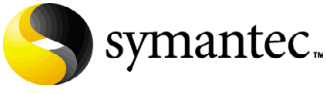
Symantec™ Client Security 用戶端指南



Symantec™ Client Security 用戶端指南

本手冊中所指的軟體內含授權許可協議，使用時必須遵守同意書中所記載的條款。

文件版本 2.0

印製地點：愛爾蘭

10 9 8 7 6 5 4 3 2 1

技術支援

「賽門鐵克全球技術支援小組」是 Symantec Security Response (賽門鐵克安全機制應變中心) 的一部份，負責全世界的支援中心。「技術支援小組」的主要角色並不是在回應有關產品特性 / 功能、安裝、架構的特定問題，與可從網路存取之技術智庫的製作內容問題。「技術支援小組」共同處理賽門鐵克內其它功能領域的問題，以便即時回答您的問題。例如，「技術支援小組」與「產品工程」和「賽門鐵克安全機制應變中心」合作，為病毒爆發與安全警示提供「警示服務」和「病毒定義檔更新」。

賽門鐵克技術支援提供的服務包括：

- 各種支援選擇，為各種規模的組織提供正確服務的選擇彈性
- 電話與網路支援元件，提供快速的回應及最新的資訊
- 升級保證，提供軟體自動升級防護
- 病毒定義檔與安全特徵的內容更新，確保最高等級的防護
- 來自 Symantec Security Response (賽門鐵克安全機制應變中心) 專家們的全球支援，為在「白金級技術支援程式」中註冊的客戶，提供各種語言一天 24 小時，一週 7 天的全球服務。
- 進階功能，如 Symantec Alerting Service 與 Technical Account Manager 角色，提供加強的回應與預先的安全支援

請拜訪我們的網站，取得有關「支援計劃」的最新資訊。根據購買的支援等級與使用的特定產品，可用的特定功能可能會有所不同。

授權與註冊

如果您操作的產品需要註冊和 / 或授權碼，可連上賽門鐵克授權與註冊網站 www.symantec.com.tw/certificate，這是註冊服務最迅速簡單的方式。或者，您也可以連上 www.symantec.com.tw/region/tw/techsupp/enterprise，選取您要註冊的產品，然後再從產品首頁選取「授權與註冊」 (Licensing and Registration) 連結。

聯絡技術支援

具有最新支援合約的客戶可以透過電話或從網路與技術支援取得聯絡，網址是 www.symantec.com.tw/region/tw/techsupp。

具有白金級技術服務合約的客戶可以透過 「白金級」網站與 「白金級技術支援」小組聯絡，網址是 www-secure.symantec.com/platinum/。

聯絡技術支援小組時，請備妥下列資訊：

- 產品版本
- 硬體資訊
- 可用記憶體、磁碟空間、NIC 資訊
- 作業系統
- 版本與修正程式
- 網路拓樸
- 路由器、閘道器和 IP 位址資訊
- 問題描述
  - 錯誤訊息 / 日誌檔
  - 聯絡賽門鐵克前執行的疑難排解
  - 最近的軟體架構變更和 (或) 網路變更

客戶服務

若要線上聯絡 「企業客戶服務」，請造訪 www.symantec.com 選取適合您所在國家的全球網站，然後選擇 「售後服務」。「客戶服務」可協助您處理下列類型的事項：

- 關於產品授權或序號的問題
- 產品註冊更新，如地址或名稱變更
- 一般產品資訊 (功能、可用語言、當地經銷商)
- 產品更新與升級的最新資訊
- 升級保證與維修合約的資訊
- Symantec Value License Program 的資訊
- 賽門鐵克技術支援選項的說明
- 非關技術的預售問題
- 遺失光碟或手冊，或是有瑕疵

目錄

第 7 章 Symantec Client Security 防火牆用戶端基礎篇

第 8 章 使用網路偵測與區域

第 9 章 防範入侵

第 11 章 監視 Symantec Client Security 防火牆用戶端

索引

Chapter 1

介紹 Symantec Client Security

本章包含以下主題：

關於 Symantec Client Security

有效防護不受到安全性威脅需要包含多層防護與回應機制的詳細安全性解決方案。Symantec Client Security 有助於防止組織網路的*用戶端*層級散佈複雜的 Internet 病毒。每個用戶端都是一個網路伺服器、工作站或個人電腦。一個網路可以包含多個用戶端，而且可以提供您存取網路與 Internet 資源的權限。

雖然您可能已經嘗試以很謹慎的方式工作了，您的網路電腦還是很容易受到數千種威脅，如病毒和駭客入侵。因此，網路時常會遭受新的威脅。表面上無害的活動 (如閱讀電子郵件和開啟檔案附件) 都可能使您的電腦以及連接您網路的所有用戶端受到威脅。只是位於相同網路的其它用戶端也會使您的用戶端電腦受到威脅。

Symantec Client Security 會使用多個整合的安全性技術防護企業網路中的所有用戶端，包括遠端使用者和手提式電腦。

安全性威脅類型

表 1-1 列出並說明用戶端容易遭受的威脅類型。

表 1-1 威脅類型

威脅類型	說明
病毒與其它威脅	可感染其它程式、開機磁區、分割磁區或支援巨集的文件之程式或程式碼。病毒會自行插入或附加到受害者的電腦。大多數的病毒只是複製，但很多也會造成傷害。 非病毒類的威脅，如廣告軟體或窺視程式，是以它們從事的行為，以及設計的目的來分類的。 請參閱第 18 頁的「關於病毒與其它威脅」。
入侵嘗試	安全性破壞，包含嘗試危及資源的完整性、機密性或可用性。入侵可能是從組織外部或內部發生。
未經授權的通訊埠掃描	攻擊者或工具嘗試侵入電腦所傳送的一連串訊息。攻擊者每次傳送一個訊息到一個通訊埠。未經授權的通訊埠掃描可協助攻擊者了解電腦執行哪些電腦網路服務，以及其弱點在哪裡。然後攻擊者就會嘗試利用可用的服務。
複雜的病毒	複雜的病毒種類和其它入侵可以用不同的方法造成破壞並四處散佈。複雜的病毒包含將其它病蟲的元素結合為單一病毒的病蟲，它可用不同的方法攻擊受害者。例如，W32.HLLW.Kazmor 是特洛伊木馬程式的後門，可讓駭客控制受到威脅的電腦。W32.HLLW.Kazmor 會利用共用磁碟機散佈到區域網路上。病蟲也會嘗試散佈到 KaZaA 檔案共用的網路。 W32.HLLW.Kazmor 會偽裝成電影或遊戲程式等，或是誘騙 KaZaA 使用者下載程式，然後將程式開啟的軟體檔案。 複雜的病毒包含混合型病毒。

表 1-1 威脅類型

威脅類型	說明
混合型病毒	將病毒、病蟲、特洛伊木馬程式和惡意程式碼與伺服器和 Internet 弱點結合，以便起始、傳送和散佈攻擊的病毒。混合型病毒使用多種方法和技術來快速散佈，並透過網路對所連接的用戶端造成廣大的損害。 混合型病毒會： ■ 造成損害。它們可以對目標 IP 位址啟動隱蔽服務攻擊、損壞 Web 伺服器或植入特洛伊木馬程式，以便於日後執行。 ■ 以多種方法散佈。它們會掃描弱點來危害系統，例如在伺服器的 HTML 檔案中嵌入程式碼，讓探訪者受到此網站的感染，或將病蟲附件加在受威脅伺服器的未授權電子郵件上。 ■ 從不同處發動攻擊。它們會將惡意程式碼放到系統的 .exe 檔中、提升 Guest 帳戶的權限等級、建立可寫入的網路共用、變更大量登錄資料，並將程序檔碼加到 HTML 檔案中。 ■ 不需人為介入即可散佈。它們會持續掃描要攻擊的脆弱伺服器的 Internet。 ■ 利用弱點。它們會利用已知的弱點，例如緩衝區超上限、HTTP 輸入驗證弱點，以及已知的預設密碼來取得未經授權的管理存取。 W32.Nimda.A@mm 是混合型病毒的範例。它是使用多種方法大量擴散的電子郵件病蟲。此病蟲會藉由電子郵件傳送，或搜尋開放的網路共用，然後嘗試將自己複製到無法修復或脆弱的 Microsoft IIS Web 伺服器。W32.Nimda.A@mm 也具有病毒的特性，會感染本機檔案和遠端網路共用上的檔案。

何處可以找到最新病毒的相關資訊

Symantec Client Security 由 Symantec Security Response (賽門鐵克安全機制應變中心) 支援。若需安全性威脅的最新資訊，請至 「賽門鐵克安全機制應變中心」網站：

www.symantec.com.tw/region/tw/avcenter/

Symantec Client Security 技術如何共同合作

Symantec Client Security 技術會以下列方式共同合作防護用戶端：

■ 當 Symantec Client Security 入侵偵測技術發現有人嘗試入侵用戶端時，便會通知 Symantec Client Security 防火牆用戶端攔截入侵者的位址達半小時之久。

- 當 Symantec Client Security 防火牆用戶端技術發現內送或外寄檔案時，便會通知防毒保護掃描該檔案。
- 如果防毒掃描判斷該檔案受到感染，便會通知 Symantec Client Security 防火牆用戶端將威脅等級提高為「高」，並採取預設動作將檔案攔截下來，使其無法存取 Internet 或進入用戶端。

附註：只有 64 位元的電腦會受到 Symantec Client Security 防毒用戶端的防護。不支援 Symantec Client Security 防火牆用戶端。

管理 Symantec Client Security

在 Symantec Client Security 設定中，您可以根據先前 Symantec Client Security 在您的電腦上的設定，來進行變更並執行作業。在某些組織中，網路管理員或「服務台」人員會安裝 Symantec Client Security，所以他們可以管理您所有的安全性需求。您不必與 Symantec Client Security 互動，便可以防護您的電腦不受到安全性的威脅。您可以依賴您公司的安全性管理團隊來防護您的用戶端。

在其它組織中，可能會安裝 Symantec Client Security，讓您可以變更某些設定。如果 Symantec Client Security 選項變淡，您便無法進行存取。

Symantec Client Security 安裝

在大多數情況下，您的網路管理員會為您網路上的所有用戶端管理 Symantec Client Security 的安裝。

在用戶端電腦上安裝 Symantec Client Security 防毒用戶端的方法有好幾種。如果您負責安裝 Symantec Client Security 防毒用戶端，則您的系統管理員可以為您提供相關說明。

如果您負責安裝 Symantec Client Security 防火牆用戶端，則您的系統管理員可以為您提供相關說明。

Symantec Client Security 防護更新

Symantec Client Security 包含更新機制，可讓您的用戶端保有最新的攻擊防範資訊。這屬於小型更新，因此可讓您對於您公司網路上的新威脅進行快速回應。在大多數情況下，您的網路管理員可為您網路上的所有用戶端管理 Symantec Client Security 的更新。

Section 1

Symantec Client Security 防毒用戶端

16

Chapter 2

介紹 Symantec Client Security 防毒用戶端

本章包含以下主題：

關於 Symantec Client Security 防毒用戶端

您的 Symantec Client Security 病毒防護可以安裝成單機版或由管理員管理的版本。單機版表示您的 Symantec Client Security 軟體不是由網路防毒管理員所管理。

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，例如家用電腦或單機型的筆記型電腦，並已使用預設選項設定或管理員預設的選項設定安裝 Symantec Client Security
- 連接至您企業網路之前即符合安全性需求的遠端電腦

Symantec Client Security 的預設設定可提供電腦完整的病毒防護。但是，您可能要加以調整，使系統效能最佳化、停用不適用的選項，並允許 Symantec Client Security 掃描病毒之外的威脅，例如廣告軟體或窺視程式。

如果您的安裝是由防毒管理員所管理，便會根據管理員的防毒政策，將某些選項鎖定或停用，甚至完全不出現。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。

您的防毒管理員將會告訴您 Symantec Client Security 有哪些用途。

附註：若選項顯示掛鎖圖示，表示您的防毒管理員已經將其鎖定，因此無法使用。除非防毒管理員先解除鎖定，否則您將無法變更這些選項。

關於連線至企業網路的遠端電腦

連線至企業網路的遠端電腦可以接收病毒定義檔與程式檔更新，也可以受到 Symantec System Center 管理員程式的管理。

系統管理員可能會要求連線至企業網路的遠端電腦符合某些安全性需求。例如，在連線至網路前，該電腦可能必須執行具備最新病毒定義檔的 Symantec Client Security。不符合安全性需求的電腦可能會被拒絕存取網路。

關於病毒與其它威脅

所謂*病毒*是一種電腦程式，會在執行時將其本身的複本附加到其它電腦程式或文件。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，並將其本身附加到其它程式或文件中。

病毒通常會傳送特殊的任務，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。

所謂的*病蟲*是一種特殊類型的病毒，它會從一台電腦複製其本身到另一台電腦上，且可使用記憶體。病蟲通常存在於其它檔案中，例如 Microsoft Word 或 Excel 文件。病蟲可以釋放出已經含有其病蟲巨集的文件。

*混合型威脅*使用多種方法及技術散佈與攻擊。例如，Nimda 病毒在 24 小時之內便造成兩百萬台以上的電腦感染，它兼具病毒和病蟲的特性，而且會以四種不同感染方式自行散佈。

在 Symantec Client Security 的內容中，病毒一詞用來涵蓋所有以疑似病毒方式運作的威脅。

其它已知的程式，例如廣告軟體或窺視程式，可能會也可能不會對電腦造成威脅。Symantec Client Security 可以偵測這些其它威脅的類別。

關於其它威脅類別

病毒以外的威脅是依照它們的行為與所設計的目的而分類。Symantec Client Security 防毒用戶端 可偵測以下衍生型威脅類別：

- *窺視軟體*：一種單機的程式，可以秘密地監視系統活動、偵測如密碼以及其它機密的資訊，再將它轉播回另一台電腦。
- *廣告軟體*：是單機或附加的程式，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，而有追蹤瀏覽的習慣。廣告軟體也可以傳送廣告的內容。

  窺視程式與廣告軟體可以在不知情的狀況下，從網站 (通常是以分享軟體或免費軟體的形式)、電子郵件訊息，以及即時傳訊軟體下載。您可能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。
- *撥號程式*：這種程式通常會利用電腦，在沒有您的許可或不知情的狀況下，透過 Internet 撥號到 900 號碼或是 FTP 網站，而產生費用。
- *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，您可能在不知情的狀況下，從由網站 (通常是以分享軟體或免費軟體的形式)、電子郵件訊息，以及即時傳訊軟體下載程式。當您嘗試要刪除它時，它可以移動垃圾筒離開滑鼠，或是使滑鼠相反地按下。
- *遠端存取程式*：允許透過 Internet 存取，從其它電腦取得資訊，或是攻擊或改變電腦程式。例如，您可能在不知情的情況下，或是在其它程序中安裝了一個程式。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。
- *駭客工具*：駭客在未經授權情況下，用來存取電腦的程式。例如，有一種駭客工具叫做按鍵記錄程式，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弱點掃描。駭客工具也可以用來建立工具，以便在建立病毒時使用。
- *追蹤軟體*：是一種單機或附加的應用程式，可追蹤使用者在 Internet 上的路徑，並將資訊傳送到目標系統。例如，該應用程式可以從網站、電子郵件訊息，或是即時傳訊軟體下載。然後它就可以取得關於使用者行為的機密資訊。
- *安全風險*：威脅與嚴格的病毒定義、特洛伊木馬程式、病蟲，或其它衍生型威脅類別不一致，但它可能代表對您的電腦與資料的威脅。

Symantec Client Security 預設會掃描病毒、特洛伊木馬程式及病蟲。您必須啟動 Symantec Client Security 的衍生型威脅掃描，以偵測其它類型的威脅。

Symantec Security Response (賽門鐵克安全機制應變中心) 網站提供關於威脅的最新資訊，並包含大量的威脅參考資訊，例如白皮書和關於病毒與其它威脅的詳細資訊。

圖 2-1 顯示關於駭客工具威脅的資訊，以及「賽門鐵克安全機制應變中心」建議的處理方式。

圖 2-1 賽門鐵克安全機制應變中心的衍生型威脅說明

請參閱第 37 頁的「存取 Symantec Security Response (賽門鐵克安全機制應變中心) 網站」。

Symantec Client Security 對病毒與其它威脅的應變方式

不論來源為何，Symantec Client Security 都能保護電腦不受病毒與其它威脅感染。來自硬碟、磁片及網路的其它病毒都將無法入侵電腦。電腦也不會受到經由電子郵件附件或其它方式傳播的病毒與其它威脅感染。例如，當您存取 Internet 時，威脅可能會在您不知情的情況下，將自身安裝在您的電腦上。

壓縮檔內的檔案也會被掃描並除毒。Internet 型的病毒不需要變更個別的程式或選項。「自動防護」掃描會自動在下載未壓縮的程式與文件檔時，進行掃描。

Symantec Client Security 會以相關動作與備份作業來因應處理受到病毒感染的檔案。根據預設，當掃描作業偵測到病毒時，Symantec Client Security 會嘗試清除受感染檔案中的病毒。如果檔案已完成清除，即表示病毒已從檔案中成功且完全地移除。如果 Symantec Client Security 因為某些原因而無法清除檔案中的病毒，Symantec Client Security 便會嘗試進行備份動作，將受到感染的檔案移到「隔離所」，使病毒無法擴散感染。

當病毒防護更新完畢之後，Symantec Client Security 會自動檢查是否有任何檔案存放在「隔離所」中，並讓您選擇是否使用新的防護資訊進行掃描。

附註：您的防毒管理員會選擇自動掃描「隔離所」中的檔案。

Symantec Client Security 可以回應某些進行刪除動作或只以備份進行記錄的威脅類別。刪除某些威脅時，也會造成您電腦上的網路瀏覽器等其它程式的問題。對於這些威脅類型，Symantec Client Security 會採取只記錄的動作。

當 Symantec Client Security 發現病毒之外的威脅時，會連結至 Symantec Security Response (賽門鐵克安全機制應變中心)，讓您可在此了解處理該威脅的最佳方式。您的系統管理員可能也會傳送一個自訂的訊息，告訴您應變的方式。

Symantec Client Security 保護您電腦的方式

病毒感染是可以輕易避免的。您電腦中的病毒能迅速偵測出並移除，它們不會傳染其它檔案而造成傷害。偵測到病毒時，Symantec Client Security 會通知您有一或多個檔案受到感染。

Symantec Client Security 提供三種防護類型：

- 自動防護：定期監視電腦活動，也就是在執行或開啟檔案時，以及進行諸如重新命名、儲存、搬移或複製等檔案修改動作時，查看是否出現病毒。「自動防護」並不會在衍生型威脅類別中搜尋威脅。
- 特徵掃描：在受感染的檔案中搜尋病毒特徵的蛛絲馬跡。此種搜尋作業即稱為*掃描*。根據管理電腦的方式，您和貴公司的防毒管理員可以起始特徵或型樣掃描，有系統地檢查電腦上的檔案是否有病毒和其它威脅，如廣告軟體或窺視程式。您可以依需求執行掃描，或排程掃描以自動執行掃描，或是在系統開機時自動執行掃描。特徵掃描會在手動與排程掃描時，搜尋衍生型威脅類別中的威脅。
- 進階啟發式：分析程式的結構、行為和其它屬性中疑似病毒的特性。在多數情況下，如果您是在更新病毒定義檔之前便遇到此威脅，則可保護電腦免於受到威脅感染 (例如透過電子郵件大量擴散的病蟲和巨集病毒)。進階啟發式會在 HTML、VBScript 和 JavaScript 檔中尋找程序檔式病毒。

Symantec Client Security 能保有最新的防護能力的原因

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。他們也會追蹤其它威脅的新類型，例如廣告軟體與窺視程式。一旦完成病毒或其它威脅辨識後，其*特徵*（病毒或威脅的相關資訊）即會被存入*病毒定義檔*，此檔案含有必要的資訊，可用來偵測及排除病毒或其它威脅。當 Symantec Client Security 掃描病毒和其它威脅時，它會搜尋這些特徵類型。

賽門鐵克會不斷追蹤新病毒，來提供更新的定義檔。Symantec Security Response（賽門鐵克安全機制應變中心）網站每天都會更新定義檔。至少會在每星期或在出現新的毀滅性病毒威脅時，都會以 LiveUpdate 提供新的定義檔。

如果新病毒太複雜，以致所發佈的新病毒定義檔不足以使用時，賽門鐵克的工程師會以最新的病毒偵測和修復元件來更新 AntiVirus 引擎。必要時，對 AntiVirus 引擎進行的更新也會包括病毒定義檔。

關於 Symantec Security Response（賽門鐵克安全機制應變中心）的角色

Symantec Client Security 背後的力量就是「賽門鐵克安全機制應變中心」。不斷增加的電腦病毒與其它威脅需要努力追蹤、辨識與分析新病毒及威脅，以及發展新的技術來保護您的電腦。

「賽門鐵克安全機制應變中心」研究專家會分解各種病毒樣本，查明其專有的特徵與行為。透過分析所得的資訊，他們進一步建立病毒定義，供賽門鐵克產品在進行掃描時藉以偵測及消滅新種病毒。

由於新種病毒散播的速度相當快速，尤其是透過 Internet 散佈時更形嚴重，「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。它可以透過 Internet 直接從您的「中央隔離所」，將受感染的檔案傳給「賽門鐵克安全機制應變中心」，使發現病毒、進行分析然後以電子郵件傳回解毒方法的時間從數天縮短到數小時，而不久的未來更可能進一步縮減到數分鐘內。

「賽門鐵克安全機制應變中心」的研究專家也會研究與製造防護電腦的技術，讓電腦不受窺視程式、廣告軟體及駭客工具等其它威脅的入侵。

「賽門鐵克安全機制應變中心」的百科全書擁有詳盡的病毒與其它威脅資訊。必要時，他們會提供關於刪除或移除該威脅的資訊。百科全書位於「賽門鐵克安全機制應變中心」網站。

請參閱第 37 頁的「存取 Symantec Security Response（賽門鐵克安全機制應變中心）網站」。

更新病毒防護的方式

您的防毒管理員會決定更新您病毒定義檔的方式。您不需要做任何事，便可以收到新的病毒定義檔。

您的防毒管理員可以設定 Symantec Client Security 中的 LiveUpdate 功能，以確定您的病毒與其它威脅防護保持最新的狀態。透過 LiveUpdate，Symantec Client Security 會自動連接特殊的網站、研判您的檔案是否需要更新、下載適當的檔案並將其安裝至適當的位置。

請參閱第 33 頁的「更新病毒防護」。

Chapter 3

Symantec Client Security 防毒用戶端基礎篇

本章包含以下主題：

開啟 Symantec Client Security 防毒用戶端

有數種開啟 Symantec Client Security 防毒用戶端 的方式。

開啟 Symantec Client Security 防毒用戶端

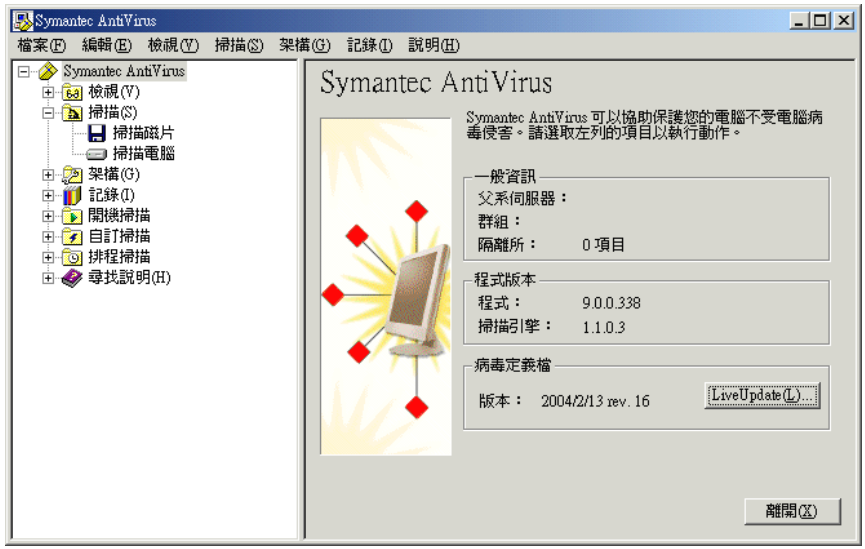
- 執行下列其中一個動作：
  - 在 Windows 工作列上，連按兩下 Symantec Client Security 防毒用戶端圖示。

    您的防毒管理員可決定是否要將此圖示顯示在工作列上。
  - 請選取 Windows 工作列上的「開始」>「程式集」>**Symantec Client Security** > **Symantec AntiVirus**。
  - 在 Windows XP 工作列上，按下「開始」>「程式集」> **Symantec Client Security** > **Symantec AntiVirus**。

瀏覽 Symantec Client Security 防毒用戶端主視窗

Symantec Client Security 防毒用戶端 主視窗分為兩個窗格。左邊的窗格會分門別類地列出您可以執行的活動。例如，「掃描」類別之下有「掃描磁片」和「掃描電腦」等作業。左窗格中的每一個圖示都代表一個類別。當您選取左窗格中的類別與其它項目時，右窗格會顯示執行作業所需的資訊。



瀏覽 Symantec Client Security 防毒用戶端 主視窗

- 在左窗格中，執行下列動作之一：
  - 按下 + 號可將資料夾展開。
  - 按下 - 號則將資料夾收合。
  - 選取任何一個項目，其相關資訊便會顯示在右窗格內。

檢視 Symantec Client Security 防毒用戶端類別

使用 Symantec Client Security 防毒用戶端 防毒用戶端執行的活動可以分為七個主要類別。每個類別都有一些您可以設定的選項。

下表並不討論您可以變更的個別選項，而是提供選項功能以及您如何找到這些選項的一般性說明。關於選項的特定資訊，請參閱線上說明。

檢視類別

您可以使用「檢視」類別來追蹤防毒活動。

表 3-1 檢視類別

選項	說明
自動防護掃描統計	檢視有關「自動防護」掃描狀態的統計數據，包括最後所掃描的檔案 (即使並未感染病毒)。
排程掃描	檢視預先建立在您電腦上執行的所有排程掃描清單，包括掃描作業名稱、排定執行時間及建立者姓名。排程掃描應由貴公司的防毒管理員或您本人建立。
隔離所	管理已隔離的中毒檔案以防其四處散播。 Symantec Client Security 只會將受病毒感染的檔案移到「隔離所」目錄。但不會移動如窺視程式和廣告軟體等其它威脅。 請參閱第 53 頁的「重新掃描隔離所內的檔案」。
備份項目	刪除中毒檔案的備份複本。Symantec Client Security 防毒用戶端 會在嘗試修複動作前先備份中毒項目的複本，作為資料安全防護屏障。在確認了 Symantec Client Security 防毒用戶端 已清除中毒項目裡的病毒後，您即應刪除「備份項目」中的複本。 Symantec Client Security 僅會備份受病毒感染的檔案。但不會備份如窺視程式和廣告軟體等其它威脅。 請參閱第 55 頁的「清除備份項目」。
修復項目	釋放病毒已清除但檔案位置不明的項目。例如，受感染的附件可能會從電子郵件訊息中移除而被隔離。當該項目在「隔離所」中清除病毒且移至「修復項目」後，您必須從「修復項目」還原該項目，並指定其還原的位置。
授權	檢視關於目前授權的資訊。目前的授權資訊包含授權狀態、續號，以及開始和到期日期。您可以啟動授權安裝精靈。

掃描類別

您可以使用「掃描」類別來執行對您的電腦進行手動掃描。

表 3-2 掃描類別

選項	說明
掃描磁片	掃描磁片及其它可移式媒體。

表 3-2 掃描類別

選項	說明
掃描電腦	隨時掃描檔案、資料夾、磁碟機或整個電腦。 請參閱第 43 頁的「起始手動掃描」。

架構類別

您可以使用「架構」類別來設定「自動防護」，以監視檔案和電子郵件附件 (適用於支援的電子郵件用戶端)。

表 3-3 架構類別

選項	說明
檔案系統自動防護	每當您存取、複製、儲存、移動或開啟任何檔案時，Norton AntiVirus 都會檢查該檔案是否受到病毒感染。 「檔案系統自動防護」包含 SmartScan 功能，啟動時，甚至可以判斷病毒變更檔案副檔名之後的檔案類型。 請參閱第 41 頁的「關於自動防護」。
「Lotus Notes 自動防護」和「Microsoft Exchange 自動防護」	對於群組軟體電子郵件用戶端 (Lotus Notes 和 Microsoft Exchange/Microsoft Outlook 用戶端)，Symantec Client Security 防毒用戶端 包含額外的電子郵件防護。

記錄類別

您可以使用「記錄」類別來追蹤資訊，包括在電腦上執行的掃描與所發現的病毒感染等資訊。

表 3-4 記錄類別

選項	說明
威脅記錄	檢視您的電腦所感染的病毒清單以及一些有關感染情況的相關資訊。檢視安裝在您電腦上的其它威脅資訊，如廣告軟體與窺視程式。其它威脅的記錄包括 Symantec Security Response (賽門鐵克安全機制應變中心) 網站的連結，其會說明威脅並提供處理指示。
掃描記錄	保留您電腦上過去曾發生的掃描作業記錄。掃描作業會連同其它相關資訊一併顯示。
事件日誌	檢視您電腦上有關防毒活動方面的記錄，包括架構變更、錯誤以及病毒定義檔資訊。

開機掃描類別

您可以在開機時，使用「開機掃描」類別來建立並架構在開機時要執行的掃描。

表 3-5 開機掃描類別

選項	說明
新增開機掃描	某些使用者會在排程掃描外加上開機掃描以補不足。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。 請參閱第 46 頁的「架構開機掃描」。

自訂掃描類別

您可以使用「自訂掃描」類別，建立您可以手動執行的預先架構掃描。

表 3-6 自訂掃描類別

選項	說明
新增自訂掃描	如果要定期掃描相同的檔案或資料夾，您可以專門針對這些項目建立自訂掃描。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感染。 請參閱第 47 頁的「架構自訂掃描」。

排程掃描類別

您可以使用「排程掃描」類別，建立在您所指定時間自動執行的預先架構掃描。

表 3-7 排程掃描類別

選項	說明
新增排程掃描	針對硬碟排定每週至少一次的掃描作業。排程掃描可確保您的電腦不會感染病毒。 請參閱第 45 頁的「建立排程掃描」。

啟動與停用自動防護

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，以防衛病毒。它會在程式執行時檢查病毒，並且監視您電腦上任何可能表示病毒存在的活動。在偵測到病毒或*疑似病毒活動*（疑似由病毒執行的事件）時，「自動防護」會警示您。

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，當您在安裝新的電腦程式時，就會發生這個情況。如果您要進行這類活動，而且要避免產生警告，您可以暫時停用「自動防護」。當您已經完成您的工作時，請確定啟動「自動防護」以確保您的電腦繼續受到防護。

您的管理員可能因為某種原因鎖定了「自動防護」，讓您無法停用，或是指定您可以暫時停用「檔案自動防護」，但超過指定的時間之後，便會自動重新啟動。

啟動與停用自動防護

Symantec Client Security 防毒用戶端 圖示會顯示在 Windows 桌面右下角的工作列中。在某些架構中，圖示不會顯示出來。

Symantec Client Security 防毒用戶端 圖示會以完整的防護罩模式出現，而且在啟動「自動防護」時，會在「啟動自動防護」旁邊出現一個勾號。

停用「自動防護」時，Symantec Client Security 防毒用戶端 圖示則會被一個通用的禁止符號（一個紅色圓圈，內有一個對角斜線）覆蓋。

從工作列啟動與停用「自動防護」

- 在 Windows 桌面的系統匣中，以滑鼠右鍵按下 Symantec Client Security 防毒用戶端 圖示，然後按下「**啟動自動防護**」。

從 Symantec Client Security 防毒用戶端 啟動或停用「自動防護」

1. 在 Symantec Client Security 防毒用戶端 的左窗格中，按下「**架構**」。
2. 在右窗格中，按下「**自動防護**」。
3. 勾選或取消勾選「**啟動自動防護**」。
4. 按下「**確定**」。
   目前的「自動防護」狀態會動態更新到勾選框的右側。

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，並在之後繼續進行。您可以暫停您起始的任何掃描。您的網路防毒管理員可決定您是否可以暫停管理員排定的掃描。

對於您的網路防毒管理員所起始的排程掃描，您也可以延遲掃描。如果您的管理員已啟動「延緩」功能，則您可以將管理員排定的掃描延緩到設定的間隔時間之後。繼續進行掃描時，便會從頭開始掃描。

如果您只是要暫時停止，之後要繼續進行掃描，則可暫停掃描。如果您不想中斷掃描，請使用「延緩」功能，將掃描延遲到較長的一段時間之後繼續進行，例如，在您做簡報做到一半時。

暫停或延緩掃描

使用下列步驟，暫停您起始的掃描，或是延緩管理員排定的掃描。如果無法使用「暫停掃描」按鈕，表示您的網路防毒管理員已停用「暫停」功能。

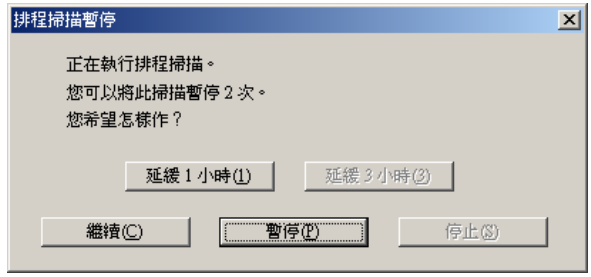
附註：當您選擇暫停掃描時，如果 Symantec Client Security 防毒用戶端 防毒用戶端正在掃描壓縮檔，則可能需要幾分鐘後才會回應。

暫停掃描

1 執行掃描時，請在「掃描電腦」對話方塊中，按下「暫停」圖示。

若是您起始的掃描，掃描會停在目前的階段，而「掃描」對話方塊也會一直開著，直到您重新啟動掃描為止。

如果是管理員排定的掃描，便會出現「排程掃描暫停」對話方塊。



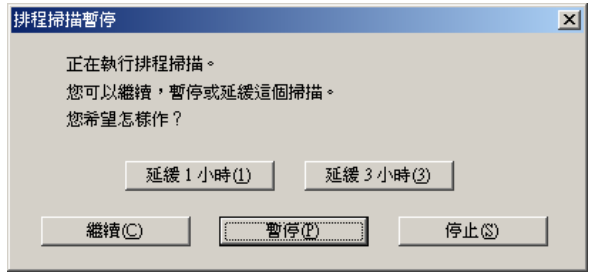
2 在「排程掃描暫停」對話方塊中，按下「暫停」。
管理員排定的掃描會停在目前的階段，而「掃描」對話方塊也會一直開著，直到您重新啟動掃描為止。

3 在「掃描」對話方塊中，按下「開始」圖示，繼續進行掃描。

延遲管理員排定的掃描

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遲掃描的時間週期。到達所設定的時間週期時，便會從頭開始掃描。在停用此功能之前，您的管理員會指定您可以延遲排程掃描的次數。

更新病毒防護

Symantec Client Security 防毒用戶端 防毒用戶端是依賴最新的資訊以偵測與移除病毒。而發生病毒問題的最常見原因之一就是在完成安裝後並未更新病毒定義檔。病毒定義檔包含關於所有新發現病毒的相關資訊。

賽門鐵克每週透過 LiveUpdate 和每天透過公佈在 Symantec Security Response (賽門鐵克安全機制應變中心) 網站上的 Intelligent Updater 檔案，提供更新的病毒定義檔。(出現新的高風險性病毒威脅時，也會公佈更新)。請務必養成每週至少更新一次病毒定義檔的習慣。自動執行排程 LiveUpdate 是讓您不要忘記更新的最簡易方法。如果有新的病毒威脅報告出現，請務必立即進行更新。

透過 LiveUpdate，Symantec Client Security 防毒用戶端 防毒用戶端會自動連線到特定的賽門鐵克 Internet 網站，並決定病毒定義是否需要更新。如果需要，它會下載適當的檔案，並將其安裝到適當位置。LiveUpdate 還會檢查與下載可用的 Symantec Client Security 防毒用戶端 防毒用戶端修正程式。一般而言，您無須設定 LiveUpdate 的每項細節。唯一需要的是 Internet 連線。

附註：您的管理員已經指定病毒定義檔可能會過期的最大天數。超過最大天數之後，若偵測到 Internet 連線，Symantec Client Security 防毒用戶端 防毒用戶端便會自動執行 LiveUpdate。

使用 LiveUpdate 排程病毒防護更新

根據預設值，LiveUpdate 排定在每個星期五晚上八點自動執行。執行排程更新時，您的電腦必須在開機狀態，並連線到 Internet。

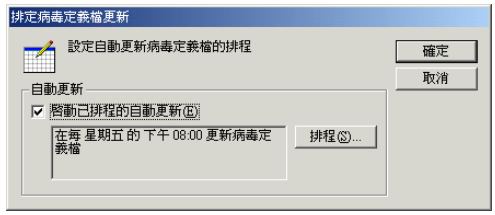
使用 LiveUpdate 排程病毒防護更新

您可以根據個人需求變更 LiveUpdate 的頻率和次數。

附註：在集中管理的網路中，您的系統管理員可能會負責散佈最新的病毒定義檔給各工作站。此時，您不須執行任何動作。

啟動排程 LiveUpdate

1 在 Symantec Client Security 防毒用戶端 的「檔案」功能表上，按下「排程更新」。



2 在「排定病毒定義檔更新」對話方塊中，勾選「啟動已排程的自動更新」。

3 按下「確定」。

4 在「排定病毒定義檔更新」對話方塊中，按下「確定」。

設定 LiveUpdate 排程選項

1 在「排定病毒定義檔更新」對話方塊中，按下「排程」。

2 在「病毒定義檔更新排程」對話方塊中，指定您要執行 LiveUpdate 的頻率、日期和時間。

3 按下「確定」。

設定進階 LiveUpdate 排程選項

1 在「病毒定義檔更新排程」對話方塊中按下「進階」。

2 在「進階排程選項」對話方塊中，執行下列動作之一：

- 若要設定 Symantec Client Security 防毒用戶端 防毒用戶端在稍晚時執行遺漏的已排程 LiveUpdate 事件，可勾選「在排定時間後的」，並設定天數。
- 若要設定 Symantec Client Security 防毒用戶端 防毒用戶端在指定的時間範圍內 (而非所設定的時間) 執行已排程的 LiveUpdate 事件，可勾選所要使用的隨機方法類型，並設定分鐘、星期幾、或日期。

3 按下「確定」。

利用 LiveUpdate 立即更新病毒防護

報告有新的病毒出現時，切勿等到下一次排程更新，應該立即更新病毒防護。

利用 LiveUpdate 立即更新病毒防護

1 在 Symantec Client Security 防毒用戶端 的左窗格中，按下 **Symantec AntiVirus**。

2 在右窗格中，按下 **LiveUpdate**。

3 必要時，在左窗格中按下「架構」來自訂 LiveUpdate 的 Internet 連線。
您可以變更您的 Internet 服務供應商連線，或是電腦透過 Proxy 伺服器連線到 Internet 的方式。
如需詳細資訊，請使用 LiveUpdate 的線上說明。

4 按「下一步」開始自動更新。

不透過 LiveUpdate 進行更新

賽門鐵克提供稱為 Intelligent Updater 的特殊程式，可以作為 LiveUpdate 的替代程式。您可以從 Symantec Security Response (賽門鐵克安全機制應變中心) 網站下載更新程式。

請參閱第 37 頁的「存取 Symantec Security Response (賽門鐵克安全機制應變中心) 網站」。

不透過 LiveUpdate 進行更新

1 將 Intelligent Updater (智慧更新程式) 下載到電腦上的任何資料夾。

2 從「我的電腦」或「Windows 檔案總管」視窗，找出並連按兩下 Intelligent Updater 程式。

3 遵循所有更新程式顯示的提示進行。
Intelligent Updater 程式會在您的電腦上搜尋 Symantec Client Security 防毒用戶端，然後在適當的資料夾內自動安裝新的病毒定義檔。

4 掃描您的磁碟以偵測新種病毒。

如需詳細資訊

若您需要 Symantec Client Security 防毒用戶端 防毒用戶端的詳細資訊，可以存取線上說明。此外，您也可以從賽門鐵克的網站取得病毒的相關資訊。

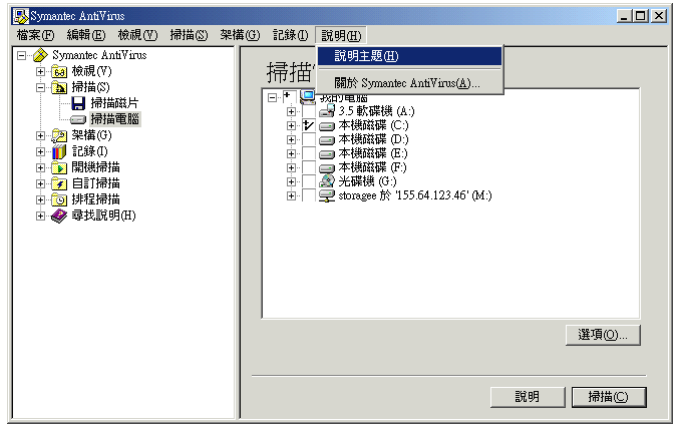
存取線上說明

Symantec Client Security 防毒用戶端 防毒用戶端線上說明列有一般資訊與逐步程序，可協助您保護電腦不受病毒侵襲。

附註：您的管理員可能已經決定不安裝說明檔。

使用 Symantec Client Security 防毒用戶端 取得說明

- 在 Symantec Client Security 防毒用戶端 中，執行下列其中一個動作：
  - 按下「說明」功能表內的「**說明主題**」。
  - 在右窗格中，按下「內容」。
    此處只顯示螢幕上您可以執行動作的上下文關聯說明。



存取 Symantec Security Response (賽門鐵克安全機制應變中心) 網站

如果您連接到 Internet，可以拜訪賽門鐵克安全機制應變中心網站，以檢視下列項目：

- 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
- 關於衍生型威脅的一般和詳細資訊

存取賽門鐵克安全機制應變中心網站

- 在您的 Internet 瀏覽器中，鍵入下列網址：
  www.symantec.com.tw/region/tw/avcenter

Chapter 4

保護您的電腦不受病毒侵襲

本章包含以下主題：

關於 Symantec Client Security 防毒政策

Symantec Client Security 預先設定的防毒政策適用於大部分的使用者。但是您可以依照個人需求變更設定。您也可以個別自訂「自動防護」、手動、排程、開機和自訂掃描的政策設定。

防毒政策會決定：

- 要掃描的內容
- 偵測到病毒時要執行什麼動作

要掃描的內容

Symantec Client Security「自動防護」預設會掃描所有檔案類型。手動、排程、開機及自訂掃描預設也會檢視所有檔案類型。

「自動防護」包括 SmartScan，它會掃描含有「程式副檔名清單」中之副檔名的所有檔案。無論這些所有執行檔及 Microsoft Office 文件的副檔名是否列在「程式副檔名清單」中，SmartScan 也會掃描它們。

請參閱第 42 頁的「修改自動防護與使用 SmartScan」。

您可以選擇根據副檔名或檔案類型 (文件與程式) 來掃描檔案，不過病毒防護能力會降低。

您也可以選擇不要掃描特定檔案。例如，如果有您知道並未感染病毒的檔案在掃描過程中觸發病毒警示，則可將該檔案從後續的掃描中排除，以防出現更多的警告。

依照檔案類型或副檔名掃描

Symantec Client Security 可以依照檔案類型或副檔名掃描您的電腦。

選取要掃描的檔案類型

1 在 Symantec Client Security 的左窗格中，選取您要變更的掃描。
   - 如果您選取手動掃描，按下「選項」。
   - 如果您選取開機、自訂或排程掃描，按下要變更的掃描名稱，然後按下「編輯」。
     這些變更只會套用到您所選取的特定掃描。
   - 如果您選取「自動掃描」，跳至步驟 2。
2 按下「選取的」，然後按下「類型」。
3 選取下列一個或多個檔案類型：
   - 文件檔：包括 Word 與 Excel 文件，以及與這些文件相關的範本檔。
   - 程式檔：包括動態連結程式庫 (.dll)、批次檔 (.bat)、通訊檔 (.com)、執行檔 (.exe) 與其它程式檔。
4 若是手動掃描，如果您想要在後續所有手動掃描永久使用這些動作，按下「儲存設定」。
5 按下「確定」。

偵測到病毒時要執行什麼動作

Symantec Client Security 防毒用戶端 會以相關動作與備份作業來因應處理受到感染的檔案。根據預設，當「自動防護」或掃描作業偵測到病毒時，Symantec Client Security 防毒用戶端 會嘗試清除受感染檔案的病毒。如果 Symantec Client Security 防毒用戶端 無法清除檔案裡的病毒，便會進行備份作業以記錄病毒清除失敗，並將受感染的檔案移到「隔離所」，使病毒無法擴散，同時讓您無法再存取該檔案。

根據您的防毒政策，您可以變更這些設定，以便在偵測到病毒時將受感染的檔案刪除或不予處理 (僅加以記錄)。在「自動防護」中，您也可以選擇拒絕存取。此外，您可以針對各種掃描類型，分別為巨集型和非巨集型病毒設定不同的處理作業。

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」包括可掃描副檔名群組，包含可執行的程式碼和所有的 .exe 與 .doc 檔的 SmartScan。當病毒變更檔案的副檔名時，SmartScan 可決定該檔案的類型。例如，即使病毒將 .doc 檔的副檔名變更為其它不同於 SmartScan 原本架構掃描的副檔名，SmartScan 還是會掃描該檔案。

若要彌補「自動防護」的不足，Symantec Client Security 防毒用戶端 會在安裝時，偵測您是否使用支援的群組軟體電子郵件用戶端，並新增對電子郵件的「自動防護」。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 6.0
- Microsoft Exchange 5.0 與 5.5、Microsoft Outlook 97、Microsoft Outlook 98 (僅限 MAPI，並非 Internet)、Microsoft Outlook 2000 和 Microsoft Outlook 2002

Symantec Client Security 防毒用戶端 也包括藉由監視所有使用 POP3 或 SMTP 通訊協定的流量，掃描其它 Internet 電子郵件程式的「自動防護」。您可以架構 Symantec Client Security 使用「Bloodhound 病毒偵測」，在內送訊息中掃描威脅，以及在外寄訊息中掃描已知的啟發式病毒。掃描外寄電子郵件有助於防止威脅的散播，例如病蟲可以利用電子郵件用戶端，透過網路來自我複製與散佈。

針對 Lotus Notes 與 Microsoft Exchange 電子郵件的掃描，Symantec Client Security 防毒用戶端 只掃描與電子郵件相關的附件。若是使用 POP3 或 SMTP 通訊協定的 Internet 電子郵件訊息掃描，Symantec Client Security 會掃描訊息內文與附加的任何附件。

當受支援的電子郵件用戶端啟動「自動防護」，而且您開啟一封有附件的訊息時，會立刻將附件下載到電腦並進行掃描。在連線速度慢時，下載具有大型附件的訊息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。

在某些情況下，必須暫時停用「自動防護」，例如在安裝新軟體時。

請參閱第 30 頁的「啟動與停用自動防護」。

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
- 使用 Secure Sockets Layer (SSL) 的 POP3
- 網頁型電子郵件，例如 Hotmail 及 Yahoo!

附註：電子郵件的「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。

修改自動防護與使用 SmartScan

「自動防護」預設為掃描所有檔案。掃描所有檔案或使用 SmartScan 可提供最大的病毒防護效果。在預設的情形下，會啟動 SmartScan。

Symantec Client Security 防毒用戶端 若只掃描選定副檔名的檔案，其速度會較快，例如 .exe、.com、.dll、.doc 和 .xls。雖然此種方法的防護效果相對較低，卻仍不失為有效的掃描動作，因為病毒只會感染某些特定的檔案類型。預設的副檔名清單代表此類檔案較易受到感染。

修改「自動防護」與使用 SmartScan

1 在 Symantec Client Security 防毒用戶端 的左窗格中，按下「架構」。

2 在右窗格中，按下「檔案系統自動防護」。

3 在「檔案類型」群組方塊中，執行下列其中一個動作：

- 按下「所有類型」，以後 Symantec Client Security 防毒用戶端 防毒用戶端便會掃描所有檔案。
- 按下「選取的」，命令 Symantec Client Security 防毒用戶端 防毒用戶端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。
- 確保已在 Symantec Client Security 防毒用戶端 中勾選 SmartScan，以便使用此功能掃描。

4 按下「確定」以儲存您的設定。

掃描病毒

除了「自動防護」這種功能最強大的防毒機制外，Symantec Client Security 防毒用戶端 還提供數種不同類型的掃描作業以增加更強大的防護功效。掃描類型包括：

- 手動掃描：隨時掃描檔案、資料夾、磁碟機或整個電腦。
- 排程掃描：按照指定頻率自動執行。
- 開機掃描：每當開啟電腦及載入 Windows 時即執行。
- 自訂掃描：隨時掃描指定的檔案集。

只要固定執行「自動防護」，通常針對所有檔案進行每週一次的排程掃描即已具備足夠防護效果。如果您的電腦經常受到病毒入侵，可以考慮增加開機掃描或每日進行排程掃描。另外，最好是養成磁片首次使用時即加以掃描的習慣，尤其是此類磁片曾經流通使用時。

關於掃描壓縮檔與編碼的檔案

Symantec Client Security 防毒用戶端 可掃描壓縮檔和編碼的檔案，例如 .zip 檔。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，以決定所支援的壓縮檔掃描類型。

如果啟動「自動防護」，便會掃描從壓縮檔移除的任何檔案，以保護電腦。

起始手動掃描

您可以隨時手動掃描病毒與其它威脅，例如廣告軟體與窺視程式。可以選取磁片上的單一檔案，或甚至整個電腦。

起始手動掃描

您可以從「我的電腦」或「Windows 檔案總管」視窗，或是 Symantec Client Security 防毒用戶端 防毒用戶端主視窗起始掃描。

從 Windows 起始手動掃描

- 在「我的電腦」或「Windows 檔案總管」視窗內，用滑鼠右鍵按下要掃描的檔案、資料夾或磁碟，然後按下「**掃描病毒**」。

附註：此項功能無法在 64 位元作業系統上使用。

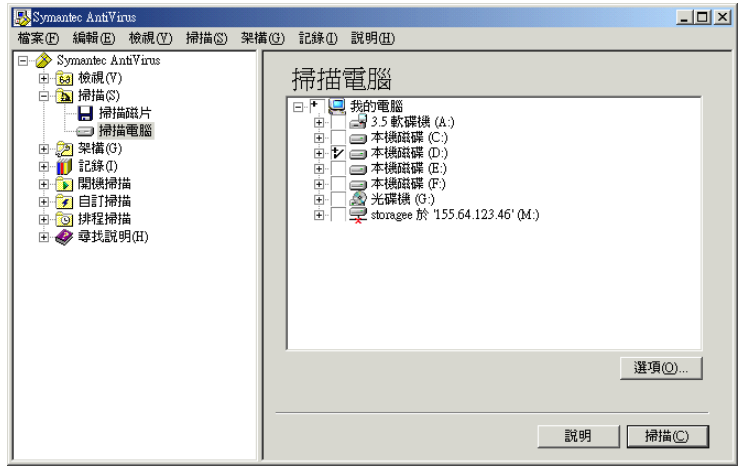
在 Symantec Client Security 防毒用戶端 中起始手動掃描

1 在 Symantec Client Security 防毒用戶端 左窗格中，展開「**掃描**」。

2 在左窗格中選取下列動作之一：

- 掃描磁片
  此選項僅適用於有配備軟碟機的電腦。

- 掃描電腦



3 在右窗格中執行下列動作：

- 連按兩下要開啟或關閉的磁碟機或資料夾。
- 勾選或取消勾選您想要掃描的項目。
  符號的意義如下：

	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。

4 按下「選項」，將已掃描的項目與偵測到病毒時的處理方式變更為預設值。
預設選項會掃描所有檔案、清除受感染檔案的病毒、以及在病毒無法移除時隔離受感染的檔案。通常只需要變更衍生型威脅與記憶體內之威脅掃描的設定。
您必須在「掃描選項」對話方塊中同時啟動這些選項。
如果只要將修改過的設定套用到目前進行的掃描，按下「確定」。若希望未來所有掃描動作均採用新的設定，按下「儲存設定」。

5 按下「掃描」。
Symantec Client Security 防毒用戶端 就會開始掃描並報告結果。

建立排程掃描

排程掃描是威脅防護的一項重要元件。請至少每週排定一次掃描作業，以確保您的電腦沒有病毒與廣告軟體與窺視程式等其它威脅存在。

附註：如果您的網路防毒管理員已經為您建立排程掃描，便會出現在「檢視」資料夾的「排程掃描」區域中，而不是在「排程掃描」資料夾中。「排程掃描」資料夾只會顯示您已經排程的掃描。

建立已排程的掃描

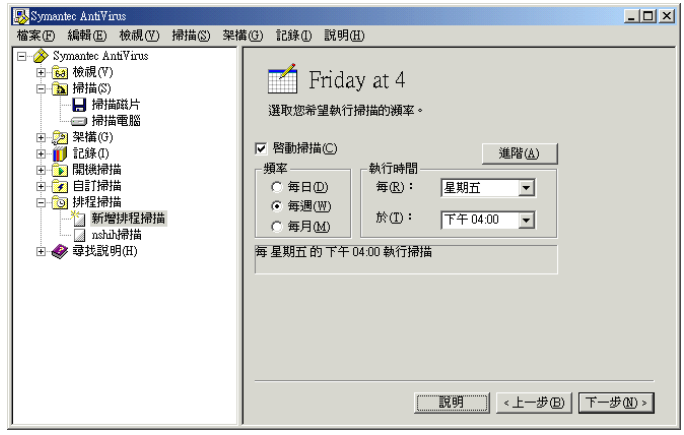
1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「**排程掃描**」。

2 在右窗格中，按下「**新增排程掃描**」。

3 輸入掃描的名稱和說明。
例如，將掃描作業稱為 Friday at 4。

4 按「下一步」。

5 設定掃描的頻率。



6 按「下一步」。

7 勾選樹狀目錄控制中的方塊以指定要掃描的位置。
您可以勾選任何東西，從整個電腦到單一檔案。
請參閱第 43 頁的「起始手動掃描」。

8 按下「選項」，將已掃描的項目與偵測到病毒時的處理方式變更為預設值。
預設選項會掃描所有檔案、清除受感染檔案的病毒、以及在病毒無法移除時隔離受感染的檔案。通常只需要變更衍生型威脅與記憶體內之威脅掃描的設定。您必須在「掃描選項」對話方塊中同時啟動這些選項。
如果只要將修改過的設定套用到目前進行的掃描，按下「確定」。若希望未來所有掃描動作均採用新的設定，按下「儲存設定」。

9 按下「儲存」。
進行排程掃描時，您的電腦必須開啟，而且必須載入「Symantec Client Security 防毒用戶端服務」。(根據預設，「Symantec Client Security 防毒用戶端服務」會在您開啟電腦時載入)。
新的掃描會新增到「排程掃描」資料夾的清單中。

架構開機掃描

某些使用者會在排程掃描外加上開機掃描以補不足。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：若您建立的開機掃描不只一個，則所有掃描動作會依照當初您建立的順序依次執行。

架構開機掃描

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「開機掃描」。

2 在右窗格中，按下「 新增開機掃描」。

3 輸入掃描的名稱和說明。

4 按「下一步」。

5 勾選樹狀目錄控制中的方塊以指定要掃描的位置。
您可以勾選任何東西，從整個電腦到單一檔案。
請參閱第 43 頁的「起始手動掃描」。

6 按下「選項」，將已掃描的項目與偵測到病毒時的處理方式變更為預設值。
預設選項會掃描所有檔案、清除受感染檔案的病毒、以及在病毒無法移除時隔離受感染的檔案。通常只需要變更衍生型威脅與記憶體內之威脅掃描的設定。您必須在「掃描選項」對話方塊中同時啟動這些選項。
如果只要將修改過的設定套用到目前進行的掃描，按下「確定」。若希望未來所有掃描動作均採用新的設定，按下「儲存設定」。

7 按下「儲存」。
掃描作業會在您開啟電腦及載入 Windows 時即執行。

架構自訂掃描

如果要定期掃描相同的檔案或資料夾，您可以專門只針對這些項目建立自訂掃描。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其它威脅感染。

架構自訂掃描

您可以建立自訂掃描，並隨時手動執行。

建立自訂掃描

1 在 Symantec Client Security 防毒用戶端 的左窗格中，按下「**自訂掃描**」。

2 在右窗格中，按下「**新增自訂掃描**」。

3 輸入掃描的名稱和說明。

4 按「**下一步**」。

5 勾選樹狀目錄控制中的方塊以指定要掃描的位置。
您可以勾選任何東西，從整個電腦到單一檔案。
請參閱第 43 頁的「起始手動掃描」。

6 按下「**選項**」，將已掃描的項目與偵測到病毒時的處理方式變更為預設值。
預設選項會掃描所有檔案、清除受感染檔案的病毒、以及在病毒無法移除時隔離受感染的檔案。通常只需要變更衍生型威脅與記憶體內之威脅掃描的設定。您必須在「掃描選項」對話方塊中同時啟動這些選項。
如果只要將修改過的設定套用到目前進行的掃描，按下「**確定**」。若希望未來所有掃描動作均採用新的設定，按下「**儲存設定**」。

7 按下「**儲存**」。

執行自訂掃描

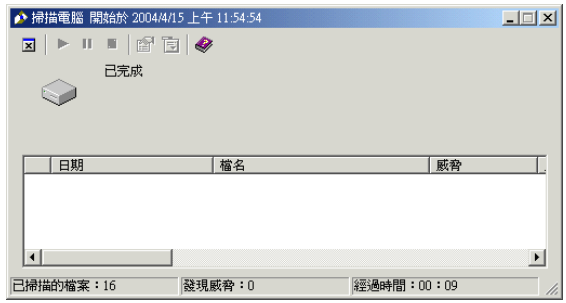
1 在 Symantec Client Security 防毒用戶端 的左窗格中，展開「**自訂掃描**」。

2 連按兩下已存檔的自訂掃描。

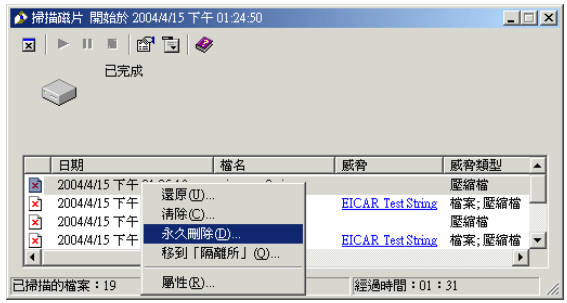
解析掃描結果

每當執行手動、排程、開機或自訂掃描時，Symantec Client Security 防毒用戶端會顯示「掃描電腦」對話方塊來報告進度。您可以暫停、重新啟動或停止掃描作

業。當掃描作業完成時，結果即會顯現在清單方塊中。若未偵測到任何病毒，清單方塊將呈空白，且狀態為「已完成」。



如果進行掃描時偵測到病毒，對話方塊會列出受感染檔案的名稱、病毒名稱和所採取的行動。根據預設，每當偵測到病毒時，系統還會發出警示。



請參閱第 51 頁的「對受感染的檔案採取的動作」。

附註：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「掃描電腦」對話方塊中。同樣地，您的管理員可能會選擇遇到病毒時不要顯示警示。

排除不進行掃描的檔案

在一些罕見的情況下，有些未帶病毒的檔案會被誤判為已受到感染。可能的原因在於特定的病毒定義檔設計是用來擷取所有可能的變種病毒。因為病毒定義檔一定會很廣泛，所以有時候 Symantec Client Security 防毒用戶端 會將未感染病毒的檔案誤判為已受到感染。

如果 Symantec Client Security 防毒用戶端 繼續將未感染病毒的檔案誤判為已受到感染，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。

如果資料夾中包含可能被偵測為威脅的軟體，例如追蹤軟體，且您公司的安全性政策允許您執行該軟體，您也可以排除該資料夾。

請參閱第 19 頁的「關於其它威脅類別」。

針對以下每一種掃描類型分別設定排除項目：「自動防護」、手動、排程、開機或自訂。不過，其間的設定程序都完全相同。

警告：請務必小心處理排除項目。將某一檔案排除在掃描作業之外時，如果該檔案未來遭受感染，系統亦不會對其採取任何動作。而這可能會對您的電腦安全造成潛在的危險。

排除某檔案進行掃描

1 在 Symantec Client Security 防毒用戶端 中，執行下列其中一個動作：

- 對於檔案系統的「自動防護」，請在左窗格中按下「**架構**」，然後在右窗格中按下「**自動防護**」。
- 對於電子郵件附件的「自動防護」，請在左窗格中按下「**架構**」，然後在右窗格中按下「**Lotus Notes 自動防護**」或「**Microsoft Exchange 自動防護**」。
- 至於其它各類型的掃描作業，則請在指定掃描類型的窗格中按下「**選項**」。

2 勾選「**排除選取的檔案及資料夾**」。

3 按下「**排除**」以指定要排除的檔案，再按下「**確定**」。

4 若要啟動預先掃描的排除項目，請勾選「**在掃描前檢查要排除的檔案**」。
不同的情況會決定此選項影響掃描效能的方式。例如：

- 如果您複製排除清單中的大型資料夾，並已啟動「在掃描前檢查要排除的檔案」，其複製過程將較短，因為該資料夾的內容已排除在掃描作業之外。
- 如果您要複製不屬於排除清單中的大型資料夾，停用「在掃描前檢查要排除的檔案」可改善效能。

5 按下「**副檔名**」。

6 指定要排除的檔案類型。
您可以使用 ? 萬用字元來指定任何字元。例如，XL? 將會排除 .xls、.xlt、.xlw 及 .xla 等類型的檔案。

7 按下「**檔案 / 資料夾**」。

8 指定要排除的內容。

9 按下「**確定**」。

Chapter 5

如果發現病毒或其它威脅時要採取什麼行動

本章包含以下主題：

對受感染的檔案採取的動作

Symantec Client Security 防毒用戶端 對於「自動防護」和各類掃描作業所設的預設選項，是偵測到受感染檔案即加以清除，但若無法清除病毒即將檔案移入「隔離所」。

如果受感染的檔案已被修復，您不必採取其它動作來防護您的電腦。

一旦完成掃描，您可以從「掃描電腦」對話方塊立即處理受感染的檔案。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。

若要稍後處理受感染的檔案，您也可以在「威脅記錄」或「隔離所」中進行。

請參閱第 53 頁的「重新掃描隔離所內的檔案」。

附註：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「掃描電腦」對話方塊中。同樣地，您的管理員可能會選擇遇到病毒時不要顯示警示。

處理受感染的檔案

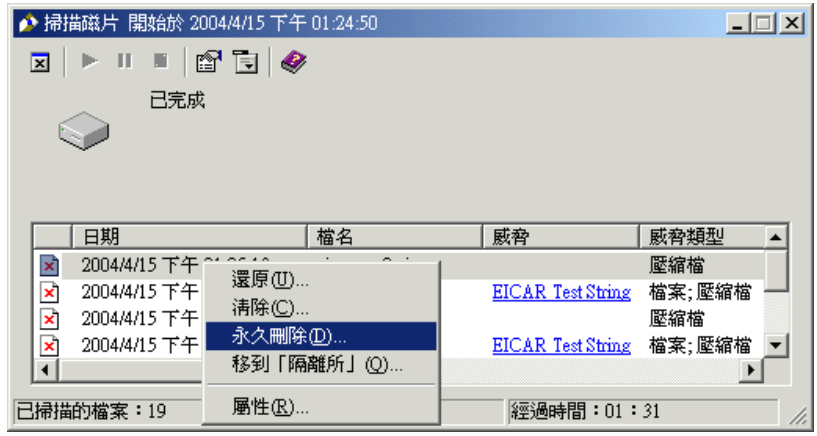
1 執行下列其中一個動作：

- 一旦掃描完成，在「掃描電腦」對話方塊中，選取您所要的檔案。
- 在 Symantec Client Security 防毒用戶端 左窗格中，展開「記錄」，按下「威脅記錄」，接著在右窗格中，選取您所要的檔案。

2 在檔案上按下滑鼠右鍵，再選取下列其中一個項目：

- 復原：如果可以，請改採前一個回應動作
- 清除：移除檔案中的病毒
- 永久刪除：刪除受到感染的檔案
- 移到隔離所：將受到感染的檔案置入「隔離所」內
- 屬性：顯示關於病毒的資訊

根據您預設的病毒偵測行動，有些選項可能會無法執行。



管理隔離所

有時候 Symantec Client Security 防毒用戶端 會偵測到目前其病毒定義無法消滅的未知病毒，或者您認為某個檔案已經受到感染，但 Norton AntiVirus 卻未在該檔案內偵測到任何病毒。「隔離所」可將電腦上受感染的檔案安全地予以隔離。已隔離的病毒即無法隨意散佈。

檔案被置入「隔離所」的方式有兩種：

- Symantec Client Security 防毒用戶端 根據其設定，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」。

Symantec Client Security 防毒用戶端 對於「自動防護」和各類掃描作業所設的預設選項，是偵測到受感染檔案即加以清除，但若無法清除病毒即將檔案移入「隔離所」。

附註：Symantec Client Security 不會將其它威脅 (例如窺視程式與廣告軟體) 置入至「隔離所」中。

手動將檔案加入至隔離所

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

2 在右窗格中，按下「隔離所」。

3 在工具列上，按下「將檔案新增至隔離所」。

4 尋找檔案，並按下「新增」。

5 按下「關閉」。

重新掃描隔離所內的檔案

如果有檔案被移入「隔離所」，請即更新您的病毒定義檔。根據管理員架構「隔離所」的方式，在更新病毒定義檔之後，便會自動掃描、清除和還原「隔離所」中的檔案，或者出現「修復精靈」，讓您重新掃描「隔離所」中的檔案。

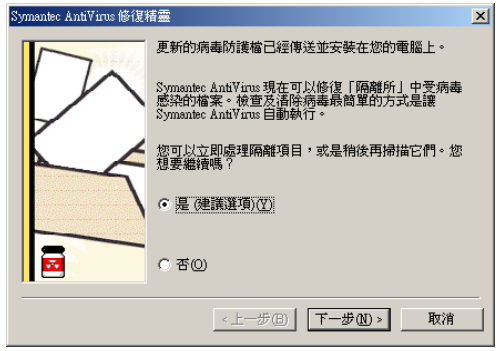
如果重新掃描「隔離所」中的檔案之後，仍無法移除病毒，請將受感染的檔案傳送給 Symantec Security Response (賽門鐵克安全機制應變中心) 進行分析。他們會開發出新的病毒定義檔以偵測及清除該病毒，而且會以電子郵件方式送交此檔案給您。

請參閱第 56 頁的「傳送可能感染病毒的檔案給 Symantec Security Response (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」，按下「是」。

2 按「下一步」，然後按照螢幕上的指示，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」中的檔案。

手動重新掃描「隔離所」中的檔案

1 更新病毒定義檔。
請參閱第 33 頁的「更新病毒防護」。

2 在 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

3 在右窗格中，按下「隔離所」。

4 從「隔離所」清單內選出該檔案。

5 執行下列其中一個動作：

- 在檔案上按下滑鼠右鍵，再按「清除」。
- 在工具列的右窗格中，按下「清除」。

6 按下「開始清除」。
系統即會以新的定義檔再次掃描該檔案，並將其放到原來的位置。

何時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」。在這種特殊的情況下，已清除病毒的檔案將會被置入「修復項目」。您必須釋放該檔案並指定一個位置。

從修復項目資料夾釋放完成除毒的檔案

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

2 在右窗格中，按下「修復項目」。

3 在檔案上按下滑鼠右鍵，再按「還原」。

4 指定已除毒檔案的位置。

清除備份項目

Symantec Client Security 防毒用戶端 會根據其設定，在嘗試修復前先備份中毒的檔案，作為資料安全防護屏障。受感染的項目成功清除病毒後，您應該從「備份項目」手動刪除該檔案，因為其備份仍然會受到感染。您也可以設定自動刪除檔案的時間週期。

請參閱第 56 頁的「自動清除隔離所、備份項目和修復項目中的檔案」。

附註：Symantec Client Security 防毒用戶端 不會備份其它的威脅，例如窺視程式與廣告軟體。

手動清除備份項目

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

2 在右窗格中，按下「備份項目」。

3 在「備份項目」清單中選取一個或多個檔案。

4 執行下列其中一個動作：

- 在檔案上按下滑鼠右鍵，再按「永久刪除」。
- 在工具列的右窗格中，按下「刪除」。

5 在「因應措施」對話方塊中，按下「 開始刪除」。

6 按下「關閉」。

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。

請參閱第 56 頁的「自動清除隔離所、備份項目和修復項目中的檔案」。

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 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

2 在右窗格中，按下「隔離所」。

3 在「隔離項目」清單中選取一個或多個檔案。

4 在檔案上按下滑鼠右鍵，再按「永久刪除」。

5 在「因應措施」對話方塊中，按下「開始刪除」。

6 按下「關閉」。

自動清除隔離所、備份項目和修復項目中的檔案

您可以設定 Symantec Client Security 防毒用戶端 在指定的時間間隔之後，自動刪除「隔離所」、「備份項目」和「修復項目」中的項目。這可防止您在建立這些檔案之後，忘記將它們從這些區域中手動移除。

自動清除檔案

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「檢視」。

2 在右窗格中，選取下列動作之一：

- 隔離所
- 備份項目
- 修復項目

3 按下「清除選項」。

4 在「清除選項」對話方塊中，勾選「啟動自動清除檔案」。

5 在「選取清除檔案的時間」文字方塊中，鍵入數字或按下箭頭來選取數字。

6 選取時間間隔。

7 按下「確定」。

8 按下「關閉」。

傳送可能感染病毒的檔案給 Symantec Security Response (賽門鐵克安全機制應變中心) 進行分析

有時候，Symantec Client Security 防毒用戶端 可能無法清除檔案中的病毒。或者，您懷疑某一個檔案已受到感染但卻無法偵測到。「賽門鐵克安全機制應變中心」會分析您的檔案來確認它是否受到感染。如果在您所傳送的檔案中發現新種病毒，「賽門鐵克安全機制應變中心」會建立特殊的更新病毒定義並傳送給您，用以偵測並消滅此種新病毒。您必須有 Internet 連線來傳送樣本以及電子郵件位址來接收回覆。

附註：在集中管理的網路中，傳送檔案給 Symantec Security Response (賽門鐵克安全機制應變中心) 通常是由「賽門鐵克中央隔離所」的防毒管理員負責處理。在此情況下，Symantec Client Security 防毒用戶端 的版本將無法使用「提交至賽門鐵克安全機制應變中心」選項。另外，如果管理員將未管理的用戶端設成不允許傳送到「賽門鐵克安全機制應變中心」，「提交至賽門鐵克安全機制應變中心」選項亦不會顯現。

從「隔離所」將檔案傳送到賽門鐵克安全機制應變中心

1 在 Symantec Client Security 防毒用戶端 左窗格中，按下「**檢視**」。

2 在右窗格中，按下「**隔離所**」。

3 從隔離項目清單中選取檔案。

4 在工具列的右窗格中，按下「**提交至賽門鐵克安全機制應變中心**」。

5 遵照精靈中的指示，蒐集必要資訊並傳送檔案以供分析。
分析結果會以電子郵件通知您，如果情況許可，還會附上最新的病毒定義。

處理衍生型威脅類別中的威脅

在 Symantec Client Security 防毒用戶端 掃描特定的威脅類型之前，您必須啟動衍生型威脅偵測。

一旦掃描完成，您可以從「掃描電腦」對話方塊或從「威脅記錄」中回應其它的威脅。

處理衍生型威脅類別中的威脅

1 執行下列其中一個動作：

- 一旦掃描完成，在「掃描電腦」對話方塊中，連按兩下您所要的檔案。
- 在 Symantec Client Security 防毒用戶端 左窗格中，展開「**記錄**」，按下「**威脅記錄**」，接著在右窗格中，連按兩下您所要的檔案。

2 在 Symantec Security Response (賽門鐵克安全機制應變中心) 網站上讀取關於威脅的資訊，然後採取建議的動作。
請參閱第 20 頁的圖 2-1，「賽門鐵克安全機制應變中心的衍生型威脅說明」。

Section 2

Symantec Client Security 防火牆用戶端

Chapter 6

介紹 Symantec Client Security 防火牆用戶端

本章包含以下主題：

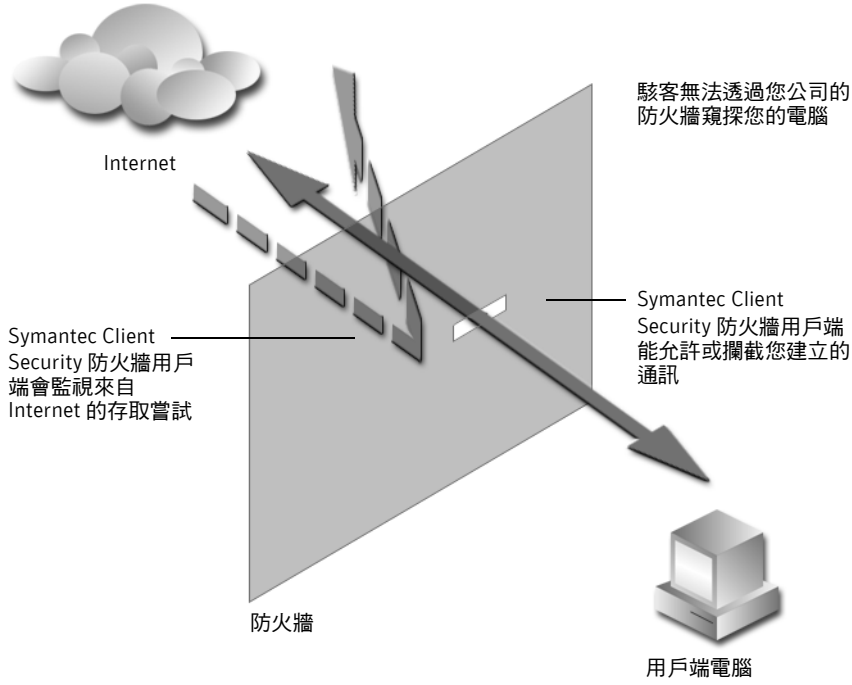
Symantec Client Security 防火牆用戶端的新增功能

Symantec Client Security 防火牆用戶端現在包含以下的功能：

設定值管理員	讓您匯入與匯出政策檔，提供備份與還原功能。 請參閱第 75 頁的「匯出及匯入政策檔」。
網路偵測	讓您依照用來連接到 Internet 的網路存取點，執行特定的規則組與區域。 請參閱第 83 頁的「使用網路偵測」。
安全通訊埠	特洛伊木馬程式規則完整地定義安全通訊埠，因此分配給這些通訊埠的流量，包含入埠與離埠，將不會觸發防火牆規則資料庫的檢查。 請參閱第 111 頁的「使用安全通訊埠」。
隱私權控管	攔截電子郵件與即時訊息中的私人資訊 (增強版)。 請參閱第 119 頁的「關於防護您的隱私權」。
廣告攔截	可讓您針對特定的網站與 HTML 字串來調整設定 (增強版)。 請參閱第 129 頁的「使用進階網站內容設定」。
日誌檢視器	協助您查看 Symantec Client Security 防火牆用戶端所採取的所有動作，以保護您的電腦 (改進版)。 請參閱第 139 頁的「使用日誌檢視器」。

關於 Symantec Client Security 防火牆用戶端

Symantec Client Security 防火牆用戶端會防止電腦受到駭客入侵、保護您的隱私權，以及除非必要的網路流量來源。



Symantec Client Security 防火牆用戶端會在您的電腦與 Internet 之間設下一道護欄。防火牆也會防止未經授權的使用者存取 Internet 上連接的個人電腦和網路。

當您連接 Internet 時，Symantec Client Security 防火牆用戶端會防止未經授權的使用者存取您的電腦、偵測可能的駭客攻擊、保護您的個人資訊，以及免除非必要的網路流量來源。

Symantec Client Security 防火牆用戶端與 Symantec Client Security

Symantec Client Security 防火牆用戶端 是 Symantec Client Security 的其中一個元件。在用戶端層級，Symantec Client Security 提供下列形式的防護措施：

- 病毒防護
- 內容過濾
- 防火牆
- 入侵偵測

上述形式的防護會利用識別與解除混合型病毒，來維護用戶端層級的網路安全。混合型病毒會使用多種方法進行攻擊，包括病蟲、電子郵件、應用軟體弱點，以及控制系統的網路共用。Code Red 及 Nimda 即為混合型病毒的例子。

Symantec Client Security 也會防範下列病毒類型：

- 檔案型、開機型及巨集型病毒
- 遠端控制特洛伊木馬程式
- 大量轉寄電子郵件型病毒，例如 Love Letter 及 Melissa
- 動態網路型病毒

如需詳細資訊，請參閱 Symantec Security Response (賽門鐵克安全機制應變中心) 網站的參考區：

www.symantec.com.tw/region/tw/avcenter

Symantec Client Security 防火牆用戶端功能

Symantec Client Security 防火牆用戶端包含數個有助於維護電腦安全的安全性工具。Internet 安全性是一個需要瞭解的複雜主題，因此 Symantec Client Security 防火牆用戶端現在包含一個 「警示小幫手」，協助您了解安全性問題、建議解決問題的方式，以及告知您如何預防未來可能發生的安全性問題。

表 6-1 列出 Symantec Client Security 防火牆用戶端提供的各項功能。

表 6-1 Symantec Client Security 防火牆用戶端功能

功能	說明
狀態檢查	追蹤關於目前連線的資訊，如 IP 來源和目的位址、通訊埠、應用程式等等。確定入埠流量對離埠流量而言是正當的回覆，並確保規則資料庫的單純化。 請參閱第 106 頁的「關於狀態檢查」。

表 6-1 Symantec Client Security 防火牆用戶端功能

功能	說明
Internet 狀態	提供您電腦的網路活動快照，讓您可以用來識別正在進行的攻擊行動，並檢視程式設定影響防護的方式。 請參閱第 135 頁的「關於監視 Symantec Client Security 防火牆用戶端」。
用戶端防火牆	防護您的電腦免於 Internet 駭客攻擊及未經授權的入侵。讓您的電腦在 Internet 上虛擬隱形。 保護遠端及漫遊使用者免於駭客的攻擊，並且防止這些系統遭受駭客入侵，以免駭客從公司網路的後門進行存取。 請參閱第 94 頁的「Symantec Client Security 防火牆用戶端防止網路受到攻擊的方式」。
入侵偵測	偵測並攔截外部使用者惡意攻擊您的電腦。 請參閱第 94 頁的「Symantec Client Security 防火牆用戶端防止網路受到攻擊的方式」。
隱私權控管	提供您多種控制層級，以便控制使用者、網路瀏覽器、即時傳訊程式與電子郵件用戶端可以在 Internet 上傳送的各種資訊。 請參閱第 119 頁的「關於防護您的隱私權」。
廣告攔截	排除橫幅廣告和其它載入較慢或有入侵性的內容，以加快您在網頁上的漫遊速度。Symantec Client Security 防火牆用戶端現在也會攔截利用 Macromedia Flash 所製作的廣告，並防止網站開啟在網頁上下方彈出的廣告視窗。 請參閱第 126 頁的「攔截廣告」。
網路偵測	讓您依照用來連接到 Internet 的網路存取點，執行特定的規則組與區域。 請參閱第 83 頁的「使用網路偵測」。
安全通訊埠	特洛伊木馬程式規則完整地定義安全通訊埠，因此分配給這些通訊埠的流量，包含入埠與離埠，將不會觸發防火牆規則資料庫的檢查。使用隨機通訊埠的程式不會嘗試使用安全的通訊埠。 請參閱第 111 頁的「使用安全通訊埠」。
設定值管理員	讓您匯入與匯出政策檔，提供備份與還原功能。 請參閱第 75 頁的「匯出及匯入政策檔」。

表 6-1 Symantec Client Security 防火牆用戶端功能

功能	說明
VPN 支援	讓 Symantec Client Security 防火牆用戶端與下列的虛擬私人網路 (VPN) 搭配使用： ■ Check Point ■ Nortel Contivity ■ Microsoft ■ IPass ■ Fiberlink 大部分的 VPN 在 VPN 用戶端作用時，您在區域網路上看不到 Internet 或其它電腦。您僅能透過您所連接的 VPN 伺服器，查看可用的連線。在加密的連線上，不支援「廣告攔截」和「隱私權控管」。

Chapter 7

Symantec Client Security 防火牆用戶端基礎篇

本章包含以下主題：

存取 Symantec Client Security 防火牆用戶端

在安裝完畢後，Symantec Client Security 防火牆用戶端會自動防護被安裝的電腦。您無須啟動要防護的程式。

存取 Symantec Client Security 防火牆用戶端

- 執行下列其中一個動作：
  - 在 Windows 系統匣中，連按兩下 Symantec Client Firewall 圖示。

- 在 Windows 工作列上，按下「開始」>「程式集」> **Symantec Client Security** > **Symantec Client Firewall**。

顯示 Symantec Client Security 防火牆用戶端系統匣功能表

Symantec Client Security 防火牆用戶端會將圖示新增至 Windows 系統匣。根據預設，Symantec Client Security 防火牆用戶端系統匣圖示會出現在您電腦螢幕的右下角。按下此圖示可開啟包含常用之 Symantec Client Security 防火牆用戶端工具的功能表。

顯示 Symantec Client Security 防火牆用戶端系統匣功能表

- 在圖示上按下滑鼠右鍵。

附註：Symantec Client Security 防火牆用戶端的「選項」視窗可讓您覆寫預設值和隱藏 Symantec Client Security 防火牆用戶端的系統匣圖示。此外，這個視窗包含不顯示「選項」、「日誌檢視器」和「統計值」功能表選項的可架構設定。

在系統匣功能表上，您可以選擇：

- 顯示 Symantec Client Security 防火牆用戶端主視窗。
- 攔截所有流量並允許規則所允許所有流量。
- 顯示「選項」視窗。
- 顯示「日誌檢視器」。
- 顯示「統計值」視窗。
- 顯示關於 Symantec Client Security 防火牆用戶端的背景資訊，例如版本編號。
- 顯示「說明」。
- 啟動與停用 Symantec Client Security 防火牆用戶端。

使用 Symantec Client Security 防火牆用戶端

Symantec Client Security 防火牆用戶端會在背景作業。依據您的使用者層級，只有在程式警示您關於新的網路連線及可能的問題時，您才會與程式進行互動，或者您可以完整存取使用者介面的功能。您可以控制您會接收到的警示數目，以及程式如何解決潛在的安全性問題。

Symantec Client Security 防火牆用戶端使用者層級

您的使用者層級會決定您可以使用的功能。使用者層級係由系統管理員所定義。

「管理員」使用者層級可以執行表 7-1 中所列的所有作業。其中也列出了「一般」及「受限」使用者層級的權限能力。

表 7-1 Symantec Client Security 防火牆用戶端使用者存取層級

作業	一般使用者層級	限制使用者層級
啟動或停用防火牆。		
啟動或停用「隱私權控管」。	✓	
啟動或停用「入侵偵測」。		
啟動或停用「自動攔截」。		
啟動或停用「安全通訊埠」。		

表 7-1 Symantec Client Security 防火牆用戶端使用者存取層級

作業	一般使用者層級	限制使用者層級
使用「設定值管理員」。		
新增與移除「私人資訊攔截」的資料。	✓	
新增、修改或刪除解除鎖定的規則。		
修改解除鎖定的規則優先順序。		
從「現在被自動攔截所攔截的電腦」視窗中移除電腦。		
從「現在被自動攔截所攔截的電腦」中將電腦新增至「限制」區域。		
將電腦新增至「限制」及「信任」區域，或是從「限制」及「信任」區域移除電腦。		
排除特徵不受「入侵偵測」監視。		
排除 IP 位址不受自動攔截攔截。		
執行「應用程式掃描」。		
存取「進階防火牆選項」。		
移除 Symantec Client Security 防火牆用戶端。		
啟動或停用「網路偵測程式」。		
啟動或停用「自動程式控管」。		
修改 Symantec Client Security 防火牆用戶端設定。		
修改「隱私權控管」設定。	✓	
修改「廣告攔截」設定。	✓	
變更「報告等級」。	✓	
檢視「事件日誌」。	✓	✓
修改「事件日誌」。	✓	
檢視「統計值」。	✓	
攔截進出您電腦的流量。	✓	
重設統計值。		
清除「入侵偵測」狀態。		
執行 LiveUpdate。	✓	✓

表 7-1 Symantec Client Security 防火牆用戶端使用者存取層級

作業	一般使用者層級	限制使用者層級
存取說明檔。	✓	✓

變更 Symantec Client Security 防火牆用戶端防護功能的設定

Symantec Client Security 防火牆用戶端的預設值會提供一個安全、自動且有效的方式來防護您的電腦。如果您想要變更或自訂您的防護，您可以從「狀態與設定」視窗中，存取所有的 Symantec Client Security 防火牆用戶端工具。

變更 Symantec Client Security 防火牆用戶端防護功能的設定

1 在主視窗中，按下「狀態與設定」。

2 連按兩下您想要自訂的功能。

3 架構功能。

4 當您完成變更時，按下「確定」。

回應 Symantec Client Security 防火牆用戶端的警示

Symantec Client Security 防火牆用戶端會監視進出您電腦的通訊活動，讓您知道何時發生危及安全性的活動。

Symantec Client Security 防火牆用戶端顯示下列警示類型：

- 安全性
- ActiveX
- 隱私權控管
- Cookie
- 入侵偵測
- Internet 通訊協定
- Java
- 聽取
- 啟動程式
- 模組指紋 (Module finger printing)
- 服務監測
- 網路偵測
- DNS

- 特洛伊木馬程式

當警示出現時，請在您決定採取行動之前先閱讀它，並判斷警示類型及威脅等級。一旦您了解危險，您就可以做選擇。詳細考慮您要做的選擇。當警示啟動時，您的電腦不會受到攻擊。

Symantec Client Security 防火牆用戶端會藉由選取建議的動作 (如果有的話)，協助您決定適當的動作。Symantec Client Security 防火牆用戶端無法對所有的警示提出建議的動作。

並非每個「安全性警示」都表示嘗試攻擊您電腦的行為。在 Internet 上，有許多無害的事件會導致「安全性警示」。部分警示可讓您選取不要再看見這些警示。

使用警示小幫手

每一個 Symantec Client Security 防火牆用戶端警示都包含一個連至「警示小幫手」的連結。「警示小幫手」包含下列關於每一個警示的自訂資訊。

- 警示的類型
- 觸發此警示的通訊
- 其它資訊
- 您應該進行的動作
- 如何減少您接收的警示數目

使用「警示小幫手」

1. 在任何警示視窗中，按下「警示小幫手」連結。
2. 在「警示小幫手」視窗中，檢視關於這個警示的資訊。
3. 若要回應這個警示，請關閉「警示小幫手」。

以「中斷連線」來停止 Internet 通訊

Symantec Client Security 防火牆用戶端包含「中斷連線」按鈕，可讓您立即停止您的電腦與其它電腦之間的通訊。在您電腦遭受攻擊時、特洛伊木馬程式在未經您的許可之下傳送個人資訊時，或是您不慎讓不信任的人士存取電腦上的檔案時，這可以協助您限制任何的破壞。

啟動這個選項時，Symantec Client Security 防火牆用戶端會停止所有進出您電腦的通訊。對外部世界來說，看起來像是您的電腦與 Internet 的連線完全中斷。

如果您想要攔截進出您電腦的所有流量，「中斷連線」會比您只使用 Internet 軟體來中斷連線更有效。大多數 Internet 程式可以在不需要使用者輸入的情況下自動連線，所以惡意程式可能會在您離開電腦時重新連線。

附註：當您提出安全性問題時，「中斷連線」可用來做為暫時的考量。如果您重新啟動電腦，Symantec Client Security 防火牆用戶端會自動允許所有進出的通訊。

以「中斷連線」來停止 Internet 通訊

1 在主視窗的上方，按下「中斷連線」。

2 使用 Symantec Client Security 防火牆用戶端工具來說明安全性問題。

3 當您已經修復問題時，請按下「允許連線」。

自訂 Symantec Client Security 防火牆用戶端

預設的 Symantec Client Security 防火牆用戶端設定會為大多數使用者提供適當的防護措施。如果您需要進行變更，請使用「選項」功能表來存取 Symantec Client Security 防火牆用戶端選項。這些選項可讓您控制更多的進階設定。

附註：如果您使用的是 Windows 2000/XP，而且您沒有「本機系統管理員」的存取權限，則您無法變更 Symantec Client Security 防火牆用戶端選項。表 7-1 提供關於使用者層級允許之變更的其它資訊。

自訂 Symantec Client Security 防火牆用戶端

1 在主視窗的上方，按下「選項」。

2 選取您要變更選項的標籤。

關於一般選項

「一般」選項可讓您在 Symantec Client Security 防火牆用戶端執行時，控制及選取您想要顯示的可見元件。表 7-2 說明「一般」選項。

表 7-2 一般選項

群組	說明
啟動 Symantec Client Security 防火牆用戶端	每當 Windows 啟動時，選取您要手動或自動執行 Symantec Client Security 防火牆用戶端。

表 7-2 一般選項

群組	說明
系統匣圖示設定值	在您存取程式設定的 Windows 工作列上，顯示 Symantec Client Security 防火牆用戶端圖示。 您也可以將連結加入至以下的 Symantec Client Security 防火牆用戶端工具： ■ 選項 ■ 日誌檢視器 ■ 統計值

關於防火牆選項

「防火牆」選項可讓您啟動進階的防護功能，並自訂您電腦用來檢視網頁的通訊埠。大多數的人不需要對這些設定進行任何變更。表 7-3 說明「防火牆」選項。

表 7-3 防火牆選項

群組	說明
檢查程式連線至 Internet 時使用的外部模組的存取設定值	當程式使用外部軟體元件連接至 Internet 時，檢查每一個元件的防火牆規則。這可以確保特洛伊木馬程式以及其它惡意程式無法附加到安全的程式上而躲避偵測。
一個程式啟動另一個程式時，檢查兩個程式的 Internet 存取設定值。	使用「程式啟動監控」，以確保特洛伊木馬程式以及其它惡意程式在您不知情的狀況下，無法啟動及操作安全的程式。如果有啟動「程式啟動監控」，每當有無法辨識的程式啟動其它程式時，您將會收到警示。然後，您可以允許或攔截無法辨識之程式的 Internet 存取。
HTTP 通訊埠清單	指定針對 Java 和 ActiveX 攔截、程序檔攔截、機密資訊和 Cookie 等過濾的通訊埠清單。如果清單是空的，將不過濾 HTTP 上的私人資訊。如果攜帶私人資訊的通訊埠未列在此處，則不透過此通訊埠過濾私人資訊的流量。若要讓這些設定生效，您必須重新開機。
攔截 IGMP	啟動及停用您電腦使用 Internet Group Membership Protocol (IGMP) 的能力。IGMP 通常用來傳送多媒體檔案至多點傳播群組。
隱藏攔截的通訊埠	選取 Symantec Client Security 防火牆用戶端是否要回應關閉未使用之通訊埠的掃描。隱藏的通訊埠不會回應掃描。
如何處理分段的 IP 封包：	選取 Symantec Client Security 防火牆用戶端要攔截已分成多個片段的所有 IP 封包，或是只出現成為攻擊一部分的封包。 這個設定只會影響 Windows 98 電腦。 Windows 2000/XP 電腦會自動重組破碎的封包。

關於安全通訊埠選項

「安全通訊埠」選項可讓您啟動及停用「安全通訊埠」技術，這個技術會保護以特洛伊木馬程式規則攔截的通訊埠，讓任何應用程式都無法使用這些通訊埠。您也可以將其它通訊埠新增至清單中。

請參閱第 111 頁的「使用安全通訊埠」。

關於設定值管理員

「設定值管理員」可讓您備份 (匯出) 及還原 (匯入) Symantec Client Security 防火牆用戶端設定值檔案。

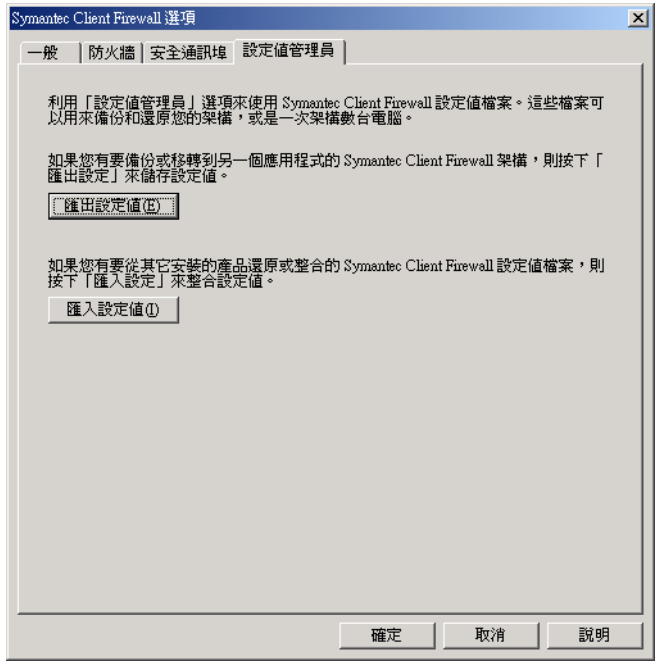
請參閱第 75 頁的「匯出及匯入政策檔」。

匯出及匯入政策檔

Symantec Client Security 防火牆用戶端可讓您匯出所有設定值，這是一項您可以用來備份防火牆架構的功能。Symantec Client Security 防火牆用戶端也可以讓您匯入所有的設定值，這是一項您可以用來還原防火牆架構的功能。您也可以使用匯出及匯入功能，將已知的架構儲存至政策檔中，並且將它安裝在數台電腦上。匯出及匯入使用 XML 檔。

匯出或匯入政策檔

1 在主視窗的上方，按下「選項」。



2 在 Symantec Client Firewall「選項」視窗的「設定值管理員」標籤上，選取下列項目之一：

- 匯出設定值
- 匯入設定值

3 在檔案選取對話方塊中，瀏覽至所要的目錄。

4 執行下列其中一個動作：

- 如果您要匯出，在「檔案名稱」方塊中，輸入要儲存此設定的檔案名稱，然後按下「儲存」。
- 如果您要匯入，選取目標檔案，然後按下「開啟」。

5 在 Symantec Client Firewall 的「選項」視窗中，按下「確定」。
如果您要匯出政策檔，在按下「確定」之前，不要在其它標籤上架構設定，否則其它標籤上的設定將不會被匯出。

暫時停用 Symantec Client Security 防火牆用戶端

有時候您會想要暫時停用 Symantec Client Security 防火牆用戶端或是它的其中一項功能。例如，您可能想要檢視線上廣告或是查看 Symantec Client Security 防火牆用戶端是否正確地防止網頁出現。

暫時停用 Symantec Client Security 防火牆用戶端及所選取的功能

停用 Symantec Client Security 防火牆用戶端也會停用所有個別的功能。您也可以停用個別的安全性功能。例如，您可能想要查看用戶端防火牆是否正確地防止程式操作。

暫時停用 Symantec Client Security 防火牆用戶端

1 在主視窗中，按下「狀態與設定」。

2 按下「安全性」。

3 在畫面的右側，按下「關閉」。

暫時停用防護功能

1 在主視窗中，按下「狀態與設定」。

2 選取您要停用的功能。

3 在畫面的右側，按下「關閉」。

透過 LiveUpdate 隨時保持最新狀態

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。LiveUpdate 利用 Internet 連線，為您的電腦取得程式更新與防護更新。

附註：LiveUpdate 會更新您電腦上的所有賽門鐵克產品。Symantec Client Security 防火牆用戶端的 LiveUpdate 只更新「入侵偵測」特徵及特洛伊木馬規則。

關於程式更新

所謂程式更新，指的是對已安裝好的產品做小幅度的改善。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。具有自動安裝來取代現有軟體碼的程式更新檔稱為修正程式。修正程式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，或是修正錯誤。

LiveUpdate 使得程式更新的取得與安裝程序全部自動化。它會從 Internet 網站中搜尋並取得檔案並加以安裝，然後刪除您電腦上遺留的檔案。

關於防護更新

防護更新是從賽門鐵克訂閱後取得的檔案，可利用最新的防威脅技術，讓您的賽門鐵克產品保持在最新狀態。您收到的防護更新取決於您使用的產品。

更新的時機

當您安裝好產品之後，請儘快執行 LiveUpdate。一旦您知道您的檔案為最新狀態後，請定期執行 LiveUpdate 以取得更新。例如，若要讓您的病毒防護保持在最新狀態，您應該一星期使用一次 LiveUpdate，或是在發現新病毒時使用。至於程式更新部分，賽門鐵克會視需要來發行。

要求更新警示

若要確保您的防護更新是最新的，您可以要求在高層級病毒爆發，或是發生其它 Internet 安全性威脅時，接收電子郵件警示。電子郵件警示會說明這個威脅、提供偵測與移除的指示，並加入讓您電腦保持在安全狀態的建議。在您接受其中任一種警示之後，您應該立即執行 LiveUpdate。

要求更新警示

1. 請至以下網站：
   securityresponse.symantec.com/avcenter
2. 在 Symantec Security Response (賽門鐵克安全機制應變中心) 網頁上，捲動至頁面的下方，然後按下 Sign up Symantec Security alerts。
3. 在安全性警示訂閱的網頁上，填寫訂閱表格。
4. 按下 Send me Symantec Security Alerts。

關於在內部網路執行 LiveUpdate

如果您在公司防火牆後連線至網路的電腦上執行 LiveUpdate，您的網路管理員可能要在網路上設定內部的 LiveUpdate 伺服器。LiveUpdate 會自動尋找這個位置。

如果您連線至內部的 LiveUpdate 伺服器時發生問題，請與您的網路管理員聯絡。

從賽門鐵克網站取得更新

當可取得新的更新時，賽門鐵克會在其網站上公佈更新。如果您無法執行 LiveUpdate，您可以從賽門鐵克網站取得新的更新。

附註：您的訂閱必須為最新狀態，才能從賽門鐵克網站取得新的防護更新。

從賽門鐵克網站取得更新

1 請至以下網站：
www.symantec.com.tw/region/tw/avcenter

2 按照連結來取得你所需要的更新類型。

使用 LiveUpdate 取得更新

LiveUpdate 會檢查安裝在您電腦上所有賽門鐵克產品的更新。

使用 LiveUpdate 取得更新

1 請在主視窗的上方，按下 **LiveUpdate**。

2 在 LiveUpdate 視窗中，按「下一步」來搜尋更新。

3 如果有更新，按「下一步」開始下載並安裝。

4 安裝完成後，請按下「完成」。

附註：某些程式更新可能會需要您在安裝後重新開機。

將 LiveUpdate 設定為互動模式或簡易模式

LiveUpdate 可以在「互動模式」或「簡易模式」下執行。在「互動模式」(預設值)下，LiveUpdate 會下載您由 LiveUpdate 技術所支援之賽門鐵克產品可用的更新清單。然後，您可以選取您要安裝的產品更新。在「簡易模式」下，LiveUpdate 會自動為您的賽門鐵克產品安裝所有可用的更新。

將 LiveUpdate 設定為「互動模式」或「簡易模式」

1 請在主視窗的上方，按下 **LiveUpdate**。

2 在 LiveUpdate 歡迎畫面上，按下「設定」。

3 在「LiveUpdate 設定」對話方塊的「一般」標籤上，選取下列其中一項：

- 互動模式
- 快速模式

4 如果您選取「快速模式」，請選取下列任一個或兩個選項：

- 當 LiveUpdate 啟動時，自動開始階段作業
- 階段作業結束時自動離開

5 若要在「加強錯誤支援」方塊中，啟動錯誤檢查，請按下「啟動加強錯誤支援」。

6 按下「確定」。

關閉快速模式

一旦您已設定以「簡易模式」執行 LiveUpdate，您可以不再從 LiveUpate 直接存取「LiveUpdate 設定」對話方塊。您必須使用 Symantec LiveUpdate 控制台。

關閉「快速模式」

1 在 Windows 工作列上，按下「開始」>「設定」>「控制台」。

2 在「控制台」視窗中，連按兩下 **Symantec LiveUpdate**。

3 在「LiveUpdate 設定」對話方塊的「一般」標籤上，按下「互動模式」。

4 按下「確定」。

如需詳細資訊

Symantec Client Security 防火牆用戶端會提供線上說明、PDF 格式的用戶端指南，以及連至賽門鐵克網站上的「知識庫」連結。

存取說明

在 Symantec Client Security 防火牆用戶端中，永遠可以取得說明。「說明」按鈕或詳細資訊的連結會提供您要完成之工作的特定資訊。「說明」功能表會為所有產品功能及您可以完成的工作，提供全面性的指南。

存取「說明」

1 請在主視窗的上方，按下「說明和支援」。

2 在主「說明」功能表上，按下「**Symantec Client Firewall** 說明」。

3 在「說明」視窗的左窗格中，選取下列任一個標籤：

- 內容：依主題顯示「說明」
- 索引：依關鍵字的字母順序列出說明主題
- 搜尋：開啟搜尋欄位，讓您可以在此輸入單字或片語

存取視窗及對話方塊說明

視窗及對話方塊說明會提供關於 Symantec Client Security 防火牆用戶端程式的資訊。這個「說明」類型是前後文相關的，也就是說，它會提供您目前所使用之對話方塊或視窗的說明。

存取視窗或對話方塊說明

◆ 如果有的話，按下「更多資訊」連結。

關於檢視 Readme 檔及版本注意事項

Readme 檔包含關於安裝及相容性問題的資訊。「版本注意事項」包含關於「Symantec Client Security *用戶端指南*」印刷後發生產品變更的技術秘訣與資訊。它們會被安裝在您硬碟中，與 Symantec Client Security 防火牆用戶端產品檔案相同的位置。

存取用戶端指南 PDF

在 Symantec Client Security 光碟中有提供 PDF 格式的 「用戶端指南」。

存取用戶端指南 PDF

您必須在您的電腦中安裝 Adobe Acrobat Reader，才能讀取 PDF。一旦您已經安裝 Adobe Acrobat Reader，就可以從光碟中讀取 PDF。

安裝 Adobe Acrobat Reader

1 將 Symantec Client Security 光碟放入光碟機中。

2 按下「**瀏覽光碟**」。

3 連按兩下 **Acrobat** 資料夾。

4 瀏覽並連按兩下 **Ar60CHT.exe**。

5 按照畫面上的指示，選取 Adobe Acrobat Reader 的資料夾，並完成安裝。

從光碟讀取用戶端指南 PDF

1 將 Symantec Client Security 光碟放入光碟機中。

2 按下「**瀏覽光碟**」。

3 連按兩下 **Docs** 資料夾。

4 連按兩下 **scsclnt.pdf**。

從 Symantec Client Security 防火牆用戶端主視窗存取賽門鐵克網站

賽門鐵克網站會提供關於 Symantec Client Security 防火牆用戶端多方面的資訊。存取賽門鐵克網站方式有許多種。

從 Symantec Client Security 防火牆用戶端主視窗存取賽門鐵克網站

1 請在主視窗的上方，按下「說明和支援」。

2 選取下列其中一項：

- 賽門鐵克服務與支援：帶領您至賽門鐵克網站的「技術支援」頁面，在這裡您可以搜尋特定問題的解決方案、更新您的病毒防護以及讀取關於防毒技術的最新資訊
- Symantec Response Center (賽門鐵克安全機制應變中心)：帶領您至「賽門鐵克安全機制應變中心」網站的首頁，這裡會列出最新的病毒威脅及安全性建議

您可以透過您的 Internet 瀏覽器存取以下的賽門鐵克網站：

www.symantec.com.tw

Chapter 8

使用網路偵測與區域

本章包含以下主題：

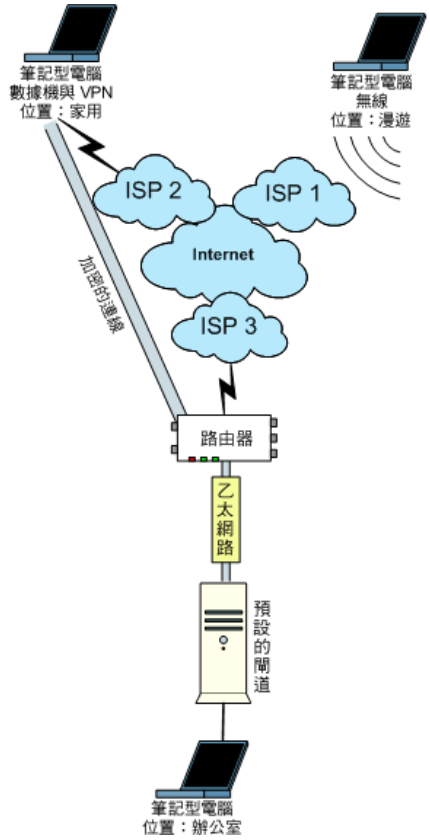
使用網路偵測

「位置」可讓您針對 Symantec Client Security 防火牆用戶端建立的不同網路連線，架構規則與區域。「位置」的目的是允許一部電腦連接至不同的網路，並且針對不同的網路自動套用適用的規則與「區域」。

例如，當用戶端使用遠端無線連線連接至網路時，您可以有您要 Symantec Client Security 防火牆用戶端強制執行的一組特定規則與「區域」，而當用戶端使用區域 Ethernet 連線連接網路時，您可以有另一組您想要 Symantec Client Security 防火牆用戶端強制執行的規則與「區域」。

圖 8-1 說明筆記型電腦使用無線連線連接至 Internet、透過 Internet 使用 VPN 連線連接至家庭辦公室，以及連接至辦公室網路的概念。

圖 8-1 從不同「位置」連接的筆記型電腦



當筆記型電腦從這三個「位置」連接時，會產生不同的網路流量，而且當它從這三個「位置」連接時，它會連接至不同的預設閘道器。例如，家庭使用者的 VPN 流量會藉著透過 VPN 供應商提供的通訊埠傳送，並連接至 ISP 2 的預設閘道器。漫遊使用者的無線流量使用 SSID 驗證透過其它的通訊埠傳送，並連接至 ISP 1 的預設閘道器。辦公室使用者的 Ethernet 流量則透過下部組織作業系統，例如 Windows 或 Netware，使用的通訊埠傳送，並連接至內部的預設閘道器。

如果您在預設的拒絕條件下執行 Symantec Client Security 防火牆用戶端規則，當如果規則不允許時，流量會被攔截，您可以架構允許來自這三個「位置」之網路流量的三種不同規則資料庫。一個政策檔案可以使用多達 64 個「位置」的不同資訊加以架構。

安裝後，Symantec Client Security 防火牆用戶端會使用以下四個「位置」架構：

- 辦公室
- 家用

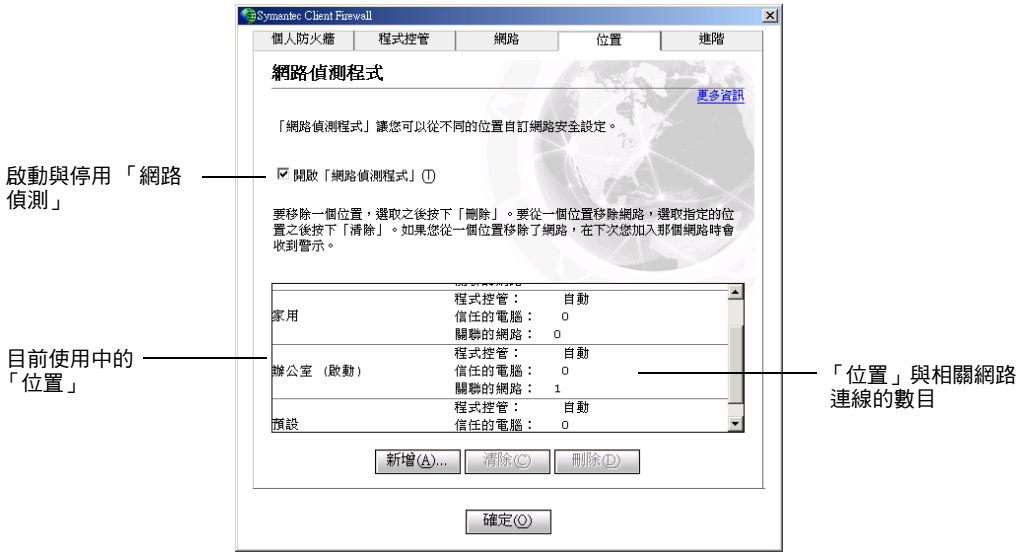
- 外出
- 預設

規則可以與一個、一些或所有的「位置」相關。「區域」只與特定的「位置」相關。當您架構規則與「區域」時，您必須為規則與「區域」選取「位置」。當「網路偵測」停用時，會使用「預設位置」。

啟動與停用網路偵測

您不需要使用「網路偵測」。當「網路偵測」停用時，會使用與「預設位置」相關的規則與「區域」。「網路偵測」的觸發機制為「網路偵測程式」。圖 8-2 顯示您啟動與停用「網路偵測程式」的位置。

圖 8-2 「位置」標籤



「位置」標籤 (「網路偵測程式」視窗) 也會顯示目前使用中的「位置」與相關網路連線的數目。當「預設位置」啟動時，相關網路連線的數目永遠為 0，因為網路規格無法與「預設位置」關聯。

啟動或停用「網路偵測」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「位置」標籤上，執行下列其中一項：

- 若要啟動「網路偵測」，請勾選「**開啟網路偵測程式**」。
- 若要停用「網路偵測」，請取消勾選「**開啟網路偵測程式**」。

選取要執行的位置

當您第一次使用 Symantec Client Security 防火牆用戶端連接到與「位置」不相關的網路，並且啟動「網路偵測」時，防火牆會提示您選取與網路連線資訊相關的「位置」。表 8-1 列出 Symantec Client Security 防火牆用戶端可能用來關聯選定「位置」的網路連線資訊。

表 8-1 網路連線資訊

屬性	說明
閘道器 MAC ID	預設閘道器的「媒體存取控制」(MAC) 位址
閘道器 IP 位址	預設閘道器的 IP 位址
子網路位址	用戶端電腦的 IP 位址與子網路遮罩
網域	網路網域名稱 (如果有的話)
SSID	無線網路服務集識別碼 (SSID)
撥接號碼	遠端存取使用的電話號碼
撥接項目說明	遠端存取點的說明
介面說明	介面的說明
介面類型	網路介面的類型
介面指標	介面的指標

選取執行的「位置」

1 連接至「網路偵測」停用的網路。
例如，顯示網頁。

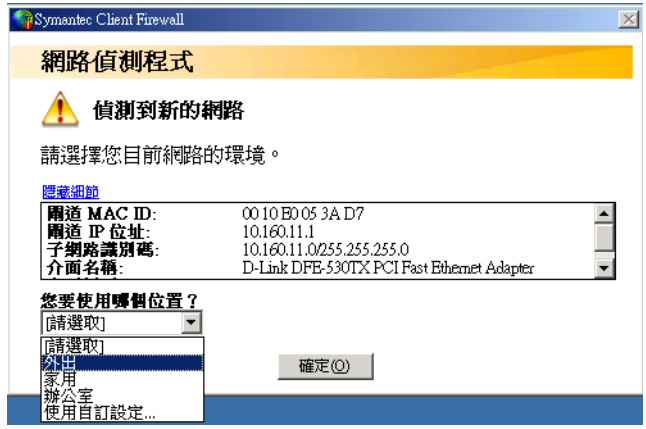
2 在主視窗中，按下「**狀態與設定**」。

3 連按兩下「**用戶端防火牆**」。

4 在 Symantec Client Firewall 視窗的「位置」標籤上，勾選「**開啟網路偵測程式**」。

5 執行某些網路活動。

例如，重新整理網頁。



6 在「網路偵測程式」視窗的「您要使用哪個位置？」之下，選取與網路連線相關的「位置」。

7 按下「確定」。

清除網路連線資訊

每一次您將網路連線資訊與「位置」關聯時，「位置」會記住此資訊。您可以將過多的網路連線數目與單一「位置」關聯，但是這會使「網路偵測」的目的失效。例如，您可以將無線、VPN 和辦公室連線的資訊與單一「位置」關聯。Symantec Client Security 防火牆用戶端可讓您清除這些關聯。

清除網路連線資訊

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「位置」標籤上，選取要清除的「位置」。

4 按下「清除」。

新增位置

Symantec Client Security 防火牆用戶端可讓您新增「位置」。當防火牆偵測到新的連線，並且以「網路偵測程式」視窗提示您時，您可以新增「位置」，而且您也可以從「位置」標籤新增「位置」。在這兩種情況下，精靈會依步驟帶您完成程序。

當您新增「位置」時，與「預設位置」相關的所有規則、「區域」與設定會自動套用到新增的「位置」。

新增「位置」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「位置」標籤上，按下「新增」。

4 在「設定程式控管」視窗中，選取下列其中一項：

- 是：當防火牆偵測到符合已知程式的流量時，自動將新的程式規則新增至「位置」。未知的程式會出現提示。
- 否：當防火牆偵測到不符合規則的流量時，提示您決定是否將新的程式規則新增至「位置」。

5 按「下一步」。

6 在「儲存位置」視窗中，輸入「位置」。

7 按「下一步」。

8 在「摘要」視窗中，按下「完成」。

關於自訂位置設定

當您建立網路「區域」與防火牆規則時，您會將這些「區域」及「規則」與「位置」關聯。

在 Symantec Client Firewall 視窗中的下列標籤可讓您將「區域」及規則與「位置」關聯：

- 網路
- 程式
- 進階

刪除位置

Symantec Client Security 防火牆用戶端可讓您刪除新增的「位置」。您無法刪除以 Symantec Client Firewall Administrator 新增的任何「位置」。當防火牆偵測到新的連線，並且以「網路偵測程式」視窗提示您時，您可以新增「位置」，而且您也可以從「位置」標籤新增「位置」。在這兩種情況下，精靈會依步驟帶您完成程序。

刪除「位置」

1. 在主視窗中，按下「狀態與設定」。
2. 連按兩下「用戶端防火牆」。
3. 在 Symantec Client Firewall 視窗的「位置」標籤上，選取要刪除的「位置」。
4. 按下「刪除」。
5. 在確認提示中，按下「是」。

將電腦新增至信任與限制區域

Symantec Client Security 防火牆用戶端可讓您將網路上與 Internet 上的電腦組織至 IP 位址定義的兩個「區域」中：信任和限制。每個「區域」都可能包含一個或多個 IP 位址項目，而且每個項目可以指定單一的 IP 位址、使用起始與結束 IP 位址的 IP 位址範圍，或是 IP 位址與子網路遮罩。圖 8-3 顯示「網路」標籤。

圖 8-3 「網路」標籤

置於「信任」區域的電腦不受 Symantec Client Security 防火牆用戶端的管制。這些電腦對您電腦的存取權限和沒有安裝 Symantec Client Security 防火牆用戶端時一樣多。您的區域網路上要共用檔案和印表機的電腦僅能使用「信任」區域。如果「信任」區域中的電腦受到攻擊，而且攻擊者已控制它，它會對您的電腦帶來風險。

防火牆會攔截來自「限制」區域中列出之 IP 位址的所有流量。如果此位址是預設閘道器，防火牆就不會攔截進出「限制」區域中之 IP 位址的流量。用戶端依然可以存取 Internet。

此外，「區域」只是「位置」的屬性。您無法建立一個「區域」，並且使它成為多個「位置」的屬性。您必須手動將「區域」新增至其它的「位置」。但是，與「預設位置」相關的所有「區域」都會自動與所有以「位置」精靈建立的新「位置」關聯。

對於 IP 位址落在「信任」區域的網站，規則、「入侵偵測」監視、Web 內容、隱私權控管和廣告攔截的設定會被忽略。

將電腦新增至「信任」或「限制」區域

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「網路」標籤上，「設定」下拉式清單，選取要新增「區域」的「位置」。

4 在「信任」或「限制」標籤上，按下「新增」。

5 在「網路」對話方塊中，選取下列其中一項：

- 個別：識別電腦的單一 32 位元號碼
- 使用範圍：IP 位址所包含的範圍，從起始的 IP 位址到結束的 IP 位址
- 使用網路位址：透過輸入一個 IP 位址與子網路遮罩所建立之 IP 位址所包含的範圍

6 在文字方塊中，輸入您要新增至「信任」或「限制」區域中之電腦的 IP 位址。

7 按下「確定」。

8 在「網路」標籤上，按下「確定」。

Chapter 9

防範入侵

本章包含以下主題：

關於防範入侵

網路攻擊行動利用電腦傳輸資訊的方法進行。Symantec Client Security 防火牆用戶端可以監視進出您電腦的資訊，並攔截攻擊行為來保護您的電腦。

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，讓個別程式進行處理。Internet 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。

網路攻擊的設計即是利用特定 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正在監聽該通訊埠，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包含在一個或多個封包中。

Symantec Client Security 防火牆用戶端防止網路受到攻擊的方式

Symantec Client Security 防火牆用戶端包含兩種防護您的電腦遠離入侵攻擊、惡意網頁內容以及特洛伊木馬程式的工具：

- Symantec Client Security 防火牆用戶端：會監視所有 Internet 上的通訊，並建立一個可以攔截或限制嘗試檢視您電腦上資訊的防護。
- 入侵偵測：分析所有進出電腦的資訊，是否有典型的攻擊資料特徵。

Symantec Client Security 防火牆用戶端監視通訊的方式

當 Symantec Client Security 防火牆用戶端啟動時，它會監視您電腦和 Internet 上其它電腦之間的通訊。它也會保護您的電腦免於表 9-1 所列的常見安全性問題。

表 9-1 常見安全性問題

問題	防護
不當連線行為	警告您其它電腦嘗試進行連線，並警告您電腦上的程式嘗試連線到其它電腦。
特洛伊木馬程式	當您的電腦發現冒充有用程式的破壞性程式時通知您。
惡意網站內容的安全性及隱私權侵犯	監視所有 Java Applet 及 ActiveX 控制項，並讓您選取要執行或攔截程式
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
入侵	偵測並攔截外部使用者攻擊您電腦的惡意流量與行為

您可以使用「安全性等級」滑動軸，控制防護的等級。您也可以控制 Symantec Client Security 防火牆用戶端如何回應不當連線行為、特洛伊木馬程式及惡意的網站內容。

請參閱第 96 頁的「自訂防火牆防護」。

入侵偵測分析流量的方式

「入侵偵測」會掃描每個進出您電腦的封包是否有攻擊特徵、用以識別攻擊者嘗試利用作業系統或程式之已知弱點的資訊排列方式。

表 9-2 列舉 Symantec Client Security 防火牆用戶端監視的攻擊範例。

表 9-2 監視的攻擊行為

攻擊	說明
Bonk	針對 Microsoft TCP/IP 堆疊的攻擊，會癱瘓受到攻擊的電腦
RDS_Shell	利用「Microsoft 資料存取元件」所屬「遠端資料服務」元件的方法，可讓遠端攻擊者使用系統權限執行指令
WinNuke	可使用 NetBIOS，將較舊的 Windows 95/98/NT 電腦加以癱瘓的方式

攻擊可能涉及多個封包，因此「入侵偵測」會使用下列兩種方法來檢查封包。它會個別掃描每個封包，尋找攻擊的典型特徵。它也會將封包視為資訊流進行監視，讓它辨識涉及多個封包的攻擊行為。

如果資訊屬於已知的攻擊行為，則「入侵偵測」會自動捨棄封包，並負責傳送資料的電腦連線。這會保護您的電腦不受任何方式的影響。

您可以修改「入侵資訊」回應攻擊的方式，只要排除攻擊特徵不受監視，然後啟動或停用可自動攔截受攻擊電腦所有通訊的「自動攔截」功能。排除某些網路行為不受攔截後，即使您的電腦遭受攻擊，您仍可以繼續進行工作。

在保護您的電腦不受攻擊的同時，Symantec Client Security 防火牆用戶端也會監視您的電腦傳送給其它電腦的所有資訊。這會確保您的電腦不會用來攻擊其他使用者，或者遭受殭屍程式利用。*殭屍*程式是一種可以暗地安裝在電腦上，然後經由遠端執行的方式對其它電腦進行集體攻擊的程式。如果 Symantec Client Security 防火牆用戶端偵測出您的電腦正在傳送典型的攻擊資訊，便會立刻攔截連線，並警告您可能會發生的問題。

若要減少您接收的警告數量，Symantec Client Security 防火牆用戶端可以只監視您電腦使用的通訊埠是否有攻擊行為。如果攻擊者嘗試經由未使用的通訊埠，或防火牆所攔截的通訊埠連線至您的電腦，Symantec Client Security 防火牆用戶端將不會通知您，因為其中沒有入侵的危險。

Symantec Client Security 防火牆用戶端不會掃描您在「信任」區域中的電腦是否有入侵行為。不過，「入侵偵測」不會監視您傳送至「信任」電腦上的資訊，是否有殭屍程式及其它遠端控制攻擊的跡象。

「入侵偵測」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。定期執行 LiveUpdate 可確保您的攻擊特徵清單維持最新狀態。

請參閱第 77 頁的「透過 LiveUpdate 隨時保持最新狀態」。

自訂防火牆防護

預設的防火牆設定會提供您適當的防護措施。如果預設的防護措施不盡完善，您可以使用「安全性等級」滑動軸來自訂防火牆。滑動軸可讓您選取某些預先設定的安全性設定。您也可以變更個別的安全性設定以自訂防火牆。

變更安全性等級滑動軸

「安全性等級」滑動軸可讓您選取「低」、「中」或「高」的安全性設定。當您變更滑動軸位置時，防護等級就會隨著變更。變更「安全性等級」滑動軸不會影響「入侵偵測」所提供的防護。

變更「安全性等級」滑動軸

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「個人防火牆」標籤上，將滑動軸移動至您要的「安全性等級」。您可以選擇：

高	防火牆會攔截所有項目，直到您允許為止。如果您已經執行「程式掃描」，您應該不會經常被「程式控管」警示中斷您的工作。 每次 ActiveX 控制項或 Java Applet 出現時，您便會收到警示訊息。未使用的通訊埠不會回應連線，而且將之隱藏起來。
中 (建議)	防火牆會攔截所有項目，直到您允許為止。如果您已經執行「程式掃描」，您應該不會經常被「程式控管」警示中斷您的工作。 ActiveX 控制項及 Java Applet 執行時，不會出現警告訊息。未使用的通訊埠不會回應連線，而且將之隱藏起來。
低	防火牆會攔截特洛伊木馬程式嘗試連接的連線。 ActiveX 控制項及 Java Applet 執行時，不會出現警告訊息。 未使用的通訊埠不會回應連線，而且將之隱藏起來。

4 按下「確定」。

變更個別的安全性設定

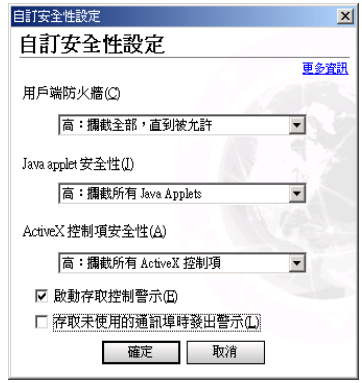
如果預設的「安全性等級」選項不符合您的需求，您可以變更 Symantec Client Security 防火牆用戶端、Java 及 ActiveX 防護等級的設定。變更個別設定會變更「安全性等級」，但是不會變更該等級中的其它安全性設定。

變更個別的安全性設定

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Security 視窗的「個人防火牆」標籤上，按下「自訂等級」。



4 在「自訂安全性設定」視窗中，執行下列一項或多項：

- 在「用戶端防火牆」下拉式清單中，選取一個等級。您可以選擇：

  高　攔截所有您未特別允許的通訊作業。您必須為每個要求 Internet 存取的程式建立防火牆規則。

  中　除非被特洛伊木馬程式規則攔截，允許所有 Internet 通訊。

  無　允許所有 Internet 通訊。

- 在「Java applet 安全性」或「ActiveX 控制項安全性」下拉式清單中，選取一個等級。您可以選擇：

  高　阻止瀏覽器透過 Internet 執行任何 Java Applet 或 ActiveX 控制項。這是最安全，也最不方便的選項。使用此設定可能會使某些網站無法正常執行。

  中　遭遇 Java Applet 和 ActiveX 控制項時便會出現提示。這樣您就可以暫時或永久的允許或攔截所遇到的每個 Java Applet 及 ActiveX 控制項。每次 Java Applet 及 ActiveX 控制項出現時，逐一回應可能有點麻煩，不過這可讓您決定要執行哪些項目。

  無　不論何時遭遇 Java Applet 與 ActiveX 控制項都要執行。

- 若要在每次未知程式存取 Internet 時能夠通知您，請勾選「**啟動存取控制警示**」。
- 若要在每次遠端電腦嘗試連接沒有程式使用的通訊埠時能夠通知您，請勾選「**存取未使用的通訊埠時發出警示**」。

5 按下「**確定**」。

6 在「個人防火牆」標籤上，按下「**確定**」。

將安全性設定重設為預設值

設定自訂安全性等級會停用「安全性等級」滑動軸。若要使用滑動軸選取預先設定的安全性等級，您必須重設安全性等級。

將安全性設定重設為預設值

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 在 Symantec Client Security 視窗的「個人防火牆」標籤上，按下「**預設等級**」。
這會將您的安全性等級重設為「中」。使用「安全性等級」滑動軸選取其它任一個預先設定的安全性等級。

自訂防火牆規則

防火牆規則會控制 Symantec Client Security 防火牆用戶端如何保護您的電腦不受惡意的連入流量、程式及特洛伊木馬程式侵襲，並停止惡意的連出流量。防火牆會自動使用這些規則檢查所有進出您電腦的流量。規則分為以下三個類別：

- 一般：使用會影響所有程式的封包過濾控制防護
- 程式：允許或攔截程式存取 Internet
- 特洛伊木馬程式：防止惡意的程式

若要自訂防火牆規則和使用大部分的防火牆功能，您必須被指派為 「管理員」的使用者層級。

請參閱第 69 頁的 「Symantec Client Security 防火牆用戶端使用者層級」。

建立新的防火牆規則

Symantec Client Security 防火牆用戶端含有 「程式控管」，會在您使用 Internet 時，為已知的程式自動建立防火牆規則。您也可以手動建立與修改規則。所有規則都與一個或多個 「位置」相關。

使用 「程式控管」建立防火牆規則有下列四種方式：

啟動 「自動程式控管」	在使用者首次執行已知的程式時，自動架構存取。這個選項是設定防火牆規則最簡單的方式。您可以為每個 「位置」啟動或停用這個選項。
使用 「程式掃描」	一次找出並架構所有 Internet 型程式的存取。您可以將規則新增至您指定的 「位置」。
回應警示	當已知程式第一次嘗試存取 Internet 時，如果 「自動程式控管」關閉，以及當未知的程式嘗試存取 Internet 時，警告使用者。然後使用者可以允許或攔截程式的 Internet 存取。您可以將規則只新增至目前的 「位置」。
手動新增 「一般」、「程式」和 「特洛伊木馬程式」規則	讓使用者嚴密地管理可以存取 Internet 的程式及服務清單。您可以將規則新增至一個或多個 「位置」。

啟動自動程式控管

當 「自動程式控管」啟動時，Symantec Client Security 防火牆用戶端會在第一次執行程式時，自動架構 Internet 的存取設定。「自動程式控管」只為賽門鐵克已識別為安全的程式版本架構 Internet 存取。

如果有未知的程式或已知程式的未知版本嘗試存取 Internet，Symantec Client Security 防火牆用戶端會警告使用者。然後使用者可以允許或攔截程式的 Internet 存取。

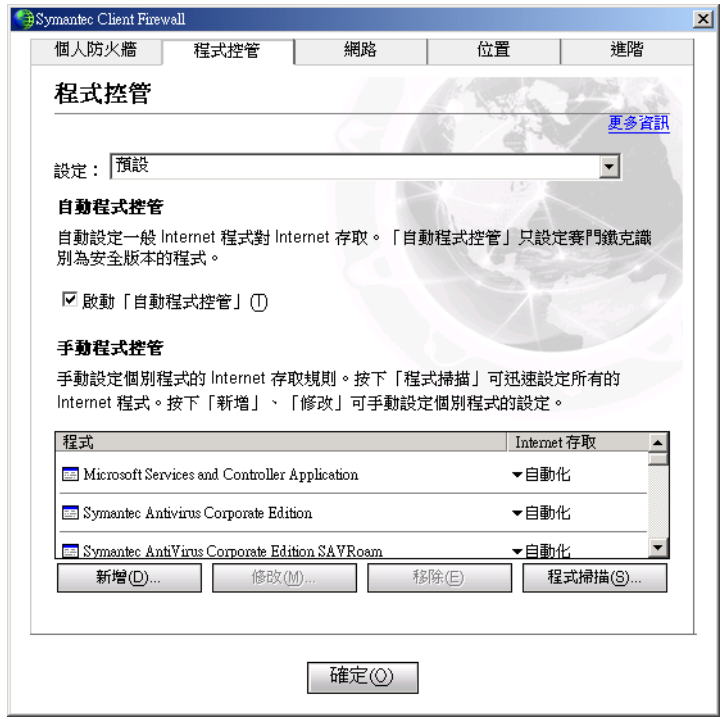
請參閱第 77 頁的「透過 LiveUpdate 隨時保持最新狀態」。

賽門鐵克會定期更新可辨識的程式清單。您應該定期執行 LiveUpdate，才能確保您的清單是最新的。

啟動「自動程式控管」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。



3 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單中，選取啟動「自動程式控管」的「位置」。

4 勾選「啟動自動程式控管」。

5 按下「確定」。

掃描及新增 Internet 型程式

掃描 Internet 型的程式是使用「程式控管」設定防火牆規則最快的方式。Symantec Client Security 防火牆用戶端會掃描電腦中可辨識的程式，並讓您選取每個程式適用的設定。

掃描及新增 Internet 型程式

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Security 視窗的「程式控管」標籤上，按下「程式掃描」。

4 在「程式掃描」視窗中，選取您電腦上要掃描的一個或多個磁碟。

5 按「下一步」。

6 執行下列其中一個動作：

- 勾選您要新增至 Internet 型程式清單的程式。
- 按下「全選」即可一次新增所有 Internet 型的程式。
- 按下「新增 」，手動新增程式。
- 選取程式並按下「修改 」，變更程式設定。

7 按「下一步」。

8 執行下列其中一個動作：

- 選取與程式相關的「位置」。
- 按下「全部選取 」，建立程式與所有「位置」的關聯。

9 按下「完成」。

10 在「程式控管」標籤上，按下「確定」。

將程式新增至程式控管

您可以將程式新增至「程式控管」，以嚴格控制程式存取 Internet 的能力。這會覆寫「自動程式控管」的所有設定。

將程式新增至「程式控管」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單，選取要新增「程式規則」的「位置」。

4 按下「新增」。

5 瀏覽並選取程式的執行檔。

6 按下「開啟」。

7 在「Internet 存取」警示中，選取您希望程式具有的存取等級。您可以選擇：

自動化 (建議)	使用這個程式的預設 Symantec Client Security 防火牆用戶端設定。這個選項不會一直出現。
允許全部	允許此程式的所有存取行為。
攔截全部	拒絕此程式的所有存取行為。
自訂	建立控制此程式存取 Internet 方式的規則。

8 如果您要查看此程式可能對您的電腦造成的任何危險，請按下「顯示細節」。

9 按下「確定」。

10 在「程式控管」標籤上，按下「確定」。

變更程式控管設定

使用 Symantec Client Security 防火牆用戶端一段時間之後，您可能會發現您必須變更程式的存取設定。例如，您可以選擇攔截程式日後進行的 Internet 連線，也可以允許先前所攔截程式的 Internet 存取。任何變更都會覆寫「自動程式控管」的設定。

變更「程式控管」設定

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「用戶端防火牆」。

3 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單中，選取包含「程式規則」要變更的「位置」。

4 在程式清單中，選取您要變更的程式。

5 按下「修改」。

6 在「程式控管」警示中，選取您希望此程式具有的存取等級。您可以選擇：

自動化 (建議)	使用這個程式的預設 Symantec Client Security 防火牆用戶端設定。這個選項不會一直出現。
允許全部	允許此程式的所有存取行為。
攔截全部	拒絕此程式的所有存取行為。
自訂	建立控制此程式存取 Internet 方式的規則。

7 按下「確定」。

8 在「程式控管」標籤上，按下「確定」。

手動建立防火牆規則

Symantec Client Security 防火牆用戶端會自動建立您所需要的大部分防火牆規則，不過您還是可以新增特定的規則。只有經驗足夠的 Internet 使用者才可以建立自己的防火牆規則。

防火牆規則會定義被允許或攔截的特定通訊類型。新增或修改規則之前，確定您了解防火牆規則的元件。

動作選項

「動作」選項可讓您指定規則要允許、攔截或監視規則中所定義的網路通訊類型。

表 9-3 說明可用的「動作」選項。

表 9-3 動作選項

選項	說明
允許	允許這種類型的通訊發生。
攔截	防止這種類型的通訊發生。
監控	當啟動追蹤時，更新 Symantec Client Security 防火牆用戶端「事件日誌」中的「防火牆」標籤。然後規則處理會繼續進行，直到找到符合的項目為止。如果沒有符合的事件，預設將會攔截該通訊，或者會有「Internet 存取控制」警示出現。

謹慎地使用「監控」動作。將規則架構成監視而不是允許或攔截，其造成的動作與用戶端的某些架構有關。舉例來說，如果「用戶端防火牆」等級設定為「高」、「存取控制警示」設定為「啟動」且「自動程式控管」也設定為「啟動」，則 Symantec Client Security 防火牆用戶端便會在用戶端電腦上自動明瞭地建立一條規則，允許已知的應用程式連上 Internet。用戶端設定的其它混合方式，有的可能會導致防火牆把設定成「監控」動作的流量攔截掉，也可能導致防火牆詢問使用者要允許或攔截某種流量。

表 9-4 所示即為「用戶端防火牆」滑動軸等級設定為「高」，搭配「存取控制警示」及「自動程式控管」設定為啟動或停用時，在各種情況下防火牆會採取的動作。

表 9-4 「用戶端防火牆」等級設定為「高」的監控動作結果

存取控制警示狀態	自動程式控管狀態	產生的防火牆動作
停用	停用	攔截。

表 9-4 「用戶端防火牆」等級設定為「高」的監控動作結果

存取控制警示狀態	自動程式控管狀態	產生的防火牆動作
啟動	停用	允許或攔截 (由使用者決定)。
停用	啟動	攔截未知的應用程式。 自動為已知的應用程式建立允許通過的規則。
啟動	啟動	允許或攔截未知的應用程式 (由使用者決定)。 自動為已知的應用程式建立允許通過的規則。

連線選項

「連線」選項可讓您指定規則要套用到入埠網路通訊、離埠網路通訊，或雙向網路通訊。

表 9-5 說明可用的「連線」選項。

表 9-5 連線選項

選項	說明
連接到其它電腦	規則套用於從您的電腦到另一台電腦的離埠連線。
來自其它電腦的連線	規則套用於從另一台電腦到您的電腦的入埠連線。
與其它電腦之間的連線	此規則適用於入埠和離埠連線。

附註：Symantec Client Security 防火牆用戶端會使用狀態檢查。因此，防火牆允許回應入埠流量的離埠流量。結果，您只需要為用戶端起始的流量建立離埠規則，例如 HTTP。

請參閱第 106 頁的「關於狀態檢查」。

電腦選項

「電腦」選項可讓您指定套用規則的電腦和網路配接卡。您所指定的電腦是您要控制通訊的電腦。

表 9-6 說明可用的「電腦」選項。

表 9-6 電腦選項

選項	說明
任何電腦	此規則適用於所有電腦。

表 9-6 電腦選項

選項	說明
只限下列的電腦和網站	此規則適用於一部電腦、指定 IP 位址範圍的多部電腦，或是網域中的多部電腦。
配接卡	規則套用於您的電腦中的特定配接卡。指定應該套用規則的配接卡的 IP 位址。

通訊協定選項

「通訊協定」選項可讓您指定規則控制的通訊協定。

表 9-7 說明可用的「通訊協定」選項。

表 9-7 通訊協定選項

選項	說明
TCP	此規則適用於傳輸控制通訊協定 (TCP) 的通訊。
UDP	此規則適用於使用者資料包通訊協定 (UDP) 的通訊。
TCP 和 UDP	此規則適用於 TCP 與 UDP 通訊。
ICMP	此規則適用於 Internet 控制訊息通訊協定 (ICMP) 的通訊。ICMP 僅適用於「一般」規則與「特洛伊木馬程式」規則。

通訊埠選項

「通訊埠」選項可讓您指定由規則控制的通訊或通訊埠類型。

表 9-8 說明可用的「通訊埠」選項。

表 9-8 通訊埠選項

選項	說明
所有類型的通訊 (所有通訊埠，包括本機和遠端)	此規則適用於使用任何通訊埠的通訊。
只有下列通訊或通訊埠類型	此規則適用於清單中所列的通訊埠。您可以在清單中新增與移除通訊埠。

追蹤選項

「追蹤」選項可讓您指定程式是否應該在網路通訊事件符合這條規則所設定的條件時，對您發出通知或者建立「事件日誌」項目。

表 9-9 說明可用的「追蹤」選項。

表 9-9 追蹤選項

選項	說明
有連線符合規則時，建立事件日誌項目	網路通訊事件符合這個規則時，在防火牆「事件日誌」中會建立一個項目。當此功能啟動時，您可以在事件發生 X 次之後，指定「只記錄」事件旁邊的事件頻率。
以「安全性警示」通知我	網路通訊事件符合這個規則時，「安全性警示」對話方塊就會出現。

說明

「說明」可讓您指定規則的名稱，如此一來便可以與其它規則加以區別。

位置選項

「位置」選項可讓您選取與規則相關的「位置」。

關於狀態檢查

Symantec Client Security 防火牆用戶端使用的狀態檢查是一個建立連線狀態表的程序，用來追蹤關於目前連線的資訊，例如來源與目標的 IP 位址、通訊埠、應用程式等等。Symantec Client Security 防火牆用戶端在檢查「一般」與「程式」規則之前，會使用此連線資訊決定流量。

例如，如果防火牆規則允許用戶端連線至網頁伺服器，防火牆便會在狀態表中記錄連線資訊。在伺服器回應時，防火牆會檢查狀態表，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到狀態表之前，規則必須允許最初的離埠流量。

因為您不需要只針對通常單向起始的流量建立允許雙向流量的規則，所以狀態檢查允許您簡化規則資料庫。通常單向起始的用戶端流量包括 Telnet (通訊埠 23)、FTP (通訊埠 20 及 21)、HTTP (通訊埠 80) 及 HTTPS (通訊埠 443)。用戶端起始此流量離埠，因此您必須針對這些通訊協定建立允許離埠流量的規則。當防火牆檢查狀態表時，會允許回傳通訊。

可能的話，只要架構離埠規則，便可以使用下列兩種方式增加用戶端安全性：

- 減少規則庫的複雜性。
- 消除病蟲或其它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。針對用戶端不起始的用戶端流量，您也可以只架構入埠規則。

狀態檢查支援指引 TCP/UDP 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，必要時您必須建立允許雙向流量的規則。例如，如果您需要用戶端使用偵測指令並接收回應，您必須建立允許雙向 ICMP 流量的規則。

防火牆規則處理的優先順序

當某部電腦嘗試連線到您的電腦，或者您的電腦嘗試連線到 Internet 上的電腦時，Symantec Client Security 防火牆用戶端會使用防火牆規則清單比對連線的類型。

防火牆規則會以狀態表開始的設定順序來處理。例如，如果入埠流量正在回應離埠流量，首先防火牆會檢查狀態表、發現入埠流量是預期的流量，然後允許此流量。即使現有的規則要攔截入埠回傳流量，也不會處理此攔截規則。

在狀態表之後，規則處理是依照規則是否鎖定而定。所有以 Symantec Client Security 防火牆用戶端建立的規則都會被解除鎖定。以 Symantec Client Firewall Administrator 建立，並匯出至 Symantec Client Security 防火牆用戶端的規則可以是鎖定或解除鎖定的。優先順序顯示於 表 9-10。

表 9-10 規則處理優先權

優先權	規則類型	使用者類型
第一	一般	鎖定
第二	程式	鎖定
第三	一般	解除鎖定
第四	程式	解除鎖定
第五	特洛伊木馬程式	鎖定
第六	特洛伊木馬程式	解除鎖定

附註：「安全通訊埠」公用程式完整防護 「特洛伊木馬程式」規則定義的通訊埠，因此架構為 「攔截」的所有 「特洛伊木馬程式」規則只針對離埠流量採取第一優先權。

請參閱第 111 頁的「使用安全通訊埠」。

新增防火牆規則

新增防火牆規則之前，您必須先決定要新增控制一般存取 Internet 的防火牆規則，或是控制程式的防火牆規則。

以下是可用的規則類型：

- 「一般」規則會影響所有應用程式存取 Internet，因為它們會檢查所有的封包。
- 「程式」規則會控制程式存取 Internet。擁有需要存取 Internet 的程式時，請使用 「程式」規則。

- 「特洛伊木馬程式」規則一般用來攔截特洛伊木馬程式所使用的通訊埠。在「一般」與「程式」規則檢查後，「特洛伊木馬程式」規則也會檢查所有的封包。

新增一般規則

您可以建立適用於電腦上所有程式的「一般」防火牆規則。

新增一般規則

1. 在主視窗中，按下「狀態與設定」。
2. 連按兩下「用戶端防火牆」。
3. 在 Symantec Client Firewall 視窗的「進階」標籤上，按下「一般」。
4. 在「一般規則」視窗中，按下「新增」。
5. 按照螢幕上的指示進行。
6. 在「進階」標籤上，按下「確定」。

新增程式規則

您可以建立適用於您電腦上特定程式的「程式控管」防火牆規則。

新增程式控管規則

1. 在主視窗中，按下「狀態與設定」。
2. 連按兩下「用戶端防火牆」。
3. 在 Symantec Client Firewall 視窗的「程式控管」標籤上，按下「新增」。
4. 在「選取程式」對話方塊中，選取一個執行檔，然後按下「開啟」。
5. 在「程式控管」警示的「您要做什麼？」下拉式清單中，按下「手動設定 **Internet** 存取」。
6. 按下「確定」。
7. 按照螢幕上的指示進行。
8. 在「程式控管」標籤上，按下「確定」。

新增特洛伊木馬程式規則

您可以建立適用於特洛伊木馬程式威脅的「特洛伊木馬」防火牆規則，並找出它們最近一次的檢查。當符合架構來中斷連線的「特洛伊木馬程式」規則時，會自動攔截起始此流量的 IP 位址。

請參閱第 116 頁的「啟動或停用自動攔截」。

新增特洛伊木馬規則

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 在「進階」標籤上，按下「**特洛伊木馬程式**」。

4 在「特洛伊木馬規則」對話方塊中，按下「**新增**」。

5 按照螢幕上的指示進行。

6 在「進階」標籤上，按下「**確定**」。

變更現有的防火牆規則

如果防火牆規則的功能不符您的需要，可以加以變更。如果您要變更規則，執行此規則的所有「位置」之規則都會變更。

變更現有的防火牆規則

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 執行下列其中一個動作：

- 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單中，選取包含欲變更之規則的「位置」。
- 在 Symantec Client Firewall 視窗的「進階」標籤上，選取「一般」或「特洛伊木馬程式」。

4 選取要變更的規則。

5 按下「**修改**」。

6 按照螢幕上的指示，變更規則的內容。

7 當您完成變更規則時，按下「**確定**」。

變更防火牆規則的順序

Symantec Client Security 防火牆用戶端會從上到下處理每個防火牆規則的清單。您可以藉由變更防火牆規則的順序來決定 Symantec Client Security 防火牆用戶端處理防火牆規則的方式。當您變更順序時，它只會影響目前選定「位置」的順序。

變更防火牆規則的順序

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 執行下列其中一個動作：

- 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單中，選取包含欲重新排序之規則的「位置」。
- 在 Symantec Client Firewall 視窗的「進階」標籤上，選取「一般」或「特洛伊木馬程式」。

4 選取您要移動的規則。

5 執行下列其中一個動作：

- 若要讓 Symantec Client Security 防火牆用戶端在處理此規則上面的規則之前先處理此規則，請按下「**上移**」。
- 若要讓 Symantec Client Security 防火牆用戶端在處理此規則下面的規則之後處理此規則，請按下「 **下移**」。

6 當您完成移動規則之後，按下「**確定**」。

暫時停用防火牆規則

如果您需要允許特定電腦或程式的存取，您可以暫時停用防火牆規則。如果您要停用規則，執行此規則的所有「位置」之規則都會停用。

暫時停用防火牆規則

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 執行下列其中一個動作：

- 在 Symantec Client Firewall 視窗的「程式控管」標籤上，按下「**修改**」，然後取消勾選您要停用之規則旁邊的方塊。
- 在 Symantec Client Firewall 視窗的「進階」標籤上，按下「一般」或「特洛伊木馬程式」，然後取消勾選您要停用之規則旁邊的方塊。

當您已完成使用需要變更的程式或電腦時，請記得重新啟動規則。

移除防火牆規則

您可以移除不再需要的防火牆規則。當您刪除規則時，系統會提示您決定要從目前的「位置」或是所有「位置」刪除規則。您無法刪除被鎖定的「一般」或「特洛伊木馬程式」規則，而且您無法刪除包含一個或多個已鎖定之規則的「程式」規則。

移除防火牆規則

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**用戶端防火牆**」。

3 執行下列其中一個動作：
   - 在 Symantec Client Firewall 視窗的「程式控管」標籤上，「設定」下拉式清單中，選取包含欲移除之規則的「位置」。
   - 在 Symantec Client Firewall 視窗的「進階」標籤上，選取「一般」或「特洛伊木馬程式」。
4 選取您要移除的規則。
5 按下「移除」。
6 當您完成移除規則之後，按下「確定」。

使用安全通訊埠

「安全通訊埠」會攔截在「特洛伊木馬程式」規則中定義為「攔截」的本機通訊埠上，以及執行 Symantec Client Security 防火牆用戶端的使用者定義的通訊埠上的 TCP 和 UDP 流量。「安全通訊埠」會完整防護通訊埠，因此來自這些通訊埠的離埠流量不會觸發防火牆規則資料庫檢查。由於規則資料庫沒有因為這些通訊埠而受到檢查，因此，即使「永遠顯示安全性警示」功能已啟動，這些通訊埠的防火牆警示訊息也不會出現。規則資料庫會因為這些通訊埠的入埠流量而受到檢查。

此外，當「安全通訊埠」啟動時，使用隨機通訊埠的 Windows 應用程式會知道這些通訊埠受到防護，並且會在隨機通訊埠定序時略過這些通訊埠。因此，「安全通訊埠」會在「一般」允許通訊埠範圍防護用戶端，以防範使用通訊埠的特洛伊木馬程式，而不中斷網路通訊。

附註：「安全通訊埠」會防護只於「特洛伊木馬程式」規則中定義做為「本機攔截」的通訊埠，並且也防護「信任」區域中的這些通訊埠。「安全通訊埠」無法防護由其它程式使用的通訊埠。此外，「程式控管」規則必須存在，以便攔截所有入埠至 SymSPort.exe 的 TCP 與 UCP 流量，否則特洛伊木馬警示仍將會出現。預設會安裝此規則。

啟動與停用安全通訊埠功能

「安全通訊埠」會防護您在「特洛伊木馬程式」規則中定義的所有通訊埠。

啟動與停用「安全通訊埠」功能

「安全通訊埠」可讓您選擇性地啟動與停用特定的通訊埠。

啟動「安全通訊埠」

1 在主視窗的上方，按下「選項」。

2 在「Symantec Client Firewall 選項」視窗的「安全通訊埠」標籤上，勾選「啟動安全通訊埠技術」，然後按下「確定」。
當通訊埠受到防護時，X 會出現在「安全的」欄，最多持續到 30 秒。

3 若要確認此通訊埠已受到防護，請重新開啟「Symantec Client Firewall 選項」視窗。

停用個別通訊埠的「安全通訊埠」

1 在通訊埠清單的「通訊協定」欄中，取消勾選列出目標通訊埠之列中的方塊。

2 按下「確定」。
當此通訊埠被釋放時，X 將不會出現在「安全的」欄。

3 若要確認此通訊埠已被釋放，請重新開啟「Symantec Client Firewall 選項」視窗。

啟動個別通訊埠的「安全通訊埠」

1 在通訊埠清單的「通訊協定」欄中，勾選列出目標通訊埠之列中的方塊。

2 按下「確定」。
當此通訊埠受到防護時，X 會出現在「安全的」欄。

3 若要確認此通訊埠已受到防護，請重新開啟「Symantec Client Firewall 選項」視窗。

停用「安全通訊埠」

1 在主視窗的上方，按下「選項」。

2 在「Symantec Client Firewall 選項」視窗的「安全通訊埠」標籤上，取消勾選「啟動安全通訊埠技術」，然後按下「確定」。
當此通訊埠被釋放時，X 會從「安全的」欄消失。

3 若要確認此通訊埠已被釋放，請重新開啟「Symantec Client Firewall 選項」視窗。

新增與移除使用者定義的通訊埠

「安全通訊埠」可讓您新增與移除額外的通訊埠。

新增與移除使用者定義的通訊埠

如果您嘗試移除以「特洛伊木馬程式」規則定義的通訊埠，此通訊埠將只變成停用。

將使用者定義的通訊埠新增至「安全通訊埠」

1 在主視窗的上方，按下「選項」。

2 在 Symantec Client Firewall 視窗的「安全通訊埠」標籤上，「通訊協定」下，選取下列項目之一：

- TCP
- UDP
- TCP、UDP

3 在「埠號」下，輸入要新增的埠號。

4 按下「新增」。
埠號列會出現在通訊埠清單中。

5 按下「確定」。

從「安全通訊埠」移除使用者定義的通訊埠

1 在通訊埠清單中，以滑鼠右鍵按下包含目標通訊埠的列，然後按下「移除」。
列出埠號的這列就會從通訊埠清單中消失。

2 按下「確定」。

附註：如果您嘗試移除以「特洛伊木馬程式」規則定義的通訊埠，此通訊埠將只變成停用。此通訊埠不會從清單中消失。

自訂入侵偵測

預設的「入侵偵測」設定會提供您適當的防護措施。如果預設的防護措施不合適，您可以自訂「入侵偵測」設定。您可以藉由排除特定的網路活動不要受到監視、啟動或停用「自動攔截」來自訂「入侵偵測」。

附註：自訂「入侵偵測」一般會使得系統變成較不安全。如果系統管理員已將特徵或 IP 位址架構為鎖定，您可能無法排除它們。

顯示入侵偵測警示

Symantec Client Security 防火牆用戶端可讓您選取在「入侵偵測」攔截連線時是否要顯示警示。

顯示「入侵偵測」警示

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「入侵偵測」。

3 在「入侵偵測」對話方塊中，勾選「當入侵偵測攔截連線時顯示警示」。

排除特定的網路活動不受監視

在某些狀況下，無害的網路活動可能看似 Symantec Client Security 防火牆用戶端攻擊特徵。如果您收到重複出現的可能攻擊警告，而且您知道這些攻擊是由安全的行為所觸發，您可以排除符合這些無害活動的攻擊特徵。

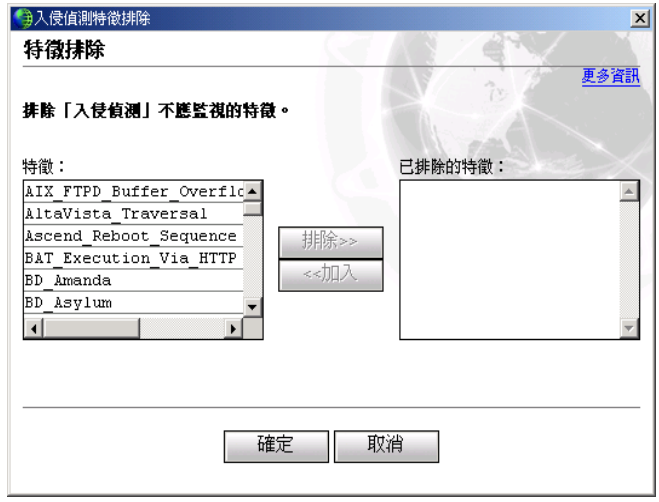
附註：您建立的每項排除都會讓您的電腦更容易遭受攻擊而且影響所有的 IP 位址。請務必善加選擇您要排除的攻擊項目。唯有無害的行為才可以排除。如果系統管理員已鎖定特徵，您可能無法排除它們。

排除攻擊特徵不受監視

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「入侵偵測」。

3 在「入侵偵測」對話方塊中，按下「進階」。



4 在「入侵偵測特徵排除」對話方塊的「特徵」清單中，選取您要排除的攻擊特徵。

5 按下「排除」。

6 完成排除特徵之後，按下「確定」。

7 按下「確定」。

加入攻擊特徵

如果您已排除您要再度監視的攻擊特徵，您可以在作用中特徵的清單中加入它們。

加入攻擊特徵

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「入侵偵測」。

3 在「入侵偵測」對話方塊中，按下「進階」。

4 在「入侵偵測特徵排除」對話方塊的「已排除的特徵」清單中，選取您要監視的攻擊特徵。

5 按下「加入」。

6 完成加入特徵之後，按下「確定」。

7 按下「確定」。

啟動或停用自動攔截

當 Symantec Client Security 防火牆用戶端偵測到攻擊時，會自動攔截來自攻擊電腦的流量，以確保您的電腦安全無虞。攻擊包含以「特洛伊木馬程式」規則指定的流量。Symantec Client Security 防火牆用戶端也會啟動「自動攔截」，自動攔截攻擊電腦的所有連入流量一段時間 (即使連入流量不符合攻擊特徵)。

「自動攔截」預設會停止來自攻擊電腦的所有入埠流量 30 分鐘，並將攻擊電腦的 IP 位址置於「自動攔截」清單中。雖然「自動攔截」會阻止遠端電腦的所有連入通訊，但是不會阻止您將資訊傳送給攻擊的電腦。

附註：在主視窗中，必須啟動「用戶端防火牆」來處理「自動攔截」IP 位址。如果停用「用戶端防火牆」，「自動攔截」也會被停用。此外，「信任區域」中的 IP 位址將不會新增至「自動攔截」清單，因此「自動攔截」IP 位址會與所有「位置」相關。

啟動或停用「自動攔截」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「入侵偵測」。

3 在「入侵偵測」對話方塊中，執行下列其中一個動作：

- 勾選「啟動自動攔截」。
- 取消勾選「啟動自動攔截」。

從 Symantec Client Security 防毒用戶端放入自動攔截

當 Symantec Client Security 防毒用戶端偵測到攻擊時，它也可以在「自動攔截」清單中放入攻擊電腦的 IP 位址。

從 Symantec Client Security 防毒用戶端放入「自動攔截」

1 在 Symantec AntiVirus 視窗中，按下「架構」>「檔案系統自動防護」。

2 在「檔案系統自動防護」視窗中，按下「啟動自動防護」。

3 按下「進階」。

4 在「自動防護進階選項」視窗的「威脅追蹤程式」之下，執行下列步驟：

- 勾選「啟用威脅追蹤程式」。
- 勾選「解析來源電腦的 IP 位址」。
- 勾選「用戶端防火牆自動攔截 IP 位址 (來源電腦)」。

5 按下「確定」。

6 在「檔案系統自動防護」視窗中，按下「確定」。

取消攔截自動攔截目前攔截的電腦

在某些個案中，Symantec Client Security 防火牆用戶端可能會將正常的活動當成是攻擊。如果您無法與應該可以通訊的電腦通訊，這些電腦可能位在「現在被自動攔截所攔截的電腦」清單上。

如果您需要存取的電腦位在「現在被自動攔截所攔截的電腦」清單上，請取消攔截。如果您已經變更您的防護設定，而且想要重設您的自動攔截清單，您可以一次取消攔截「現在被自動攔截所攔截的電腦」清單上的所有電腦。

取消攔截自動攔截目前攔截的電腦

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**入侵偵測**」。

3 在「入侵偵測」對話方塊中，執行下列其中一個動作：

- 若要取消攔截一台電腦，選取電腦的 IP 位址，然後按下「**不攔截**」。
- 若要取消攔截「目前被自動攔截所攔截的電腦」清單上的所有電腦，按下「**全部不攔截**」。

將特定電腦排除在自動攔截之外

某些正常的 Internet 活動會一再被 Symantec Client Security 防火牆用戶端視為攻擊。例如，某些 Internet 服務供應商會掃描您電腦上的通訊埠，以確保您遵守服務合約範圍。若要防止正常活動中斷您使用 Internet，您可以排除這些活動不被「自動攔截」所攔截。

從「自動攔截」中排除特定活動

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**入侵偵測**」。

3 在「入侵偵測」對話方塊中，按下「**例外**」。

4 執行下列其中一個動作：

- 在「目前攔截的電腦」清單中，選取所攔截的 IP 位址，然後按下「**移除**」。
- 按下「**新增**」，然後輸入 IP 位址、IP 位址範圍，或是包含您要排除之電腦的網路位址。

5 完成排除 IP 位址之後，按下「**確定**」。

附註：您無法移除系統管理員已鎖定的 IP 位址。

限制被攔截的電腦

您可以將遭攔截的電腦加入到您的「限制」區域，以便永久防止該電腦存取您的電腦。加入「限制」區域的電腦不會出現攔截清單中，這是因為 Symantec Client Security 防火牆用戶端會自動拒絕受限電腦的任何連線。

限制被攔截的電腦

1. 在主視窗中，按下「**狀態與設定**」。
2. 連按兩下「**入侵偵測**」。
3. 在「入侵偵測」對話方塊中，「目前被自動攔截所攔截的電腦」清單內，選取要新增至「限制」區域的位址。
4. 按下「**限制**」。
5. 完成限制電腦之後，按下「**確定**」。

Chapter 10

防護網頁瀏覽階段作業

本章包含以下主題：

關於防護您的隱私權

每次您瀏覽 Internet 時，電腦及網站會蒐集有關您的資訊。您的某些資訊來自您填寫的表格，以及您在網頁上選擇的項目。其它資訊則來自您的瀏覽器，瀏覽器會自動提供您上次瀏覽的網頁資訊及您正在使用的電腦類型。

許多網站會將蒐集到的資訊儲存在 cookie 中，並且置放在您的硬碟上。如果您返回已經在您的電腦上設定 cookie 的網站，網頁伺服器便會開啟並讀取 cookie。

大多數的 cookie 都不具威脅性。網站會使用這些資訊讓網頁更加個人化、記住您在網站上進行的選擇，並且傳送針對您電腦最佳化的網頁。不過，網站也會使用 cookie 來追蹤您的 Internet 使用狀況及瀏覽習慣。

惡意的使用者會在您不知情的狀況下蒐集您的個人資訊。如果您在 Internet 上傳送資訊，資訊必須先經過許多電腦，才會到達目的地。在傳送期間，可能會有其他人攔截並竊取這個資訊。

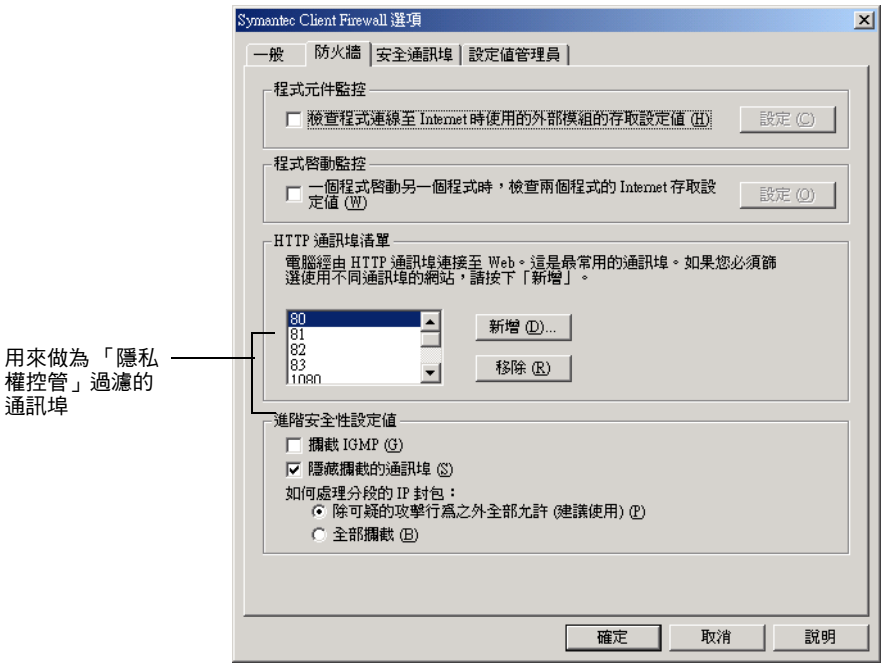
電腦包含某些基本的安全性功能，不過可能不足以防護您的個人資訊。「隱私權控管」協助防護您的隱私權時，會提供多種控制 cookie 的層級，以及瀏覽器傳送給網站的其它資訊。

「隱私權控管」也可以確保您不在 Internet 上傳送信用卡號碼之類的私人資訊，除非已經加密或您特別允許才會傳送。「隱私權控管」只過濾純文字。

關於選取通訊埠來監視隱私權

「Symantec Client Firewall 選項」視窗包含「隱私權控管」所監視的通訊埠清單。圖 10-1 顯示通訊埠清單的位置。

圖 10-1 用來做為「隱私權控管」過濾的 HTTP 通訊埠清單



當您選取「隱私權控管」功能與選項時，假設這些功能與選項會在這些通訊埠上執行。如果此通訊埠清單是空的，而且有啟動「隱私權控管」，「隱私權控管」就會被有效地停用，因為它不知道要監視哪一個通訊埠。

預設的通訊埠是大多數網頁流量常用的通訊埠。但是，架構網頁伺服器讓一般與自訂內部應用程式搭配使用的 HTTP 流量使用不同的通訊埠非常容易。如果您使用採用不同通訊埠的自訂網頁型應用程式，當您想要在這些通訊埠上執行「隱私權控管」時，您必須將這些通訊埠新增至此清單中。

附註：此通訊埠清單不適用於即時傳訊程式與電子郵件用戶端的「隱私權控管」。

識別要防護的私人資訊

許多網站都會要求輸入您的姓名、電子郵件位址及其它個人資訊。在著名的大型網站上提供這些資訊通常很安全，不過惡意的網站會使用這些資訊來侵犯您的隱私。其他人也可能攔截經由網頁、電子郵件訊息和即時傳訊程式所傳送的資訊。

「隱私權控管」可讓您建立不公開訊息的訊息清單。如果您嘗試在 Internet 上傳送受保護的資訊，Symantec Client Security 防火牆用戶端會發出安全風險的警告，或者攔截連線。

輸入私人資訊的秘訣

因為 Symantec Client Security 防火牆用戶端完全以您輸入至程式中的方式攔截個人資訊，所以最好只輸入部份的數字。例如，電話號碼可以輸入為 888-555-1234，也可以不加上破折號 (8885551234) 或加上空格 (888 555 1234)，也可以使用兩個以上的欄位加以分隔。這些格式的共同點是後四碼 (1234) 永遠在一起。因此，保護最後四碼的防護效果比保護整組號碼更有效。

輸入部分資訊有兩個好處。第一，您不會在其他人可能找到的地方輸入完整的號碼。第二，它可讓 Symantec Client Security 防火牆用戶端攔截您在使用多個文字方塊輸入電話號碼或信用卡號碼的網站上所輸入的私人資訊。

關於隱私權控管與 SSL

大多數處理信用卡交易的網站都使用 Secure Sockets Layer (SSL) 連線來加密您的電腦與伺服器之間的連線。因為流量被加密，所以「隱私權控管」無法攔截透過 SSL 連線傳送的私人資訊。然而，因為資訊被加密，所以只有電子郵件的收件者可以讀取此訊息。必要時，您可以停用您電腦建立 SSL 連線的能力。

請參閱第 123 頁的「自訂隱私權控管設定」。

設定隱私權控管等級

Symantec Client Security 防火牆用戶端會提供預先設定的安全性等級，以協助您一次設定多個「隱私權控管」選項。「隱私權等級」滑動軸可讓您選取低、中或高的防護。

設定「隱私權控管等級」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，將滑動軸移動至您想要的「隱私權等級」。您可以選擇：

高	所有的個人資訊都會被攔截，並在每次 cookie 出現時都顯示警示。

中 (建議)	如果有私人資訊被輸入網頁表單、電子郵件訊息或即時傳訊程式中，則出現警示。隱藏已從網站瀏覽的 URL。Cookie 不會被攔截。
低	機密資訊不會被攔截。Cookie 不會被攔截。隱藏瀏覽網站的作業。

4 按下「確定」。

新增私人資訊

您必須將您要防護的資訊加入 Symantec Client Security 防火牆用戶端「私人資訊」清單中。

新增私人資訊

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，按下「私人資訊」。

4 在「私人資訊」對話方塊中，按下「新增」。

5 在「新增私人資訊」對話方塊的「資訊類別」下拉式清單中，選取一個類別。

6 在「說明」文字方塊中輸入說明，以協助您記住保護此資訊的原因。

7 請在「保護的資訊」文字方塊中，輸入您要攔截透過非安全 Internet 連線所傳送的資訊。

8 在「防護私人資訊的時機：」下，選取以下一個或多個程式來檢查私人資訊：

- 網路
- 即時通訊
- 電子郵件

9 按下「確定」。

修改或移除私人資訊

您可以在任何時候修改或移除私人資訊。

修改或移除私人資訊

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，按下「私人資訊」。

4 在「私人資訊」對話方塊中，選取您要修改或移除的私人資訊。

5 選取下列其中一項：

- 修改
- 移除

6 按下「確定」。

自訂隱私權控管設定

如果「隱私權控管等級」設定不符合您的需求，您可以變更「私人資訊」、「Cookie 攔截」、「瀏覽器隱私權」及「安全連線」的設定。例如，當允許網站使用您的瀏覽器資訊自訂其網頁時，您可以攔截所有嘗試傳送的私人資訊。

「隱私權控管」會防護表 10-1 所列出的四個區域。

表 10-1 「隱私權控管」防護區域

防護	說明
私人資訊	攔截您不要在 Internet 上傳送的特定字串
Cookie 攔截	停止網站擷取儲存在 cookie 檔中的個人資訊，並停止將它們寫入您的硬碟中。
瀏覽器隱私權	防護關於您的瀏覽習慣與瀏覽器軟體的資訊
安全連線 (https)	防止您使用 SSL 建立連接線上商店及其它網站的安全連線

當您自訂設定時，「隱私權控管等級」滑動軸會變成無法使用。

啟動「隱私權控管等級」滑動軸

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，按下「預設等級」。

變更私人資訊設定

您可以變更「私人資訊」設定，以控制 Symantec Client Security 防火牆用戶端如何處理嘗試在 Internet 上傳送「私人資訊」清單中的資訊。

變更「私人資訊」設定

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，按下「自訂等級」。

4 在「自訂隱私權設定」對話方塊中，選取您要的「私人資訊」設定。您可以選擇：

高	攔截所有連出的私人資訊
中	每當您嘗試傳送私人資訊至非安全的網站，或者透過即時傳訊程式或電子郵件訊息傳送時，便發出警示
無	不攔截私人資訊

5 按下「確定」。

變更 Cookie 攔截設定

許多網站會將蒐集到的資訊儲存在置放於您硬碟的 cookie 中。如果您返回已經在您的電腦上設定 cookie 的網站，網頁伺服器便會開啟並讀取 cookie。變更「Cookie 攔截」設定，以控制 Symantec Client Security 防火牆用戶端如何處理在您的電腦上置放 cookie 的網站。

附註：Cookie 分為暫時性 (暫時的) 與永久性 (永久的，直到您刪除它們) 兩種。Symantec Client Security 防火牆用戶端將兩者視為相同。

變更「Cookie 攔截」設定

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「隱私權控管」。

3 在「隱私權控管」視窗中，按下「自訂等級」。

4 在「自訂隱私權設定」對話方塊中，選取您要的「Cookie 攔截」設定。您可以選擇：

高	攔截所有 cookie
中	每當 cookie 出現時便發出警示
無	允許 cookie

5 按下「確定」。

啟動與停用瀏覽器隱私權

「瀏覽器隱私權」是一項「隱私權控管」功能，可防止網站蒐集關於您瀏覽器軟體與瀏覽習慣的資訊。

「瀏覽器隱私權」會防止網站得知您所使用的瀏覽器類型、您上次參觀的網站，以及有關您瀏覽習慣的其它資訊。如果某些使用 JavaScript 的網站無法辨識您所使用的瀏覽器類型，這些網站可能會運作不正常。

啟動或停用瀏覽器隱私權

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**隱私權控管**」。

3 在「隱私權控管」視窗中，按下「**自訂等級**」。

4 在「自訂隱私權設定」對話方塊中，執行下列其中一個動作：

- 若要啟動「瀏覽器隱私權」，勾選「**啟動瀏覽器隱私權功能**」。
- 若要停用「瀏覽器隱私權」，取消勾選「**啟動瀏覽器隱私權功能**」。

5 按下「**確定**」。

停用與啟動安全連線

當您拜訪安全的網站時，您的瀏覽器會設定連接該網站的加密連線。「私人資訊」無法透過加密的連線進行過濾。如果您要確定您並未將私人資訊傳送至安全網站，您可以停用安全連線。

如果您停用安全連線，您的瀏覽器將無法加密所傳送的任何資訊。只有在您使用「私人資訊」過濾時，才應該停用安全連線。

停用或啟動安全連線

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下「**隱私權控管**」。

3 在「隱私權控管」視窗中，按下「**自訂等級**」。

4 在「自訂隱私權設定」對話方塊中，執行下列其中一個動作：

- 若要啟動安全連線，勾選「**啟動安全連線 (https)**」。
- 若要停用安全連線，取消勾選「**啟動安全連線 (https)**」。

5 按下「**確定**」。

攔截廣告

許多網站會使用積極的技巧，在它們的網頁上引起您注意廣告。某些網站已開始使用較大、較顯著的廣告，而某些網站則依賴您進入或離開網站時出現的視窗。隨著顯示網頁所需時間的增加，某些廣告會包含攻擊性的內容，造成軟體的衝突，或使用技巧來開啟額外的瀏覽器視窗。

「廣告攔截」有助於避免這些問題。當「廣告攔截」啟動時，Symantec Client Security 防火牆用戶端會透明化移除以下項目：

- 廣告橫幅
- 上下方彈出的廣告
- Macromedia Flash 型廣告與動畫

廣告攔截的運作方式

Symantec Client Security 防火牆用戶端會根據以下三種準則，偵測與攔截廣告：大小、位置與字串。

請參閱第 132 頁的「關於建立識別要攔截或允許之廣告的文字字串」。

根據大小攔截

大多數的線上廣告使用一個或多個標準大小。Symantec Client Security 防火牆用戶端現在可以攔截與一般廣告大小相同的影像、Flash 動畫與其它 HTML 元件。

根據位置攔截

Internet 上的每個檔案都有獨特的位址或 URL。當您檢視網頁時，您的電腦會連線到 URL，並顯示儲存在該處的檔案。如果該頁面指向圖形與其它多媒體內容，您的瀏覽器會將這些檔案顯示為網頁的部分。

當您前往一個包含橫幅廣告的網頁時，用來顯示頁面的指示可能包含以下項目：

<p> 來自於「清潔公司」的歡迎詞 <img src="http://www.spammersRus.com/nifty_images/image7.gif">

您的瀏覽器會在畫面上顯示來自於「清潔公司」的歡迎詞。接著它會連接到 www.spammersRus.com，並請求一個具有以下名稱的檔案：/nifty_images/image7.gif。(字尾為 .gif 表示這是一個圖形交換格式的檔案，一個常見的影像檔格式)。在 www.spammersRus.com 的電腦會將檔案傳送至顯示此影像的瀏覽器。

如果「廣告攔截」已啟動，而且您連線至網站，Symantec Client Security 防火牆用戶端會掃描網頁，並且將內容與下列兩個清單進行比較：

- Symantec Client Security 防火牆用戶端自動攔截的預設廣告清單。使用 LiveUpdate 保持最新的廣告攔截清單。

- 當您攔截特定廣告時建立的清單。您可以在清單中新增或修改。

如果頁面包含來自被攔截網域的檔案，Symantec Client Security 防火牆用戶端會移除連結，並下載頁面的其它部分。您也可以為個別的網站架構「廣告攔截」設定。

請參閱第 132 頁的「架構廣告攔截設定」。

啟動與停用廣告攔截

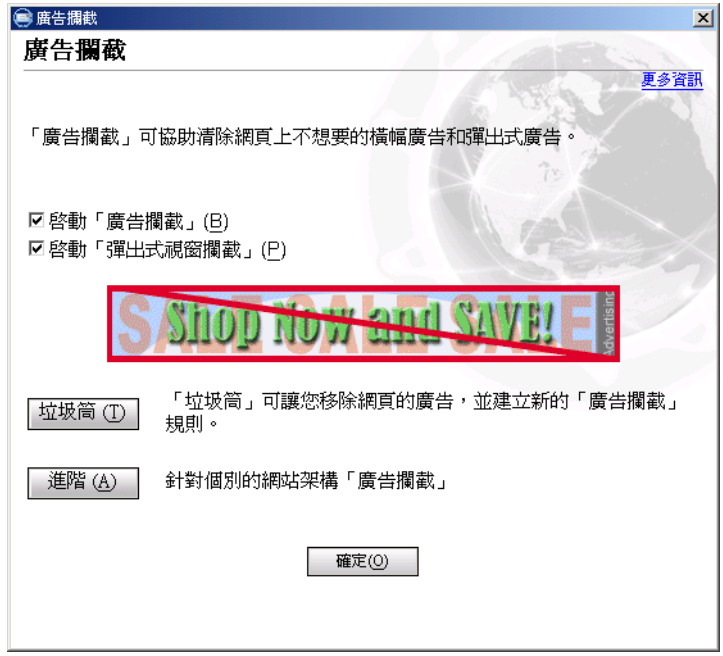
當您的瀏覽器下載網頁時，Symantec Client Security 防火牆用戶端會搜尋被攔截的廣告位址。如果發現與要攔截之廣告清單相符的位址，它會移除此廣告，讓它不會出現在您的瀏覽器中。它會留下網頁其餘完整的部分，因此您可以檢視沒有廣告的頁面。當「廣告攔截」停用時，「進階」視窗中的設定也會被停用。

請參閱第 129 頁的「使用進階網站內容設定」。

啟動與停用「廣告攔截」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「廣告攔截」。



3 在「廣告攔截」視窗中，執行下列其中一項：
- 若要啟動「廣告攔截」，請勾選「啟動廣告攔截」。
- 若要停用「廣告攔截」，取消勾選「啟動廣告攔截」。

4 按下「確定」。

啟動與停用彈出式視窗攔截

上下彈出式廣告是當您拜訪或離開網站時，網站所開啟的第二個視窗。上方彈出式廣告會出現在目前視窗的上方，而下方彈出式廣告則出現在目前的視窗之後。

當「彈出式視窗攔截」啟動時，Symantec Client Security 防火牆用戶端會自動攔截網站在您不知情的情況下，用來開啟第二個視窗的程式碼。當您按下連結或執行其它動作時，所開啟第二個視窗的網站將不會受到影響。

啟動或停用「彈出式視窗攔截」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下「廣告攔截」。

3 在「廣告攔截」視窗中，執行下列其中一項：
- 若要啟動「彈出式視窗攔截」，請勾選「啟動彈出式視窗攔截」。
- 若要停用「彈出式視窗攔截」，請取消勾選「啟動彈出式視窗攔截」。

4 按下「確定」。

使用垃圾筒

當您使用 Internet 時，您可能會發現未包含在預設 Symantec Client Security 防火牆用戶端「廣告攔截」清單中的廣告。您可以使用「垃圾筒」，將這些廣告新增至您個人的攔截廣告清單。

使用「垃圾筒」

1 開啟您的網路瀏覽器，然後檢視包含您要攔截之廣告的頁面。

2 在主視窗中，按下「狀態與設定」。

3 連按兩下「廣告攔截」。

4 在「廣告攔截」視窗中，確認已勾選「啟動廣告攔截」。

5 按下「垃圾筒」。

6 若要藉由視窗的安排而可以同時看到廣告與「垃圾筒」視窗，執行下列其中一項：

- 如果您使用的是 Microsoft Internet Explorer，將不想要的廣告從網站拖曳至「廣告攔截」視窗。
- 如果您使用的是 Netscape，在廣告上按下滑鼠右鍵，然後按下「**複製影像位置**」。在「垃圾筒」中，按下「**貼上**」。
  廣告的位址就會出現在「垃圾筒」視窗的「廣告詳細資訊」行中。

7 選取下列其中一項：

- 新增：攔截此位址。
- 修改：將項目新增至「廣告攔截」清單中之前，變更此項目。
  例如，如果廣告位址是 http://www.advertise.org/annoying/ads/numberone.gif，您可能將它變更為 http://www.advertise.org/annoying/ads/，來攔截該網站上這個廣告目錄中的所有檔案。

8 按下「**確定**」。

使用進階網站內容設定

「Web 內容選項」可以讓您控制 Symantec Client Security 防火牆用戶端如何處理互動式線上內容、廣告與可能的隱私權侵犯。「Web 內容選項」安排在下列的三個標籤：

- 全域設定值
  當網站嘗試取得關於您瀏覽器或拜訪過之網站的資訊，或是使用動畫影像、程序檔、Flash，以及其它作用中的內容時，讓您控制 Symantec Client Security 防火牆用戶端所採取的預設動作。
- 使用者設定值
  可讓您針對個別網站，自訂「Cookie 攔截」、「彈出式視窗攔截」以及 ActiveX 與 Java Applet。
- 廣告攔截
  在個別的網站上，讓您指定您要攔截或允許的個別字串。

附註：所有「Web 內容」過濾會在「Symantec Client Firewall 選項」視窗的「防火牆」標籤上，「HTTP 通訊埠清單」中所指定的通訊埠上執行。如果此清單是空白的，防火牆不會執行「Web 內容選項」。此外，「信任」區域中的電腦會忽略「Web 內容」設定。

架構全域設定值

「全域設定值」可以讓您控制 Symantec Client Security 防火牆用戶端在網站嘗試取得關於瀏覽器之資訊或使用動畫影像、程序檔與其它作用中內容時所採取的行動。表 10-2 說明這些設定。

表 10-2 全域設定值

設定	說明
關於瀏覽器的資訊	攔截或允許網站取得關於您電腦與網路瀏覽器的資訊。
已拜訪的網站的資訊	攔截或允許網站取得關於您在線上階段作業期間拜訪過之網站的資訊。
動畫影像	攔截或允許動畫影像執行。影像仍會出現，但不會有動畫。
程序檔	攔截或允許程序檔。
Flash 動畫	攔截或允許以 Macromedia Flash 製作的動畫及廣告。

如果停用「隱私權控管」視窗中的「隱私權控管」設定，會忽略關於瀏覽器資訊及已拜訪網站資訊的「全域設定值」。

啟動與停用全域設定值

「全域設定值」對話方塊可讓您設定所有網站的預設值，並且允許您針對個別網站設定特定的允許或攔截設定。

某些網站使用 Flash 建立瀏覽工具列。攔截 Flash 可能會使這些網站無法使用。

啟動或停用「全域設定值」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下以下任一項：

- 隱私權控管
- 廣告攔截

3 在「隱私權控管」或「廣告攔截」視窗中，按下「進階」。

4 在「進階」視窗中，執行下列其中一項：

- 要變更所有網站的預設值，在「Web 內容選項」標籤上，按下「(預設值)」。
- 若要覆寫單一網站的預設值，在「Web 內容選項」標籤上，選取網站的名稱，然後在「全域設定值」標籤的一個或多個設定之下，取消勾選「使用預設值」。

5 針對您要邊更的每個設定，選取以下其中一項：
- 允許
- 攔截

6 按下「確定」。

7 在「隱私權控管」或「廣告攔截」視窗中，按下「確定」。

架構使用者設定值

「使用者設定值」可以讓您自訂個別網站的「Cookie 攔截」、「彈出式廣告攔截」與 ActiveX 及 Java Applet 設定。這些設定會覆寫出現在其它對話方塊中的預設值。表 10-3 說明這些設定並識別包含此預設值的對話方塊。

表 10-3 使用者設定值

設定	說明	對話方塊
Cookie	攔截或允許網站在您的電腦上建立與讀取 cookie 檔	隱私權控管，自訂隱私權設定
Java Applet	攔截或允許 Java Applet 執行	用戶端防火牆，自訂安全性設定
ActiveX 控制項	攔截或允許 ActiveX 控制項執行	用戶端防火牆，自訂安全性設定
彈出式廣告	攔截或允許彈出式廣告	廣告攔截

Cookie 分為永久性與暫時性兩種。Symantec Client Security 防火牆用戶端將兩者視為相同。

架構「使用者設定值」

1 在主視窗中，按下「狀態與設定」。

2 連按兩下以下任一項：
- 隱私權控管
- 廣告攔截

3 在「隱私權控管」或「廣告攔截」視窗中，按下「進階」。

4 在「進階」視窗的「Web 內容選項」標籤上，選取一個網站名稱。

5 在「使用者設定值」標籤的一個或多個設定之下，取消勾選預設值。

6 針對您要取消勾選的每個設定，選取以下其中一項：
- 允許
- 攔截

7 按下「確定」。

8 在「隱私權控管」或「廣告攔截」視窗中，按下「確定」。

架構廣告攔截設定

「廣告攔截」設定可以讓您指定在個別網站上要攔截或允許的個別廣告橫幅或廣告影像群組。Symantec Client Security 防火牆用戶端根據兩種標準偵測與攔截廣告：它們的大小與位置。

附註：如果您要使用 Symantec Client Firewall Administrator 將政策檔匯出至 Symantec Client Security 防火牆用戶端，而且如果「橫幅攔截用戶端設定」被停用，則 Symantec Client Security 防火牆用戶端上的「廣告攔截」也會被停用。

關於建立識別要攔截或允許之廣告的文字字串

您可以建立能辨識個別廣告橫幅的字串清單，以控制 Symantec Client Security 防火牆用戶端是否顯示特定的廣告。「廣告攔截」字串是 HTML 位址的部分。如果檔案位址的任何部分與字串相符，Symantec Client Security 防火牆用戶端會自動攔截該檔案。Symantec Client Security 防火牆用戶端提供用來決定顯示網頁時應該攔截哪些影像的「廣告攔截」清單 (預設)。

當「廣告攔截」啟動時，會掃描所有網頁，找出 (預設) 清單中指定的 HTML 字串。Symantec Client Security 防火牆用戶端會尋找用來呈現廣告的 HTML 頁面中被攔截的字串。在網路瀏覽器顯示頁面之前，包含符合字串的 HTML 結構會被 Symantec Client Security 防火牆用戶端移除。

請確定您置於 (預設) 清單中的字串不會過於廣泛。例如，www 本身就不是攔截的好字串，因為幾乎所有 URL 都包含 www。例如 www.slowads 的字串比較有效，因為它只會攔截來自 slowads 網域的圖形，而不影響其它網站。

您定義「廣告攔截」字串的方式會影響 Symantec Client Security 防火牆用戶端過濾資料時的限制程度。例如，如果您在 (預設) 攔截清單中新增 spammersRus.com 字串，您會攔截 spammersRus.com 網域中的所有資料。如果您更加精確，在 www.spammersRus.com 的特定網站攔截清單中新增 /images/image7.gif 字串，就只會攔截該特定影像。

您也可以建立允許字串，允許網頁顯示符合字串的影像。這可以讓您覆寫個別網站 (預設) 攔截清單中任何字串的攔截效果。允許規則優先於任何網站的「攔截」規則。

附註：所有新增、修改與移除字串的功能都可以藉由以滑鼠右鍵按下字串取得，包含排序的其它功能。

新增廣告攔截字串

您可以在所有網站或個別網站的「廣告攔截」清單中新增字串。「廣告攔截」僅支援小寫字元。

新增「廣告攔截」字串

1 在主視窗中，按下「狀態與設定」。

2 連按兩下以下任一項：

- 隱私權控管
- 廣告攔截

3 在「隱私權控管」或「廣告攔截」視窗中，按下「進階」。

4 在「進階」視窗的「廣告攔截」標籤上，執行下列其中一項：

- 若要攔截所有網站上的字串，在「Web 內容選項」標籤上，按下「**(** 預設值 **)**」。
- 若要在網站上攔截清單中的字串，請跳至步驟 5。

5 在「Web 內容選項」標籤上，選取網站的名稱，然後在「廣告攔截」標籤上，按下「新增」。

6 在「新增 HTML 字串」對話方塊中，選取您要採取的動作。您可以選擇：

攔截	攔截符合此字串的廣告。
允許	允許符合此字串的廣告。

7 輸入要攔截或允許的 HTML 字串。

8 按下「確定」。

9 在「進階」視窗中，按下「確定」。

10 在「隱私權控管」或「廣告攔截」視窗中，按下「確定」。

修改與移除廣告攔截字串

如果您稍後認為「廣告攔截」字串限制太多、不夠廣泛，或不適當，您可以加以修改或移除。

修改或移除「廣告攔截」字串

1 在主視窗中，按下「狀態與設定」。

2 連按兩下以下任一項：

- 隱私權控管
- 廣告攔截

3 在「隱私權控管」或「廣告攔截」視窗中，按下「進階」。

4 在「進階」視窗的「廣告攔截」標籤上，執行下列其中一項：
- 若要修改或移除 (預設) 清單中的字串，在「Web 內容選項」標籤上，按下「**(預設值)**」。
- 若要修改或移除網站專有的字串，請跳至步驟 5。

5 在「Web 內容選項」標籤上，選取網站的名稱。

6 在「廣告攔截」標籤的「HTML 字串」清單中，選取您要修改或移除的字串。

7 執行下列其中一個動作：
- 若要修改字串，請按下「**修改**」、輸入您的變更，然後按下「**確定**」。
- 若要移除字串，請按下「**移除**」，然後按下「**是**」。

8 在「進階」視窗中，按下「**確定**」。

9 在「隱私權控管」或「廣告攔截」視窗中，按下「**確定**」。

新增與刪除網站

Symantec Client Security 防火牆用戶端可讓您將網站新增至網站清單或從網站清單中刪除網站。

新增與刪除網站

1 在主視窗中，按下「**狀態與設定**」。

2 連按兩下以下任一項：
- 隱私權控管
- 廣告攔截

3 在「隱私權控管」或「廣告攔截」視窗中，按下「**進階**」。

4 在「進階」視窗的「Web 內容選項」標籤上，執行下列其中一項：
- 若要新增網站，按下「**新增網站**」、輸入網站或網域名稱，然後按下「**確定**」。
- 若要刪除網站，選取網站的名稱、按下「**移除網站**」，然後按下「**是**」。

5 在「進階」視窗中，按下「**確定**」。

6 在「隱私權控管」或「廣告攔截」視窗中，按下「**確定**」。

Chapter 11

監視 Symantec Client Security 防火牆用戶端

本章包含以下主題：

關於監視 Symantec Client Security 防火牆用戶端

Symantec Client Security 防火牆用戶端會維持每次進出 Internet 連線的記錄，及程式防護您電腦的動作。您應該定期檢視這項資訊，以便找出潛在的安全風險。

Symantec Client Security 防火牆用戶端 訊有下列三個來源：

- 「狀態」視窗：關於防火牆和內容攔截之活動的資訊
- Symantec Client Firewall 的「狀態」視窗：關於 Symantec Client Security 防火牆用戶端所採取的網路活動及動作的詳細資訊
- 日誌檢視器：使用者的 Internet 活動及 Symantec Client Security 防火牆用戶端 採取的動作。

檢視記錄的資訊時，檢視下列項目：

- 「目前狀態」視窗中的最近攻擊狀況
- 拒絕存取的次數，特別是來自單一 IP 位址的存取
- 一系列來自相同 IP 位址的埠號，這可能表示通訊埠掃描 (攻擊者會嘗試掃描您電腦上的許多通訊埠，並尋找可存取的通訊埠)

■ 不明程式的大量網路活動

平常會發現許多不規則的拒絕存取 (不是來自相同的 IP 位址，也不是針對一系列的埠號)。您可能也會發現所記錄的存取次數是因為您自己的電腦活動所導致，如連線至 FTP 伺服器和傳送電子郵件。

如果您發現上述的任何項目，這可能是攻擊的證據。

檢視統計值視窗

「統計值」視窗提供您前一次啟動 Window 以來的電腦網路活動快照。使用這項資訊可以辨識正在進行的攻擊行為，並可以檢視「隱私權控管」設定如何影響防護。表 11-1 說明由「統計值」視窗所提供的資訊。

表 11-1 統計值視窗資訊

區段	資訊
用戶端防火牆	最近針對此電腦進行的攻擊，包括最近攻擊的時間及最常攻擊電腦的 IP 位址。
最新攔截到的線上內容	已經攔截或允許的 cookie 數目、私人資訊和網頁廣告，以及已經攔截私人資訊的次數

檢視「統計值」視窗

◆ 在主視窗中，按下「統計值」。

重設統計值視窗資訊

重新啟動 Windows 時，Symantec Client Security 防火牆用戶端會自動清除「統計值」視窗中的所有統計值。您也可以手動清除統計值。這有助於瞭解架構變更是否影響統計值。

重設「統計值」視窗資訊

1 在主視窗中，按下「**統計值**」。

2 在「統計值」視窗中，按下「**清除統計值**」。

檢視 Symantec Client Firewall 的「統計值」視窗

除了「統計值」視窗中的整體統計值，Symantec Client Security 防火牆用戶端還會維護可追蹤 Internet 使用率的即時網路計數器，以及 Symantec Client Security 防火牆用戶端所採取的動作。表 11-2 說明與 Symantec Client Firewall「統計值」視窗一起提供的資訊。

表 11-2 Symantec Client Firewall 的「統計值」視窗資訊

窗格	資訊
網路	傳送及接收的 TCP 及 UDP 位元組、開放式網路連線次數，以及程式啟動後的開放式網路同時連線最高次數
線上內容	Cookie、私人資訊、攔截的網頁廣告，以及 HTTP 連線的數量
防火牆 TCP 連線	攔截及允許的 TCP 連線數量
防火牆 UDP 資料包	攔截及允許的 UDP 連線數量
防火牆規則	為您的防火牆定義的所有規則，以及關於允許、攔截，或不符合防火牆規則的通訊數資訊
網路連線	目前連線的資訊，包括正在進行連線的程式、正在使用的通訊協定，以及連接的電腦位址或名稱
最後 60 秒	網路及 HTTP 連接次數，以及每種連線類型的速度

檢視詳細的統計值

1 在主視窗中，按下「**統計值**」。

2 在「統計值」視窗中，按下「**詳細的統計值**」。

重設統計值計數器

您可以重設計數器來清除所有的統計值，並且再次開始累計。這有助於瞭解架構變更是否影響統計值。

重設統計值計數器

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall「統計值」視窗的「檢視」功能表上，按下「重設」。

選擇性顯示統計值

您可以一次檢視所有的詳細統計值，也可以僅顯示某些類別。

選擇性顯示統計值

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall「統計值」視窗的「檢視」功能表上，按下「選項」。

4 在 Symantec Client Firewall 的「統計值選項」視窗中，選取您要顯示的一項或多項統計值類別。

5 按下「確定」。

架構欄位

「詳細的統計值」視窗可以在一欄或兩欄中顯示資訊。這兩個視窗的配置都包含相同的統計值。

架構欄位

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall 的「統計值」視窗中，執行下列其中一項：

- 若要根據目前的視窗寬度，自動調整為一欄或兩欄顯示，可在「檢視」功能表上，按下「直欄」>「自動」。
- 若要永遠顯示為一欄，可在「檢視」功能表上，按下「直欄」>「一個」。
- 若要永遠顯示為兩欄，可在「檢視」功能表上，按下「直欄」>「兩個」。

永遠顯示詳細的統計值視窗

即使程式在全螢幕視窗中執行，您也可以永遠顯示「詳細的統計值」視窗。這在找出可能會發生安全性問題的未使用網路活動時非常有用。

永遠顯示詳細的統計值視窗

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall「統計值」視窗的「檢視」功能表上，按下「最上層顯示」。

使用日誌檢視器

Symantec Client Security 防火牆用戶端會記錄關於您所參觀的網站資訊、防火牆所採取的動作，以及已經觸發的警示。此日誌包含「統計值」視窗所報告的某些活動詳細資料。

「事件日誌」分為 10 個標籤，如表 11-3 所示。

表 11-3 日誌檢視器標籤

標籤	資訊
內容攔截	Symantec Client Security 防火牆用戶端 所攔截的 Java Applet 及 ActiveX 控制項詳細資訊。
連線	此電腦所進行的 TCP/IP 網路連線記錄。當連線關閉時，會記錄連線。
防火牆	防火牆所攔截的流量，包括處理的規則、顯示的警示、攔截的未使用通訊埠，以及自動攔截事件。
入侵偵測	監視的攻擊特徵及發現與攔截的入侵數量 (不論「入侵偵測」是否啟動)。
隱私權	已經攔截的 Cookie，包括 Cookie 的名稱及要求 Cookie 的網站。所列出的資訊與 Cookie 設定有關。
私人資訊	已傳送或攔截的私人資訊。
系統	啟動或停用 Symantec Client Security 防火牆用戶端的時間、連線活動，以及對於規則、pRule 與 IDS 設定的管理員更新。
架構	關於規則與 IDS 特徵之架構變更與更新的資訊。
網站歷程	電腦所拜訪的 URL，這會提供網站活動記錄。

表 11-3 日誌檢視器標籤

標籤	資訊
警示	所有警示活動，包括一般「Internet 存取控制」警示，以及由 Symantec Client Security 防火牆用戶端電腦上可能的攻擊所觸發的安全性警示。

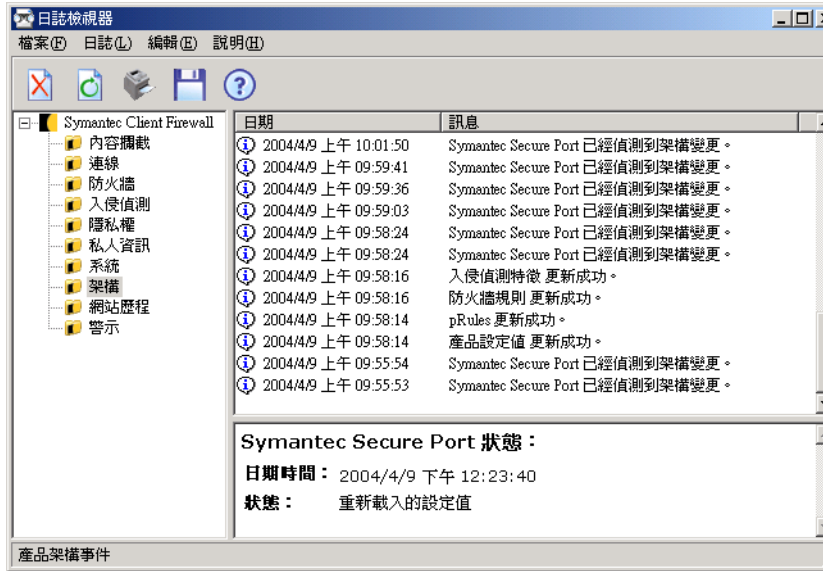
檢視日誌

您可以從「統計值」視窗檢視 Symantec Client Security 防火牆用戶端日誌。

檢視日誌

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。



3 在「日誌檢視器」視窗中，選取您要檢視的日誌。

4 完成後，選取另一個日誌，或按下「檔案」>「結束」，關閉「日誌檢視器」視窗。

重新整理日誌

當您從一個日誌移到另一個時，這些日誌就會自動重新整理。若要檢視從您開始檢視「日誌檢視器」起發生的網路事件，您可以手動重新整理所有日誌或個別的日誌。

重新整理日誌

您可以重新整理所有日誌和個別的日誌。

一次重新整理所有日誌

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」中，以滑鼠右鍵按下 **Symantec Client Firewall**，然後按下「重新顯示所有類別」。

重新整理個別的日誌

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」中，以滑鼠右鍵按下您要重新整理的日誌，然後按下「重新顯示類別」。

清除日誌

如果您主動使用 Internet，或者其它電腦經常連線到您的電腦，「日誌檢視器」可能會包含數以百計的連線資訊。這可能會讓識別入侵者活動或評估您變更 Symantec Client Security 防火牆用戶端設定的影響更加不容易。

您可以清除「日誌檢視器」標籤來移除記錄的資訊。這可讓您查看設定變更如何影響防護。您可以清除單一「日誌檢視器」標籤，或一次清除整個「日誌檢視器」。

清除日誌

您可以清除單一「日誌檢視器」標籤上或整個「日誌檢視器」上的事件。

清除單一日誌

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下您要清除的日誌，然後按下「清除類別」。

一次清除所有日誌

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下 **Symantec Client Firewall**，然後按下「清除所有類別」。

變更日誌檢視器的大小

「日誌檢視器」會在個別的檔案中儲存每個標籤的資訊。您可以變更「日誌檢視器」的檔案大小，以便管理所佔用的硬碟空間。檔案達到大小的上限時，新的事件會覆寫最舊的事件。

日誌檔的大小預設介於 64 KB 和 2048 KB 之間。如果您要查看長達一段時間的資訊，請增加日誌的檔案大小。如果您需要復原硬碟空間，請減少檔案大小。變更日誌檔的大小會清除該日誌中的所有資訊。

變更「日誌檢視器」的大小

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下日誌，然後按下「變更日誌檔大小」。

4 在「日誌檔大小」對話方塊中，選取一個新的檔案大小。

5 按下「確定」。

在日誌檢視器中調整欄寬

您可以變更「日誌檢視器」中的欄寬。

在「日誌檢視器」中調整欄寬

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，您要檢視的標籤上，指向欄位標題右側的邊界線。游標會由指標變更為重新調整大小的工具。

4 將邊界線拖曳至所需的寬度。

停用記錄

您可以選取 Symantec Client Security 防火牆用戶端在日誌中追蹤的資訊類型。Symantec Client Security 防火牆用戶端預設會追蹤每個類別中的事件。如果您不需要個別日誌中所包含的資訊，可以停用它們。

停用記錄

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下您要停用的日誌，然後按下「停用記錄」。

列印和儲存日誌及統計值

當您存取 Internet 時，日誌中較舊的資訊及統計值會被覆寫成較新的資料。若要保留較舊的 Internet 使用資訊，或者要在文字檔或其它文件中匯出此項資訊，可列印或儲存「日誌檢視器」及統計值。

列印和儲存日誌及統計值

您可以列印和儲存日誌及統計值。

列印日誌資訊

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下您要列印的日誌，然後按下「列印類別」。

列印統計值資訊

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall「統計值」視窗的「檔案」功能表上，按下「列印」。

4 在「列印」視窗中，按下「列印」。

將日誌資訊儲存至文字檔

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「檢視日誌」。

3 在「日誌檢視器」視窗中，以滑鼠右鍵按下您要儲存的日誌，然後按下「匯出類別」。

4 指定文字檔的位置及名稱。

5 按下「存檔」。

將統計值儲存為文字檔

1 在主視窗中，按下「統計值」。

2 在「統計值」視窗中，按下「詳細的統計值」。

3 在 Symantec Client Firewall「統計值」視窗的「檔案」功能表上，按下「存檔」。

4 指定文字檔的位置及名稱。

5 按下「存檔」。

索引

五劃

六劃

七劃

八劃

十三劃

十四劃

十五劃

十六劃

十七劃

十八劃

二十劃