。

選項	敘述
停用 Symantec Endpoint Protection	關閉全部的用戶端防護。 在您停用用戶端後，命令文字會從「停用」變更為「啟用」。您可以選取此命令開啟全部的用戶端防護。

請參閱第 119 頁的「重新驗證電腦」。

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，當您在 Windows 工作列上需要更多空間時，可以將它隱藏。

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」頁面，「用戶端管理」旁，按下「架構設定」。
3. 在「用戶端管理設定」對話方塊中「一般」標籤上的「顯示選項」下，選取您要變更的位置。
4. 取消勾選「在通知區域中顯示 **Symantec Endpoint Protection** 圖示」。
5. 按下「確定」。

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」頁面，「用戶端管理」旁，按下「架構設定」。
3. 在「用戶端管理設定」對話方塊的「顯示選項」下，選取您要變更的位置。
4. 勾選「在通知區域中顯示 **Symantec Endpoint Protection** 圖示」。
5. 按下「確定」。

保持電腦最新防護功能的方式

賽門鐵克公司的工程師會不斷追蹤各種電腦病毒的活動，藉以發現新的病毒。他們也會追蹤混合型威脅、安全風險 (如間諜軟體) 以及可藉由電腦連接 Internet 時攻擊的其他漏洞。在識別出風險之後，他們便會撰寫特徵 (即關於風險的資訊)，然後將它儲存在定義檔中。此定義檔包含偵測、刪除和修復風險攻擊所需的資訊。當

Symantec Endpoint Protection 掃描病毒和安全風險時，便會搜尋這些類型的特徵。

用戶端必須保持最新的其他項目還包括允許和限制的程序清單以及攻擊特徵。程序清單可協助「主動型威脅防護」識別可疑的程式行為，即使用戶端並未識別出特定的威脅。攻擊特徵則可提供「入侵防護系統」保護電腦不受入侵所需的資訊。

除了定義檔、程序清單和攻擊特徵，用戶端還必須不定期更新元件。這些元件包括「防毒和防間諜軟體防護」引擎、「主動型威脅防護」引擎以及「網路威脅防護」防火牆。更新則可能有次要缺點修復或產品加強功能。

賽門鐵克會持續不斷提供更新。賽門鐵克安全機制應變中心每天都會更新定義。每星期或在出現新的毀滅性病毒威脅時，都會以 LiveUpdate 提供新的定義。

附註：您的管理員可能會控制用戶端的定義更新頻率。

請參閱第 23 頁的「關於 LiveUpdate」。

關於賽門鐵克安全機制應變中心的角色

Symantec Endpoint Protection 背後的力量就是賽門鐵克安全機制應變中心。「賽門鐵克安全機制應變中心」研究專家會分解各種病毒和安全風險樣本，查明其專有的特徵與行為。他們會使用此資訊開發賽門鐵克產品用以偵測、排除和修復病毒與安全風險所造成影響的定義。

由於新種病毒散播的速度相當快速，賽門鐵克安全機制應變中心已開發出自動化的軟體分析工具。若您能將受感染的檔案從電腦傳送給賽門鐵克安全機制應變中心，將能大幅縮短發現病毒、進行分析和開發出解毒方法的時間。

「賽門鐵克安全機制應變中心」的研究專家也會研究與開發防護電腦的技術，讓電腦不受如間諜軟體、廣告軟體及駭客工具等安全風險的入侵。

「賽門鐵克安全機制應變中心」所維護的百科全書提供詳盡的病毒和安全風險資訊。必要時，他們會提供關於移除風險的資訊。百科全書位於賽門鐵克安全機制應變中心網站，網址如下：

http://www.symantec.com/zh/tw/enterprise/security_response/index.jsp

受管用戶端更新防護功能的方式

您的管理員會決定更新您病毒和安全風險定義的方式。您不需要做任何事，便可以收到新的定義。

您的管理員可以設定 Symantec Endpoint Protection 中的 LiveUpdate 功能，以確保您的病毒和安全風險防護保持在最新的狀態。LiveUpdate 會連接儲存更新的電腦，判斷您的用戶端是否需要更新，然後下載和安裝適當的檔案。儲存更新的電腦

可能是公司內部的 Symantec Endpoint Protection Manager 伺服器。或者，也可能是透過 Internet 存取的 Symantec LiveUpdate 伺服器。

請參閱第 23 頁的「關於 LiveUpdate」。

非受管用戶端上的防護如何進行更新

管理員不會更新非受管用戶端上的防護。您可以使用 LiveUpdate 更新軟體和定義檔。如果您的非受管用戶端使用預設 LiveUpdate 設定，它會透過網際網路從 Symantec 伺服器每週檢查一次更新。

您可以變更 LiveUpdate 檢查更新的頻率。如果您知道有病毒或其他安全風險爆發時，還可以手動執行 LiveUpdate。

請參閱第 23 頁的「關於 LiveUpdate」。

關於安全性政策

安全性政策是一組安全性設定，由受管用戶端的管理員架構和部署於用戶端中。安全性政策會決定用戶端設定，包括您可檢視和存取的選項。

受管用戶端會連線至管理伺服器，並自動接收最新的安全性政策。如果您無法進行網路存取，管理員會指示您手動更新安全性政策。

請參閱第 15 頁的「更新安全性政策」。

更新安全性政策

控制用戶端防護的設定儲存於電腦中的一個政策檔案中。此安全性政策檔案通常會自動更新。但是，您的管理員可能會在特定情況下指示您手動更新安全性政策。

附註：您可以檢視系統日誌，確認作業已成功更新政策。

請參閱第 128 頁的「檢視日誌及日誌詳細資料」。

更新安全性政策

1. 在 Windows 通知區域中，用滑鼠右鍵按下用戶端圖示。
2. 在快顯功能表中，按下「更新政策」。

其他詳細資訊的位置

若您需要詳細資訊，可以存取線上說明。您可以從賽門鐵克安全機制應變中心網站取得有關病毒及安全風險的其他資訊，網站 URL 是：

http://www.symantec.com/zh/tw/enterprise/security_response/index.jsp

存取線上說明

用戶端線上說明系統提供一般資訊與程序，協助您保護電腦不受病毒和安全風險的侵襲。

附註：您的管理員可能已經決定不安裝說明檔。

存取線上說明

- 在主視窗中，執行下列其中一項：
  - 按下「說明及支援」，然後按下「說明主題」。
  - 在任何個別的對話方塊中，按下「說明」。
    只有在您可以執行動作的螢幕上才有上下文關聯說明。
  - 在任何視窗中，按 **F1**。如果該視窗有上下文關聯說明，則會出現上下文關聯說明。如果沒有上下文關聯說明，則會出現完整的說明系統。

存取賽門鐵克安全機制應變中心網站

如果您可以連線網際網路，您即可造訪賽門鐵克安全機制應變中心網站檢視下列項目：

- 包含關於所有已知病毒資訊的「病毒百科全書」
- 關於惡作劇病毒的資訊
- 關於一般病毒與病毒威脅的白皮書
- 關於安全風險的一般資訊及詳細資訊

若要存取賽門鐵克安全機制應變中心網站，請使用下列 URL：

- 在您的網際網路瀏覽器中，鍵入下列網址：
  http://www.symantec.com/zh/tw/enterprise/security_response/index.jsp

2

回應用戶端

本章包含以下主題：

關於用戶端互動

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。如果用戶端上已啟用 Symantec Endpoint Protection，您可能會有下列類型的用戶端互動：

病毒或安全風險偵測	如果「自動防護」或掃描偵測出病毒或安全風險，「Symantec Endpoint Protection 偵測結果」對話方塊便會出現，其中顯示關於感染的詳細資訊。對話方塊也會顯示 Symantec Endpoint Protection 處理風險時採取的動作。除了檢視活動和關閉對話方塊之外，您通常不需要採取其他任何動作。然而，若有必要，您也可以採取進一步的行動。 請參閱第 18 頁的「處理受感染的檔案」。
應用程式相關通知	當電腦上的程式嘗試存取網路時，Symantec Endpoint Protection 會提示您允許或拒絕存取。 請參閱第 19 頁的「回應應用程式相關的通知」。
安全性警示	Symantec Endpoint Protection 會通知您已攔截程式，或已偵測危害您電腦的攻擊。 請參閱第 22 頁的「回應安全性警示」。

如果用戶端上已啟用 Symantec Network Access Control，您可能會看見「網路存取控制」訊息。如果安全性設定未符合管理員架構的標準，就會顯示這個訊息。

請參閱第 22 頁的「回應網路存取控制通知」。

處理受感染的檔案

「自動防護」預設會持續在您的電腦上執行。若是非受管用戶端，當您啟動電腦時，就會執行自動產生的快速掃描。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。「自動防護」在偵測到風險時，會顯示結果對話方塊。掃描執行時，會出現掃描對話方塊，顯示掃描結果。若是受管用戶端，您的管理員可能會關閉這些類型的通知。

如果您收到這類通知，可能需要對受感染的檔案採取動作。

「自動防護」和所有掃描類型的預設選項是，偵測到時，將受感染檔案中的病毒清除。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」。本機「隔離所」是一個特殊的位置，保留給受感染的檔案及相關系統副作用使用。若是安全風險，用戶端會隔離受感染的檔案，並移除或修復其副作用。用戶端無法修復檔案時，會將該偵測記錄下來。

附註：病毒只要放到「隔離所」，便不會擴散。當用戶端將檔案移到「隔離所」，您便無法存取該檔案。

Symantec Endpoint Protection 修復受病毒感染的檔後，您不必採取其他動作來防護您的電腦。如果用戶端隔離了受安全風險感染的檔案，接著加以移除並修復，則您不必採取其他動作。

您可能不需要對檔案採取動作，但可能會想要對檔案執行其他動作。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。

您可以利用通知，立即對檔案採取動作。您也可以使用日誌檢視或「隔離所」，稍後對檔案執行動作。

請參閱第 63 頁的「解譯掃描結果」。

請參閱第 132 頁的「從風險日誌和威脅日誌隔離風險及威脅」。

請參閱第 74 頁的「關於隔離所」。

處理受感染的檔案

1 執行下列其中一項動作：

- 一旦掃描完成，在掃描進度對話方塊中，選取您所要的檔案。
- 在「掃描結果」對話方塊中，選取您要的檔案。

- 在用戶端的側邊看板中，按下「檢視日誌」，再按「防毒和防間諜軟體防護」旁邊的「檢視日誌」。在日誌檢視中選取您要的檔案。

2 在檔案上按下滑鼠右鍵，再選取下列其中一個選項：

- 還原採取的動作：還原採取的動作。
- 清除：移除檔案中的病毒。
- 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。
- 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。
- 匯出：將「隔離所」的內容匯出為逗號分隔 (*.csv) 檔案或 Access 資料庫 (*.mdb) 檔案。
- 屬性：顯示有關病毒或安全風險的資訊。

某些情況下，用戶端可能無法執行您選取的動作。

關於病毒造成的損壞

如果 Symantec Endpoint Protection 在發生感染時馬上發現，用戶端清除受感染的檔案後，該檔案可能就可以完全正常使用。但是，在某些情況下，Symantec Endpoint Protection 可能會清除已遭病毒破壞的受感染檔案。例如，Symantec Endpoint Protection 可能發現損壞文件檔案的病毒，Symantec Endpoint Protection 會移除病毒，但無法修復受感染檔案的內部損壞。

關於通知與警示

您可能會在電腦上看見幾種不同類型的通知。這些通知通常會說明狀況，並且指出用戶端嘗試解決問題的方法。

您可能會看見下列幾種通知類型：

- 應用程式相關通知
- 安全性警示

回應應用程式相關的通知

您可能會看見一個通知詢問您是否要允許應用程式或服務執行。

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。
- 用戶端使用「快速切換使用者」切換使用者。
- 您的管理員升級了用戶端軟體。

您可能會看見下列訊息，通知您有應用程式或服務嘗試存取您的電腦：

```
Internet Explorer (IEXPLORE.EXE) 正嘗試
使用遠端通訊埠 80 (HTTP - 全球資訊網) 來連線至 www.symantec.com。
您是否要允許這項程式存取網路?
```

回應嘗試存取網路的應用程式

1. 在訊息方塊中，按下「詳細資料」。

   您可檢視有關連線和應用程式的更多資訊，這些資訊包括檔案名稱、版本號碼及路徑。

2. 如果您要在下次此應用程式嘗試存取您的網路連線時記住您的選擇，按下「記住我的答案，請勿再針對這項應用程式詢問我」。

3. 執行下列其中一項工作：

   - 若要允許應用程式存取網路連線，請按下「是」。
     只有在您可以辨識應用程式並確定要讓它存取網路連線時，才按下「是」。
     如果您不確定是否要允許應用程式存取網路連線，請詢問您的管理員。
   - 若要阻止應用程式存取網路連線，請按下「否」。

   表 2-1 顯示您可以如何回應詢問您是否要允許或攔截應用程式的通知。

表 2-1 應用程式許可通知

如果按下	如果您勾選「記住我的答案...」核取方塊？	用戶端...
是	是	允許應用程式並不再詢問。
是	否	允許應用程式，並且每次都詢問。
否	是	攔截應用程式並不再詢問。
否	否	攔截應用程式，並且每次都詢問。

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 107 頁的「架構應用程式限定設定」。

變更應用程式通知

有時候，您可能會看見一條訊息，指出應用程式已變更。

"Telnet 程式自從上次開啟後已變更，
這可能是因為您最近曾經進行更新。
您是否要允許存取網路?"

列於下列訊息中的應用程式嘗試存取您的網路連線。雖然用戶端辨識出應用程式的名稱，但是自從上次用戶端遭遇過這個應用程式之後，這個程式已有過變更。很可能是最近產品進行了升級。每個新產品版本會使用與舊版本不同的檔案指紋檔案。用戶端偵測到檔案指紋檔案已變更。

快速切換使用者通知

如果您使用 Windows Vista/XP，您會看見下列其中一個通知：

"Symantec Endpoint Protection 無法顯示
使用者介面。如果您使用的是「Windows XP 快速使用者切換」，
請確定所有其他使用者都已登出 Windows 後，嘗試登出 Windows 再登入。

如果您使用的是「終端機服務」，則不支援使用者介面。"

或

"Symantec Endpoint Protection 並未執行但將會啟動。
然而，Symantec Endpoint Protection 無法顯示使用者介面。
如果您使用的是「Windows XP 快速使用者切換」，
請確定所有其他使用者都已登出 Windows 後，嘗試登出 Windows 再登入。
如果您使用的是「終端機服務」，則不支援使用者介面。"

快速切換使用者是一種Windows功能，讓您不需登出電腦就可以快速切換使用者。多位使用者可以同時共用一台電腦，並且在來回切換時不需要關閉執行的程式。如果您使用「快速切換使用者」切換使用者，會出現下列其中一個視窗。

若要回應快速切換使用者訊息，請按照對話方塊中的指示操作。

自動更新通知

如果用戶端軟體已自動更新，您會看見下列通知：

Symantec Endpoint Protection 偵測到 Symantec Endpoint Protection Manager
已有更新版本。
是否要立即下載?

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」。

回應安全性警示

安全性警示會在通知區域圖示上方顯示一個通知。您只需要按下「確定」表示您已讀取訊息。通知顯示的原因如下：

攔截應用程式訊息

根據管理員設定的規則，您電腦啟動的應用程式遭到攔截。例如，您會看見下列訊息：

應用程式 `Internet Explorer` **已被攔截，**
檔案名稱為 `IEXPLORE.EXE`。

這些通知表示您的用戶端已攔截您指定為不信任的流量。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。

入侵

您的電腦受到攻擊，警示通知您這個情況，或提供處理方法的指示。例如，您會看見下列訊息：

攔截 `IP` **位址** `192.168.0.3` **的流量，**
從 `10/10/2006 15:37:58` **到** `10/10/2006 15:47:58`。
已記錄「通訊埠掃描」攻擊。

您的管理員可能已停用用戶端電腦上的入侵預防通知。若要檢視您用戶端偵測到的攻擊類型，您可以讓用戶端顯示入侵預防通知。

請參閱第 106 頁的「架構入侵預防通知」。

回應網路存取控制通知

如果 Symantec Network Access Control 用戶端未符合安全性政策，則可能無法存取網路。在此狀況下，您可以會看見訊息，說明由於「主機完整性」檢查失敗，因此 Symantec Enforcer 攔截您的流量。網路管理員可能在此訊息中加入文字，說明可以採取的矯正動作。

回應網路存取控制通知

1 按照訊息方塊中顯示的建議程序進行。

2 在訊息方塊中，按下「確定」。

在關閉訊息方塊之後，開啟用戶端，檢視其中是否顯示任何關於還原網路存取的建議程序。

3

管理用戶端

本章包含以下主題：

關於 LiveUpdate

LiveUpdate 可使用網際網路連線在電腦上進行程式和防護更新。

所謂程式更新，指的是對已安裝好的產品做小幅度的修改。與產品升級不同，後者指的是將整套產品更換成較新的版本。程式更新的建立通常是用來擴充作業系統或硬體的相容性、調整效能問題，或是修正程式錯誤。至於程式更新部分，賽門鐵克會視需要來發行。

附註：某些程式更新可能會需要您在安裝後重新開機。

LiveUpdate 會自動進行更新擷取和安裝。它會從 Internet 網站中搜尋取得檔案並加以安裝，然後刪除您電腦上遺留的檔案。

防護更新檔利用最新防護技術使賽門鐵克產品保持在最新狀態。您收到的防護更新視您安裝在電腦上的產品而定。

依預設，LiveUpdate會在排程間隔自動執行。根據您的安全性設定，您可以手動執行 LiveUpdate。可能也可以停用 LiveUpdate 或變更 LiveUpdate 排程。

在排程間隔執行 LiveUpdate

您可以建立排程，以便 LiveUpdate 在排程間隔自動執行。

在排程間隔執行 LiveUpdate

1. 在用戶端的側邊看板中，按下「變更設定」>「用戶端管理」>「架構設定」。
2. 在「用戶端管理設定」對話方塊中，按下「排程更新」。
3. 在「排程更新」標籤上，勾選「啟用自動更新」。
4. 在「頻率」群組方塊中，選取每日、每週或每月執行更新。
5. 在「當」群組方塊中，選取在哪一天、哪一週或每天什麼時間執行更新。
6. 若要指定如何處理錯過的更新，請按下「進階」。
7. 在「進階排程選項」對話方塊中，選取 LiveUpdate 重試已遺漏更新的選項。

   若需這些選項的詳細資訊，請按下「說明」。
8. 按下「確定」。
9. 按下「確定」。

手動執行 LiveUpdate

您可以使用 LiveUpdate 更新軟體和定義檔。LiveUpdate 會從 Symantec 網站擷取新的定義檔，然後置換舊的定義檔。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。這些最新的資訊皆是透過賽門鐵克的LiveUpdate技術傳播。

使用 LiveUpdate 取得更新

- 在用戶端的側邊看板中，按下 **LiveUpdate**。

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

測試您電腦的安全

您可以使用掃描的方式，測試您電腦不受威脅和病毒入侵的能力。此步驟的掃描對確定您電腦不受入侵是非常重要的。結果可幫助您在用戶端上設定各選項以保護您的電腦不受攻擊。

測試您電腦的安全

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」>「測試網路安全」。

4 在賽門鐵克安全檢查網站，執行下列一項：

- 若要檢查線上威脅，請按下「安全掃描」。
- 若要檢查病毒，請按下「病毒偵測」。

5 在「使用者授權合約」對話方塊中，按下「我同意」，然後再按「下一步」。

如果您在步驟 4 按下了「病毒偵測」，請按下「我同意」，然後再按「下一步」。

在任何時候，如果您想要停止掃描，請按下「停止」。

6 當掃描完成時，關閉對話方塊。

關於位置

位置會參考根據您的網路環境所制定的安全性政策。例如，如果您從家裡使用筆記型電腦連線至辦公室網路，管理員可以設定一個名為家用 (Home) 的位置。如果您是在辦公室使用筆記型電腦，則可以使用一個名為辦公室 (Office) 的位置。其他位置可能包括 VPN、分公司辦公室或旅館。

因為您的安全需求和使用需求可能會因不同網路環境而有所不同，因此用戶端可以在這些位置間切換。例如，當您的筆記型電腦連線至辦公室網路時，用戶端可以使用一組較嚴格的政策 (由管理員架構)。但當連線至家用網路時，用戶端則可以使用一組能讓您存取較多架構選項的政策。管理員會依此原則規劃和架構您的用戶端，以便用戶端能自動為您消除這些差異。

附註：在受管環境中，只有在管理員提供了必要的權限時，您才能變更位置。

變更位置

若有必要，您可以變更位置。例如，您可能需要切換至某個位置，以便同事能夠存取您電腦上的檔案。根據您的安全性政策和電腦的使用中網路而定，會提供一份可用位置的清單。

附註：根據可用的安全性政策，您不一定能存取超過一個以上的位置。您可能會發現按下某個位置時，並沒有變更該位置。這表示您的網路架構不適合該位置。例如，只有在偵測到辦公室區域網路 (LAN) 時，才能夠使用稱為「辦公室」的位置。如果您目前不在相關的網路上，就無法變更該位置。

變更位置

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「變更設定」頁的「用戶端管理」旁，按下「架構設定」。
3. 在「一般」標籤的「位置選項」下方，選取您要變更至的位置。
4. 按下「確定」。

關於竄改防護

「竄改防護」提供Symantec應用程式的即時防護。它可以阻擋惡意軟體(如病蟲、特洛伊木馬程式、病毒及安全風險) 的攻擊。

您可以設定「竄改防護」採取下列動作：

- 攔截竄改嘗試並記錄事件
- 記錄竄改事件但不干擾竄改事件

除非您的管理員變更預設設定，否則會同時為受管用戶端和非受管用戶端啟用「竄改防護」。當「竄改防護」偵測到竄改嘗試時，預設會採取的動作是在「竄改防護日誌」中記錄該事件。您可以架構「竄改防護」在偵測到竄改嘗試時，在您的電腦上顯示通知。您可以自訂這個訊息。除非您啟用該功能，否則「竄改防護」不會通知您有關竄改嘗試的事件。

如果您使用的是非受管用戶端，則可以變更您的「竄改防護」設定。如果您使用的是受管用戶端，只要您的管理員允許，也可以變更這些設定。

初次使用 Symantec Endpoint Protection 時，若您每週監控一次日誌，最好保留預設動作「僅記錄事件」。在沒有發現誤判，可以放心時，就可以將「竄改防護」設定為「攔截並記錄事件」。

附註：如果您使用協力廠商的安全風險掃描程式來偵測並防禦不想要的廣告軟體和間諜軟體，該掃描程式通常會影響賽門鐵克程序。如果您在執行協力廠商的安全風險掃描程式的同時啟用「竄改防護」，「竄改防護」會產生大量的通知和日誌項目。最佳的做法是讓「竄改防護」一直保持在啟用狀態，並在產生的事件數目過多時，使用日誌過濾功能。

啟用、停用與架構竄改防護

您可以啟用或停用「竄改防護」。如果啟用「竄改防護」，您可以選擇當它偵測到嘗試竄改賽門鐵克軟體的事件時，所要採取的動作。您也可以讓「竄改防護」顯示訊息，通知您發生了竄改嘗試事件。如果您要自訂訊息，可以使用「竄改防護」會填入適當資訊的預先定義變數。

如需預先定義變數的相關資訊，請按「竄改防護」標籤上的「說明」。

啟用或停用竄改防護

1. 在主視窗的側邊看板中，按下「變更設定」。
2. 在「用戶端管理」旁邊，按下「架構設定」。
3. 在「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. 在主視窗的側邊看板中，按下「變更設定」。
2. 在「用戶端管理」旁邊，按下「架構設定」。
3. 在「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，選取「攔截並記錄事件」或「僅記錄事件」。
4. 如果您要在「竄改防護」偵測到可疑的行為時收到通知，請勾選「在偵測出竄改時顯示通知訊息」。

   如果您啟用這些通知訊息，就可以收到關於 Windows 程序以及賽門鐵克程序的通知。
5. 若要自訂所顯示的訊息，請在訊息欄位中輸入新的文字或刪除任何您想刪除的文字。
6. 按下「確定」。

部分 2

Symantec Endpoint Protection

4

介紹 Symantec Endpoint Protection

本章包含以下主題：

關於 Symantec Endpoint Protection

您可以將 Symantec Endpoint Protection 安裝為單機版或由管理員管理的版本。單機版是指管理員不會管理 Symantec Endpoint Protection 軟體，所以是屬於單機型用戶端。

如果您管理自己的電腦，必須是下列其中一種類型：

- 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。
- 連接至您企業網路之前即符合安全性需求的遠端電腦。

Symantec Endpoint Protection 預設設定會藉由使用桌面防火牆和主機架構入侵預防，提供「防毒和防間諜軟體防護」、「主動型威脅防護」以及「網路威脅防護」。您可以調整這些預設設定，以符合公司的需求、使系統效能最佳化，並停用不需要的選項。

如果是由管理員管理您的電腦，則根據管理員的安全性政策，某些選項可能會鎖定或無法使用。您的管理員可以在您的電腦上執行掃描，並可設定排程掃描。

您的管理員會告訴您應該使用 Symantec Endpoint Protection 執行哪些作業。

Symantec Endpoint Protection 保護您電腦的方式

Symantec Endpoint Protection 提供安全性政策，其中包含多種防護功能來保護您的電腦。

下列幾種防護功能將搭配運作，保護您的電腦不受風險入侵：

- 防毒和防間諜軟體防護
- 網路威脅防護
- 主動型威脅防護

關於防毒和防間諜軟體防護

「防毒和防間諜軟體防護」可確保您的電腦不受已知病毒與安全風險的威脅。因為可以迅速偵測出並移除您電腦中的病毒，因此它們就無法散佈到其他檔案並造成傷害。病毒和安全風險所造成的影響可以修復。當 Symantec Endpoint Protection 用戶端偵測到病毒或安全風險時，根據預設，用戶端會通知您偵測的結果。如果您不想收到通知，則您或管理員可以架構用戶端，使其自動處理風險。

「防毒和防間諜軟體防護」可提供以特徵為基礎的掃描，其包括下列功能：

- 自動防護掃描
  「自動防護」會持續執行，並透過監控您電腦上的活動，為您的電腦提供即時防護。「自動防護」會在檔案執行或開啟時，檢查是否有病毒或安全風險，也會在您修改檔案時，檢查是否有病毒或安全風險。例如，您可能會重新命名、儲存檔案，或在資料夾之間移動或複製檔案。
- 排程、開機及隨選掃描
  您或管理員可以架構其他要在您電腦上執行的掃描。這些掃描會搜尋受感染檔案中殘留的病毒特徵，也會搜尋受感染檔案中安全風險的特徵與系統資訊。您或管理員都可以起始掃描，有系統地檢查電腦上的檔案是否有病毒和安全風險。安全風險可能包括廣告軟體和間諜軟體。

關於網路威脅防護

Symantec Endpoint Protection 用戶端提供可自訂的防火牆，可保護您的電腦免遭侵入和不當使用，不論其為惡意或無意。它會偵測並識別已知的通訊埠掃描及其他常見的攻擊。然後，防火牆會選擇允許或攔截各種網路服務、應用程式、通訊埠以及元件來作為回應。它包含數種類型的防護防火牆規則及安全性設定，可保護用戶端電腦，避開可能造成傷害的網路流量。

網路威脅防護提供防火牆及入侵預防特徵，可攔截入侵攻擊和惡意內容。防火牆可根據各種條件，允許或攔截流量。

防火牆規則可以決定您的電腦要允許或攔截嘗試透過您的網路連線，存取您電腦的入埠或離埠應用程式或服務。防火牆規則可以有系統地允許或攔截，來自或傳至特

定IP位址及通訊埠的入埠或離埠應用程式及流量。安全性設定可偵測並識別常見的攻擊、在受到攻擊之後傳送電子郵件訊息、顯示可自訂訊息，以及執行其他相關的安全工作。

請參閱第 91 頁的「關於網路威脅防護」。

關於主動型威脅防護

「主動型威脅防護」可確保您的電腦擁有不受不明威脅攻擊的零時差防護。此項防護利用啟發式掃描，可分析程式的結構、行為和其他屬性，找出是否有疑似病毒的特性。在多數情況下，它可以保護電腦免於各類威脅，像是大量郵件病蟲和巨集病毒等。您可能會在更新病毒及安全風險定義之前，遇到病蟲和巨集病毒。主動型威脅掃描會在 HTML、VBScript 和 JavaScript 檔案中尋找程序檔式威脅。

主動型威脅掃描也可以偵測可能出於惡意目的的商用應用程式。這些商用應用程式包括遠端控制程式或按鍵記錄器。

您可以架構主動型威脅掃描來隔離偵測到的項目。可以手動還原主動型威脅掃描所隔離的項目。用戶端也可以自動還原隔離的項目。

5

Symantec Endpoint Protection 用戶端基礎

本章包含以下主題：

關於病毒與安全風險

Symantec Endpoint Protection 用戶端可以同時掃描病毒和安全風險，如間諜軟體或廣告軟體。這些風險可能會將電腦和網路置於危險之中。防毒和防間諜軟體掃描也會偵測核心等級的 Rootkit。Rootkit 是任何試圖在電腦作業系統藏匿的程式，可能會被用於惡意的企圖。

根據預設，包括「自動防護」掃描在內的所有防毒和防間諜軟體掃描，都會檢查病毒、特洛伊木馬程式、病蟲，以及所有類別的安全風險。

表 5-1 描述病毒和安全風險的類型。

表 5-1 病毒和安全風險

風險	敘述
病毒	執行時將本身的副本附加在其他電腦程式或文件的程式或程式碼。每當受感染的程式執行，或使用者開啟含有巨集病毒的文件時，就會啟動附加的病毒程式。病毒接著會將本身附加到其他程式和文件。 病毒通常會造成負載，例如在特定日期顯示訊息。其中有些病毒特別會藉著破壞程式、刪除檔案或重新將硬碟格式化來損毀資料。
惡意 Internet 機器人	在 Internet 上執行自動化工作以做惡意用途的程式。 機器人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。某些病蟲會藉由在磁碟之間自我複製來散播，某些則是只在記憶體中複製來拖慢電腦速度。
特洛伊木馬程式	包含偽裝或隱藏為無害程式碼的程式，例如，遊戲或公用程式。
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。混合型威脅使用多種方法和技術來快速散佈，並透過網路造成廣大的損害。
廣告軟體	是獨立或附加的程式，可透過Internet秘密地收集個人資訊，並將它轉遞回另一台電腦。廣告軟體可能會因為廣告的目的，而追蹤瀏覽習慣。廣告軟體也可以傳送廣告的內容。 廣告軟體可以在使用者不知情的狀況下，從網站 (通常是以分享軟體或免費軟體的形式) 下載，或者以電子郵件訊息或即時傳訊程式送達。通常使用者會因為接受軟體程式的「使用者授權合約」，而在不知情的狀況下載廣告軟體。
撥接工具	這種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，撥號到 900 號碼或是 FTP 網站。使用者通常會因此需要付費。
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	這種程式會企圖以幽默或嚇人的方式改變或中斷電腦的作業。例如，該程式可以從網站、電子郵件訊息或即時傳訊程式下載，當使用者嘗試要刪除它時，它可以移動「資源回收筒」遠離滑鼠，或使滑鼠按下造成相反的結果。
其他	這是不符合病毒、特洛伊木馬程式、病蟲或其他安全風險類別嚴格定義的任何其他安全風險。
遠端存取程式	這種程式允許由其他電腦透過Internet存取，以得到資訊，或是攻擊或改變使用者的電腦。您可能會安裝合法的遠端存取程式。程序可能會在您不知情的狀況下安裝這種應用程式。這個程式可以在修改或不修改原始遠端存取程式的情況下，被用於惡意的企圖。

風險	敘述
間諜軟體	是一種獨立程式，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。 間諜軟體可以在使用者不知情的狀況下，從網站 (通常是以分享軟體或免費軟體的形式) 下載，或者以電子郵件訊息或即時傳訊程式送達。通常使用者會因為接受軟體程式的「使用者授權許可協議」，而在不知情的狀況下載間諜軟體。
追蹤軟體	是一種獨立或附加的應用程式，可追蹤使用者在 Internet 上的路徑，並將資訊傳送到目標系統。例如，該應用程式可以從網站、電子郵件訊息或即時傳訊程式下載，然後它就可以取得關於使用者行為的機密資訊。

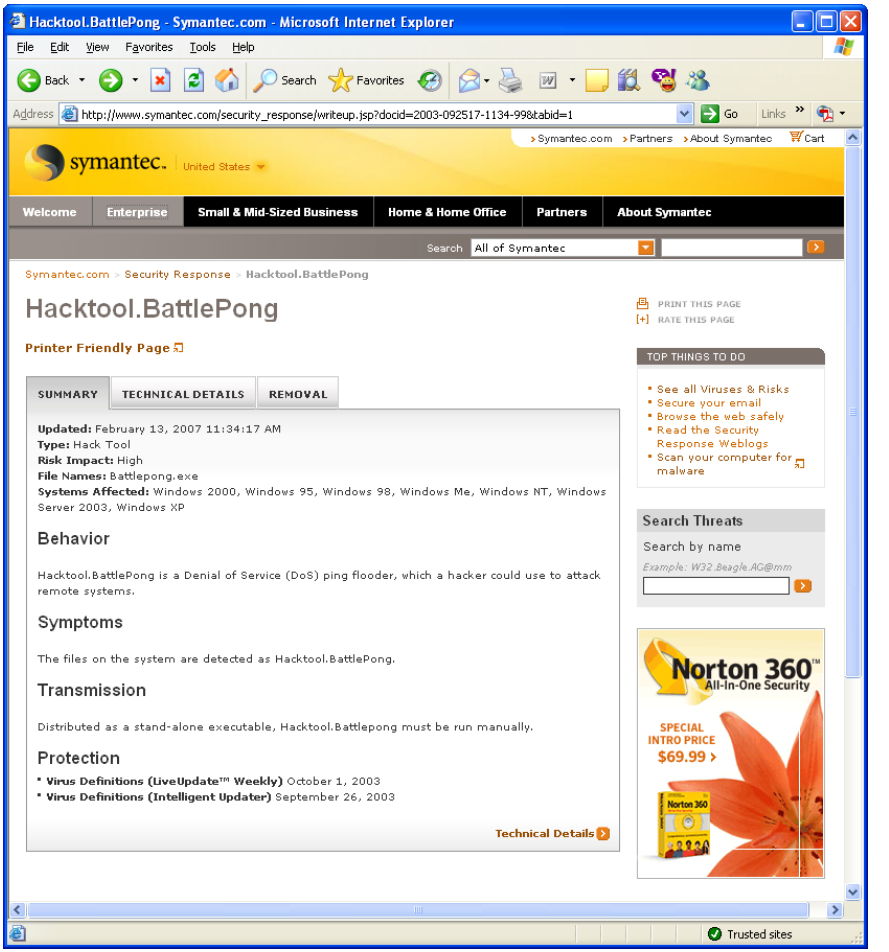
根據預設，防毒和防間諜軟體掃描會進行下列操作：

- 偵測、移除及修復病毒、病蟲、特洛伊木馬程式和混合型威脅所造成的副作用。
- 偵測、移除及修復安全風險所造成的副作用，例如廣告軟體、撥接工具、駭客工具、惡作劇程式、遠端存取程式、間諜軟體、追蹤軟體等等。

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。

圖 5-1 顯示關於駭客工具的資訊，以及賽門鐵克安全機制應變中心建議的處理方式。

圖 5-1 賽門鐵克安全機制應變中心安全風險敘述



用戶端如何回應病毒和安全風險

不管來源為何，用戶端都能保護電腦不受病毒與安全風險的感染。來自硬碟、磁片及網路的病毒和安全風險都將無法入侵電腦。電腦也不會受到經由電子郵件附件或其他方式傳播的病毒與安全風險感染。例如，當您存取網際網路時，安全風險可能會在您不知情的情況下，自行安裝在您的電腦上。

壓縮檔內的檔案也會被掃描，並清除病毒和安全風險。不需針對網際網路型的病毒變更個別的程式或選項。「自動防護」會自動在下載未壓縮的程式與文件檔時，進行掃描。

當用戶端偵測到病毒時，根據預設，用戶端會嘗試從受感染的檔案中清除病毒。用戶端也會嘗試修復病毒的作用。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，用戶端會將受感染的檔案移至隔離所。病毒無法從隔離所擴散感染。

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。

附註：您的管理員可能會選擇自動掃描隔離所中的檔案。

根據預設，用戶端會針對安全風險隔離受感染的檔案。用戶端還會傳回安全風險已變更為先前狀態的系統資訊。部分安全風險無法完全移除，因為會造成您電腦上的其他程式 (如網頁瀏覽器) 執行失敗。您的防毒及防間諜軟體設定可能不會自動處理風險。此時，用戶端會在停止某個程序或重新啟動電腦之前提示您。或者，您可以架構您的設定，對安全風險使用「略過(只記錄)」動作。

當用戶端軟體發現安全風險時，會在掃描視窗中包含一個賽門鐵克安全機制應變中心的連結。在賽門鐵克安全機制應變中心網站，您可以瞭解更多有關安全風險的資訊。您的管理員還可以傳送自訂訊息。

啟用與停用防護元件

您可以在電腦上啟用或停用防護。

停用任何防護時，狀態頁面最上方的狀態列會指出已關閉該防護。您可以按下「修正」選項，來啟用所有停用的防護。或者，分別啟用個別防護。

啟用與停用防毒和防間諜軟體防護

如果您尚未變更預設選項設定，「自動防護」會在您啟動電腦時載入，以阻擋病毒和安全風險。「自動防護」會在程式執行時，檢查其是否有病毒或安全風險。它也會監控您電腦上任何可能指出有病毒或安全風險存在的活動。在偵測到病毒、疑似病毒活動 (疑似由病毒執行的事件)，或安全風險時，「自動防護」會發出警示。

您可以啟用或停用用於檔案及程序的「自動防護」功能。您也可以啟用或停用用於 Internet 電子郵件的自動防護功能，以及用於電子郵件群組軟體應用程式的自動防護功能。在受管環境中，您的管理員可以鎖定這些設定。

當想要停用自動防護的時候

在某些情況下，「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」。請務必在完成工作後啟用「自動防護」以確保電腦繼續受到防護。

如果停用「自動防護」，其他類型的掃描 (排程或開機掃描) 仍會依照您或管理員的架構執行。

管理員可能會鎖定「自動防護」，讓您無法任意停用它。相反地，管理員也可能會指定您可以暫時停用「自動防護」，但在指定的一段時間過了之後，「自動防護」就會自動再次開啟。

關於自動防護以及防毒和防間諜軟體防護狀態

「自動防護」設定會決定用戶端和 Windows 通知區域中的防毒和防間諜軟體防護狀態。

當有任何類型的「自動防護」停用時，防毒和防間諜軟體狀態在狀態頁面上顯示成紅色。

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。

當停用檔案和程序的「自動防護」時，用戶端圖示會顯示常見的禁止符號，即紅色圓圈中間一條斜線。當「檔案系統自動防護」啟用時，圖示會出現綠點。

啟用或停用檔案系統自動防護

您可以啟用或停用「自動防護」監控檔案系統，但前提必須是管理員沒有鎖定設定。

從工作列啟用或停用檔案系統自動防護

- 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**」。

從用戶端啟用或停用檔案系統自動防護

- 在用戶端的「狀態」頁面上，在「防毒和防間諜軟體防護」旁執行下列其中一項動作：
  - 按下「選項」>「啟用防毒和防間諜軟體防護」。
  - 按下「選項」>「停用防毒和防間諜軟體防護」。

啟用或停用電子郵件的自動防護

您可以啟用或停用 Internet 電子郵件、Microsoft Outlook 電子郵件或 Lotus Notes 電子郵件的「自動防護」。您的管理員可能會鎖定這些設定。

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「防毒和防間諜軟體防護」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，勾選或取消勾選「啟用 **Lotus Notes** 自動防護」。

4 按下「確定」。

啟用與停用網路威脅防護

在某些情況下，您可能會想要停用網路威脅防護。例如，您可能想要安裝某個應用程式，但用戶端可能會攔截它時。

您的管理員可能已針對您可以停用防護的時機與時間長短設定了以下限制：

- 用戶端允許所有流量或只允許所有離埠流量。
- 停用防護的時間長度。
- 在重新啟動用戶端之前，可以停用防護的次數。

如果您可以停用防護，就可以隨時重新啟用。管理員也可以隨時啟用或停用防護，而且會覆寫您設定的防護狀態。

請參閱第 91 頁的「關於網路威脅防護」。

請參閱第 107 頁的「攔截攻擊電腦」。

啟用或停用網路威脅防護

◆ 在用戶端中，於「狀態」頁面的「網路威脅防護」旁邊，執行以下其中一項動作：

- 按下「選項」>「啟用網路威脅防護」。
- 按下「選項」>「停用網路威脅防護」。

啟用或停用主動型威脅防護

啟用「掃描特洛伊木馬程式和病蟲」和「掃描按鍵記錄器」等設定時，會啟用「主動型威脅防護」。如果停用兩者其中一項設定，用戶端就會顯示「主動型威脅偵測」狀態為已停用。

請參閱第 81 頁的「關於主動型威脅防護」。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

啟用或停用主動型威脅防護

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「主動型威脅掃描設定」對話方塊的「掃描詳細資料」標籤中，勾選或取消勾選「特洛伊木馬程式及病蟲」下的「掃描特洛伊木馬程式和病蟲」。
4. 在「按鍵記錄器」下，勾選或取消勾選「掃描按鍵記錄器」。
5. 按下「確定」。

用戶端與 Windows 資訊安全中心搭配使用

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

表 5-2 顯示 WSC 中的防護狀態報告。

表 5-2 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「檔案系統自動防護」	關閉 (紅色)
已安裝 Symantec Endpoint Protection，但未啟用「檔案系統自動防護」，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 Rtvscan 已手動關閉	關閉 (紅色)

表 5-3 顯示 WSC 中報告的 Symantec Endpoint Protection 防火牆狀態。

表 5-3 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)

賽門鐵克產品狀況	防火牆狀態
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)
尚未安裝或啟用 Symantec Firewall，但已安裝並啟用協力廠商的防火牆	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。

暫停和延緩掃描

「暫停」功能可讓您在掃描作業的任一階段停止掃描，並在之後恢復掃描。您可以暫停您起始的任何掃描。您的網路管理員可以決定您是否可以暫停管理員排定的掃描。

若是您的網路管理員所起始的排程掃描，也可能允許您延緩掃描。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。恢復掃描時，會從頭開始掃描。

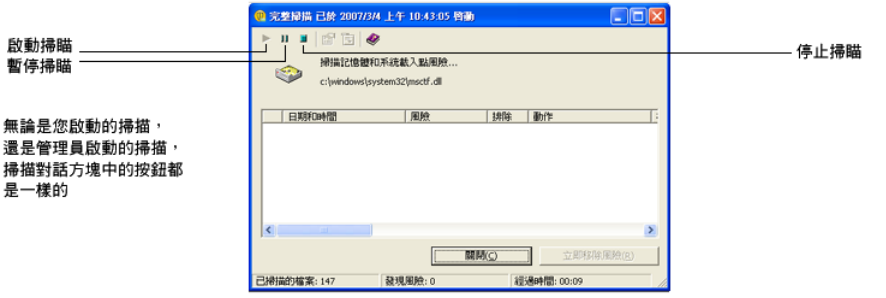
如果您想要在短暫停止之後恢復掃描，可暫停掃描。若延後掃描的時間較長，請使用「延緩」功能。

使用下列程序，可暫停您或管理員起始的掃描。如果無法使用「暫停掃描」選項，表示您的網路管理員已停用「暫停」功能。

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。

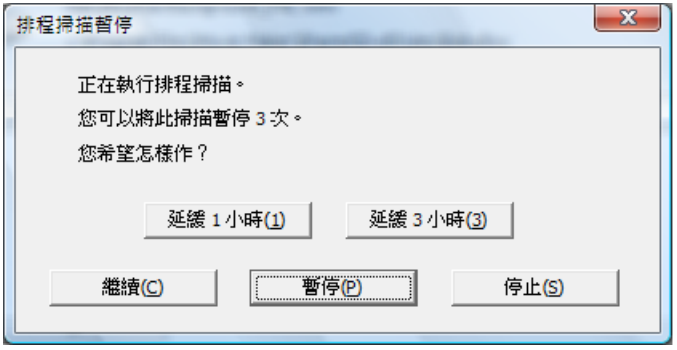
暫停掃描

1 執行掃描時，請在「掃描」對話方塊中，按下「暫停掃描」圖示。



若是您起始的掃描，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，直到您重新啟動掃描為止。

若是您的管理員起始的掃描，則會出現「排程掃描暫停」對話方塊。



2 在「排程掃描暫停」對話方塊中，按下「暫停」。

管理員排定的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，直到您重新啟動掃描為止。

3 在「掃描」對話方塊中，按下「開始掃描」圖示，繼續進行掃描。

延緩管理員排定的掃描

1 執行管理員排定的掃描時，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，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。當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。

6

管理防毒和防間諜軟體防護

本章包含以下主題：

關於防毒和防間諜軟體防護

Symantec Endpoint Protection 用戶端包含適用於多數使用者的預設防毒和防間諜軟體設定。您可以變更設定，自訂安全性網路的設定。您也可以自訂「自動防護」、排程、開機和隨選等各種掃描的政策設定。

防毒和防間諜軟體設定包含下列設定：

- 掃描的項目

- 偵測到病毒或安全風險時要執行什麼動作

關於掃描檔案

防毒和防間諜軟體掃描預設會掃描所有檔案類型。排程、開機及隨選掃描預設也會檢查所有檔案類型。

您可以選擇根據副檔名掃描檔案，但是這會降低病毒和安全風險的防護能力。如果您選取了要掃描的檔案副檔名，即使病毒變更檔案的副檔名，「自動防護」也能判斷檔案的類型。

請參閱第 52 頁的「架構「自動防護」判斷檔案類型」。

您也可以選擇不掃描特定檔案。例如，您可能知道某個檔案不會在掃描時觸發病毒警示。因此您可以設定，後續的掃描不掃描這個檔案。

如果電子郵件應用程式使用的是單一收件匣檔案

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，則您應該建立集中式例外，才不會掃描收件匣檔案。Outlook Express、Eudora、Mozilla 或 Netscape 都是將所有電子郵件儲存在單一收件匣檔案的電子郵件應用程式。您可以架構用戶端來隔離用戶端偵測出的病毒。如果用戶端在收件匣檔案中偵測到病毒，用戶端就會隔離整個收件匣。如果用戶端隔離收件匣，您就無法存取電子郵件。

賽門鐵克一般會建議您對檔案進行掃描。然而，如果不掃描收件匣檔案，開啟電子郵件訊息時，用戶端還是會偵測病毒。開啟電子郵件訊息時，如果用戶端發現病毒，則用戶端會安全地隔離或刪除訊息。

您也可以架構集中式例外，不掃描檔案。

請參閱第 72 頁的「針對防毒和防間諜軟體掃描架構集中式例外」。

關於根據副檔名掃描

用戶端可根據副檔名掃描電腦。

您可以選擇以下類型的檔案副檔名：

文件檔	包括 Microsoft Word 與 Excel 文件，以及與這些文件關聯的範本檔。用戶端會搜尋文件檔是否受巨集病毒感染。
程式檔	包括動態連結程式庫 (.dll)、批次檔 (.bat)、命令檔 (.com)、執行檔 (.exe) 與其他程式檔。用戶端會搜尋程式檔是否受檔案病毒感染。

將檔案副檔名新增至「自動防護」掃描的掃描清單

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。

3 在「防毒和防間諜軟體防護設定」對話方塊的「檔案系統自動防護」標籤上，按下「檔案類型」下的「選取的」。

4 按下「副檔名」。

5 在文字方塊中，輸入要新增的副檔名，然後按下「新增」。

6 若有需要，重複步驟 5。

7 按下「確定」。

將檔案副檔名新增至隨選掃描、排程掃描或開機掃描的掃描清單

1 在用戶端的側邊看板中，按下「掃描威脅」。

2 在要為其新增檔案副檔名的掃描按下滑鼠右鍵，然後選取「編輯」。

這些變更只會套用到您所選取的特定掃描。

3 在「掃描選項」標籤的「檔案類型」下，選取「選取的副檔名」，然後按下「副檔名」。

4 輸入要新增的副檔名，然後按下「新增」。

5 若有需要，重複步驟 4。

6 按下「確定」。

關於掃描所有檔案類型

用戶端可以掃描您電腦中任何副檔名的所有檔案。掃描所有檔案可確保最徹底的防護。相較於依據副檔名掃描，掃描所有檔案較為費時，但是防護病毒及安全風險效果較佳。

關於排除掃描項目

您可以將用戶端架構為排除掃描某個安全風險。您可能會想要排除掃描某個風險。例如，在您工作時，可能需要使用某個廣告軟體。用戶端可能不允許該廣告軟體。如果貴公司的安全性政策是允許廣告軟體，您便可以排除掃描該風險。

用戶端可能會將檔案標記為受感染；但該檔案並沒有病毒。原因可能是，特定的病毒定義設計是用來擷取所有可能的變種病毒。因為病毒定義一定會很廣泛，所以有時用戶端會將未感染病毒的檔案誤判為已受到感染。

如果防毒和防間諜軟體掃描一直將未感染病毒的檔案誤判為受到感染，您可將該檔案從掃描項目中排除。所謂排除項目是指您不希望或不需要進行掃描的項目。

貴公司的安全性政策可能允許您執行用戶端報告為風險的軟體。在這種情況下，您可以排除包含該軟體的資料夾。

使用集中式例外，可排除掃描的項目。例外會套用到所有執行的防毒和防間諜軟體掃描。您的管理員可能也會架構例外。管理員定義的例外，會優先於使用者定義的例外。

請參閱第 72 頁的「針對防毒和防間諜軟體掃描架構集中式例外」。

警告：請謹慎使用排除項目。如果您排除掃描某個檔案，如果該檔案後來遭受感染，用戶端也不會採取清除的動作。而這可能會對您的電腦安全造成潛在的風險。

關於防止巨集病毒感染

用戶端會自動偵測並移除多數 Microsoft Word 與 Excel 巨集病毒。如果定期執行排程掃描，電腦就可以免受巨集病毒感染。「自動防護」也會定期偵測和清除任何偵測到的巨集病毒。

若要最有效防範巨集病毒感染，請執行下列動作：

- 啟用「自動防護」。「自動防護」會持續掃描存取過或修改過的檔案。
- 可以的話，為您的電子郵件執行「自動防護」。
- 停用自動巨集即可保護您的通用範本檔。

Symantec Endpoint Protection 用戶端偵測到病毒或安全風險時

病毒和安全風險感染檔案時，用戶端會以不同的方式回應風險類型。對於各類風險，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。

依預設，用戶端偵測到病毒時，用戶端會先清除受感染檔案中的病毒。然後，如果用戶端無法清除檔案，就會記錄失敗的狀況，並且將受感染的檔案移至「隔離所」。

依預設，用戶端偵測到安全風險時，會將風險隔離。用戶端也會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。

附註：在「隔離所」中，風險不會擴散。如果用戶端將檔案移至「隔離所」，您就無法存取這個檔案。用戶端也可以回復對已隔離項目所造成的變更。

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。

附註：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。

關於自動防護

「自動防護」是防範病毒攻擊的最佳選擇。每當您存取、複製、儲存、移動或開啟檔案時，「自動防護」都會掃描檔案以確保並未感染病毒。

「自動防護」會掃描包含可執行程式碼的檔案副檔名和所有的 .exe 與 .doc 檔。即使病毒變更檔案的副檔名，「自動防護」仍可判斷出該檔案的類型。例如，病毒可能將檔案的副檔名變更為另一種副檔名，而這種副檔名與您架構「自動防護」應掃描的檔案副檔名不同。

如果您的管理員未鎖定設定，您便可以啟用或停用「自動防護」。

請參閱第 39 頁的「啟用與停用防毒和防間諜軟體防護」。

關於自動防護與安全風險

「自動防護」預設會執行下列動作：

- 掃描安全風險，如廣告軟體或間諜軟體
- 隔離受感染的檔案
- 移除或修復安全風險的副作用

您可以停用「自動防護」中的安全風險掃描。

請參閱第 53 頁的「停用與啟用自動防護安全風險掃描及攔截」。

如果「自動防護」偵測到某個程序持續下載安全風險到您的電腦，便會顯示通知並記錄偵測。(「自動防護」必須架構為傳送通知。)如果程序持續下載同一安全風險，則電腦上會顯示多次通知，且「自動防護」會記錄多個事件。為避免多次通知和記錄多個事件，「自動防護」會在偵測到三次時，自動停止傳送關於該安全風險的通知。此外，「自動防護」在偵測到三次後，也會停止記錄該事件。

在某些情況下，「自動防護」不會停止傳送安全風險的通知，也不會停止記錄安全風險事件。

在下列任一情況下，「自動防護」會持續傳送通知和記錄事件：

- 在用戶端電腦上，您或您的管理員可以停用攔截安裝安全風險時 (已啟用預設設定)。
- 對程序下載的安全風險類型所採取的動作含有「略過」動作時。

關於自動防護與電子郵件掃描

「自動防護」也會掃描支援的群組軟體電子郵件用戶端。

它會針對下列電子郵件用戶端提供防護：

- Lotus Notes 4.5x、4.6、5.0 和 6.x

- Microsoft Outlook 98/2000/2002/2003/2007 (MAPI 與 Internet)
- Microsoft Exchange Client 5.0 和 5.5

附註：「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。

「防毒和防間諜軟體防護」也包括藉由監控所有使用 POP3 或 SMTP 通訊協定的流量，掃描其他 Internet 電子郵件程式的「自動防護」。您可以將用戶端軟體架構為掃描內送和外寄訊息是否含有風險。掃描外寄電子郵件有助於防止威脅利用電子郵件用戶端，透過網路自我複製與散佈而達到散播的目的。

附註：64 位元電腦不支援 Internet 電子郵件掃描。

針對 Lotus Notes 與 Microsoft Exchange 電子郵件的掃描，「自動防護」只掃描與電子郵件關聯的附件。

針對使用 POP3 或 SMTP 通訊協定的 Internet 電子郵件掃描，「自動防護」會掃描下列項目：

- 郵件的本文
- 郵件的任何附件

當您開啟夾帶附件的郵件時，只要符合以下陳述，附件就會立即下載到電腦進行掃描：

- 使用 Microsoft Exchange 用戶端或透過 MAPI 的 Microsoft Outlook。
- 已針對電子郵件啟用「自動防護」。

在連線速度慢時，下載夾帶大型附件的郵件會影響電子郵件的效能。如果您經常收到大型附件，您可能會想要停用這項功能。

請參閱第 53 頁的「停用與啟用自動防護安全風險掃描及攔截」。

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。

電子郵件掃描不支援以下的電子郵件用戶端：

- IMAP 用戶端
- AOL 用戶端
- 網頁型電子郵件，例如 Hotmail、Yahoo!Mail 和 GMAIL

停用加密電子郵件連線的「自動防護」處理

您可以透過安全連結來收發電子郵件。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，但不會掃描有加密的郵件。

即使「自動防護」不會掃描使用安全連線的電子郵件，它仍會繼續防護電腦不受附件所含風險的威脅。當您將電子郵件的附件儲存至硬碟機時，「自動防護」會掃描該附件。

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」。

如有必要，您可以停用加密電子郵件的處理。停用這些選項時，「自動防護」會掃描寄出或收到的未加密電子郵件，但會攔截加密電子郵件。如果您重新啟用選項，然後試著傳送加密電子郵件時，只有重新啟動電子郵件應用程式，「自動防護」才不會攔截該電子郵件。

附註：如果您針對「自動防護」停用加密連線，則這項變更會在您登出 Windows 並再次登入後才會生效。如果所做的變更需要立即生效，請登出後再登入。

停用加密電子郵件連線的「自動防護」處理

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「Internet 電子郵件防護」標籤上，按下「進階」。
4. 在「連線設定」下方，取消勾選「允許加密的 **POP3** 連線」及「允許加密的 **SMTP** 連線」。
5. 按下「確定」。

檢視自動防護掃描統計

「自動防護掃描統計」會顯示上一次「自動防護」掃描的狀態、最後一個掃描的檔案，以及病毒感染與安全風險資訊。

檢視自動防護掃描統計

- 在用戶端的「狀態」頁面，按下「防毒和防間諜軟體防護」旁邊的「選項」>「檢視檔案系統自動防護統計」。

檢視風險清單

您可以檢視「防毒和防間諜軟體防護」偵測出的目前風險。這份清單是根據您目前的病毒定義而建立的。

檢視風險清單

- 在用戶端「狀態」頁的「防毒和防間諜軟體防護」旁，按下「選項」>「檢視威脅清單」。

架構「自動防護」判斷檔案類型

「自動防護」預設為掃描所有檔案。只掃描選定副檔名的檔案，可能會更快完成掃描。

例如，您可能只想要掃描下列副檔名：

- .exe
- .com
- .dll
- .doc
- .xls

病毒通常只對某些類型的檔案有影響。但是，如果只掃描特定副檔名，防護力會降低，因為「自動防護」不會掃描所有檔案。預設的副檔名清單代表此類檔案較易受到病毒感染。

「自動防護」會掃描包含可執行程式碼的檔案副檔名和所有的 .exe 與 .doc 檔。即使病毒變更檔案的副檔名，它仍可判斷出該檔案的類型。例如，即使病毒變更了 .doc 檔案的副檔名，它仍可掃描該檔案。

為確保電腦獲得最佳防護，免受病毒和安全風險的威脅，您應該將「自動防護」架構為掃描所有檔案類型。

架構「自動防護」判斷檔案類型

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「檔案系統自動防護」標籤的「檔案類型」下方，執行下列其中一項動作：
   - 按下「所有類型」，掃描所有檔案。
   - 按下「選取的」，只掃描符合副檔名清單的檔案，再按下「副檔名」，變更預設的副檔名清單。
4. 如果選取了「選取的」，請勾選或取消勾選「檢查檔案內容以決定檔案類型」。
5. 按下「確定」。

停用與啟用自動防護安全風險掃描及攔截

「自動防護」預設會執行下列動作：

- 掃描安全風險，如廣告軟體或間諜軟體
- 隔離受感染的檔案
- 嘗試移除或修復安全風險所造成的影響

如果攔截安全風險的安裝並不影響電腦的穩定性，則「自動防護」還是會依據預設攔截安裝。如果賽門鐵克判定攔截安全風險可能會損及電腦穩定性，則「自動防護」會允許安裝該風險。「自動防護」也會立即採取對該風險所架構的動作。

但有時候，您可能暫時需要停用「自動防護」中的安全風險掃描，然後再重新啟用。您可能還需要停用攔截安全風險，以控制「自動防護」回應某些安全風險的時間。

附註：您的管理員可能會鎖定這些設定。

停用與啟用「自動防護」安全風險掃描及攔截

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「檔案系統自動防護」標籤的「選項」下方，執行下列其中一項動作：
   - 勾選或取消勾選「掃描安全風險」。
   - 勾選或取消勾選「攔截安裝安全風險」。
   - 勾選或取消勾選「掃描網路磁碟機上的檔案」。
4. 按下「確定」。

架構網路掃描選項

架構網路掃描包含下列選項：

- 架構「自動防護」是否信任執行「自動防護」之遠端電腦上的檔案。
- 指定電腦是否應該使用快取來儲存「自動防護」掃描來自網路的檔案記錄。

「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。

但是，當您讀取遠端電腦上的檔案時，「自動防護」可能不會掃描這些檔案。「自動防護」預設會嘗試信任「自動防護」的遠端版本。如果兩台電腦都啟用信任選項，則本機「自動防護」會檢查遠端電腦的「自動防護」設定。如果遠端「自動防護」設定提供的安全等級高於或等於本機設定時，本機「自動防護」就會信任遠端「自動防護」。當本機「自動防護」信任遠端「自動防護」時，本機「自動防護」

不會掃描從遠端電腦讀取的檔案。因為，本機電腦相信，遠端「自動防護」已掃描過檔案。

附註：從遠端電腦複製的檔案，本機「自動防護」一律都會掃描。

信任選項會預設啟用。如果您停用信任選項，網路效能可能會降低。

停用信任「自動防護」的遠端版本

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「檔案系統自動防護」標籤上，按下「進階」。
4. 在「自動防護進階選項」對話方塊中，按下「其他進階選項」下方的「網路」。
5. 在「網路掃描設定」下方，取消勾選「信任執行「自動防護」的遠端電腦檔案」。
6. 按下「確定」，直到返回主視窗。

您可以將電腦架構為使用網路快取。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。不重複掃描相同的檔案，系統效能可能會獲得改善。您可以設定「自動防護」掃描並記住的檔案(項目)數目；也可以設定逾時多久之後，讓電腦將項目從快取中移除。只要超過逾時時間，電腦就會移除項目。如果您再次從遠端電腦要求那些檔案，則「自動防護」會再掃描檔案。

架構網路快取

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「防毒和防間諜軟體設定」對話方塊中，按下「檔案系統自動防護」標籤上的「進階」。
4. 在「自動防護進階選項」對話方塊中，按下「其他進階選項」下方的「網路」。
5. 在「網路掃描選項」對話方塊中，勾選或取消勾選「網路快取」。
6. 如果啟用了網路快取，請使用預設值，或執行下列其中一項動作：
   - 使用箭頭或輸入您想要「自動防護」掃描並記住的檔案(項目)數目。
   - 輸入秒數，表示您希望項目保留在快取中的時間，經過這段時間後，電腦再清除快取。
7. 按下「確定」。

進行防毒和防間諜軟體掃描

「自動防護」是最有效的防護機制，可防範病毒感染和安全風險。除了「自動防護」之外，「防毒和防間諜軟體防護」另包括不同類型的掃描，可提供更進一步的防護。

表 6-1 描述可用的掃描

表 6-1 可用的掃描

類型	敘述
自訂掃描	隨時掃描檔案、資料夾、磁碟機或整部電腦。您可以選取電腦中要掃描的部分。
快速掃描	快速掃描系統記憶體，以及經常受病毒和安全風險攻擊的位置。
完整掃描	掃描整部電腦，包括開機磁區和系統記憶體。若要掃描網路磁碟機，可能需輸入密碼。
排程掃描	按照指定頻率自動執行。
開機掃描	您一開啟電腦並登入時執行。
使用者定義	隨時掃描指定的檔案集。

只要啟用「自動防護」，每日快速掃描和每週一次針對所有檔案的排程掃描即可提供充分防護。如果病毒經常攻擊您的電腦，請考慮增加開機完整掃描或每日排程掃描。

您也可以架構搜尋可疑行為而非已知風險的掃描頻率。

請參閱第 84 頁的「架構主動型威脅掃描的執行頻率」。

Symantec Endpoint Protection 用戶端如何偵測病毒和安全風險

用戶端會掃描電腦的開機磁區、記憶體與檔案中是否有病毒與安全風險，防止病毒感染電腦。掃描引擎會利用定義檔中所找到的病毒和安全風險特徵，進行徹底掃描，尋找執行檔中的任何已知病毒。防毒和防間諜軟體掃描會搜尋文件檔的可執行部分，尋找是否有巨集病毒。

您可以手動進行掃描，或是排定在您離開電腦時掃描。

表 6-2 描述用戶端會掃描的電腦元件。

表 6-2 用戶端掃描的電腦元件

元件	敘述
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。
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。

關於定義檔

病毒檔包括任何位元數的程式碼，若被破解，就會顯示某種型樣。這些型樣可在受感染的檔案中追蹤到。型樣也稱為特徵。而廣告軟體或間諜軟體等安全風險，也具有可辨識的特徵。

定義檔包含已知病毒特徵及已知安全風險特徵的清單，但不包括有害的病毒程式碼。掃描軟體會在您電腦的檔案中搜尋是否有列在定義檔中的已知特徵。如果發現符合的病毒型樣，表示該檔案已受到感染。用戶端會使用定義檔判斷造成感染的病毒，並修復其造成的副作用。如果發現安全風險，用戶端會使用定義檔隔離它，並修復其副作用。

新型的病毒和安全風險層出不窮，您應該確保電腦擁有最新的定義檔，應該確保用戶端可偵測並清除最新的病毒和安全風險。

關於掃描壓縮檔

防毒和防間諜軟體掃描會對壓縮檔的內部進行掃描。例如，掃描會對 .zip 檔案中包含的檔案掃描。您的管理員最多可以指定掃描壓縮檔中 10 層深的壓縮檔。請與管理員聯繫，以瞭解所支援的壓縮檔掃描類型。

如果已啟用「自動防護」，則會掃描壓縮檔中的任何檔案。

起始隨選掃描

您可以隨時手動掃描病毒與安全風險，例如廣告軟體與間諜軟體。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「快速掃描」與「完整掃描」。您也可以建立隨選執行的自訂掃描。

請參閱第 60 頁的「建立隨選掃描和開機掃描」。

您可以按下「說明」，取得這個程序中各選項的詳細資訊。

從 Windows 起始掃描

- 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**」。

  此項功能無法在 64 位元作業系統上使用。

在用戶端起始掃描

- 執行下列其中一項動作：
  - 在用戶端「狀態」頁的「防毒和防間諜軟體防護」旁，按下「**選項**」>「**執行快速掃描**」。
  - 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：
    - 在「快速掃描」下，按下「**執行快速掃描**」。
    - 在「完整掃描」下，按下「**執行完整掃描**」。
    - 在掃描清單中，在任何掃描按下滑鼠右鍵，然後按下「**立即掃描**」。
      隨即會開始掃描。電腦會出現進度視窗，顯示掃描的進度和結果。

架構防毒和防間諜軟體掃描

您可以架構數種不同的掃描，保護您的電腦免於病毒與安全風險入侵。

建立排程掃描

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」視窗的掃描清單中。

附註：如果管理員已建立排程掃描，這個掃描就會出現在「掃描威脅」視窗的掃描清單中。

進行排程掃描時，您的電腦必須開啟，而且必須載入「Symantec Endpoint Protection 服務」。依預設，「Symantec Endpoint Protection 服務」會在您開啟電腦時載入。

您可以按下「說明」，取得程序中所使用選項的詳細資訊。

建立已排程的掃描

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「掃描的項目」對話方塊中，選取下列其中一種掃描進行排程：
   - 自訂掃描：掃描電腦上所選取區域是否有病毒和安全風險。
   - 快速掃描：掃描電腦中最常受病毒和安全風險感染的區域。
   - 完整掃描：掃描整部電腦是否有病毒和安全風險。
4. 如果您選取「自訂」，請勾選適當的核取方塊，指定要掃描的位置。

   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。該資料夾或磁碟機內的所有項目亦會被選取。

   
   未選取個別資料夾或磁碟機，但資料夾或磁碟機內的一或多個項目已被選取。

5. 按「下一步」。
6. 在「掃描選項」對話方塊中，您可以選取下列其中一項動作：

- 變更掃描項目的預設設定。
  預設設定為掃描所有檔案。
- 指定偵測出病毒或安全風險時用戶端的回應方式。
  依預設，用戶端會清除受感染檔案中的病毒，然後修復任何副作用。如果用戶端無法移除病毒，就會將檔案隔離。
  依預設，用戶端會隔離安全風險，並移除或修復任何副作用。如果用戶端無法隔離並修復風險，用戶端就會記錄這個事件。

7 在「掃描增強功能」下，勾選任一位置。

8 按下「進階」。

9 您可以設定下列任一選項：

- 壓縮檔選項
- 備份選項
- 對話選項
- 調整選項
- 儲存體移轉選項

10 在「對話選項」下的下拉式清單中，按下「顯示掃描進度」。

11 按下「確定」。

12 在「掃描選項」對話方塊中，您也可以變更下列選項：

- 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。
- 集中式例外：建立安全風險偵測的例外。

13 按「下一步」。

14 在「掃描的時間」對話方塊中，按下「在指定時間」，然後按下「下一步」。

15 在「排程」對話方塊中，指定掃描的頻率和時間。

16 按下「進階」。

17 在「進階排程選項」對話方塊中，執行下列動作：

- 勾選「重試未執行的掃描」。然後設定掃描要在幾小時內執行。例如，您可以設定原本排定時間的三天後，每週對遺漏事件執行一次掃描。
- 勾選或取消勾選「即使沒有任何使用者登入,也執行此掃描」。不管此設定為何，如果使用者已登入，使用者定義的掃描一定會執行。

對於管理型用戶端，管理員可能會覆寫這些設定。

18 按下「確定」。

19 在「排程」對話方塊中，按「下一步」。

20 在「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

21 按下「完成」。

關於建立多重排程掃描

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。

建立隨選掃描和開機掃描

除排程掃描之外，某些使用者在開機或登入時會額外進行自動掃描。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。

附註：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。

「防毒和防間諜軟體防護」也包括「自動產生的快速掃描」這個開機掃描。使用者一登入電腦，自動產生的掃描就會檢查電腦上經常感染的區域。您也可以按照架構任何隨選掃描的方式，編輯這類掃描。然而，您無法停用針對電腦記憶體和其他經常感染區域檔案進行的掃描。

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。

隨選掃描必須手動操作才能起始。

請參閱第 57 頁的「起始隨選掃描」。

您可以按下「說明」，取得程序中所使用選項的詳細資訊。

建立隨選掃描或開機掃描

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 在「掃描的項目」對話方塊中，選取下列其中一種掃描進行排程：

- 自訂

- 快速
- 完整

4 按「下一步」。

5 如果選取「自訂」，請在「選取檔案」對話方塊中，勾選需要掃描的相應檔案和資料夾。

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。該資料夾或磁碟機內的所有項目亦會被選取。

未選取個別資料夾或磁碟機，但資料夾或磁碟機內的一或多個項目已被選取。

6 按「下一步」。

7 在「掃描選項」對話方塊中，您可以選取下列其中一項動作：

- 變更掃描項目的預設設定。
  預設設定為掃描所有檔案。
- 指定偵測出病毒或安全風險時用戶端的回應方式。
  依預設，用戶端會清除受感染檔案中的病毒，然後修復任何副作用。如果用戶端無法移除病毒，就會將檔案隔離。
  依預設，用戶端會隔離安全風險，並移除或修復任何副作用。如果用戶端無法隔離並修復風險，用戶端就會記錄這個事件。

8 在「掃描增強功能」下，勾選任一位置。

9 按下「進階」。

10 在「進階掃描選項」對話方塊中，您可以設定下列任一選項：

- 壓縮檔選項
- 備份選項
- 對話選項
- 調整選項

- 儲存體移轉選項

11 在「對話選項」下的下拉式清單中，按下「顯示掃描進度」，然後按下「確定」。

12 完成架構進階選項之後，按下「確定」。

13 您也可以變更下列選項：

- 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。
- 集中式例外：建立掃描的例外。

14 完成架構掃描選項之後，按下「下一步」。

15 在「掃描的時間」對話方塊中，執行下列其中一個動作：

- 按下「隨選」。
- 按下「啟動時」。

16 在「掃描的時間」對話方塊中，按下「下一步」。

17 輸入掃描的名稱和說明。

例如，將掃描作業稱為：MyScan1

18 按下「完成」。

編輯與刪除開機掃描、使用者定義的掃描與排程掃描

您可以編輯與刪除現有的開機掃描、使用者定義的掃描與排程掃描。如果某些選項無法架構用於特定的掃描類型，就不提供使用。

編輯掃描

1 在用戶端的側邊看板中，按下「掃描威脅」。

2 在「掃描」清單中，在所要編輯的掃描上按下滑鼠右鍵，再按「編輯」。

3 在「掃描的項目」、「掃描選項」和「掃描名稱」標籤上進行所需的變更。

若是排程掃描，您也可以修改排程。

4 按下「確定」。

刪除掃描

1 在用戶端的側邊看板中，按下「掃描威脅」。

2 在「掃描」清單中，在所要編輯的掃描上按下滑鼠右鍵，再按「刪除」。

3 在「確認刪除」對話方塊中，按下「是」。

解譯掃描結果

每當執行隨選掃描、排程掃描、開機掃描或使用者定義的掃描時，用戶端軟體預設會顯示掃描進度對話方塊，以報告進度。此外，「自動防護」可以在每次偵測到病毒或安全風險時，都顯示結果對話方塊。您可以停用這些通知。

在集中管理的網路中，管理員起始的掃描作業可能不會出現在掃描進度對話方塊中。同樣地，您的管理員可能會選擇用戶端偵測到病毒或安全風險時不要顯示結果。

如果用戶端在掃描期間偵測到風險，掃描進度對話方塊會顯示含有下列資訊的結果：

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

根據預設，偵測到病毒或安全風險時會發出通知。

附註：執行用戶端的作業系統語言可能無法解譯病毒名稱中的某些字元。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 病毒名稱可能含有全形字元。這些字元在英文版作業系統上執行用戶端的電腦上，會變成問號。

如果您架構用戶端軟體顯示掃描進度對話方塊，則可以暫停、重新啟動或停止掃描。掃描完成時，結果會顯示在清單中。若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」。

請參閱第 43 頁的「暫停和延緩掃描」。

關於與掃描結果或「自動防護」結果的互動

掃描進度對話方塊和「自動防護」結果對話方塊有類似的選項。如果用戶端需要終止程序或應用程式，或停止服務，「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。

表 6-3 描述選項和結果對話方塊。

表 6-3 結果對話方塊中的選項

按鈕	敘述
立即移除風險	顯示「移除風險」對話方塊。 在「移除風險」對話方塊中，您可以對每個風險選取下列其中一個選項： ■ 是 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。 ■ 否 關閉結果對話方塊時，會出現一個對話方塊。 該對話方塊會提醒您是否仍需採取動作。不過，「移除風險」對話方塊不會顯示，直到您重新啟動電腦。
關閉	如果不必對風險採取任何動作，會關閉結果對話方塊。 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。

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 18 頁的「處理受感染的檔案」。

將防毒和防間諜軟體掃描的資訊傳送至賽門鐵克安全機制應變中心

您指定將「自動防護」或掃描偵測率相關資訊自動傳送至賽門鐵克安全機制應變中心。偵測率的資訊可協助賽門鐵克調整病毒定義更新。偵測率會顯示由客戶偵測出的大部分病毒和安全風險。「賽門鐵克安全機制應變中心」可移除未偵測的特徵，並且將區分的特徵清單提供給有需要的客戶。分割的清單可提升防毒和防間諜軟體掃描的效能。

傳送偵測率預設為啟用。

附註：您的管理員可能會鎖定傳送設定。

您也可以將「隔離所」中的項目傳送至賽門鐵克。

請參閱第 78 頁的「將可能感染病毒的檔案傳送至賽門鐵克安全機制應變中心進行分析」。

將防毒和防間諜軟體掃描的資訊傳送至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「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「傳送」標籤上，勾選「自動傳送防毒和安全風險偵測」。
4. 按下「確定」。

架構對病毒與安全風險執行的動作

您可以架構當 Symantec Endpoint Protection 用戶端偵測到病毒或安全風險時，希望它採取的動作。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掛鎖圖示，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。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

架構對病毒與安全風險執行的動作

1 在「掃描動作」對話方塊的樹狀結構中，選取一個病毒或安全風險類型。

依據預設，每個安全風險子類別都會自動架構為使用整個安全風險類別所設定的動作。

2 若要架構類別或類別中的特定實例使用不同的動作，請勾選「覆寫針對安全風險架構的動作」，然後僅針對該類別設定動作。

3 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。這是要對病毒執行的第一個預設動作設定。

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，會移除受感染檔案中、開機磁區和分割區表中的病毒。 這也可以讓病毒無法擴散，用戶端通常可以及早發現並清除病毒，不會使其對您的電腦造成損害。 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。

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。

刪除風險

從電腦硬碟機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及安全風險感染的備份副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)」作為對巨集與非巨集病毒執行的第二個動作。

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，則可能會想要使用此動作。 其他動作可能是將檔案移到「隔離所」。

若是安全風險，受感染檔案會維持不變，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。 這是對安全風險執行的第二個預設動作設定。

您的管理員可能會送出自訂訊息，說明應該如何回應。

請參閱第 68 頁的「對病毒指派第二個動作的秘訣」。

請參閱第 69 頁的「對安全風險指派第二個動作的秘訣」。

4 您可以針對您想要設定特定動作的每個類別，重複步驟 1 與 3。

5 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。

6 按下「確定」。

對病毒指派第二個動作的秘訣

當您選取病毒的第二個動作時，請考慮以下事項：

電腦上檔案的管理方式

如果您將重要的檔案儲存在電腦而未備份，就不應該使用「刪除風險」動作。雖然用這方式可刪除病毒，但也可能損失重要資料。

另一個應該考量的事項是系統檔案。病毒通常攻擊可執行檔。您可使用「忽略 (只記錄)」或「隔離風險」動作，來檢查哪些檔案已受感染。例如，病毒可能攻擊Command.com。如果用戶端無法清除感染，您可能會無法還原檔案。該檔案對於系統很重要。您可以使用「忽略」動作，以確保可以存取檔案。

感染您電腦的病毒類型	不同病毒類型的目標會鎖定您電腦中不同的區域來感染。開機病毒會感染開機磁區、分割區表、主要開機記錄，有時是感染記憶體。當開機型病毒分成多個部分時，也可能會感染執行檔，而且這種感染的處理方式與檔案型病毒類似。 檔案型病毒通常會感染具有.exe、.com 或 .dll 副檔名的執行檔。 巨集病毒會感染文件檔以及與這些文件關聯的巨集。 依照您可能需要復原的檔案類型來選取動作。
在電腦上執行的掃描類型	所有的掃描會在沒有您的同意下，自動執行動作。如果您在掃描之前沒有變更動作，將會使用預設的動作。因此，預設的第二個動作是設計用來提供您控制病毒爆發情形的能力。 若是自動執行的掃描，例如， 排程掃描和「自動防護」掃描， 請勿指派具有永久效果的第二個動作。例如，您可能會在已知檔案受感染時，執行隨選掃描。您可以將「刪除風險」和「清除風險」動作限制為此類隨選掃描。

對安全風險指派第二個動作的秘訣

當您針對安全風險選取第二個動作時，請考量您對檔案所需的控制程度。如果您將重要的檔案儲存在電腦而未備份，就不應該使用「刪除風險」動作。儘管用此方式可以刪除安全風險，但這可能會造成電腦上其他應用程式無法運作。改用「隔離風險」動作，可在必要時，復原用戶端所做的變更。

關於風險影響等級

賽門鐵克會評估安全風險，判斷它們會在電腦上造成多大的影響。

以下因素的等級有低、中或高：

- 隱私權影響
- 效能影響
- 隱密性
- 移除難度

等級低的因素，表示影響輕微。等級中的因素，表示有些影響。等級高的因素，表示在該區域影響顯著。如果某個特定的安全風險尚未評估，則使用預設等級。如果安全風險已經過評估，但某個特定的因素並不適用於這個風險，則使用等級「無」。

當您針對已知安全風險架構集中式例外時，這些等級會顯示在「安全風險例外」對話方塊中。您可以使用這些等級來判斷要排除掃描哪些安全風險，允許保留在電腦上。

表 6-4 描述等級因素，以及高等級對每個因素所代表的意義。

表 6-4 風險影響因素

等級因素	敘述
隱私權影響	考量安全風險存在電腦中時會造成的隱私權損失程度。 高等級表示個人或其他機密資訊可能遭竊。
效能影響	考量安全風險會降低電腦效能的程度。 高等級表示效能嚴重降低。
隱密性等級	考量判斷出安全風險是否存在於電腦上的容易程度。 高等級表示安全風險會嘗試隱藏其存在。
移除等級	考量將安全風險從電腦中移除的困難度。 高等級表示該風險不容易移除。
整體等級	整體等級是其他因素的平均值。此等級表示是否有其他應用程式賴此安全風險才能正常運作。
相依程式	此等級表示是否有其他應用程式賴此安全風險才能正常運作。

架構病毒與安全風險的通知

根據預設，當掃描發現病毒或安全風險時，會發出通知。此外，當掃描軟體需要終止服務或停止程序時，也預設會發出通知。掃描軟體可能也需要移除或修復病毒或安全風險的作用。

您可以為掃描架構下列的通知：

偵測選項
: 撰寫當用戶端在您的電腦上發現病毒或安全風險時，您要顯示的訊息。

  架構「檔案系統自動防護」時，可以選取顯示對話方塊的額外選項。 該對話方塊會包含「自動防護」在您電腦發現風險的結果。

矯正選項
: 架構用戶端發現病毒或安全風險時，是否發出通知。也可以在用戶端需要終止程序或停止服務以便移除或修復風險時，先發出通知。

您可以撰寫您希望在電腦上顯示的偵測訊息。若要撰寫訊息，請直接輸入訊息欄位。您可以在訊息欄位中按滑鼠右鍵，來選取要放入訊息的變數。

表 6-5 描述在通知訊息中可用的變數欄位。

表 6-5 訊息變數欄位

欄位	敘述
VirusName	發現的病毒或安全風險名稱。
ActionTaken	用戶端偵測到病毒或安全風險時，所執行的動作。此動作可為架構的第一或第二個動作。
Status	檔案的狀態：「受感染」、「未感染」或「已刪除」。 系統預設不使用這個訊息變數。若要顯示此資訊，請手動將此變數加入訊息中。
Filename	受病毒或安全風險感染的檔案名稱。
PathAndFilename	感染病毒或安全風險之檔案的完整路徑及名稱。
Location	病毒或安全風險所在的電腦磁碟機。
Computer	病毒或安全風險所在的電腦名稱。
User	出現病毒或安全風險時登入的使用者名稱。
Event	事件的類型，例如「發現風險」。
LoggedBy	偵測病毒或安全風險的掃描類型。
DateFound	發現病毒或安全風險的日期。
StorageName	應用程式受影響的區域，如「檔案系統自動防護」或「Lotus Notes 自動防護」。
ActionDescription	偵測到病毒或安全風險後所採取回應動作的完整敘述。

您可以針對使用者定義的掃描和「自動防護」架構通知。通知架構包括矯正選項。矯正選項僅適用於掃描和「檔案系統自動防護」。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

架構病毒與安全風險的通知

1 執行下列其中一項動作：

- 若是新的掃描，請在「掃描選項」對話方塊中，按下「通知」。
- 若是現有的掃描，請在「掃描選項」標籤上，按下「通知」。

- 若是「自動防護」，請在「防毒和防間諜軟體防護設定」對話方塊中，按下任一「自動防護」標籤上的「通知」。

2 在「掃描通知選項」對話方塊的「偵測選項」下方，勾選「在偵測出安全風險時顯示通知訊息」。如果希望在掃描發現病毒或安全風險時，您的電腦上就會顯示訊息，請勾選此選項。

3 在訊息方塊中，執行下列任何或全部動作來建立您要的訊息：

- 按下即可輸入或編輯文字。
- 按下滑鼠右鍵，按下「插入欄位」，然後選取要插入的變數欄位。
- 按下滑鼠右鍵，然後選取「剪下」、「複製」、「貼上」、「清除」或「復原」。

4 若是「自動防護」架構，請勾選或取消勾選「顯示自動防護結果對話方塊」。

此參數會顯示或隱藏含有「檔案系統自動防護」發現病毒和安全風險時執行結果的對話方塊。

5 在「矯正選項」下方，勾選您要針對掃描或「檔案系統自動防護」設定的選項。可用選項如下：

自動終止程序	將掃描架構為，需要終止程序才能移除或修復病毒或安全風險時， 自動終止程序。掃描終止程序之前，系統不會提示使用者儲存資料。
自動停止服務	將掃描架構為，需要停止服務才能移除或修復病毒或安全風險時，自動停止服務。 掃描停止服務之前， 系統不會提示使用者儲存資料。

6 按下「確定」。

針對防毒和防間諜軟體掃描架構集中式例外

集中式例外是指您要排除掃描的項目，如特定安全風險或特定檔案。通常您不必建立例外。

您的管理員可能已經針對受管用戶端建立掃描的集中式例外。您可檢視管理員定義的例外，但無法修改。如果您建立的集中式例外與管理員定義的例外衝突，則會優先採取管理員定義的例外。

此程序說明從「變更設定」頁面架構集中式例外。您也可以在建立或修改隨選掃描、排程掃描或開機掃描時，或在修改「自動防護」設定時，架構例外。例外會套用到所有防毒和防間諜軟體掃描。如果您在建立或編輯特定掃描時，架構例外，該例外會套用到所有防毒和防間諜軟體掃描。

附註：您也可以針對主動型威脅掃描架構集中式例外。

如需有關這些程序中使用選項的更多資訊，您可以按下「說明」。

排除掃描安全風險

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「集中式例外」旁，按下「架構設定」。
3. 在「集中式例外」對話方塊的「使用者定義例外」標籤上，按下「新增」>「安全風險例外」>「已知風險」。
4. 在「新增已知安全風險例外」對話方塊中，勾選您要排除掃描的安全風險。
5. 若要記錄偵測到或略過安全風險時的事件，請勾選「偵測到安全風險時記錄」。
6. 按下「確定」。
7. 在「集中式例外」對話方塊中，按下「關閉」。

排除掃描檔案

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「集中式例外」旁，按下「架構設定」。
3. 在「集中式例外」對話方塊的「使用者定義例外」標籤上，按下「新增」>「安全風險例外」>「檔案」。
4. 在「新增安全風險檔案例外」對話方塊中，選取檔案或輸入要排除的檔名，再按下「新增」。
5. 在「集中式例外」對話方塊中，按下「關閉」。

排除掃描資料夾

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「集中式例外」旁，按下「架構設定」。
3. 在「集中式例外」對話方塊的「使用者定義例外」標籤上，按下「新增」>「安全風險」>「資料夾」。
4. 在「新增安全風險資料夾例外」對話方塊中，選取資料夾，或輸入要排除的資料夾名稱。
5. 若要排除選定資料夾的子資料夾，請勾選「包括子資料夾」。
6. 選取您要排除的資料夾，然後按下「新增」。
7. 在「集中式例外」對話方塊中，按下「關閉」。

排除掃描副檔名

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「集中式例外」旁，按下「架構設定」。
3. 在「集中式例外」對話方塊的「使用者定義例外」標籤上，按下「新增」>「安全風險例外」>「副檔名」。
4. 在「新增安全風險副檔名例外」對話方塊中，輸入要排除的副檔名。

   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。
5. 按下「新增」。
6. 重複步驟 4 到步驟 5，新增更多副檔名。
7. 在「集中式例外」對話方塊中，按下「關閉」。

關於隔離所

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。您可能會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。「隔離所」可將電腦上可能受感染的檔案安全地予以隔離。隔離病毒之後，病毒便不會散播到您的電腦或網路上的其他電腦。

關於隔離所中受感染的檔案

您可以檢視隔離所中受感染的檔案。

您可以檢視檔案的下列資訊：

- 風險
- 檔案名稱
- 類型
- 原始位置
- 狀態
- 日期

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。

當用戶端將受感染的檔案移至「隔離所」時，病毒風險便不會自我複製，也不會感染其他檔案。這個動作是針對巨集與非巨集病毒感染所建議的第二個動作。

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。病毒和巨集病毒都可以隔離。開機病毒無法隔離。開機型病毒通常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」。

您也可以檢視受感染檔案的屬性。

請參閱第 76 頁的「在隔離所中檢視檔案及檔案的細節」。

關於處理隔離所中受感染的檔案

在檔案移至「隔離所」之後，您可以執行下列任一動作：

- 將選取的檔案還原至它的原始位置。
- 永久刪除選取的檔案。
- 收到更新病毒定義之後，重新掃描檔案。
- 將「隔離所」的內容匯出為逗號分隔 (*.csv) 檔案或 Access 資料庫 (*.mdb) 檔案。
- 手動新增檔案至「隔離所」。您可以瀏覽要移至「隔離所」的檔案位置，並選取檔案。
- 將檔案傳送至賽門鐵克安全機制應變中心。按照畫面精靈的指示，傳送選取的檔案進行分析。

請參閱第 75 頁的「管理隔離所」。

關於處理受到安全風險感染的檔案

您可以將因為安全風險而隔離的檔案留置在「隔離所」中，也可以將這些檔案刪除。您應該將它們留在「隔離所」中，直到確定電腦上的應用程式未遺失任何功能為止。

如果您刪除與安全風險有關的檔案，電腦上的某個應用程式可能無法正常運作。應用程式可能需要您刪除的相關檔案。「隔離所」是較安全的選項，因為它可以被回復。若電腦上的任何應用程式在隔離相關的程式檔案之後便無法正常運作，則您可以將檔案還原。

附註：成功執行應用程式之後，您可能需要刪除檔案，以節省磁碟空間。

管理隔離所

檔案置入「隔離所」的方式有下列數種：

- 用戶端會根據其架構，將進行「自動防護」或掃描作業時所偵測到的受感染項目移至「隔離所」。
- 您可以手動選取某一個檔案，並將其加入至「隔離所」。

「自動防護」和所有掃描類型的預設選項是，偵測到時，將受感染檔案中的病毒清除。如果無法清除檔案，掃描軟體則會將檔案置入「隔離所」。若是安全風險，其預設選項是將受感染的檔案放置在「隔離所」中，並修復安全風險所造成的副作用。

手動將檔案加入至「隔離所」

1. 在用戶端的側邊看板中，按下「檢視隔離所」。
2. 按下「新增」。
3. 選取要新增至隔離所的檔案，然後按下「新增」。

在隔離所中檢視檔案及檔案的細節

您可以檢視已置入「隔離所」的檔案。您可以檢視檔案的詳細資訊。這些詳細資訊包含病毒名稱，以及發現檔案的所在電腦名稱。

在隔離所中檢視檔案及檔案的細節

1. 在用戶端的側邊看板中，按下「檢視隔離所」。
2. 在您想要檢視的檔案上按下滑鼠右鍵，然後按下「屬性」。

重新掃描隔離所內的檔案是否有病毒

如果有檔案被移入「隔離所」，請即更新您的定義。更新定義時，可能會自動掃描、清除或還原「隔離所」中的檔案。如果出現「修復精靈」，則您可以重新掃描「隔離所」中的檔案。

重新掃描「隔離所」中的檔案之後，如果用戶端仍然無法移除病毒，則您可以將受感染的檔案傳送至賽門鐵克安全機制應變中心進行分析。

請參閱第 78 頁的「將可能感染病毒的檔案傳送至賽門鐵克安全機制應變中心進行分析」。

使用「修復精靈」重新掃描「隔離所」中的檔案

1. 如果出現「修復精靈」，請按下「是」。
2. 按「下一步」。

   按照畫面指示，重新掃描「隔離所」中的檔案。

手動重新掃描檔案

您可以手動重新掃描「隔離所」內的檔案是否有病毒，但不能重新掃描是否有安全風險。

手動重新掃描「隔離所」中的檔案是否有病毒

1. 更新您的定義。
2. 在用戶端的側邊看板中，按下「檢視隔離所」。
3. 選取檔案，然後按下「全部重新掃描」。

當修復的檔案無法放回原來的位置

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。

從「隔離所」釋放已除毒的檔案

1. 在用戶端的側邊看板中，按下「檢視隔離所」。
2. 在已修復的檔案上按下滑鼠右鍵，然後按下「還原」。
3. 指定已除毒檔案的位置。

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。您也可以設定自動刪除檔案的時間週期。

請參閱第 78 頁的「自動從隔離所刪除檔案」。

手動清除備份項目

1. 在用戶端的側邊看板中，按下「檢視隔離所」。
2. 選取一或多個備份檔。
3. 按下「刪除」。

從隔離所刪除檔案

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。

從「隔離所」手動刪除檔案

1. 在用戶端的側邊看板中，按下「檢視隔離所」。
2. 選取一或多個檔案。
3. 按下「刪除」。

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。

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」。

   在架構的時間過期之後，用戶端會刪除檔案。
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」。

將可能感染病毒的檔案傳送至賽門鐵克安全機制應變中心進行分析

有時候，用戶端可能無法清除檔案中的病毒。或者，您可能認為檔案受到感染，但是用戶端卻未偵測出感染狀況。如果您將檔案傳送到 Symantec Security Response

(賽門鐵克安全機制應變中心)，他們可以分析您的檔案，以確認是否受到感染。您必須具有網際網路連線，才能傳送樣本。

附註：如果管理員停用這些類型的傳送，則「提交至賽門鐵克安全機制應變中心」選項將無法使用。

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。

7

管理主動型威脅防護

本章包含以下主題：

關於主動型威脅防護

「主動型威脅防護」可提供零時差攻擊防護。零時差攻擊防護是指可以防範不明威脅或漏洞。「主動型威脅防護」可以掃描電腦中疑似惡意行為的作用中程序。由於不明威脅沒特徵可加以識別，因此主動型威脅掃描會標示可疑的行為，識別潛在的風險。

預設的「主動型威脅防護」掃描設定適用於多數的使用者。您可以變更設定，以因應電腦所需的啟發式防護層級。

變更「主動型威脅防護」設定之前，您應該先考慮下列問題：

- 電腦出現威脅時您是否需要收到相關資訊？
- 您需要掃描程序的頻率和時間為何？
- 您希望分配多少電腦資源給「主動型威脅防護」？

附註：如果管理員並未鎖定主動型威脅掃描設定，您就可以架構設定。鎖定的設定會用上鎖的掛鎖圖示表示。鎖定的設定標籤是灰色的。

關於主動型威脅掃描

主動型威脅掃描不同於防毒和防間諜軟體掃描。主動型威脅掃描會檢查出現可疑行為的特定程序或應用程式類型。

主動型威脅掃描會偵測疑似特洛伊木馬程式、病蟲或按鍵記錄器的程序。您可以啟用或停用偵測。

除了特洛伊木馬程式、病蟲和按鍵記錄器之外，主動型威脅掃描也會偵測疑似廣告軟體和間諜軟體的程序。您無法架構主動型威脅掃描處理這些偵測類型的方式。如果主動型威脅掃描偵測到廣告軟體或間諜軟體，而您需要允許這些軟體出現在用戶端電腦上，則您或管理員應該建立集中式例外。

請參閱第 88 頁的「架構主動型威脅掃描的集中式例外」。

主動型威脅掃描也會偵測常見的惡意用途商用應用程式。賽門鐵克會整理一份清單列出這類商用應用程式，並且會定期更新這份清單。這類應用程式包括會監控或記錄使用者按鍵輸入的商用應用程式，以及遠端控制使用者電腦的商用應用程式。您可以設定 Symantec Endpoint Protection 處理這類偵測結果的方式。

表 7-1 會描述主動型威脅掃描所偵測的程序。

表 7-1 主動型威脅掃描所偵測的程序

程序類型	敘述
特洛伊木馬程式和病蟲	疑似特洛伊木馬程式或病蟲特徵的程序。 主動型威脅掃描會使用啟發式掃描，搜尋疑似特洛伊木馬程式或病蟲的程序。這些程序不一定是威脅。
按鍵記錄器	疑似按鍵記錄器特徵的程序。 主動型威脅掃描會偵測商用按鍵記錄器，但是也會偵測疑似按鍵記錄器行為的不明程序。
商用應用程式	可能用於惡意用途的已知商用應用程式。 主動型威脅掃描會偵測各種類型的商用應用程式。您可以架構兩種類型的動作：按鍵記錄器和遠端控制程式。
廣告軟體和間諜軟體	疑似廣告軟體和間諜軟體特徵的程序 主動型威脅掃描會使用啟發式掃描，偵測疑似廣告軟體和間諜軟體的不明程序。這些程序不一定是風險。

關於主動型威脅掃描的例外

除非您的管理員鎖定了集中式例外設定，否則您可以為主動型威脅掃描建立一些例外。

您的管理員也可以為主動型威脅掃描建立集中式例外。但是您不能修改管理員建立的例外。

請參閱第 88 頁的「架構主動型威脅掃描的集中式例外」。

關於主動型威脅掃描偵測

主動型威脅掃描會記錄、隔離或終止偵測出的潛在惡意程序。從掃描結果對話方塊、「主動型威脅防護」日誌或「隔離所」清單，您可以檢視偵測的結果。

請參閱第 63 頁的「關於與掃描結果或「自動防護」結果的互動」。

請參閱第 75 頁的「管理隔離所」。

請參閱第 128 頁的「檢視日誌及日誌詳細資料」。

附註：主動型威脅掃描設定不會影響防毒和防間諜軟體掃描，因為掃描是使用特徵偵測已知風險。Symantec Endpoint Protection 會先偵測已知的風險。

依預設，用戶端會進行下列動作：

- 記錄偵測出的常見商用應用程式
- 記錄偵測出的行為疑似特洛伊木馬程式、病蟲或按鍵記錄器的程序
- 隔離疑似特洛伊木馬程式、病蟲或按鍵記錄器行為的程序，並隔離需要矯正的程序

主動型威脅掃描隔離偵測結果時，也會一併處理程序的任何副作用。內容更新下載至電腦之後，如果用戶端重新掃描偵測結果，用戶端或許能夠將程序還原至電腦。如果程序不再被視為惡意行為，用戶端就會還原程序。用戶端也會還原程序的所有副作用。然而，用戶端不會自動重新啟動程序。

如果是商用按鍵記錄器或遠端控制應用程式的偵測結果，您或管理員可以指定不同的動作。例如，您可以忽略商用按鍵記錄器的偵測結果。用戶端忽略應用程式時，會允許應用程式，而不會記錄偵測結果。

如果偵測到特洛伊木馬程式、病蟲或按鍵記錄器，您可以指定特定動作，讓用戶端偵測到結果時都使用這個動作。

關於處理誤報

主動型威脅掃描有時候會有偵測誤報。這些掃描會搜尋可疑行為的應用程式和程序，不會搜尋已知的病毒或安全風險。一般而言，這些掃描通常會標示不需要偵測的項目。

如果主動型威脅掃描偵測到您認為不算問題的程序，您可以建立例外，這樣日後掃描時就不會再標示這些程序。如果使用者定義的例外和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。

請參閱第 88 頁的「架構主動型威脅掃描的集中式例外」。

若要盡量減少誤報的偵測結果，請確定賽門鐵克的主動型威脅掃描內容是最新的。版本會出現在「主動型威脅防護」的「狀態」頁中。您可以執行LiveUpdate，下載最新的內容。

附註：管理員可排程自動更新。

如果您選擇自行管理特洛伊木馬程式、病蟲和按鍵記錄器的偵測，可以變更主動型威脅掃描的靈敏度。然而，變更靈敏度可能不會變更誤報的數量，只會變更偵測到的總數量。

請參閱第 84 頁的「管理主動型威脅偵測」。

架構主動型威脅掃描的執行頻率

您可以架構主動型威脅掃描的執行頻率。

附註：增加主動型威脅掃描的執行頻率，可能會影響電腦效能。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

架構主動型威脅掃描的執行頻率

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「主動型威脅掃描設定」對話方塊的「掃描頻率」標籤上，勾選「使用自訂掃描頻率」。
4. 執行下列其中一項或多項動作：
   - 在「掃描間隔」旁邊，設定掃描程序間隔的時間長度，單位是天數、時數和分鐘數。
   - 勾選「立即掃描新程序」，可在偵測到新程序時，立即加以掃描。

管理主動型威脅偵測

管理員可能會鎖定主動型威脅偵測設定。如果您的設定沒有鎖定，或者您正在執行非受管用戶端，就可以架構主動型威脅偵測要偵測的程序類型。

附註：目前不支援在 Windows 伺服器作業系統上偵測特洛伊木馬程式、病蟲及按鍵記錄器。在執行伺服器作業系統的用戶端上，掃描選項無法使用。如果您的管理員在政策中修改這些選項，然後將政策套用到您的電腦，則選項可能會顯示為勾選但無法使用。

啟用特洛伊木馬程式、病蟲或按鍵記錄器偵測時，您可以選擇如何管理偵測。根據預設，主動型威脅掃描使用Symantec預設值。這表示用戶端會決定偵測的動作(未出現在使用者介面上的預設值不會反映 Symantec 預設值。當您手動管理偵測時，無法使用的設定才會反映您使用的預設設定)。

一般來說，Symantec 預設設定即是處理偵測的最佳方式。不過，若您熟悉電腦上的掃描結果，可能會想手動架構動作和靈敏度等級。若要架構這些參數，請停用 Symantec 預設值選項。

為將誤報偵測減至最少，賽門鐵克建議您一開始使用賽門鐵克管理的預設值。等過了一段時間，您可以觀察用戶端偵測的誤報數。如果數目很少，您可以逐步調整主動型威脅掃描設定。例如，對於特洛伊木馬程式和病蟲偵測，您可以將靈敏度滑桿調得比預設值高些。在設定新架構之後，您可以再觀察主動型威脅掃描的結果。

附註：若為受管用戶端，您的管理員通常會架構適合您電腦的主動型威脅掃描設定。

對於商用應用程式，您可以指定主動型威脅掃描偵測到商用按鍵記錄器或商用遠端控制程式時，要採取的動作類型。您可以變更這些設定，而不論特洛伊木馬程式、病蟲或按鍵記錄器的架構為何。

指定主動型威脅掃描偵測的程序類型

您可以架構主動型威脅掃描是否掃描特洛伊木馬程式、病蟲或按鍵記錄器。管理員可能會鎖定其中某些設定。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

指定主動型威脅掃描偵測的程序類型

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「主動型威脅掃描設定」對話方塊的「掃描詳細資料」標籤中，勾選或取消勾選「特洛伊木馬程式及病蟲」下的「掃描特洛伊木馬程式及病蟲」。
4. 在「按鍵記錄器」下，勾選或取消勾選「掃描按鍵記錄器」。
5. 按下「確定」。

指定偵測特洛伊木馬程式、病蟲和按鍵記錄器的動作和靈敏度等級

如果您選擇自行管理特洛伊木馬程式、病蟲和按鍵記錄器的偵測作業，則可以架構當偵測到這些程序時所要採取的動作。主動型威脅掃描偵測時，一律都會使用該動作。例如，您可能將動作設為「只記錄」。如果主動型威脅掃描偵測到某個程序，並將之歸類為真陽性時，用戶端就會記錄該偵測，而不會隔離該程序。

您還可以設定不同的靈敏度等級，來偵測特洛伊木馬程式、病蟲和按鍵記錄器。靈敏度等級會決定主動型威脅掃描在掃描程序時要多靈敏。靈敏度越高，能夠偵測更多。請記得，這些偵測當中，有些可能是誤判。靈敏度等級的高低可能不會改變主動型威脅掃描所產生的誤報率。只會影響偵測總數量。

在電腦上尚未看到主動型威脅掃描的結果之前，您可能會想先維持較低的靈敏度等級。如果靈敏度等級較低時，主動型威脅掃描無法產生任何偵測，則可以增加靈敏度。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

針對特洛伊木馬程式和病蟲設定動作和靈敏度等級

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「主動型威脅掃描設定」對話方塊中，於「掃描詳細資料」標籤的「特洛伊木馬程式及病蟲」下方，確定已勾選「掃描特洛伊木馬程式及病蟲」，然後取消勾選「使用賽門鐵克定義的預設值」。
4. 在「靈敏度」右方，左右移動滑桿，以分別降低或增加靈敏度。
5. 在下拉式清單中，選取「記錄」、「終止」或「隔離」。
6. 按下「確定」。

針對按鍵記錄器設定動作和靈敏度等級

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「主動型威脅掃描設定」對話方塊中，於「掃描詳細資料」標籤的「按鍵記錄器」下方，確定已勾選「掃描按鍵記錄器」，然後取消勾選「使用賽門鐵克定義的預設值」。
4. 選取「低」或「高」，來設定靈敏度等級。
5. 在下拉式清單中，選取「記錄」、「終止」或「隔離」。
6. 按下「確定」。

設定偵測到商用應用程式時採取的動作

您可以變更主動型威脅掃描偵測到特定類型的商用應用程式時，用戶端要採取的動作。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

設定偵測到商用應用程式時採取的動作

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「主動型威脅防護」旁，按下「架構設定」。
3. 在「主動型威脅掃描設定」對話方塊的「掃描詳細資料」標籤上，在「商用應用程式」底下執行下列任何動作：
   - 設定商用按鍵記錄器的動作為「記錄」、「終止」、「隔離」或「略過」。
   - 設定商用遠端控制應用程式的動作為「記錄」、「終止」、「隔離」或「略過」。
4. 按下「確定」。

架構主動型威脅掃描偵測的通知

您可以架構當主動型威脅掃描偵測到威脅時顯示訊息。依預設，用戶端在偵測時會顯示訊息。當偵測需要用戶端終止服務或停止程序時，也會通知您。

附註：您的管理員可以鎖定這些設定。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

啟用或停用主動型威脅掃描偵測的通知

1. 在用戶端中，按下「變更設定」。
2. 在「主動型威脅防護」旁，按下「架構設定」。
3. 在「主動型威脅掃描設定」對話方塊的「通知」標籤上，勾選「偵測到時顯示訊息」。
4. 勾選或取消勾選「終止程序前提示」和「停止服務前提示」。
5. 按下「確定」。

將主動型威脅掃描相關資訊傳送至賽門鐵克安全機制應變中心

依預設，主動型威脅掃描會將偵測到的程序的資訊傳送至賽門鐵克安全機制應變中心。掃描傳送資訊之後，賽門鐵克會分析資訊，判斷威脅是否確實存在。如果賽門鐵克判斷威脅確實存在，就會產生解決威脅的特徵。賽門鐵克的更新版定義會提供特徵。

傳送程序的資訊時，會傳送下列資訊：

- 執行檔的路徑
- 執行檔
- 涉及威脅的檔案和登錄檔載入點的相關資訊
- 內部狀態資訊
- 主動型威脅掃描使用的內容版本

不會傳送任何識別電腦的個人資訊。

將主動型威脅掃描偵測傳送至賽門鐵克安全機制應變中心的功能依預設為啟用。

附註：您的管理員可能會鎖定傳送設定。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

啟用或停用傳送資訊至賽門鐵克安全機制應變中心的功能

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「防毒和防間諜軟體防護」旁，按下「架構設定」。
3. 在「防毒和防間諜軟體防護設定」對話方塊的「傳送」標籤，勾選或取消勾選「自動傳送主動型威脅掃描偵測」。
4. 按下「確定」。

架構主動型威脅掃描的集中式例外

您可以建立主動型威脅掃描的例外，但前提必須是管理員沒有鎖定設定。

若要建立例外，請選取目前電腦上的一個檔案。當主動型威脅掃描偵測到有作用中的程序使用該檔案時，用戶端會套用您在例外中指定的動作。

例如，您可能在電腦上執行的應用程式會使用名為 foo.exe 的檔案。當 foo.exe 執行時，主動型威脅掃描也會跟著執行。用戶端判斷 foo.exe 可能為惡意程式。掃描結果對話方塊會出現，顯示用戶端已隔離 foo.exe。您可以建立例外，指定主動型威脅

掃描忽略 foo.exe。用戶端接著便會還原 foo.exe。當您再次執行 foo.exe 時，用戶端會忽略 foo.exe。

您的管理員可能也會針對您的掃描建立集中式例外。您可檢視管理員定義的例外，但無法修改。如果您建立的集中式例外與管理員定義的例外衝突，則會優先採取管理員定義的例外。

如需有關程序中使用選項的更多資訊，您可以按下「說明」。

架構主動型威脅掃描的集中式例外

1. 在用戶端的側邊看板中，按下「變更設定」。
2. 在「集中式例外」旁，按下「架構設定」。
3. 在「使用者定義例外」標籤上，按下「新增」，然後選取「主動型威脅掃描例外」。
4. 在「新增主動型威脅掃描例外」對話方塊中，鍵入程序名稱或選取要為其建立例外的檔案。
5. 在「動作」下拉式清單中，選取「略過」、「只記錄」、「隔離」或「終止」。
6. 按下「新增」。

8

管理網路威脅防護

本章包含以下主題：

關於網路威脅防護

網路攻擊是利用電腦傳輸資訊的方式進行的。Symantec Endpoint Protection 用戶端可以藉由監控進出電腦的資訊，以及攔截可能的攻擊來防護您的電腦。

資訊會以封包的形式在 Internet 上流通。每個封包都有一個表頭，其中包含傳送端電腦的相關資訊、設定的接收端、封包中資訊的處理方式，以及應該接收封包的通訊埠。

通訊埠是一種通道，用來將來自 Internet 上的資訊流分為數個路徑，讓個別應用程式進行處理。Internet 應用程式在電腦上執行時，會監聽一個或多個通訊埠，並接受傳送到這些通訊埠的資訊。

網路攻擊即是利用特定 Internet 程式的弱點。攻擊者會使用工具，將包含惡意程式碼的封包傳送到特定通訊埠。如果容易遭受這類攻擊的程式監聽該通訊埠，程式碼便會讓攻擊者存取、停用，甚至控制電腦。用來進行攻擊的程式碼可能存在於一或多個封包中。

用戶端安裝時即已預設好「網路威脅防護」的設定。在大多數情況下，您無須變更設定。保留設定一般不會有問題。不過，如果您對網路有深入的瞭解，可以視需要變更用戶端防火牆，微調防護功能。

用戶端防止受到網路攻擊的方式

用戶端具備下列工具，可防護電腦不受入侵攻擊：

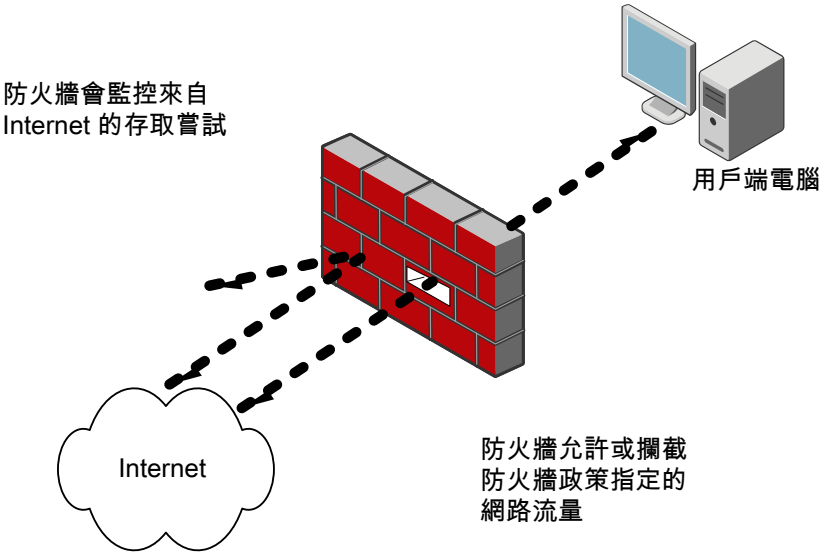
防火牆	監控所有Internet通訊，並建立防護罩來攔截或限制檢視電腦上資訊的嘗試。
入侵預防	分析所有入埠資訊和離埠資訊，檢查是否出現具攻擊特徵的資料模式。

若要評估進一步防護電腦的方式，可以測試電腦是否易受外部網路攻擊和病毒入侵。若要測試電腦，您可以執行幾項掃描。

請參閱第 24 頁的「測試您電腦的安全」。

關於防火牆

防火牆是一種軟體，會在電腦與Internet之間設下一道護欄。防火牆可防止未經授權的使用者存取連上Internet的個人電腦和網路。它會偵測可能的駭客攻擊、保護個人資訊，以及排除非必要的網路流量來源，如入侵嘗試。



所有進入或離開私人網路的資訊都必須通過防火牆。防火牆會檢查資訊封包，攔截不符合所指定安全準則的封包。防火牆檢查資訊封包的方式是使用防火牆規則。防火牆政策包含一或多個規則，這些規則會搭配運作以允許或攔截使用者存取網路，只有授權的流量可以通過。防火牆政策會定義授權的流量。

防火牆會在背景作業。您的管理員會決定您可以與用戶端互動的程度，即允許或禁止您架構防火牆規則和防火牆設定。用戶端可能只會通知您有新的網路連線和可能的問題，或者您可以完整存取用戶端的使用者介面。

防火牆監控通訊的方式

當防火牆啟動時，它會監控您電腦和 Internet 上其他電腦之間的通訊。

防火牆會使用下列任一方法防止不當連線嘗試：

- 攔截入埠流量和離埠流量。
- 警告您其他電腦嘗試進行連線，並警告您電腦上的應用程式嘗試連線到其他電腦。

您可以自訂防火牆的防護功能，控制防護等級。

關於入侵預防系統

入侵預防系統 (IPS) 是 Symantec Endpoint Protection 用戶端在防火牆後的第二層防護。入侵預防系統是一種作業於安裝用戶端及啟用 IPS 系統電腦上的網路系統。如果偵測到已知攻擊，會自動以一或多種入侵預防方法攔截攻擊。

入侵預防系統會分析所有入埠及離埠資訊，檢查攻擊的典型資料模式。它偵測並攔截外部使用者企圖攻擊您電腦的惡意流量及嘗試。入侵預防也會監控離埠流量，並預防病蟲的散播。

表 8-1 列出入侵預防系統監控的常見安全問題。

表 8-1 常見安全問題

問題	防護
通訊埠掃描	隱藏電腦上未使用的通訊埠，並偵測通訊埠掃描。
服務阻斷攻擊	檢查所有網路封包是否有特定的已知攻擊，這些攻擊會限制您電腦使用您通常期望具有的服務。
入侵	偵測並攔截外部使用者企圖攻擊您電腦的惡意流量及嘗試，並掃描離埠流量，以防病蟲擴散。

入侵預防分析流量的方式

入侵預防系統會掃描每個進出您網路中電腦的封包是否有攻擊特徵，以及用以識別攻擊者嘗試利用作業系統或程式之已知弱點的封包順序。

如果資訊符合已知的攻擊，則 IPS 會自動捨棄封包。IPS 還可以切斷與傳送資料的電腦的連線一段指定時間。這項功能稱為「主動回應」，會保護您網路上的電腦不受任何方式的影響。

用戶端包括下列可辨識攻擊特徵的 IPS 引擎類型。

Symantec IPS 特徵	Symantec IPS 特徵使用可掃描多個封包的串流式引擎。Symantec IPS 特徵會攔截階段作業層的網路資料並擷取在應用程式及網路堆疊間流通的訊息段。 Symantec IPS 會使用下列兩種方法檢查封包。它會個別掃描每個封包，搜尋與規格不符並且會癱瘓 TCP/IP 堆疊的型樣。它也會將封包視為資訊流進行監控，搜尋針對特定服務意圖攻擊或癱瘓系統的命令。IPS 能夠記得先前封包的型樣或部分型樣的清單，並且可以將這個資訊套用至隨後的封包檢驗中。 IPS 會根據列有大量攻擊特徵的清單來偵測並攔截可疑的網路活動。賽門鐵克提供已知威脅清單，您可以使用賽門鐵克 LiveUpdate 在用戶端上更新這份清單。根據預設，Symantec IPS 引擎及相關 IPS 特徵集會安裝於用戶端上。
自訂 IPS 特徵	自訂 IPS 特徵使用一個封包式的引擎分別掃描每個封包。 串流式及封包式的引擎都會偵測攻擊 TCP/IP 堆疊、作業系統元件及應用程式層的網路資料中的特徵。然而，封包式特徵偵測到 TCP/IP 堆疊中攻擊的速度會比串流式特徵快。封包式引擎不會偵測掃描多個封包的特徵。封包式 IPS 引擎的限制比較多，因為它無法緩衝部分相符項，並且只能掃描單個封包酬載。

入侵預防系統將偵測到的攻擊記錄在安全日誌中。自訂的 IPS 特徵可能將偵測到的攻擊記錄在封包日誌中。

請參閱第 105 頁的「架構入侵預防」。

檢視網路活動

您可以檢視有關您電腦的入埠流量及離埠流量的資訊。您還可以檢視從用戶端服務啟動後所執行的應用程式及服務清單。表 8-2 說明用戶端會對流量採取的動作，並顯示用戶端對存取用戶端電腦或網路的應用程式所採取動作的代表圖示。

表 8-2 在應用程式存取用戶端或網路時，用戶端會採取的動作

圖示	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。
	詢問	詢問是否允許入埠流量存取您的電腦或公司網路。 如果您或您的管理員架構讓用戶端詢問您是否允許您的應用程式存取網路資源，圖示中會顯示一個黃色的小問號。您可以設定用戶端記住您的回應，這樣您就不需要重複告知用戶端。

圖示	動作	敘述
	攔截	阻止入埠流量及離埠流量存取網路或網際網路連線。

附註：用戶端不會偵測來自 PDA (個人數位助理) 裝置的網路流量。

檢視流量記錄

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」。

如需圖形和欄位的詳細資訊，請按下「說明」。

3 按下「關閉」。

您可以顯示流量為廣播流量或單點傳播流量。廣播流量是在特定子網路傳送至每部電腦的網路流量，不會特別導向至您的電腦。單點傳播流量則會特別導向至您的電腦。

顯示或隱藏 Windows 服務和廣播流量

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 在「網路活動」對話方塊中，用滑鼠右鍵按下「執行應用程式」欄位，然後執行下列動作：

- 若要顯示或隱藏 Windows 服務，請勾選或取消勾選「顯示 **Windows** 服務」。
- 若要顯示廣播流量，請勾選「顯示廣播流量」。
- 若要顯示單點傳播流量，請取消勾選「顯示廣播流量」。

4 按下「關閉」。

變更應用程式圖示顯示的方式

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「執行中的應用程式」欄位中，在應用程式上按下滑鼠右鍵，然後按下列其中一種檢視：

- 大圖示
- 小圖示

- 清單
- 應用程式詳細資料
- 連線詳細資料

4 按下「關閉」。

架構防火牆

預設的防火牆設定可以保護您的電腦。如果預設設定不適用，您可以自訂「防火牆政策」。若要自訂「防火牆政策」，您可以新增或變更下列防火牆功能：

防火牆規則	監控所有 Internet 通訊，並建立一道防護來攔截或限制對電腦上資訊的檢視嘗試。防火牆規則可讓 Internet 上的其他人看不見您的電腦。 防火牆規則會保護遠端使用者不受駭客攻擊，並可防止駭客透過這些電腦從後門進入企業網路。您可以在防火牆攔截使用者電腦上的應用程式時，通知使用者。
智慧型流量過濾	允許大多數網路所需要的特定類型流量。這類流量包括 DHCP、DNS 及 WINS 流量。
流量與隱藏設定	啟用其他流量功能，如驅動程式層級防護、NetBIOS防護、Token Ring 流量、DNS 反向搜尋及隱藏模式設定等。

您的管理員不一定會給予您自訂防火牆規則及防火牆設定的權限。如果您沒有權限，管理員會建立防火牆規則並啟用「防火牆政策」中的設定，然後將政策派送給用戶端。如果您有權限，則可以在用戶端上建立規則並修改設定，以適用於您的網路環境。您的管理員可能已架構用戶端，將其所建立的規則和您建立的規則合併在一起。

您可以在某些時候 (如安裝新軟體期間) 停用防護。

請參閱第 41 頁的「啟用與停用網路威脅防護」。

關於防火牆規則

當一台電腦嘗試與另一台電腦連線時，防火牆會將連線類型與其防火牆規則清單進行比較。防火牆規則控制用戶端如何保護用戶端電腦不受惡意入埠流量及離埠流量的侵襲。防火牆自動根據這些規則檢查所有入埠及離埠的封包。然後，防火牆根據規則中指定的資訊允許或攔截封包。

關於規則項目

防火牆規則描述允許或攔截網路連線的條件。

表 8-3 描述用於定義防火牆規則的準則。

表 8-3 防火牆規則條件

條件	敘述
觸發條件	應用程式、主機、通訊協定和網路配接卡。 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 True，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。

例如，某項規則可能指示，每日上午 9 時至下午 5 時之間，允許 IP 位址 192.58.74.0 存取遠端通訊埠 80。

表 8-4 描述可以在防火牆規則中定義的觸發條件。

表 8-4 防火牆規則觸發條件

觸發條件	敘述
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。

觸發條件	敘述
通訊協定	通訊協定觸發條件會根據所述的網路流量，識別產生作用的一項或多項網路通訊協定。 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。 您可以定義下列類型的通訊協定： ■ 所有 IP 通訊協定 任何通訊協定。 ■ TCP 通訊埠或通訊埠範圍。 ■ UDP 通訊埠或通訊埠範圍。 ■ ICMP 類型和代碼。 ■ 特定 IP 通訊協定 通訊協定編號 (IP 類型)。 範例：Type 1 = ICMP，Type 6 = TCP，Type 17 = UDP
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。

關於狀態檢查

防火牆會使用狀態檢查，此程序可追蹤關於目前連線的資訊，例如來源與目標IP位址、通訊埠、應用程式等等。用戶端在檢查防火牆規則之前，會使用此連線資訊決定流量的方向。

例如，如果防火牆規則允許用戶端連線至網頁伺服器，防火牆便會記錄連線資訊。在伺服器回應時，防火牆發現從網頁伺服器到用戶端的回應是預期的，便會允許網頁伺服器流量流到起始的用戶端，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。

狀態檢查可讓您簡化規則資料庫，因為您不需要針對一般只有單向起始的流量建立允許雙向流量的規則。通常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)。用戶端會起始這些離埠流量，因此您只須針對這些通訊協定建立允許離埠流量的規則。防火牆會允許傳回流量。

藉由只架構離埠規則，您便可以使用下列方式增加用戶端安全性：

- 減少規則庫的複雜性。
- 消除病蟲或其他惡意程式在只架構進行離埠流量的通訊埠上連線至用戶端的可能性。對於用戶端不起始的用戶端流量，您也可以只架構入埠規則。

狀態檢查支援導向 TCP 流量的所有規則。狀態檢查不支援過濾 ICMP 流量的規則。對於 ICMP，您必須在必要時建立允許雙向流量的規則。例如，若要用戶端使用 Ping 命令並接收回應，您必須建立允許雙向 ICMP 流量的規則。

關於 UDP 連線

對於 UDP 通訊，用戶端會分析第一個 UDP 資料包，並將對初始資料包所採取的動作，套用到目前程式工作階段的所有後續 UDP 資料包。相同電腦之間的入埠或離埠流量會被認為是 UDP 連線的一部分。

對於狀態 UDP 流量，當建立 UDP 連線時，即允許入埠 UDP 通訊，即使防火牆規則攔截它也一樣。例如，如果有某個規則攔截特定應用程式的入埠 UDP 通訊，但您選擇允許離埠 UDP 資料包，則在目前的應用程式工作階段中，將允許所有入埠 UDP 通訊。對於無狀態 UDP，您必須建立允許入埠 UDP 通訊回應的防火牆規則。

若應用程式關閉通訊埠，UDP 工作階段會在 60 秒後逾時。

關於規則處理順序

防火牆規則會依序排列，排列的優先順序為從最高到最低，或在規則清單中為從上到下。防火牆會依此順序檢查規則。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，以取得如何處理封包的資訊。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。

您可以在優先順序類別中排列規則的順序，以便讓防火牆按照邏輯的順序進行評估。您可以將規則排序，以便根據獨特性進行評估，限制最嚴格的規則先評估，最普通的規則則最後評估。例如，如果您建立攔截流量的規則，就必須將這些規則置於上方，因為其他規則可能允許流量。

表 8-5 顯示防火牆處理各項規則與設定的順序。

表 8-5 防火牆處理規則、防火牆設定、IPS 特徵和 IPS 設定的順序

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	智慧型流量過濾
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

新增規則

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。

新增規則

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. 若要定義規則的網路配接卡，請在「套用此規則到以下網路配接卡」下拉式清單中，選取網路配接卡。
6. 若要選擇是否在螢幕保護程式狀態下啟用規則，請選取「套用此規則，當螢幕保護程式為」下拉式清單中的選項。
7. 若要指定螢幕保護程式的狀態，請選取「套用此規則，當螢幕保護程式為」下拉式清單中的選項。
8. 若要定義規則的觸發條件，請選取下列其中一個標籤：
   - 主機
   - 通訊埠和通訊協定
   - 應用程式

   如需各個標籤選項的詳細資訊，請按下「說明」。
9. 若要定義規則有效或無效的期間，請按下「排程」，然後設定排程。
10. 完成變更時，按下「確定」。
11. 在「架構防火牆規則」對話方塊中，確定已勾選「規則名稱」欄，以啟用規則。
12. 按下「確定」。

變更規則的順序

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，只會影響目前選定位置的順序。

請參閱第 99 頁的「關於規則處理順序」。

變更規則的順序

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：
   - 若要讓防火牆處理此規則的前一項規則，請按藍色向上箭頭。
   - 若要讓防火牆處理在此規則的下一項規則，請按藍色向下箭頭。
5. 當您完成移動規則之後，按下「確定」。

啟用與停用規則

您必須啟用規則，由防火牆進行處理。新增規則時，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」對話方塊中，針對需要啟用或停用的規則，勾選或取消勾選「規則名稱」欄旁的核取方塊。
4. 按下「確定」。

匯出和匯入規則

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「存檔」。
6. 按下「確定」。

匯入規則

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「開啟舊檔」。

6 按下「確定」。

編輯和刪除規則

如果規則的功能不符合您的需要，您可以變更這些規則。

您可以移除先前已新增而目前不再需要的防火牆規則。

編輯規則

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，選取規則，然後按下「編輯」。

4 變更任何標籤上的設定。

5 當您完成變更規則時，按下「確定」。

刪除規則

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，選取一項或多項規則，然後按下「刪除」。

4 在出現的訊息方塊中，按下「是」。

5 按下「確定」。

啟用流量設定和隱藏網頁瀏覽設定

您可以在「防火牆政策」中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網路攻擊類型的侵襲。

表 8-6 定義您可以啟用的流量和隱藏設定。

表 8-6 流量和隱藏網頁瀏覽設定

選項	敘述
啟用驅動程式層級防護	檢查來自 TCP/IP 堆疊及其他通訊協定驅動程式的流量。 企業網路中的大部分攻擊是因 Windows TCP/IP 連線而產生。其他攻擊則可能利用其他通訊協定驅動程式啟動。任何存取網路的通訊協定驅動程式都是網路應用程式。除非規則明確允許存取，否則用戶端都會攔截通訊協定驅動程式存取網路。若通訊協定驅動程式試圖存取網路，系統會顯示通知並詢問您是否允許。
啟用 NetBIOS 防護	攔截來自外部閘道的 NetBIOS 流量。 您可使用 LAN 上共用的「網路上的芳鄰」檔案和印表機，保護電腦免受任何外部網路利用 NetBIOS 侵入。 此選項會攔截並非由定義的 ICANN 內部範圍內之 IP 位址發出的 NetBIOS 封包。ICANN 內部範圍包括 10.x.x.x、172.16.x.x、192.168.x.x 和 169.254.x.x，但不包括 169.254.0.x 和 169.254.255.x 子網路。NetBIOS 封包包括 UDP 88、UDP 137、UDP 138、TCP 135、TCP 139、TCP 445，以及 TCP 1026。
允許 Token Ring 流量	允許透過 Token Ring 配接卡連線的用戶端電腦存取網路，不論用戶端上的防火牆規則為何。 如果停用此設定，任何透過 Token Ring 配接卡連線的電腦所送出的流量都無法存取企業網路。防火牆不會過濾 Token Ring 流量，不是允許所有 Token Ring 流量，就是攔截所有 Token Ring 流量。
在防火牆啟動之前及防火牆停止之後攔截所有流量	當防火牆因任何原因停止執行時，攔截用戶端電腦的全部入埠流量和離埠流量。 下列是電腦未受到防護的時間： ■ 在用戶端電腦開啟後，防火牆服務啟動前。 ■ 在防火牆服務停止，用戶端電腦停止後。 這段時間是安全上的小漏洞，可能會允許未經授權的通訊。此設定可防止未經授權的應用程式與其他電腦通訊。
允許初始 DHCP 和 NetBIOS 流量	允許啟用網路連線的初始流量。此流量包括允許用戶端取得 IP 位址的初始 DHCP 和 NetBIOS 流量。
啟用隱藏模式網頁瀏覽	偵測來自任何通訊埠上網頁瀏覽器的 HTTP 流量，並移除瀏覽器名稱和版本號碼、作業系統，以及參考網頁。這可防止網站得知電腦使用哪種作業系統和瀏覽器。但是，不會偵測 HTTPS (SSL) 流量。
啟用 TCP 重新排序	防止入侵者假借 (或詐騙) 他人的 IP 位址。 駭客使用 IP 詐騙，劫取兩台電腦 (例如，電腦 A 和 B) 之間的通訊階段作業。駭客可能送出會造成電腦 A 通訊中斷的資料封包。接著便可冒充是電腦 A 與電腦 B 通訊並發出攻擊。 為防護電腦，TCP 重新排序會隨機設定 TCP 序號。
啟用作業系統指紋偽裝	防止偵測用戶端電腦的作業系統。 用戶端會變更 TCP/IP 封包的 TTL 和識別值，以防止作業系統被識別出來。

選項	敘述
啟用防 MAC 詐騙	只有在對特定主機發出位址解析通訊協定 (ARP) 要求，才允許入埠及離埠 ARP 流量。這會攔截所有其他非預期的 ARP 流量，並記錄在安全日誌中。

啟用流量設定和隱藏網頁瀏覽設定

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「網路威脅防護設定」對話方塊中，按下「防火牆」。
4. 在「防火牆」標籤上的「流量設定」和「隱藏設定」群組方塊中，勾選核取方塊啟用設定。
5. 按下「確定」。

啟用智慧型流量過濾

您可以啟用「智慧型流量過濾」，允許大多數網路上的 DHCP、DNS 和 WINS 流量。「智慧型流量過濾」可允許已架構使用 DHCP、DNS 和 WINS 的網路連線進行離埠要求和入埠回應。

「智慧型流量過濾」可讓 DHCP、DNS 或 WINS 用戶端從伺服器接收 IP 位址，同時又能防護用戶端不受網路攻擊，其方式如下：

- 如果用戶端傳送要求至伺服器，用戶端會等待五秒後再允許入埠回應。
- 如果用戶端沒有傳送要求至伺服器，則每項過濾均不會允許封包。

智慧型過濾會允許發出要求的封包，但不會攔截封包。防火牆規則才會允許或攔截封包。

啟用智慧型流量過濾

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「防火牆」。
4. 勾選下列一或多個核取方塊：
   - 啟用智慧型 **DHCP**
   - 啟用智慧型 **DNS**
   - 啟用智慧型 **WINS**
5. 按下「確定」。

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。
  您可以架構您的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。
- 當防火牆停止執行時。
  在用戶端電腦開啟後，防火牆服務啟動之前，或是在防火牆服務停止，電腦關閉之後這段時間，電腦都不會受到防護。這段時間是安全上的小漏洞，可能會允許未經授權的通訊。
- 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。管理員可能已經架構不提供這個選項。

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「網路威脅防護設定」對話方塊中，按下「**Microsoft Windows** 網路」。
4. 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」。
5. 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「網路威脅防護設定」對話方塊中，按下「防火牆」。
4. 在「防火牆」標籤上，按下「在防火牆啟動之前及防火牆停止之後攔截所有流量」。
5. 選擇性按下「允許初始 **DHCP** 和 **NetBIOS** 流量」。
6. 按下「確定」。

架構入侵預防

您可以自訂入侵預防設定，變更預設的防護功能。

您可以啟用：

- 入侵預防系統特徵，偵測及預防網路攻擊。

- 入侵預防設定，預防通訊埠掃描和服務阻斷攻擊。
- 主動回應，這會自動攔截發出攻擊的電腦。

一般來說，當您停用電腦上的入侵預防設定時，電腦會變得較不安全。不過，您可能需要停用這些設定，以避免誤報或對用戶端電腦進行疑難排解。

用戶端會在「安全日誌」中記錄入侵預防系統偵測到的攻擊和安全性事件。用戶端可能會在「封包日誌」中記錄攻擊和事件。

附註：管理員可能已經架構不提供這些選項。

啟用入侵預防設定

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「網路威脅防護設定」對話方塊中，按下「入侵預防」。
4. 若要啟用設定，請勾選下列任何核取方塊：
   - 啟用入侵預防
   - 啟用阻絕服務偵測
   - 啟用通訊埠掃描偵測

   若需設定的相關資訊，請按下「說明」。
5. 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。

附註：管理員可能已經架構不提供這些選項。

架構入侵預防通知

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「入侵預防」。
4. 勾選「顯示入侵預防通知」。

5 若要在通知出現時聽見嗶聲，請勾選「通知使用者時使用音效」。

6 在「顯示通知的秒數」欄位中，輸入想要通知顯示的時間長度。

7 按下「確定」。

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。用戶端會啟用一個主動回應，自動攔截特定期間內所有進出攻擊電腦 IP 位址的全部通訊。單一位置會攔截攻擊電腦的 IP 位址。

更新的 IPS 特徵、更新的服務阻斷特徵及通訊埠掃描也會觸發主動回應。

您可以在安全日誌中檢視攻擊電腦的IP位址。您還可以透過停止安全日誌中的主動回應，取消攔截攻擊。

攔截攻擊電腦

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「入侵預防」。

4 勾選「幾秒後自動攔截攻擊者 **IP** 位址」，然後輸入秒數。

輸入從 1 秒到 999,999 秒的數字。預設時間是 600 秒 (10 分鐘)。

5 按下「確定」。

如果您不想等候這段預設的時間再取消攔截 IP 位址，您可以立即取消攔截。

取消攔截攻擊電腦

1 在用戶端的側邊看板中，按下「檢視日誌」。

2 在「用戶端管理」旁，按下「檢視日誌」>「安全日誌」。

3 在「安全日誌」中，選取在「事件類型」欄中包含「主動回應」的列，然後按下「動作」>「停止主動回應」。

若要取消攔截已攔截的 IP 位址，請按下「動作」>「停止全部主動回應」。如果您取消攔截一個主動回應，「事件類型」欄會顯示「已取消主動回應」。如果主動回應逾時，「事件類型」欄會顯示「主動回應」已斷開。

4 在顯示的訊息方塊中，按下「確定」。

5 按下「檔案」>「結束」。

架構應用程式限定設定

您可以針對自用戶端服務啟動以來執行的，或已要求網路存取權限的應用程式，架構其設定。

您可以架構某些限制，例如應用程式可以使用的IP位址和通訊埠。您可以檢視和變更用戶端針對每個嘗試透過網路連線進行存取的應用程式所採取的動作。您可以針對特定應用程式架構設定，來建立應用程式型的防火牆規則。

附註：如果防火牆規則和應用程式限定設定發生衝突，則會優先採用防火牆規則。例如，攔截 1 AM 和 8 AM 之間所有流量的防火牆規則會覆寫特定視訊應用程式的排程。

「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執行的應用程式和服務。

請參閱第 94 頁的「檢視網路活動」。

架構應用程式限定設定

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」>「檢視應用程式清單」。
3. 在「檢視應用程式清單」對話方塊中，選擇您要架構的應用程式，然後按下「架構」。
4. 在「架構應用程式設定」對話方塊的「應用程式的信任 IP」欄位中，輸入 IP 位址或 IP 位址範圍。
5. 在「遠端伺服器通訊埠」或「本機通訊埠」群組方塊中，選擇 TCP 或 UDP 通訊埠。
6. 若要指定流量的方向，請按下列一或兩個項目：
   - 若要允許離埠流量，請按下「允許連出連線」。
   - 若要允許入埠流量，請按下「允許連入連線」。
7. 若要在螢幕保護程式執行時套用規則，請按下「在啟用螢幕保護程式時允許」。
8. 若要設定限制生效或無效的排程，請按下「啟用排程」。
9. 選取下列其中一個項目：
   - 若要指定限制生效的時間，請按下「下列週期期間」。
   - 若要指定限制無效的時間，請按下「排除下列期間」。
10. 設定排程。
11. 按下「確定」。
12. 在「檢視應用程式清單」對話方塊中，若要變更動作，請在應用程式上按下滑鼠右鍵，然後按下「允許」或「攔截」。
13. 按下「確定」。

您也可以從「網路活動」對話方塊中變更應用程式的動作。

從網路活動對話方塊中變更應用程式的動作

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「執行中的應用程式」欄位中，在應用程式或服務上按下滑鼠右鍵，然後按下「允許」、「攔截」或「終止」。

4 按下「關閉」。

當您變更應用程式的動作時，該應用程式會顯示在「應用程式」清單中。

停止應用程式或服務

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「執行中的應用程式」欄位中，在應用程式上按下滑鼠右鍵，然後按下「終止」。

4 按下「確定」。

移除應用程式的限制

您可以移除應用程式的限制。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。

您可以將應用程式或服務停止執行，直到應用程式再次嘗試存取您的電腦為止，例如您重新啟動電腦時。

移除應用程式的限制

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」>「檢視應用程式清單」。

3 在「檢視應用程式清單」對話方塊中，執行下列其中一個動作：

- 若要移除清單中的應用程式，請先選取應用程式，然後按下「移除」。
- 若要移除清單中的全部應用程式，請按下「全部移除」。

4 按下「是」。

共用檔案及資料夾

指定網路介面卡，並設定網路瀏覽權限。

1 在「工具」功能表中，按下「選項」。

2 按下「網路上的芳鄰」。

3 按下「網路介面」下拉式清單方塊，並選取您端點的網路介面卡。

4 若要啟用端點以瀏覽和共用網路中任何配置的資源，請按下列其中一個或兩個核取方塊：

允許瀏覽「網路上的芳鄰」的檔案及印表機	允許您瀏覽指定網路上的其他端點及印表機。這可讓您存取網路上的其他檔案。如果您停用此項目，則您將無法複製網路位置上的檔案。
允許其他人分享我的檔案及印表機	允許指定網路的其他使用者瀏覽您的端點。

5 按下「確定」。

部分 3

Symantec Network Access Control

9

Symantec Network Access Control 基礎

本章包含以下主題：

關於 Symantec Network Access Control

Symantec Network Access Control 用戶端會評估電腦是否受到適當保護並遵從政策，才會允許它連線到公司網路。

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，如防毒和防火牆應用程式。如果電腦沒有執行必要的軟體，那麼您或用戶端就必須更新軟體。如果安全軟體不是最新的，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。

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。驗證和強制執行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」是所有評估和動作等的基礎安全性政策。

這個網路存取控制程序包含下列步驟：

- 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規定。例如，政策會檢查最近更新防毒定義的狀況，並檢查套用至作業系統的最新修正程式有哪些。
- 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。
  d
  請參閱第 116 頁的「關於強制執行」。
  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 22 頁的「回應網路存取控制通知」。
- 用戶端會矯正非遵從電腦。
  如果用戶端發現「主機完整性政策」要求不符，則用戶端會安裝所需的軟體，或要求您進行安裝。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 115 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更多有關「主機完整性」的檢查結果。

關於更新主機完整性政策

用戶端會定期更新「主機完整性政策」。管理員可能會要求您在下次排程更新之前，先更新「主機完整性政策」，以便進行測試。除此之外，您不需要更新政策。

請參閱第 15 頁的「更新安全性政策」。

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防毒應用程式。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「網路存取控制」旁，按下「選項」>「立即檢查」。
3. 如果出現確認「主機完整性」檢查已執行的訊息，則按下「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。

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。

檢視 Symantec Network Access 日誌

Symantec Network Access Control 用戶端會使用下列日誌，監控作業程序各個細項：

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. 若要檢視系統日誌，請在「網路存取控制」旁，按下「選項」>「檢視日誌」。
3. 若要檢視安全日誌，請在「用戶端管理日誌」的「系統日誌」對話方塊中，按下「檢視」>「安全日誌」。
4. 按下「檔案」>「結束」。

請參閱第 123 頁的「關於日誌」。

關於強制執行

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。

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，可驗證「主機完整性」的結果和用戶端電腦的識別，之後才允許電腦網路存取。

授予用戶端存取網路之前，Enforcer 會先檢查下列資訊：

- Symantec Network Access Control 用戶端執行。
- 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。

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：

- 未驗證的用戶端或協力廠商請求者，會將使用者資訊和遵從資訊傳送至受管 802.11 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，用戶端可以使用協力廠商請求者或內建請求者。

表 9-1 描述可以針對 802.1x 驗證架構的選項類型。

表 9-1 802.1x 驗證選項

選項	敘述
協力廠商請求者	使用協力廠商 802.1x 請求者。 LAN Enforcer 可和 RADIUS 伺服器和協力廠商 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 用戶端和協力廠商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。
透明模式	將用戶端當作 802.1x 請求者使用。 如果管理員不希望使用 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協力廠商 802.1x 請求者。

選項	敘述
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。

架構用戶端使用協力廠商請求者

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」>「**802.1x**」。
3. 按下「啟用 **802.1x** 驗證」。
4. 按下「確定」。

   您也必須設定防火牆規則，允許協力廠商 802.1x 請求者驅動程式存取網路。

   請參閱第 100 頁的「新增規則」。

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」>「**802.1x**」。
3. 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」>「區域連線」。
2. 在「區域連線狀態」對話方塊的「一般」標籤上，按下「內容」。
3. 在「區域連線內容」對話方塊中，按下「驗證」。

4 在「驗證」標籤上，按下「EAP類型」下拉式清單，然後選取下列其中一項驗證通訊協定：

- 智慧卡或其他憑證
- 受保護的 EAP (PEAP)
- Symantec NAC Transparent Mode

5 按下「確定」。

6 按下「關閉」。

重新驗證電腦

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

出現下列其中一項事件時，網路可能會攔截電腦：

- 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。
- 您需要登入至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命令。

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」。

部分 4

監控與記錄

10

使用和管理日誌

本章包含以下主題：

關於日誌

日誌包含您電腦上與安全相關的活動記錄，其中包括病毒和安全風險活動、架構變更，以及錯誤。此外，還包括病毒和安全風險定義檔資訊、電腦狀態，以及進出您電腦的流量等相關資訊。這些記錄稱為事件或項目。日誌會顯示這些事件以及所有相關的其他資訊。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。

日誌是追蹤電腦活動，以及其與其他電腦和網路互動情形的重要方法。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。當多人共用一部電腦時，您可能可以識別引入風險的人員，並協助其採取更好的預防措施。「網路防護」日誌可以協助您偵測潛在威脅活動，如通訊埠掃描等。它們也可以用來回溯檢查威脅活動的來源。您也可以使用「網路防護」日誌來協助排解連線問題或可能的網路攻擊。

如果您安裝了 Symantec Endpoint Protection，就可以使用下列日誌檢視：

- 掃描日誌，由「防毒和防間諜軟體防護」產生
- 風險日誌，由「防毒和防間諜軟體防護」產生

- 系統日誌，由「防毒和防間諜軟體防護」產生
- 威脅日誌，由「主動型威脅防護」產生
- 系統日誌，由「主動型威脅防護」產生
- 竄改防護日誌，由「竄改防護」產生
- 流量日誌，由「網路威脅防護」產生
- 封包日誌，由「網路威脅防護」產生
- 安全日誌，由「用戶端管理」及「網路威脅防護」產生
- 控制日誌，由「用戶端管理」產生
- 系統日誌，由「用戶端管理」產生

如果您安裝了 Symantec Network Access Control，就可以使用下列日誌：

- 安全日誌
- 系統日誌

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。

如需日誌的詳細資訊，可按下 F1，檢視該日誌的說明。

表 10-1 描述每個日誌及其用途。

表 10-1 用戶端日誌及敘述

日誌	敘述
掃描日誌	「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。 您可以在「掃描日誌」中執行下列工作： ■ 檢視某段時間內，已在您電腦上發生的掃描清單。掃描會和這些掃描的其他相關資訊一起顯示。 ■ 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。

日誌	敘述
風險日誌	「風險日誌」包含已感染您電腦的病毒及安全風險 (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。 您可以在「風險日誌」中執行下列工作： ■ 檢視與病毒及安全風險相關的事件清單。 ■ 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 清除您電腦中的風險。 ■ 永久刪除您電腦中的風險。 ■ 復原 Symantec Endpoint Protection 在刪除風險或修復其副作用時所做的變更。 ■ 隔離已在您電腦上偵測到的風險。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。
防毒和防間諜軟體防護系統日誌	「防毒和防間諜軟體防護系統日誌」包含您電腦上與病毒及安全風險相關系統活動的資訊。這項資訊包含架構變更、錯誤及定義檔資訊。 您可以在「防毒和防間諜軟體防護系統日誌」中執行下列工作： ■ 檢視與防毒和防間諜軟體相關的事件清單。 ■ 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 過濾日誌中的資訊，以便只檢視一種或數種類型的事件。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。
威脅日誌	「威脅日誌」包含「主動型威脅防護」已在您電腦上偵測到的威脅相關資訊。這些包含作為惡意用途的商用應用程式。範例為特洛伊木馬程式、病蟲或按鍵記錄器，或大量郵件病蟲、巨集病毒及程序檔式威脅。 您可以在「威脅日誌」中執行下列工作： ■ 檢視與「主動型威脅防護」威脅相關的事件清單。 ■ 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 終止已在您電腦上找到的惡意程式或惡意程序。 ■ 還原隔離所中的項目。 ■ 將您電腦上偵測到的威脅放入「隔離所」。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。 **附註：**可使用哪些動作按鈕取決於所選日誌項目所適用的動作。
主動型威脅防護系統日誌	「主動型威脅防護系統日誌」包含您電腦上與「主動型威脅防護」相關系統活動的相關資訊。 您可以在「主動型威脅防護系統日誌」中執行下列工作： ■ 檢視與「主動型威脅防護」相關的系統事件。 ■ 將資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 過濾日誌中的資訊，以便只檢視一種或數種類型的事件。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。

日誌	敘述
竄改防護日誌	「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。 您可以在「竄改防護日誌」中執行下列工作： ■ 檢視與「竄改防護」相關的事件清單。 ■ 將日誌中的資料匯出為逗號分隔文字檔案，以便在其他應用程式中使用。 ■ 在項目上按滑鼠右鍵，可檢視其屬性。
流量日誌	「流量日誌」包含您電腦透過網路進行的連線相關資訊。 您可以在「流量日誌」中執行下列工作： ■ 檢視每當您電腦連接至網路時的連入流量事件及連出流量事件清單。 ■ 從「檔案」功能表，清除日誌中的所有項目。 ■ 從「檔案」功能表，將日誌中的資料匯出為Tab分隔文字檔案，以便在其他應用程式中使用。 ■ 從「檔案」功能表，存取「網路威脅防護」設定，然後變更您可以變更的設定。 ■ 從「檢視」功能表，切換本機檢視和來源檢視。 ■ 從「過濾」功能表，透過選取時間範圍來過濾項目。 ■ 從「動作」功能表，回溯檢查用於嘗試攻擊的資料封包，以找出其來源。請注意，並非每個項目都可以回溯檢查。 **附註：**不適合特定項目或您的管理員不允許的動作都無法使用。
封包日誌	「封包日誌」包含透過您電腦的通訊埠進出的資料封包相關資訊。 您可以在「封包日誌」中執行下列工作： ■ 檢視每當您電腦連接至網路時的連入流量事件及連出流量事件清單。 ■ 從「檔案」功能表，清除日誌中的所有項目。 ■ 從「檔案」功能表，將資料匯出為 Tab 分隔文字檔案、網路監控格式或 Netxray 格式，以便在其他應用程式中使用。 ■ 從「檔案」功能表，存取「網路威脅防護」設定，然後變更您可以變更的設定。 ■ 從「檢視」功能表，切換本機檢視和來源檢視。 ■ 從「過濾」功能表，透過選取時間範圍來過濾項目。 ■ 從「動作」功能表，回溯檢查用於嘗試攻擊的資料封包，以找出其來源。請注意，並非每個項目都可以回溯檢查。

日誌	敘述
控制日誌	「控制日誌」包含應用程式存取的登錄機碼、檔案和 DLL，以及您電腦所執行應用程式的相關資訊。 您可以在「控制日誌」中執行下列工作： ■ 檢視控制事件的清單。 ■ 從「檔案」功能表，清除日誌中的所有項目。 ■ 從「檔案」功能表，將日誌中的資料匯出為 Tab 分隔文字檔案，以便在其他應用程式中使用。 ■ 從「檢視」功能表，切換本機檢視和來源檢視。 ■ 從「過濾」功能表，透過選取時間範圍來過濾項目。
安全日誌	「安全日誌」包含以您電腦為目標且可能帶來潛在威脅的活動相關資訊。服務阻斷攻擊、通訊埠掃描及執行檔變更等活動都是範例。 您可以在「安全日誌」中執行下列工作： ■ 檢視與安全相關的事件。 ■ 從「檔案」功能表，清除日誌中的所有項目。 ■ 從「檔案」功能表，將日誌中的資料匯出為 Tab 分隔文字檔案，以便在其他應用程式中使用。 ■ 從「檢視」功能表，切換本機檢視和來源檢視。 ■ 從「過濾」功能表，根據時間範圍或嚴重性來過濾項目。 ■ 從「動作」功能表，回溯檢查用於嘗試攻擊的資料封包，以找出其來源。請注意，並非每個項目都可以回溯檢查。 ■ 讓用戶端停止攔截其他電腦所進行的攻擊。
系統日誌	「系統日誌」包含發生在您電腦上的所有作業變更相關資訊。範例包括當服務啟動或停止、電腦偵測網路應用程式或架構軟體時的活動。 您可以在「系統日誌」中執行下列工作： ■ 檢視每當您的電腦連接至網路時的系統事件清單。 ■ 從「檔案」功能表，清除日誌中的所有項目。 ■ 從「檔案」功能表，將日誌中的資料匯出為 Tab 分隔文字檔案，以便在其他應用程式中使用。 ■ 從「過濾」功能表，根據時間範圍或嚴重性來過濾項目。

附註：如果您登入的是受管用戶端，部分日誌中的某些選項可能無法使用。是否能使用這些選項取決於您的管理員所允許的項目。這個注意事項適用於「網路威脅防護」及「用戶端管理流量」、「封包」、「控制」、「安全」及「系統」日誌。

在任何日誌中，不適合特定項目的選項可能無法使用。

檢視日誌及日誌詳細資料

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. 在您要檢視的日誌類型旁邊，按下「檢視日誌」，再按下日誌名稱。

   您可以從任何「網路威脅防護」日誌及「用戶端管理」日誌的檢視畫面切換至其他日誌的檢視畫面。若要存取其他日誌，請使用對話方塊上方的「檢視」功能表。
3. 如果已開啟一個「網路威脅防護」或「用戶端管理」日誌的檢視畫面，請按下「本機檢視」或「來源檢視」。

   日誌中的直欄會根據您選擇的是本機檢視或來源檢視而改變。本機檢視會從本機通訊埠及遠端通訊埠的觀點來顯示內容。這種觀點較常用於主機型防火牆。來源檢視會從來源通訊埠及目的通訊埠的觀點來顯示內容。這種觀點較常用於網路型防火牆。

如果「網路威脅防護」日誌和「用戶端管理」日誌中的項目有更多資訊可以提供時，這些資訊會顯示在下列位置：

- 「敘述」資訊會顯示在日誌檢視畫面的左下方窗格。
- 「資料」資訊會顯示在日誌檢視畫面的右下方窗格。

您也可以檢視「防毒和防間諜軟體防護」、「竄改防護」及「主動型威脅防護」日誌中任何項目的詳細資料。若是「風險」日誌，詳細資料還會提供額外的資訊，這些資訊不會顯示在日誌檢視主視窗中。

檢視「防毒和防間諜軟體防護」、「竄改防護」及「主動型威脅防護」日誌中的日誌項目詳細資料

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「防毒和防間諜軟體防護」、「竄改防護」或「主動型威脅防護」旁邊，按下「檢視日誌」。
3. 按下您要檢視的日誌名稱。
4. 在清單中的項目上按下滑鼠右鍵，然後選取「屬性」。

過濾日誌檢視

您可以利用幾種不同的方式過濾部分日誌的檢視。您可以依發生的時段過濾「網路威脅防護」和「用戶端管理」日誌中的事件、依靈敏度等級過濾部分「網路威脅防護」日誌中的事件、依事件類型過濾「防毒和防間諜軟體防護」系統日誌和「主動型威脅防護」系統日誌中的事件。

依時段過濾項目

部分日誌可以依事件發生的時段過濾。

依時段過濾日誌項目

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「網路威脅防護」或「用戶端管理」右側，按下「檢視日誌」。
3. 按下要檢視的日誌名稱。
4. 在日誌檢視視窗中，按下「過濾器」，然後選取要檢視日誌事件的時段。

   例如，如果選取「2 週日誌」，日誌檢視器會顯示過去 14 天記錄的事件。

按嚴重性等級過濾項目

您可以按嚴重性等級過濾「網路威脅防護安全日誌」、「用戶端管理安全日誌」和「系統日誌」檢視中的資訊。根據預設，所有嚴重性等級的事件都會顯示。

按嚴重性等級過濾日誌項目

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「網路威脅防護」或「用戶端管理」右邊，按下「檢視日誌」，然後再按下「安全日誌」或「系統日誌」。
3. 在日誌檢視視窗中，按下「過濾器」，然後再按下「嚴重性」。
4. 選取並取消勾選下列一項：
   - 重要 (僅安全日誌)
   - 主要 (僅安全日誌)
   - 次要 (僅安全日誌)
   - 錯誤 (僅系統日誌)
   - 警告 (僅系統日誌)
   - 資訊

   取消勾選項目會將該嚴重性等級的事件自檢視中清除。
5. 您可以按下「嚴重性」，然後再選取另一個等級自檢視清除其他嚴重性等級。

依事件類別過濾系統日誌

在「防毒和防間諜軟體防護」系統日誌和「主動型威脅防護」系統日誌中，事件會分類如下：

- 架構變更
- Symantec AntiVirus 啟動/關閉

- 病毒定義檔
- 略過掃描
- 轉送到隔離所伺服器
- 傳送至賽門鐵克安全機制應變中心
- 載入/卸載自動防護
- 用戶端管理與漫遊
- 日誌轉送
- 未授權通訊 (拒絕存取) 警告
- 登入與憑證管理
- 用戶端遵從
- 主動型威脅掃描載入錯誤
- 主動型威脅掃描商用應用程式載入錯誤
- 不支援主動型威脅掃描作業系統

您可以只顯示特定的事件類型，來減少出現在這兩個「系統日誌」中的事件數目。例如，如果只要檢視與「自動防護」相關的事件，可以只選取「載入/卸載自動防護」類型。如果選取一個類型，並不會停止記錄其他類別的事件。這只會在您顯示「系統日誌」時，隱藏其他類別。

附註：只有相關的事件才能排除在檢視以外。

依事件類別過濾系統日誌

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「防毒和防間諜軟體防護」或「主動型威脅防護」旁，按下「檢視日誌」。
3. 按下「系統日誌」。
4. 按下「過濾」。
5. 勾選或取消勾選一或多個事件類別。
6. 按下「確定」。

管理日誌大小

您可以架構項目保存在日誌中的時間。刪除較舊的項目以免讓日誌佔用太多的磁碟空間。您還可以為網路威脅防護日誌和用戶端管理日誌設定使用的空間容量。

架構防毒和防間諜軟體防護日誌項目和主動型威脅防護日誌項目的保留時間

架構保留日誌項目的時間

1. 在用戶端「狀態」頁的「防毒和防間諜軟體防護」旁，按下「選項」，然後按「變更設定」。
2. 在「一般」標籤中，設定在這些日誌中保留項目的數值和時間單位。比您設定的值更舊的項目都會予以刪除。
3. 按下「確定」。

架構網路威脅防護日誌及用戶端管理日誌的大小

您可以設定每個「網路威脅防護」日誌及「用戶端管理」日誌的日誌大小。

變更日誌的大小

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，在「日誌」標籤上的「日誌檔大小上限」文字欄位中，輸入您想要的日誌檔大小 KB 數上限。

   由於電腦可用空間有限，您應該維持較小的日誌檔大小。除了「控制日誌」和「封包日誌」以外，所有日誌的預設大小均為512KB。「控制日誌」和「封包日誌」的預設大小則為 1024 KB。
3. 按下「確定」。

架構網路威脅防護日誌項目和用戶端管理日誌項目的保留時間

您可以指定要將項目儲存在每個日誌中的天數。達到天數上限後，就會取代最舊的項目。您可能會想要刪除項目來節省空間，或保留項目以檢閱電腦的安全性。

設定保留日誌項目的天數

1. 在用戶端「狀態」頁面的「網路威脅防護」或「用戶端管理」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，在「日誌」標籤上的「儲存每個日誌項目」文字欄位中，輸入日誌項目的儲存天數上限。
3. 按下「確定」。

關於刪除防毒和防間諜軟體系統日誌的內容

您無法透過使用者介面永久移除「系統日誌」的事件記錄。

刪除網路威脅防護日誌及用戶端管理日誌的內容

如果您的管理員允許，您可以清除「網路威脅防護」日誌及「用戶端管理」日誌的內容。在清除日誌後，每個日誌又會立即開始儲存項目。

附註：如果清除選項無法使用，您就沒有刪除日誌內容的權限。

如果您有權限，也可以從日誌本身的「檔案」功能表清除日誌的內容。

刪除日誌的內容

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「架構網路威脅防護」對話方塊的「日誌」標籤上，於您所要的日誌旁邊，按下「清除日誌」。
3. 當要求您確認時，請按下「是」。
4. 按下「確定」。

從風險日誌和威脅日誌隔離風險及威脅

您可以隔離已經記錄到「主動型威脅防護威脅記錄日誌」的威脅、從「防毒和防間諜軟體風險日誌」隔離風險，或也可以從「防毒和防間諜軟體風險日誌」清除和刪除風險。

隔離風險或威脅

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「防毒和防間諜軟體防護」或「主動型威脅防護」旁，按下「檢視日誌」，然後按下所要的日誌名稱。
3. 選取風險或威脅，然後按下「隔離」。

   根據風險偵測的預設動作，Symantec Endpoint Protection 不一定能夠執行您選取的動作。如果威脅或風險成功置入隔離所，您會看到成功訊息。您不需要執行任何進一步動作，電腦已經安全而不會受到此風險或威脅的影響。您可以將因為風險而被隔離的檔案留在「隔離所」中，或者將它們刪除。您應該將它們留在「隔離所」中，直到確定電腦上的應用程式未遺失任何功能為止。

   請參閱第 74 頁的「關於隔離所中受感染的檔案」。

   若 Symantec Endpoint Protection 無法將風險或威脅置入隔離所，您會看到錯誤訊息。在此情況下，請聯絡您的管理員。

您也可以清除和刪除風險及威脅，以及視情況從這些日誌還原動作。

請參閱第 18 頁的「處理受感染的檔案」。

使用網路威脅防護日誌及用戶端管理日誌

「網路威脅防護」日誌及「用戶端管理」日誌可讓您追蹤電腦的活動，以及其與其他電腦和網路的互動。這些日誌會記錄嘗試透過您的網路連線，進出您電腦之流量的相關資訊。這些日誌也會記錄防火牆政策套用至用戶端後之結果的相關資訊。

您可以從一個中央位置管理「網路威脅防護」用戶端日誌及「用戶端管理」用戶端日誌。「安全」、「流量」及「封包」日誌可讓您追蹤回溯檢查某些資料的來源。它會使用 ICMP 來判斷電腦與另一台電腦上的入侵者之間的所有躍點來追蹤回溯。

附註：這些日誌的某些選項可能會因管理員為用戶端設定的控制類型而無法使用。

重新整理網路威脅防護日誌及用戶端管理日誌

重新整理日誌

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「網路威脅防護」或「用戶端管理」右側，按下「檢視日誌」，再按下您要的日誌名稱。
3. 在「檢視」功能表上，按下「重新整理」。

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。如果您的管理員允許，您就可以啟用或停用「封包日誌」。

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」。

停止主動回應

用戶端偵測出的任何入侵都會觸發主動回應。主動回應會在一段特定的時間內自動攔截已知入侵者的IP位址。如果管理員允許，您可以在「安全日誌」中立即停止主動回應。

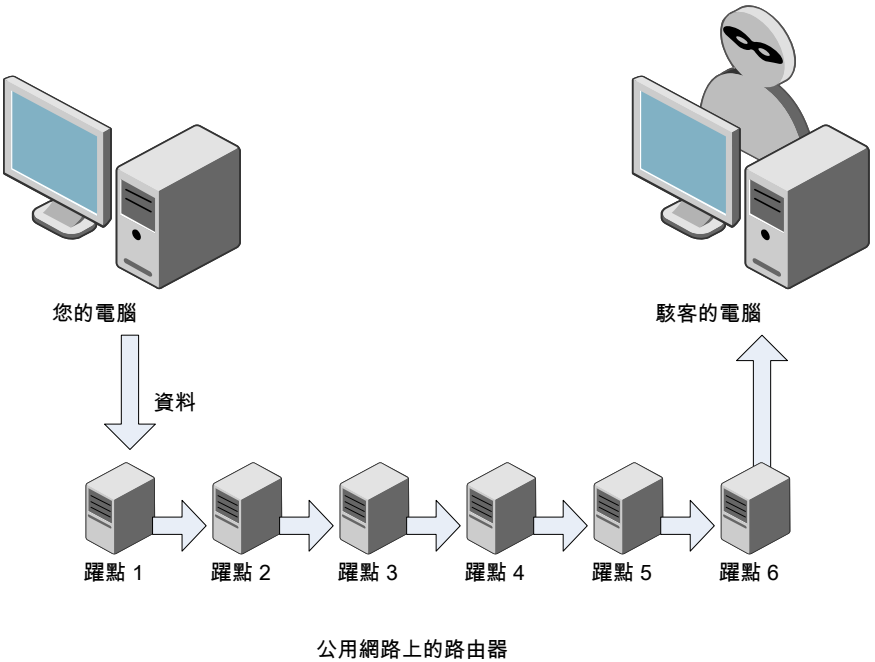
請參閱第 107 頁的「攔截攻擊電腦」。

回溯檢查記錄事件的來源

您可以回溯檢查事件，確切找出記錄事件的資料來源。如同鑑識人員在犯罪現場追查罪犯的蹤跡一般，回溯檢查會顯示連入流量進行的各個確切步驟或躍點。躍點是路由器之類的轉進點，封包會在Internet的各個電腦之間傳輸時通過躍點。回溯檢查會反向追蹤資料封包，找出資料經過哪些路由器到達您的電腦。

圖 10-1 顯示用戶端如何找出記錄事件的資料來源。

圖 10-1 回溯檢查封包



對於某些日誌項目，您可以追蹤攻擊嘗試中使用的資料封包。資料封包經過的各個路由器都有 IP 位址。您可以檢視 IP 位址和其他詳細資訊。顯示的資訊不保證可找出真正的駭客。最後的躍點IP位址會列出駭客連接的路由器所有人，這不一定是駭客自己。

您可以回溯檢查「安全日誌」和「流量日誌」中的某些記錄事件。

回溯檢查記錄事件

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「網路威脅防護」或「用戶端管理」右側，按下「檢視日誌」。然後，按下包含想要追蹤項目的日誌。
3. 在日誌檢視視窗中，選取想要追蹤的項目列。

4 按下「動作」，然後按下「回溯檢查」。

5 在「回溯檢查資訊」對話方塊中，按下**Whois>>**，檢視各個躍點的詳細資訊。

可向下捲動的窗格中顯示流量事件開始的IP位址所有人詳細資訊。您可以使用Ctrl-C 和 Ctrl-V，將面板中的資訊剪貼至要傳送給管理員的電子郵件訊息中。

6 再次按下 **Whois <<** 以隱藏資訊。

7 完成之後，按下「確定」。

在 Symantec Network Access Control 使用用戶端管理日誌

如果您已安裝 Symantec Network Access Control，可以從「安全日誌」和「系統日誌」的「動作」功能表中，執行下列工作：

- 更新政策
  請參閱第 15 頁的「更新安全性政策」。
- 檢查主機完整性
  請參閱第 115 頁的「執行主機完整性檢查」。

匯出日誌資料

您可以將某些日誌中的資訊匯出為逗號分隔值 (.csv) 或 Access 資料庫 (*.mdb) 格式的檔案。Csv 格式是大多數試算表及資料庫程式用來匯入資料的常用檔案格式。將資料匯入至另一個程式後，您就可以使用該資料來建立簡報、圖形或是與其他資訊結合。您可以將「網路威脅防護」日誌及「用戶端管理」日誌中的資訊匯出為 Tab 分隔文字檔案。

您可以將下列日誌匯出為 .csv 或 .mdb 檔：

- 防毒和防間諜軟體系統日誌
- 防毒和防間諜軟體風險日誌
- 防毒和防間諜軟體掃描日誌
- 主動型威脅防護系統日誌
- 主動型威脅防護威脅日誌
- 竄改防護日誌

附註：如果您以任何方式過濾了日誌資料，然後再將其匯出，就只會匯出目前過濾後的資料。對於匯出為 Tab 分隔文字檔案的日誌則沒有這種限制。那些日誌中的所有資料都會匯出。

請參閱第 128 頁的「過濾日誌檢視」。

您可以將下列日誌匯出為 Tab 分隔 .txt 檔：

- 用戶端管理控制日誌
- 網路威脅防護封包日誌
- 用戶端管理安全日誌
- 用戶端管理系統日誌
- 網路威脅防護流量日誌

附註：除了 Tab 分隔文字檔案以外，您還可以將「封包日誌」的資料匯出為網路監控格式或 NetXray 格式。

將資料匯出為 .csv 檔

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「防毒和防間諜軟體防護」或「主動型威脅防護」旁邊，按下「檢視日誌」。
3. 按下您要的日誌名稱。
4. 在日誌視窗中，確定您要儲存的資料已顯示出來。

   按下「匯出」。
5. 在「另存新檔」對話方塊中，輸入檔案名稱。
6. 瀏覽至您要儲存檔案的目錄。
7. 按下「存檔」。

將「網路威脅防護」日誌資料或「用戶端管理」日誌資料匯出為文字檔

1. 在用戶端的側邊看板中，按下「檢視日誌」。
2. 在「網路威脅防護」或「用戶端管理」右側，按下「檢視日誌」。
3. 按下您要匯出其資料的日誌名稱。
4. 按下「檔案」，再按下「匯出」。

   如果您選擇了「封包日誌」，也可以按下「匯出為網路監控格式」或「匯出為 **Netxray** 格式」。
5. 在「另存新檔」對話方塊中，輸入檔案名稱。
6. 瀏覽至您要儲存檔案的目錄。

   按下「存檔」。

索引