Symantec AntiVirus™ Corporate Edition 用户端指南

Symantec AntiVirus™ Corporate Edition 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 10.0

版權聲明

商標

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

如果您所使用的產品需要註冊和 (或) 授權碼，註冊服務最快速、最簡單的方式就是至賽門鐵克授權與註冊網站：www.symantec.com.tw/certificate。或者，您可以到 www.symantec.com.tw/region/tw/techsupp/enterprise，選擇您要註冊的產品，然後從「產品」首頁選擇「授權與註冊」(Licensing and Registration) 連結。

聯絡技術支援

目前具有支援合約的客戶可以透過電話或網站：www.symantec.com.tw/region/tw/techsupp，聯絡「技術支援小組」。

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」可用來協助處理下列類型的問題：

- 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 3 章 防止您的電腦受到病毒與安全風險的入侵

第 4 章 發現病毒或安全風險時要執行什麼動作

索引

Chapter 1

Symantec AntiVirus 簡介

本章包含下列主題：

關於 Symantec AntiVirus

您可以將 Symantec AntiVirus™ 的病毒及安全風險防護安裝為單機版或由管理員管理的版本。單機版表示您的 Symantec AntiVirus 軟體不是由網路管理員所管理。

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膝上型電腦，並已使用預設選項設定或管理員預設的選項設定來安裝 Symantec AntiVirus
- 連接至您企業網路之前即符合安全性需求的遠端電腦

Symantec AntiVirus 預設的設定為您的電腦提供病毒和安全風險的防護。然而，您可能想要調整它們以符合您公司的需求、最佳化系統效能，或停用不需要的選項。

如果您的安裝是由管理員所管理，便會根據管理員的安全性政策，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。

您的管理員會告訴您 Symantec AntiVirus 有哪些用途。

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

關於更新單機電腦

單機電腦也可以連線至 Internet。在 Symantec AntiVirus 說明文件中，對於「單機」這個名詞有不同的解釋。單機電腦沒有連接至伺服器，因此不會從伺服器接收病毒和安全風險定義檔更新，也無法受到 Symantec System Center 管理員程式的管理。

如果您在單機電腦上安裝 Symantec AntiVirus，則您必須負責更新病毒和安全風險定義檔。賽門鐵克每個月都會提供數次新的定義檔。需要更換新的定義檔時，您將會收到警示。

您可以使用 LiveUpdate™ 更新病毒和安全風險定義檔。LiveUpdate 會從賽門鐵克網站擷取新的定義檔，並取代 Symantec AntiVirus 目錄中的舊定義檔。您需要數據機或 Internet 連線。

請參閱第 31 頁的「利用 LiveUpdate 立即更新防護」。

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和安全風險定義檔，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和安全風險定義檔的 Symantec AntiVirus。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

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上。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。

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。

所謂*混合型威脅*是將病毒、病蟲、特洛伊木馬程式和惡意程式碼與伺服器和 Internet 的弱點結合，以便起始、傳送和散佈攻擊的病毒。混合型威脅使用多種方法和技術進行繁殖和攻擊，並透過網路造成廣大的損害。

在 Symantec AntiVirus 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。Symantec AntiVirus 可以偵測、刪除、隔離病毒，及修復病毒所造成的副作用。

所謂*安全風險*是一種已知的程式，屬於如廣告軟體或間諜軟體的類別，可能會也可能不會對電腦造成安全上的風險。Symantec AntiVirus 可以偵測、隔離，和修復這些安全風險類別內，由風險所造成的副作用。

請參閱第 13 頁的「關於安全風險」。

病毒散播的方式

病毒可透過網路、數據機或磁性媒介散播。大多數開機型病毒只能經由磁片散播。多重型病毒特別難以捉摸，因為它們會以檔案病毒的形式傳送、感染開機磁區及經由磁片傳輸。

LAN、Internet 與全球電子郵件連線的成長已加速病毒散佈的速度。區域型病毒爆發之後，受感染的檔案可以透過電子郵件，快速散播到公司或全世界的其它部分。病毒感染的主要威脅來自於被共用，然後被開啟並使用的檔案。

病毒類型

病毒的分類是依照它們感染與嘗試躲避偵測的方式而定。基本病毒類型是根據它們所感染的電腦區域而定義，例如開機病毒、檔案病毒與巨集病毒。

其它類型的破壞型程式碼包括病蟲和特洛伊木馬程式。這類破壞性程式碼與病毒不同，因為它們不會複製。

開機病毒

開機病毒會在磁片的開機磁區或硬碟的開機磁區或主要開機記錄 (分割磁區) 中插入指令。開機病毒是某些最成功的病毒。

當電腦從受感染的磁片開機時，病毒會感染硬碟，並將其程式碼載入到記憶體中。病毒所散佈的磁片不一定要是開機磁片。病毒會存在於常駐記憶體中，並感染其存取的任何磁片。感染開機磁區的磁片或硬碟不會感染任何檔案，除非該病毒為多重病毒。真正的開機病毒無法傳播到伺服器，或是在網路上傳播。

請參閱第 13 頁的「關於主要開機記錄」。

檔案病毒

檔案病毒會在執行序列中插入指令，以便附加到 .com、.exe 與 .dll 等執行檔中。執行受感染的檔案時，插入的指令會執行病毒程式碼。程式碼完成執行後，檔案會繼續正常的執行序列。由於發生得十分迅速，您不會發現病毒已被執行。

檔案病毒可分為三個子類別：

- 常駐記憶體：留在記憶體中，成為常駐 (TSR) 程式，而且通常會感染所有已執行的檔案。
- 直接動作：執行、感染其它檔案，並卸載。
- 輔助：自行與執行檔結合，而不需加以修改。例如，病毒可能會建立輔助檔 Word.com，然後將它附加在 Word.exe 檔案。開啟 Word 程式時，便會執行受感染的 Word.com 檔、執行病毒活動，然後執行 Word.exe 檔。

檔案病毒引起的損失，包含顯示螢幕訊息等擾人活動及資料損毀等等。

巨集病毒

巨集病毒與其它病毒不同之處在於它們並不會感染程式檔，而是感染文件。許多巨集病毒的共同目標是像 Microsoft Word 與 Lotus AmiPro® 等文字處理程式，以及像 Microsoft Excel 等試算表。

Word 會使用巨集執行格式化文字，與開啟及關閉文件等動作。巨集病毒可以修改 Word 應用程式所定義的巨集，使其執行覆寫或重新定義 Word 預設定義等惡意動作。

巨集病毒引起的損失，可從在文件中插入不想要的文字，到大幅降低電腦功能。

感染 Word 的巨集病毒通常將與 Normal.dot 範本相關的巨集當作共同目標。這是一個通用範本，因此所有 Word 檔案都會被感染。

關於主要開機記錄

主要開機記錄包含在硬碟的第一個磁區中。開機程序的一部分包括賦予硬碟控制權。同時，程式位於啟動作業系統以載入隨機存取記憶體 (RAM) 的硬碟第一個磁區中。

開機病毒會移動、覆寫或刪除主要開機記錄，造成損壞。例如，Monkey 病毒會將主要開機記錄移動到硬碟的第三個磁區，然後將其本身的程式碼放在第一個磁區中。移動主要開機記錄會讓您無法從硬碟開機。

請參閱第 12 頁的「開機病毒」。

關於安全風險

安全風險是依照它們所從事的行為與所設計的目的而分類。和病毒和病蟲不同，安全風險不會自我複製。

Symantec AntiVirus 可以偵測、隔離、刪除，和移除或修復下列安全風險類別所造成的副作用：

- *間諜軟體*：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。
  間諜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「使用者授權協議」，而在不知情的狀況下載間諜軟體。
- *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。
  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。
- *撥號工具*：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，導致增加費用。
- *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。
- *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，它可以讓垃圾桶遠離滑鼠，或是使滑鼠以相反的方式被按下。
- *其它*：不符合其它任何安全風險類別，但可能對您的電腦或資料造成安全風險的安全風險。

- *遠端存取*：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。
- *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。

所有預設的 Symantec AntiVirus 掃描作業皆包括「自動防護」掃描、檢查病毒、特洛伊木馬程式、病蟲，以及所有安全風險的類別。

請參閱第 38 頁的「使用自動防護」。

請參閱第 46 頁的「起始手動掃描」。

Symantec™ Security Response (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。該網站同時內含大量的參考資訊，例如，關於病毒與安全風險的白皮書和詳細資訊。

圖 1-1 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 1-1 賽門鐵克安全機制應變中心安全風險說明

請參閱第 33 頁的「存取 Symantec Security Response (賽門鐵克安全機制應變中心) 網站」。

Symantec AntiVirus 如何處理病毒和安全風險

不管來源為何，Symantec AntiVirus 都能保護電腦不受病毒與安全風險的感染。來自硬碟、磁片及跨越網路的其它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它方式傳播的病毒與安全風險感染。例如，當您存取 Internet 時，安全風險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，並清除病毒和安全風險。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 AntiVirus 會以第一個動作與第二個動作來處理受到病毒或安全風險感染的檔案。

根據預設，當掃描作業偵測到病毒時，Symantec AntiVirus 會嘗試清除受感染檔案中的病毒，並修復病毒所造成的影響。如果檔案已完成清除，即表示病毒已成功且完全地移除。如果 Symantec AntiVirus 因為某些原因而無法清除檔案中的病毒，Symantec AntiVirus 便會嘗試進行第二個動作，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 AntiVirus 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：您的管理員會選擇自動掃描「隔離所」中的檔案。

預設情形下，Symantec AntiVirus 會針對安全風險隔離受感染的檔案，並傳回安全風險已被變更為其上一個狀態的系統資訊。完全移除某些安全風險時，會造成您電腦上的其它程式 (如網頁瀏覽器) 執行失敗。如果 Symantec AntiVirus 未被架構為自動處理風險，它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 Symantec AntiVirus 為只使用安全風險的僅記錄動作。

當 Symantec AntiVirus 搜索安全風險時，它也會在掃描視窗內顯示一個 Symantec Security Response (賽門鐵克安全機制應變中心) 的連結，讓您可以深入瞭解安全風險。您的系統管理員也可以傳送自訂的訊息。

Symantec AntiVirus 如何保護您的電腦

病毒感染是可以避免的。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。病毒和安全風險所造成的影響可以修復。偵測到病毒或安全風險時，Symantec AntiVirus 預設會通知您有一或多個檔案受到影響。如果您不想要收到通知，則您或管理員可以將 Symantec AntiVirus 架構為自動處理風險。

Symantec AntiVirus 提供這些防護類型：

- 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、移動或複製等檔案修改動作時，查看是否出現病毒和安全風險。
- 特徵掃描：搜尋受感染檔案內殘留的病毒特徵，以及受感染檔案內安全風險的特徵與系統資訊。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受到病毒和安全風險的感染，如廣告軟體或間諜軟體。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。
- 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，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 AntiVirus 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。他們也會追蹤新的安全風險，例如廣告軟體與間諜軟體。在辨識病毒或安全風險後，其*特徵*（病毒或安全風險的相關資訊）即會被存入*定義檔*，此檔案含有必要的資訊，可用來偵測、排除和修復病毒或安全風險所造成的影響。當 Symantec AntiVirus 掃描病毒和安全風險時，它會搜尋這些特徵的類型。

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。

如果新病毒和安全風險太複雜，以致所發佈的新定義檔不足以使用時，賽門鐵克的工程師會以最新的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定義檔。

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

Symantec AntiVirus 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安全風險需要努力追蹤、辨識與分析，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在掃描期間，用以偵測、排除和修復新病毒與安全風險所造成影響的定義檔。

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」，將受感染的檔案傳送給「賽門鐵克安全機制應變中心」，使發現病毒、進行分析然後進行解毒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，他們會提供關於刪除或移除該風險的資訊。百科全書位於「賽門鐵克安全機制應變中心」網站。

請參閱第 33 頁的「存取 Symantec Security Response (賽門鐵克安全機制應變中心) 網站」。

病毒和安全風險防護如何進行更新

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

您的管理員可以設定 Symantec AntiVirus 中的 LiveUpdate 功能，以確定您的病毒和安全風險防護保持最新的狀態。透過 LiveUpdate，Symantec AntiVirus 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 29 頁的「更新病毒和安全風險防護定義檔」。

Chapter 2

Symantec AntiVirus 基礎篇

本章包含下列主題：

關於安全資訊授權

安全資訊授權是由賽門鐵克公司所授與，可更新電腦上的賽門鐵克軟體。安全資訊授權能確保賽門鐵克產品可以在指定的時間週期，接收最新的更新檔。安全資訊更新包括病毒和安全風險定義檔。

您必須在每一部執行 Symantec AntiVirus 的電腦上，配置或安裝安全資訊授權。

附註：在部分企業中，賽門鐵克安全資訊更新是由網站授權來管理。在這些狀況下，將不適用安全資訊授權，因此您不需要參考此節的內容。

賽門鐵克用戶端可以在沒有安全資訊授權的情況下，接收一次安全資訊更新。您可以向賽門鐵克要求安全資訊授權的未來更新，這樣能確保新安裝的軟體可以提供最新的防護功能。因此，不具備有效安全資訊授權的電腦不能接收安全資訊更新。

安全資訊授權以下列的方式安裝：

- 對於透過 Symantec System Center 管理的用戶端，當它登入父系伺服器時，會自動收到它的授權使用者個數。您不需要進行任何動作來安裝安全資訊授權。
- 對於以協力廠商散佈工具管理的用戶端，您的管理員將會確認您的用戶端會自動收到授權。您不需要進行任何動作來安裝安全資訊授權。
- 對於未管理的用戶端，它不使用 Symantec System Center，則需要您來安裝安全資訊授權檔。您的管理員將會提供安全資訊授權檔，或是通知您用於安裝的安全資訊授權檔位置。

將安全資訊授權安裝至未管理的用戶端

您的管理員將利用下列任一種方式，提供安全資訊授權檔：

- 使用電子郵件傳送安全資訊授權檔給您。
- 將安全資訊授權檔放置在網路磁碟機上，並通知您位置。

將安全資訊授權安裝至未管理的用戶端

1. 在 Symantec AntiVirus 中，按下「檢視」>「授權」。
2. 在右窗格中，按下「安裝授權」。
3. 在「授權安裝精靈」的步驟 1 中，按下「瀏覽」，找出安全資訊授權檔，再按「下一步」。
4. 在「授權安裝精靈」的步驟 2，確認授權資訊，然後按「下一步」。
5. 若要關閉「授權安裝精靈」，按下「完成」。

開啟 Symantec AntiVirus

您可以透過數種方式開啟 Symantec AntiVirus。

開啟 Symantec AntiVirus

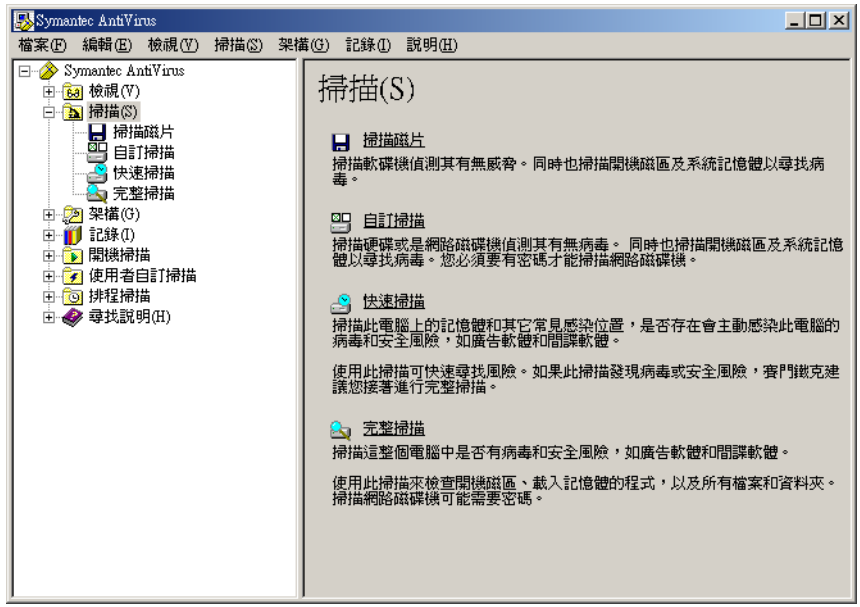
- 執行下列其中一個動作：
  - 在 Windows 工作列上，連按兩下 Symantec AntiVirus 圖示。

    您的管理員可以決定是否要將此圖示顯示在工作列上。
  - 在 Windows 或 Windows XP 工作列上，依情況按下「開始」>「程式集」> **Symantec Client Security** > **Symantec AntiVirus** 或「開始」>「程式集」> **Symantec Client Security** > **Symantec AntiVirus**。

瀏覽 Symantec AntiVirus 主視窗

Symantec AntiVirus 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」、「自訂掃描」、「快速掃描」和「完整掃描」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 AntiVirus 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 AntiVirus 類別

使用 Symantec AntiVirus 執行的活動可以分為幾個主要類別。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」類別來追蹤防毒和安全風險活動。

表 2-1　　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。排程掃描可以由您或您公司的管理員建立。
隔離所	管理已隔離的受感染檔案以防其散播病毒或安全風險的影響。 請參閱第 69 頁的「重新掃描隔離所內的檔案是否有病毒」。
備份項目	刪除中毒檔案的備份複本。Symantec AntiVirus 會在嘗試修復前，先備份受感染項目的複本，作為資料安全防護屏障。在確認了 Symantec AntiVirus 已清除受病毒感染的項目後，您即應刪除「備份項目」中的複本。 Symantec AntiVirus 會在受安全風險感染的檔案被放到「隔離所」時，備份檔案。它也會保留受到安全風險 (如間諜軟體和廣告軟體) 感染之登錄檔設定和系統載入點的複本。系統載入點是特別具有安全風險弱點的軟體區域。 **附註**：在某些情形下，刪除安全風險可能會導致應用程式無法運作。在您刪除安全風險項目以釋放磁碟空間之前，確定您不需要利用它以執行任何應用式。 請參閱第 72 頁的「清除備份項目」。
修復項目	已被清除或修復的項目，以及原始位置已經無法使用的項目，例如網路磁碟機。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。

表 2-1 檢視類別

選項	說明
授權 僅適用於安全資訊授權；如果使用網站授權，則項目不會出現在功能表中。	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 2-2 掃描類別

選項	說明
掃描磁片	掃描磁片及其它可移式媒體。
自訂掃描	隨時執行檔案、資料夾、磁碟機或整個電腦的手動掃描。 請參閱第 46 頁的「起始手動掃描」。
快速掃描	對電腦上的系統記憶體，以及所有的常見病毒和安全風險位置執行非常快速的掃描。
完整掃描	對您的系統，包括開機磁區和系統記憶體執行完整掃描。掃描網路磁碟機時可能會需要輸入密碼。

架構類別

您可以使用「架構」類別來設定「自動防護」，以監視您的檔案和電子郵件附件 (針對支援的電子郵件用戶端)，並設定「竄改防護」以保護賽門鐵克應用程式不被竄改。

表 2-3 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，它都會檢查該檔案以確認是否受到病毒或安全風險的感染。 「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 38 頁的「使用自動防護」。

表 2-3 架構類別

選項	說明
Internet 電子郵件自動防護 「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 AntiVirus 包含額外的電子郵件防護。對於 Internet 電子郵件，Symantec AntiVirus 會防護使用 POP3 或 SMTP 通訊協定的進出電子郵件訊息。
竄改防護	「竄改防護」會保護賽門鐵克應用程式不受未經授權的來源竄改。

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和安全風險等資訊。

表 2-4 記錄類別

選項	說明
威脅記錄	檢視下列項目的清單： ■ 您的電腦所感染的病毒以及其它與感染情況相關的資訊。 ■ Symantec AntiVirus 會偵測並記錄的安全風險，如廣告軟體和間諜軟體，或將它隔離和修復，或者從您的電腦上刪除。安全風險的「威脅記錄」包含一個提供額外資訊的 Symantec Security Response (賽門鐵克安全機制應變中心) 網頁連結。
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，與病毒和安全風險相關的活動日誌，包括架構變更、錯誤，和定義檔資訊。
竄改記錄	檢視嘗試竄改您電腦上賽門鐵克應用程式，但已被「竄改防護」所阻檔的清單。

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 2-5 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 50 頁的「建立開機掃描」。
自動產生的快速掃描	每當使用者登入電腦時，此掃描便會檢查電腦記憶體中的檔案，及電腦上其它常見的感染點，看看是否受到病毒及安全風險感染。除了您無法停止掃描記憶體中的檔案，或電腦上其它常見感染點，您可以使用與架構手動掃描一樣的方式架構此掃描。 **附註**：此掃描類型只能用於未受管理的用戶端上。

使用者定義的掃描類別

您可以使用「使用者定義的掃描」類別，建立您可以手動執行的預先架構掃描。

表 2-6 使用者定義的掃描類別

選項	說明
新的使用者定義掃描	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掃描。不論何時，您都可以快速地確認所指定的檔案與資料夾並未受到病毒及安全風險的感染。 請參閱第 51 頁的「建立使用者定義的掃描」。

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 2-7 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受到病毒和安全風險的感染。 請參閱第 48 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，以阻擋病毒和安全風險。它會在程式執行時檢查病毒和安全風險，並且監視您電腦上任何可能表示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」會出現警示。

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「檔案系統自動防護」

Symantec AntiVirus 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 AntiVirus 圖示會顯示為一個完整的盾牌。當您以滑鼠右鍵按下圖示時，若「檔案系統自動防護」被啟動，會在「啟動自動防護」旁邊出現一個勾號。

停用「檔案系統自動防護」時，Symantec AntiVirus 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）所覆蓋。

從工作列啟動和停用「檔案系統自動防護」

- 在 Windows 桌面上的系統匣中，以滑鼠右鍵按下 Symantec AntiVirus 圖示，然後再按下「啟動自動防護」。

從 Symantec AntiVirus 啟動和停用「檔案系統自動防護」

1. 在 Symantec AntiVirus 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. 勾選或取消勾選「啟動自動防護」。
4. 按下「確定」。
   目前的「檔案系統自動防護」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。您的網路管理員可以決定您是否可以暫停管理員排定的掃描。

對於您的網路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，表示您的網路管理員已停用「暫停」功能。

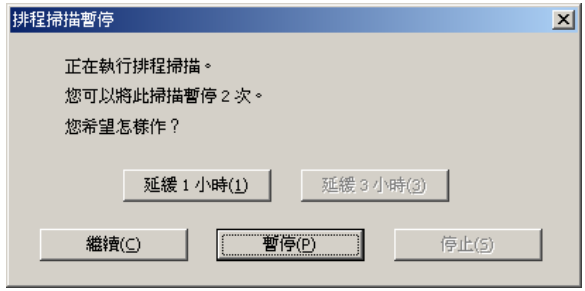
附註：當您選擇暫停掃描時，如果 Symantec AntiVirus 正在掃描壓縮檔，則可能需要幾分鐘後才會回應。

暫停掃描

1 執行掃描時，請在「掃描」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。



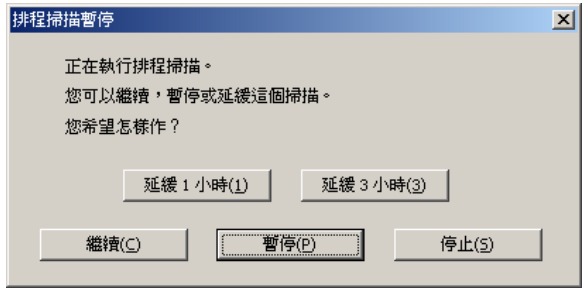
2 在「排程掃描暫停」對話方塊中，按下「暫停」。
管理員排定的掃描會停在目前的階段，而「掃描」對話方塊也會一直開著，直到您重新啟動掃描為止。

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。

更新病毒和安全風險防護定義檔

Symantec AntiVirus 必須依賴最新的資訊才能偵測、清除，及修復病毒和安全風險所造成的影響。而發生病毒或安全風險問題的最常見原因之一，就是在完成安裝之後，並未更新定義檔。定義檔內含有關最新搜索到之病毒和安全風險所需的偵測和修復資訊。

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 AntiVirus 會自動連線到特定的賽門鐵克網站，並判斷病毒和安全風險定義檔是否需要更新。如果需要，它會下載適當的檔案，並將其安裝到適當位置。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和安全風險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 AntiVirus 便會自動執行 LiveUpdate。

使用 LiveUpdate 排程更新

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。

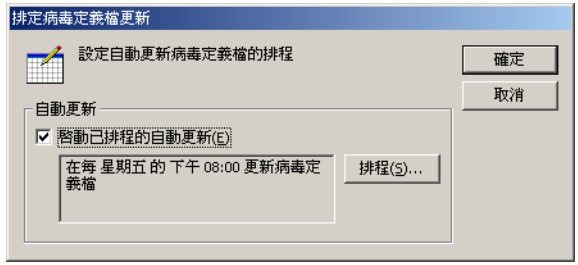
使用 LiveUpdate 排程更新

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，您的管理員可能會負責散佈更新的病毒和安全風險定義檔給各工作站。此時，您不須執行任何動作。

啟動排程 LiveUpdate

1 在 Symantec AntiVirus 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」。

附註：此項更新包括病毒和安全風險定義檔兩者。

3 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」，直到返回 Symantec AntiVirus 主視窗。

設定進階 LiveUpdate 排程選項

1 在「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，按下「排程」。

3 在「病毒定義檔更新排程」對話方塊中按下「進階」。

4 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 AntiVirus 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 **x** 天內處理遺漏執行的事件」，並設定天數。
- 若要設定 Symantec AntiVirus 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，選取所要使用的隨機方法類型，並設定分鐘、星期幾的間隔或日期。

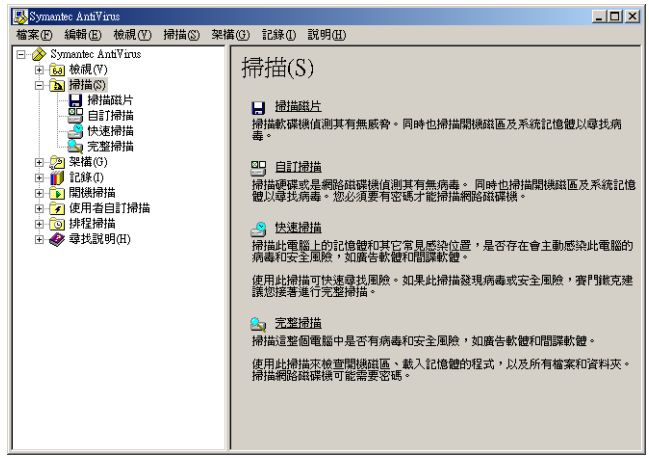
5 按下「確定」，直到返回 Symantec AntiVirus 主視窗。

利用 LiveUpdate 立即更新防護

報告有新的病毒出現時，切勿等到下一次排程更新，您應該立即更新病毒和安全風險防護。

利用 LiveUpdate 立即更新病毒防護

1 在 Symantec AntiVirus 的左窗格中，按下 **Symantec AntiVirus**。



2 在右窗格中，按下 **LiveUpdate**。

3 必要時，在 LiveUpdate 對話方塊中按下「選項」>「設定」，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 33 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 AntiVirus，然後在適當的資料夾內自動安裝新的病毒和安全風險定義檔。
4. 掃描您的電腦，以偵測新種病毒和安全風險。

使用 Symantec AntiVirus 和 Windows 資訊安全中心

如果您要使用 Windows XP Service Pack 2 上執行的 Windows 資訊安全中心 (WSC) 監控安全狀態，則您可以在 WSC 中查看 Symantec AntiVirus 的狀態。

表 2-8 顯示 WSC 中報告的防護狀態。

表 2-8 WSC 防護狀態報告

賽門鐵克產品狀況	防護狀態
未安裝 Symantec Antivirus	找不到 (紅色)
已安裝 Symantec Antivirus，並進行全面防護	啟動 (綠色)
已安裝 Symantec AntiVirus，而且病毒及安全風險定義檔已經過期	過期 (紅色)
已安裝 Symantec AntiVirus，而未啟動「檔案系統自動防護」。	關閉 (紅色)
已安裝 Symantec AntiVirus、未啟動「檔案系統自動防護」，而且病毒及安全風險定義檔已經過期	關閉 (紅色)
已安裝 Symantec Antivirus，但 Rtvscan 已被手動關閉	關閉 (紅色)

如需詳細資訊

如果您需要關於 Symantec AntiVirus 的詳細資訊，請參閱線上「說明」。此外，您也可以從賽門鐵克的網站取得病毒和安全風險的相關資訊。

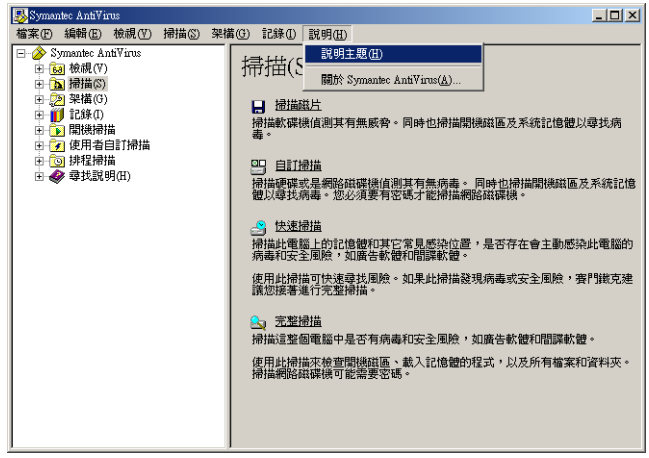
存取線上說明

Symantec AntiVirus 線上說明系統擁有一般資訊與逐步程序，可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。

取得使用 Symantec AntiVirus 的說明

- 在 Symantec AntiVirus 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
- 關於安全風險的一般和詳細資訊

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 3

防止您的電腦受到病毒與安全風險的入侵

本章包含下列主題：

關於防毒與安全風險政策

Symantec AntiVirus 預先設定的防毒與安全風險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、開機和使用者定義掃描的政策設定。

防毒與安全風險政策可決定：

- 要掃描的內容
- 偵測到病毒或安全風險時要執行什麼動作

要掃描的內容

Symantec AntiVirus 「自動防護」預設會掃描所有檔案類型。手動、排程、開機及使用者定義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 40 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，不過病毒與安全風險防護能力會降低。

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 AntiVirus 可依檔案類型，或依副檔名來掃描電腦。依照檔案類型掃描可讓 Symantec AntiVirus 決定該檔案的類型，而不管其副檔名。由於病毒只會感染某些類型的檔案，因此這是一個有效的掃描方式，可確保掃描所有可能容易感染病毒的檔案。

依照檔案類型掃描可讓 Symantec AntiVirus 掃描被惡意病毒重新命名的檔案。但是，這個選項的速度比依照附檔名掃描來得慢。

您可以從以下類型的檔案中選擇：

- 文件檔：包括 Microsoft Word 與 Excel 文件，以及與這些文件相關的範本檔。Symantec AntiVirus 會掃描文件檔是否受到巨集病毒感染。
- 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。Symantec AntiVirus 會搜尋程式檔是否受到檔案病毒感染。

依照檔案類型或副檔名掃描

Symantec AntiVirus 可依檔案類型，或依副檔名來掃描電腦。

選取要掃描的檔案類型

1. 在 Symantec AntiVirus 的左窗格中，選取要變更的掃描。
   - 若您從「掃描」類別中選取一個掃描，按下「選項」。
   - 如果您選取開機、使用者定義或排程掃描，按下您所要的特定掃描，按下「編輯」，再按下「選項」。
     這些變更只會套用到您所選取的特定掃描。
2. 按下「選取的檔案類型」，然後按下「類型」。

3 選取下列一種或兩種檔案類型：

- 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 若要在所有後續掃描使用這些動作，按下「儲存設定」。

5 按下「確定」。

在掃描清單中新增副檔名

1 在 Symantec AntiVirus 的左窗格中，選取要變更的掃描。

- 若您從「掃描」類別中選取一個，按下「選項」。
- 如果您選取開機、使用者定義或排程掃描，按下要變更的掃描名稱，按下「編輯」，再按下「選項」。
  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「選取的副檔名」，然後按下「副檔名」。

3 輸入要新增的副檔名，然後按下「新增」。

4 若有需要，重複步驟 3。

5 按下「確定」。

關於掃描所有檔案類型

Symantec AntiVirus 可以掃描您電腦中的所有檔案 (無論副檔名或檔案類型為何)。掃描所有檔案類型可確保掃描最為徹底，因為這個選項可讓 Symantec AntiVirus 在可能未被搜尋到的檔案中偵測病毒與安全風險。掃描所有檔案類型比依選取的檔案類型或副檔名掃描費時，但也比較徹底。

如果您必須在短時間內完成掃描，應該將「自動防護」掃描或閒置掃描 (可使用時) 設定為依副檔名掃描，然後將排程掃描架構為至少每週一次，以徹底檢查您的電腦。

關於防止巨集病毒感染

Symantec AntiVirus 掃描程式會自動偵測並移除大部分 Microsoft Word 與 Excel 巨集病毒。定期執行排程掃描、開機掃描或「自動防護」，您就可以保護電腦不受巨集病毒感染。Symantec AntiVirus 會定期搜尋並清除偵測到的任何巨集病毒。

若要使防止巨集感染最佳化，請執行下列步驟：

- 啟動「自動防護」。「自動防護」會不斷掃描已存取 (例如執行或開啟檔案) 或修改 (例如重新命名檔案、修改檔案、建立檔案、複製檔案或將檔案移動到某個位置) 的檔案。

- 可以的話，為您的電子郵件執行「自動防護」。
- 將所有掃描選項設定為依照「所有類型」掃描。
- 停用自動巨集以保護您的通用範本檔。

偵測到病毒或安全風險時要執行什麼動作

Symantec AntiVirus 會以第一與第二個動作來處理受病毒或安全風險感染的檔案。根據預設，當「自動防護」或掃描作業偵測到病毒時，Symantec AntiVirus 會嘗試清除受感染檔案的病毒。如果 Symantec AntiVirus 無法清除檔案裡的病毒，便會進行第二個動作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。

根據預設，當「自動防護」或掃描期間偵測到安全風險時，Symantec AntiVirus 會隔離受感染的檔案，並嘗試移除或修復該安全風險對電腦進行的變更。隔離安全風險可確保該安全風險不再作用於電腦上，並確保必要時，Symantec AntiVirus 可以回復變更。如果 Symantec AntiVirus 無法完成此動作，第二個動作便是將威脅記錄下來並略過。

您可以變更每個掃描類型的這些設定，並針對每個安全風險類別和個別安全風險，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。為避免電腦處在不穩定的狀態下，Symantec AntiVirus 會等應用程式安裝完後，再隔離該風險。然後移除或修復風險造成的影響。

使用自動防護

「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 檔的副檔名變更為不同於 SmartScan 原本設定掃描的副檔名，SmartScan 還是會掃描該檔案。

關於自動防護與安全風險

根據預設，「自動防護」會掃描如廣告軟體與間諜軟體等安全風險，隔離受感染的檔案，並移除或修復安全風險所造成的副作用。您可以停用 「自動防護」中的安全風險掃描。

請參閱第 41 頁的「停用與啟用自動防護中的安全風險掃描」。

關於自動防護與電子郵件掃描

若要彌補「自動防護」的不足，Symantec AntiVirus 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.x
- Microsoft Outlook 98/2000/2002/2003 (MAPI 與 Internet)
- Microsoft Exchange Client 5.0 和 5.5

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。

Symantec AntiVirus 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 AntiVirus 使用 「Bloodhound™ 病毒偵測」，在內送訊息中掃描威脅與安全風險，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。

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，Symantec AntiVirus 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 AntiVirus 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 26 頁的「啟動與停用自動防護」。

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

如果使用 SSL 連線，停用電子郵件掃描

若您的 Internet 服務供應商使用 SSL 通訊協定，啟用 Symantec AntiVirus 電子郵件掃描時，傳送電子郵件訊息可能會發生問題。在此情況下，可能需要停用 Symantec AntiVirus 電子郵件掃描。

即使在停用 Internet 電子郵件用戶端掃描後，「檔案系統自動防護」會繼續保護電腦，避免遭受附件中的病毒與安全風險入侵。當您將附件儲存至硬碟時，「檔案系統自動防護」會掃描該電子郵件附件。

停用電子郵件掃描程式後，請確定有啟用 「自動防護」，並定時執行 LiveUpdate，以確保 「自動防護」處於最佳設定。「自動防護」可針對任何來源 (包括 Internet) 提供即時的病毒防護，並在存取電子郵件附件時自動掃描該附件。

停用電子郵件掃描

1. 在 Symantec AntiVirus 的左窗格中，按下 「**架構**」。
2. 在右窗格中，按下 「**< 電子郵件 > 自動防護**」。
3. 取消勾選 「**啟動 < 電子郵件 > 自動防護**」。
4. 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、最後一次掃描的檔案，以及病毒感染與安全風險資訊。

檢視自動防護掃描統計

- 在 Symantec AntiVirus 的 「檢視」功能表上，按下 「**自動防護掃描統計**」。

修改自動防護與使用 SmartScan

「自動防護」預設為掃描所有檔案。掃描所有檔案與使用 SmartScan 可提供最大的病毒與安全風險防護效果。在預設的情形下，會啟用 SmartScan。

Symantec AntiVirus 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

病毒掃描動作，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病毒感染。

修改「自動防護」與使用 SmartScan

1. 在 Symantec AntiVirus 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**」，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。
   - 確保已勾選 SmartScan，以便使用此功能掃描。
4. 按下「**確定**」以儲存您的設定。

停用與啟用自動防護中的安全風險掃描

根據預設，「自動防護」會掃描如廣告軟體與間諜軟體等安全風險，隔離受感染的檔案，並嘗試移除或修復安全風險所造成的影響。但有時候，您可能必須暫時停用「檔案系統自動防護」中的安全風險掃描，然後再重新啟用。

附註：您的管理員可能會鎖定此設定。

停用與啟用自動防護中的安全風險掃描

1. 在 Symantec AntiVirus 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「選項」下，勾選或取消勾選「**掃描安全風險**」。
4. 按下「**確定**」。

使用竄改防護

「竄改防護」可防止賽門鐵克應用程式被病蟲、特洛伊木馬程式、病毒與安全風險所竄改。

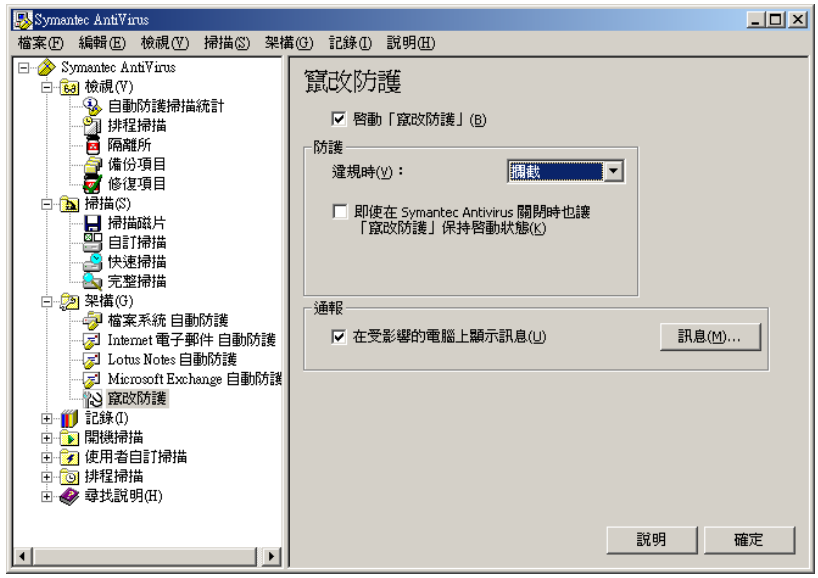
啟用、停用與架構竄改防護

啟用「竄改防護」時，您可以架構 Symantec AntiVirus，攔截或記錄修改賽門鐵克應用程式的次數。您也可架構一個在 Symantec AntiVirus 偵測到竄改動作時顯示的訊息。

附註：若您的電腦由管理員所管理，且「竄改防護」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。

啟用、停用和架構竄改防護

1 在 Symantec AntiVirus 的左窗格中，按下「竄改防護」。



2 在右窗格中，勾選或取消勾選「啟動竄改防護」。

3 若啟用「竄改防護」，請在「防護」下拉式清單中，執行下列任一項：

- 若要攔截未授權的活動，按下「攔截」。
- 若要記錄未授權的活動，但仍允許活動執行，按下「只記錄」。

4 勾選或取消勾選「即使在 **Symantec AntiVirus** 關閉時也讓「竄改防護」保持啟動狀態」。

5 在「通報」下，勾選或取消勾選「在受感染的電腦上顯示訊息」。

6 按下「確定」。

建立竄改防護訊息

「竄改防護」可讓您建立訊息，以便在「竄改防護」偵測到對賽門鐵克程序的攻擊時顯示。您建立的訊息中可包含自行輸入的文字與您選取的欄位。您所選取的欄位是變數，可填入識別為攻擊特性的值。

表 3-1 說明您可以選取的欄位。

表 3-1　　竄改防護訊息欄位名稱與說明

欄位	說明
檔名	對受防護的程序進行攻擊的檔名。
路徑與檔名	對受防護的程序進行攻擊的檔案完整路徑與名稱。
位置	防止被竄改的電腦硬體或軟體區域。若是「竄改防護」訊息，這是賽門鐵克應用程式。
電腦	被攻擊的電腦名稱。
使用者	發生攻擊時登入的使用者名稱。
發現日期	攻擊發生的日期。
因應措施	「竄改防護」對攻擊執行的動作。
系統事件	發生的竄改類型。
項目類型	程序攻擊的目標類型。
參與者程序 ID	攻擊賽門鐵克應用程式的程序 ID 號碼。
參與者程序名稱	攻擊賽門鐵克應用程式的程序名稱。
目標路徑名稱	程序攻擊的目標位置。
目標程序 ID	程序攻擊的目標程序 ID。
目標終端機階段作業 ID	事件發生時的終端機階段作業 ID。

使用下列格式建立訊息：

```
Text that you type: [Field Name 1] [Field Name 2] (Optional and
additional text that you type [Field Name x])
```

以下範例訊息表示哪種程序嘗試採取何種動作，以及採取動作的時間：

日期：[發現日期]

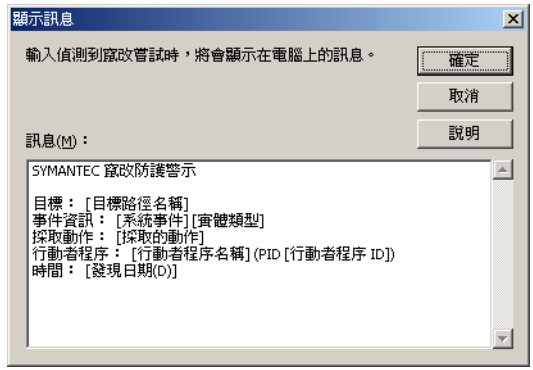
程序位置：[路徑及檔名] (名稱：[參與者程序名稱])

攻擊：[目標路徑名稱] [目標程序 ID]

建立竄改防護訊息

1　在 Symantec AntiVirus 的左窗格中，按下「竄改防護」。

2 在右窗格的「通報」下，確定勾選「在受影響的電腦上顯示訊息」，然後按下「訊息」。



3 在「訊息」方塊中按一下，以插入游標。

4 使用鍵盤移動游標、新增列、輸入與刪除文字。

5 將游標移至您想插入欄位的位置，按下滑鼠右鍵，按下「插入欄位」，然後選取要插入的欄位。
請參閱第 43 頁的「竄改防護訊息欄位名稱與說明」。

6 必要時，重複步驟 4 與 5。

7 在欄位上按下滑鼠右鍵，然後選取「剪下」、「複製」、「貼上」、「清除」或「復原」。

8 按下「確定」。

掃描病毒與安全風險

除了「自動防護」這種功能最強大的防毒與安全風險機制外，Symantec AntiVirus 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。可用的掃描類型包括：

- 自訂掃描：隨時掃描檔案、資料夾、磁碟機或整個電腦。您可以選取電腦中要掃描的部份。
- 快速掃描：快速掃描常被病毒與安全風險所攻擊的系統記憶體與位置。
- 完整掃描：掃描整部電腦，包括開機磁區與系統記憶體。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：每當開啟電腦及載入 Windows 時即執行。
- 使用者定義的掃描：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日的快速掃描，與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，可以考慮增加開機時完整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。

Symantec AntiVirus 如何偵測病毒與安全風險

Symantec AntiVirus 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。Symantec AntiVirus「搜尋引擎」會利用定義檔中發現的病毒與安全風險特徵進行徹底掃描，尋找執行檔中的已知病毒。Symantec AntiVirus 會在文件檔的可執行部份，搜尋是否有巨集病毒。

您可以在等待時進行掃描，或是安排在您離開電腦時掃描。

掃描期間所發生的事

在掃描的過程中，Symantec AntiVirus 會在電腦的記憶體、開機磁區與您選取的磁碟機中，掃描可辨識感染或存在風險的病毒與安全風險特徵。

電腦記憶體

Symantec AntiVirus 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中。目前仍沒有適當的方法可以清除病毒進入記憶體的途徑。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

Symantec AntiVirus 會在電腦的開機磁區中檢查是否有開機病毒。將對兩個項目進行檢查：分割區表與主要開機紀錄。

軟碟機

常見的病毒散佈方式是透過電腦開關時，仍留在軟碟機中的磁片。啟動掃描時，如果磁碟機中仍有磁片，Symantec AntiVirus 會搜尋軟碟機的開機磁區與分割表。當您關機時，如果將磁片留在磁碟機中，畫面會出現提示，請您取出磁片，以避免可能的感染。

選取的檔案

Symantec AntiVirus 會掃描個別的檔案。針對大部分的掃描類型，您可以選取要掃描的檔案。Symantec AntiVirus 會使用型樣掃描，在檔案中搜尋稱為「型樣」或「特徵」的病毒蹤跡。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，Symantec AntiVirus 會根據預設，嘗試

從檔案清除病毒。如果無法清除檔案，Symantec AntiVirus 會隔離該檔案，防止電腦進一步受到感染。

Symantec AntiVirus 亦會使用型樣掃描，在檔案與登錄機碼中搜尋安全風險的特徵。如果發現安全風險，Symantec AntiVirus 預設會隔離受感染的檔案，並修復該風險造成的影響。若無法完成此動作，便記錄此動作。

掃描結束後會列出結果。

關於定義檔

病毒檔包括程式碼位元，若被破解，就會顯示某種型樣 (也稱為特徵)。這些病毒型樣可在受感染的檔案中追蹤到。而廣告軟體或間諜軟體等安全風險，亦擁有可辨識的型樣或特徵。

定義檔包含已知病毒型樣或特徵及已知安全風險特徵之清單，但不包括有害的病毒程式碼。掃描程式會搜尋電腦檔案中，是否有定義檔發現的已知型樣。如果發現符合的病毒型樣，表示該檔案已受到感染。Symantec AntiVirus 可以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，Symantec AntiVirus 會使用定義檔隔離它，並修復其副作用。

由於幾乎每天都會出現新的病毒與安全風險，因此必須定期更新定義檔，確保 Symantec AntiVirus 可偵測與清除最近的病毒與安全風險。

關於掃描壓縮檔與編碼的檔案

Symantec AntiVirus 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。手動掃描包括「快速掃描」與「完整掃描」。

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 AntiVirus 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**」。

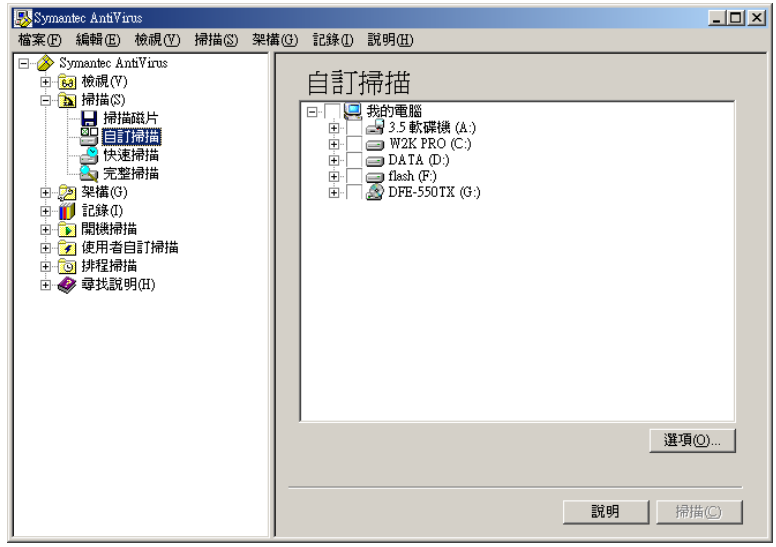
附註：此項功能無法在 64 位元作業系統上使用。

在 Symantec AntiVirus 中起始手動掃描

1 在 Symantec AntiVirus 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。
- 自訂掃描
- 快速掃描
- 完整掃描



3 若您在右窗格中選取「掃描磁片」或「自訂掃描」，請執行下列動作：

- 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 針對所有的手動掃描，按下「**選項**」來變更掃描內容與偵測到病毒或安全風險時如何因應的預設值。
預設設定如下所示：

- 預設設定為掃描所有檔案。
- 若是病毒，動作的預設設定為清除受感染檔案的病毒、修復其影響，以及在病毒無法移除時隔離受感染的檔案。
- 若是安全風險，動作的預設設定為隔離安全風險、修復其副作用，以及在無法隔離及修復時記錄風險。

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「**進階**」，架構排程掃描期間出現的掃描進度對話方塊。

6 在「掃描進階選項」對話方塊的「對話方塊」選項下拉式清單中，按下「**顯示掃描進度**」，然後按下「**確定**」。

7 在「掃描選項」對話方塊中，按下「**確定**」。

8 在 Symantec AntiVirus 主視窗中，按下「**掃描**」。
Symantec AntiVirus 就會開始掃描並報告結果。

架構掃描

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間諜軟體等安全風險存在。

附註：如果您的網路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 AntiVirus 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 選取下列其中一種掃描類型進行排程：

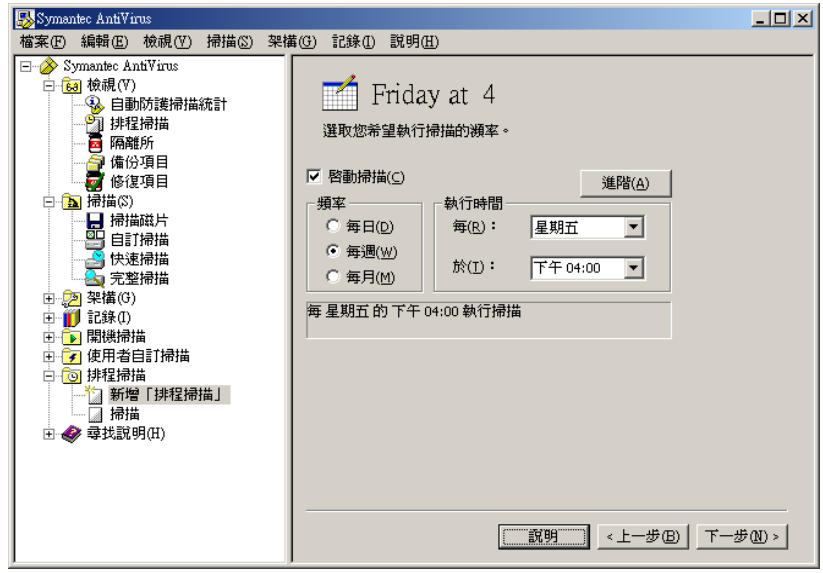
- 快速掃描
- 完整掃描
- 自訂掃描

4 按「下一步」。

5 輸入掃描的名稱和說明。
例如，將掃描作業稱為 Friday at 4。

6 按「下一步」。

7 指定掃描頻率與時間，再按「下一步」。



8 若選取「自訂掃描」，請在右窗格中勾選適當的勾選框，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 46 頁的「起始手動掃描」。

9 按下「選項」，將已掃描的項目與偵測到病毒或安全風險時的處理方式變更為預設值。
預設設定如下所示：

- 預設設定為掃描所有檔案。
- 若是病毒，動作的預設設定為清除受感染檔案的病毒、修復其影響，以及在病毒無法移除時隔離受感染的檔案。

- 若是安全風險，動作的預設設定為隔離安全風險、移除或修復其副作用，或者在無法隔離及修復時記錄風險。

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**」。

10 按下「**進階**」，架構排程掃描期間出現的掃描進度對話方塊。

11 在「掃描進階選項」對話方塊的下拉式清單中，按下「**顯示掃描進度**」，然後按下「**確定**」。

12 在「掃描選項」對話方塊中，按下「**確定**」。

13 在 Symantec AntiVirus 主視窗中，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 AntiVirus 服務」。根據預設，「Symantec AntiVirus 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。

關於建立多重排程掃描

如果您安排多個掃描同時在同一台電腦上進行，可能會降低電腦 CPU 的使用率，或導致其中一個或多個排程掃描無法開始。例如，如果您安排下午一點在電腦上開始分別進行三個掃描，其中一個掃描 C 磁碟機，一個掃描 D 磁碟機，另一個則掃描 E 磁碟機，其中一個或多個掃描可能無法啟動。在這個範例中，比較好的解決方案是建立一個掃描 C、D 及 E 磁碟機的排程掃描。

建立開機掃描

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。

Symantec AntiVirus 亦提供一個稱作「自動產生的快速掃描」的開機掃描，僅供未受管理的用戶端使用。每當使用者登入電腦時，此掃描便會檢查電腦記憶體中的檔案，及電腦上其它常見的感染點，看看是否受到病毒及安全風險感染。除了您無法停止掃描記憶體中的檔案，或電腦上其它常見感染點，您可以使用與架構手動掃描一樣的方式架構此掃描。

建立開機掃描

1 在 Symantec AntiVirus 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 選取下列其中一種掃描類型進行排程：
- 快速掃描
- 完整掃描
- 自訂掃描

4 按「下一步」。

5 輸入掃描的名稱和說明。

6 按「下一步」。

7 若選取「自訂掃描」，請在右窗格中勾選適當的勾選框，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 46 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或安全風險時的處理方式變更為預設值。
預設設定如下所示：
- 預設設定為掃描所有檔案。
- 若是病毒，動作的預設設定為清除受感染檔案的病毒、修復其影響，以及在病毒無法移除時隔離受感染的檔案。
- 若是安全風險，動作的預設設定為隔離安全風險、移除或修復其副作用，以及在無法隔離及修復時記錄風險。

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「進階」，架構開機掃描期間出現的掃描進度對話方塊。

10 在「掃描進階選項」對話方塊的下拉式清單中，按下「顯示掃描進度」，然後按下「確定」。

11 在「掃描選項」對話方塊中，按下「確定」。

12 在 Symantec AntiVirus 主視窗中，按下「儲存」。
掃描作業會在您開啟電腦及載入 Windows 時即執行。

建立使用者定義的掃描

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使用者定義的掃描。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。

建立使用者定義的掃描

您可以建立使用者定義的掃描，並隨時手動執行。

建立使用者定義的掃描

1 在 Symantec AntiVirus 左窗格中，按下「使用者自訂的掃描」。

2 在右窗格中，按下「新增使用者自訂的掃描」。

3 選取下列其中一種掃描類型進行排程：

- 快速掃描
- 完整掃描
- 自訂掃描

4 按「下一步」。

5 輸入掃描的名稱和說明。

6 按「下一步」。

7 若選取「自訂掃描」，請在右窗格中勾選適當的勾選框，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 46 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或安全風險時的處理方式變更為預設值。
預設設定如下所示：

- 預設設定為掃描所有檔案。
- 若是病毒，動作的預設設定為清除受感染檔案的病毒、移除或修復其影響，以及在病毒無法移除時隔離受感染的檔案。
- 若是安全風險，動作的預設設定為隔離安全風險、移除或修復其副作用，以及在無法隔離及修復時記錄風險。

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「進階」，架構排程掃描期間出現的掃描進度對話方塊。

10 在「掃描進階選項」對話方塊的下拉式清單中，按下「顯示掃描進度」，然後按下「確定」。

11 在「掃描選項」對話方塊中，按下「確定」。

12 在 Symantec AntiVirus 主視窗中，按下「儲存」。

執行使用者定義的掃描

1 在 Symantec AntiVirus 左窗格中，展開「使用者自訂的掃描」。

2 在已存檔的使用者定義掃描上連按兩下。

編輯與刪除開機、使用者定義與排程掃描

您可以隨時架構現有的掃描。必要時，也可刪除掃描。

編輯與刪除掃描

您可以編輯與刪除現有的開機、使用者定義與排程掃描。若某些選項無法針對特定的掃描類型架構，會呈現灰色。

編輯掃描

1. 在 Symantec AntiVirus 左窗格中，選取要編輯的掃描。
2. 按下「編輯」。
3. 請執行下列任一項：
   - 若為使用者定義的掃描，在「檔案」標籤上，選取要掃描的檔案、資料夾或磁碟機。
   - 若為排程掃描，則在「排程」標籤上，選取新的掃描頻率與掃描日期和時間。
   - 在「名稱 / 說明」標籤上，編輯該掃描的名稱與說明。
4. 必要時，按下「選項」，以變更下列掃描選項：
   - 檔案類型：根據副檔名或檔案類型掃描
   - 掃描增強功能：掃描載入記憶體的程式檔案，掃描常見感染位置，在掃描選取的檔案與資料夾前，先掃描知名病毒與安全風險的蹤跡
   - 檔案與資料夾排除
   - 進階掃描選項壓縮檔，儲存裝置移轉等等。
   - 發現病毒或安全風險時所執行的動作
   - 調節選項
   - 通知：「偵測選項」可在發現病毒或安全風險時，讓您建構一個訊息。「矯正選項」可讓您架構在矯正動作 (如停止服務) 執行前，是否要通知您。
5. 按下「確定」，直到返回 Symantec AntiVirus 主視窗。

刪除掃描

- 在 Symantec AntiVirus 左窗格中，以滑鼠右鍵按下要刪除的掃描，然後按下「刪除」。

架構病毒與安全風險的動作

對掃描病毒與安全風險均很重要的一個部份，就是架構 Symantec AntiVirus 偵測到病毒或安全風險時，所要採取的動作。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。

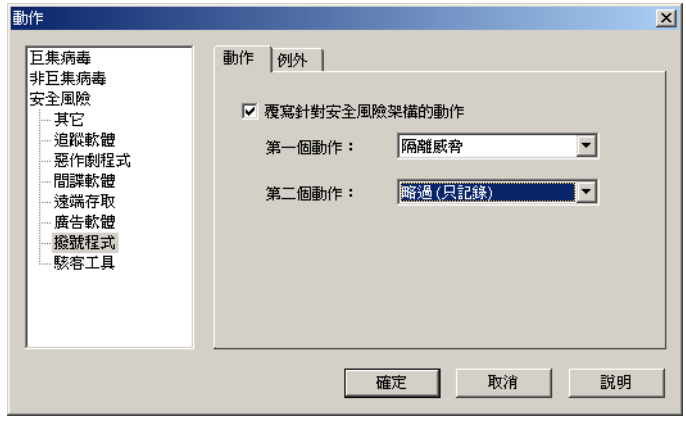
這個程序使用「完整掃描」作為架構範例，但在您架構其它掃描時，可用相同方式架構病毒、安全風險項目與類別的動作。

架構病毒與安全風險的動作

1 在左窗格中，展開「**掃描**」，然後按下「**完整掃描**」。

2 在右窗格中，按下「**選項**」。

3 在「掃描選項」視窗中，按下「**動作**」。



4 在「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。
根據預設，每個安全風險子類別 (如間諜軟體) 會被自動架構為使用整個安全風險類別最上層所設定的動作。
若要架構類別或類別中的特定複本使用不同的動作，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。

5 從以下選項中選取第一與第二個動作：

清除威脅

移除受感染檔案中的病毒。此為針對病毒的第一個預設動作。

附註：此動作無法用於安全風險。

針對病毒的第一個動作應永遠為「清除」。如果 Symantec AntiVirus 成功地從檔案中清除病毒，您將不需要採取任何其它的動作。您的電腦將免於病毒的困擾，而且病毒不再容易被散播到您電腦的其它區域。

當 Symantec AntiVirus 清除檔案時，它會從受感染的檔案、開機磁區或分割表中移除病毒，並排除病毒散播的能力。Symantec AntiVirus 通常可以在病毒對您的電腦造成破壞之前，找出並清除它。

但在某些情況下，根據病毒已經造成的破壞程度，清除的檔案可能無法再使用。這是病毒感染的結果，而非清除動作的結果。

某些受感染的檔案無法被清除。

隔離威脅

執行下列其中一個動作：

- 若是病毒，將受感染的檔案從其原始位置移到「隔離所」。在「隔離所」中的受感染檔案將無法散佈病毒。此為針對病毒的第二個預設動作。
- 若是安全風險，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。此為針對安全風險的第一個預設動作。
  「隔離所」包含了所有執行動作的記錄，若有需要，您可將電腦回復至 Symantec AntiVirus 移除風險之前的狀態。

刪除威脅

從電腦硬碟上刪除受感染的檔案。如果 Symantec AntiVirus 無法刪除檔案，Symantec AntiVirus 所採取動作的額外資訊會出現在「通報」對話方塊和「事件日誌」中。

因為檔案會被永久刪除，且無法從「資源回收筒」中復原，所以只有當您使用沒有病毒或安全風險的備份檔，來取代受感染的檔案時，才能使用這個動作。

附註：當您架構安全風險的動作時，請小心使用此動作，因為在某些情況下，刪除安全風險可能會造成應用程式喪失功能。

略過
(只記錄)

執行下列其中一個動作：

- 若是病毒，略過受感染的檔案，保持原樣。病毒依然在檔案中，可能會將病毒傳播到您電腦的其它部分。「威脅記錄」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)」作為巨集與非巨集病毒的第二個動作。
  當您進行大規模、自動化的掃描 (如排程掃描) 時，除非您計劃在稍後檢視掃描結果，並採取其它動作，例如將檔案移動至「隔離所」，否則請勿選取這個動作。
- 若是安全風險，會略過受感染檔案，並在「威脅記錄」中置入一個項目，保留威脅記錄。請使用此選項來手動控制 Symantec AntiVirus 處理安全風險的方法。此為針對安全風險的第二個預設動作。

您的系統管理員可能會傳送一個自訂的訊息，說明應變的方式。

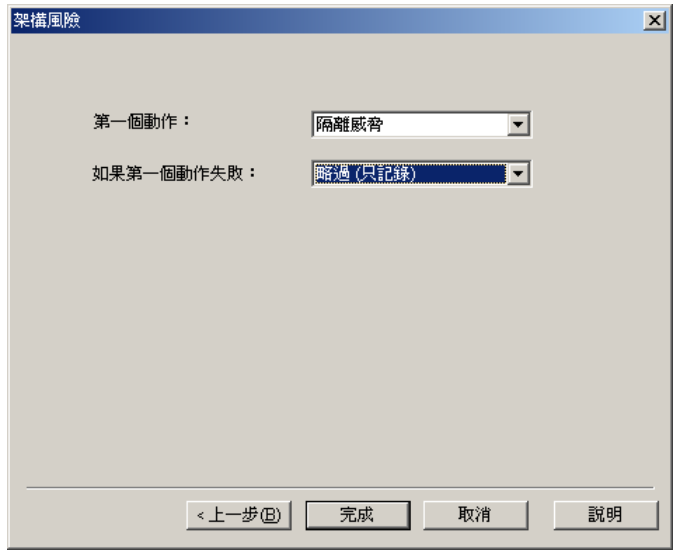
請參閱第 57 頁的「指派病毒第二個動作的秘訣」。
請參閱第 58 頁的「指派安全風險第二個動作的秘訣」。

6 您可以針對您想要設定特定動作的每個類別，重複步驟 4 與 5。

7 若您在樹狀結構中選取一個安全風險類別，您可以按下「例外」標籤，替該安全風險類別的一個或多個特定複本架構自訂動作。

8 按下「新增」。

9 在「選取風險」對話方塊的清單中，選取您要架構自訂動作的特定風險，然後按「下一步」。



10 在「架構風險」對話方塊中，選取在 Symantec AntiVirus 偵測到選取的風險時，所要採取的第一與第二個動作，然後按下「完成」。

11 您可以針對您想要設定特定動作的每個安全風險，重複步驟 8 到 10。

12 按下「確定」，直到返回 Symantec AntiVirus 主視窗。

指派病毒第二個動作的秘訣

當您選取病毒的第二個動作時，請考慮以下事項：

- 您在檔案上所需要的控制等級
  如果您將重要的檔案儲存在電腦上時並未備份，您就不應該使用像「刪除威脅」這樣的動作。雖然您可能可以用這種方式刪除病毒，但您也可能遺失重要的資料。
  另一個考量則是您的系統檔案。由於某些系統檔案有執行檔的副檔名，因此它們可能會被病毒攻擊。雖然有些不方便，但使用「略過 (只記錄)」或「隔離威脅」動作是一個好主意，因為您可以藉此檢查已經受感染的檔案。例如，如果 Command.com 受到檔案病毒的感染，而且 Symantec AntiVirus 無法清除感染，您可能無法還原這個檔案。不過，使用「略過 (只記錄)」指令可以在關閉電腦之前，省去不還原 Command.com 所造成的其它麻煩。
- 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。開機型病毒會感染開機磁區、分割區表、主要開機記錄，有時候也會感染記憶體。當開機型病毒分

成多個部分時，它們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 或是 .dll 這些副檔名的執行檔。巨集病毒會感染文件檔以及與這些文件相關的巨集。依照您可能需要復原的檔案類型來選取動作。

- 要執行的掃描類型
  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。結果，預設的第二個動作的設計會被用來提供您控制病毒爆發情形的能力。針對自動執行的掃描，例如排程掃描、閒置掃描 (在 32 位元電腦上)，以及「自動防護」掃描，則不會指派具有永久效果的第二個動作。例如，當您已經知道檔案受到感染時，將「刪除威脅」與「清除威脅」或「刪除威脅」動作限制為您所執行的手動掃描。

指派安全風險第二個動作的秘訣

當您選取安全風險的第二個動作時，請考慮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上時並未備份，您就不應該使用「刪除風險」動作。雖然以此方式可以刪除安全風險，但是您可能會造成電腦上其它應用程式無法運作。改用「隔離風險」動作，在必要時，讓復原 Symantec AntiVirus 所做的變更。

架構病毒與安全風險的通知

根據預設，當 Symantec AntiVirus 掃描發現病毒或安全風險時，會發出通知。根據預設，當 Symantec AntiVirus 需要中止服務或停止程序，以移除或修復病毒或安全風險的影響時，也會發出通知。

您可以為掃描架構下列的通知：

偵測選項	當 Symantec AntiVirus 在電腦上發現病毒或安全風險時，建構您要顯示的訊息。 若您架構的是「檔案系統自動防護」，您可以選取額外的選項，以便在「自動防護」在電腦上發現病毒與安全風險時，顯示一個包含結果的對話方塊。
矯正選項	架構在 Symantec AntiVirus 發現病毒或安全風險，以及是否要中止程序或停止服務以完成風險的移除或修復時，您是否要收到通知。

您可以直接在訊息欄位中輸入文字來建構您要顯示在電腦上的偵測訊息，亦可在訊息欄位中按下滑鼠右鍵來選取變數。

表 3-2 說明在通知訊息中可用的變數欄位。

表 3-2　　通知訊息變數欄位

欄位	說明
安全風險名稱	發現的病毒或安全風險名稱。
回應措施	回應偵測到病毒或安全風險後所採取的動作。此動作可為架構的第一或第二個動作。
狀態	檔案的狀態：已受感染、未受感染，或已刪除。 系統預設不會使用這個訊息變數。若要顯示此資訊，手動將此變數加入訊息中。
檔名	受病毒或安全風險感染的檔名。
路徑及檔名	受病毒或安全風險感染的檔案之完整路徑及名稱。
位置	病毒或安全風險所在之電腦磁碟。
電腦	發現病毒或安全風險的電腦名稱。
使用者	發現病毒或安全風險時登入的使用者名稱。
事件	事件的類型，例如「發現風險」。
掃描類型	偵測到病毒或安全風險的掃描類型，如手動、排程等等。
發現日期	發現病毒或安全風險的日期。
儲存體名稱	受影響的應用程式區域，如「檔案系統自動防護」或「Lotus Notes 自動防護」。
動作說明	回應偵測到病毒或安全風險後所採取動作的完整說明。

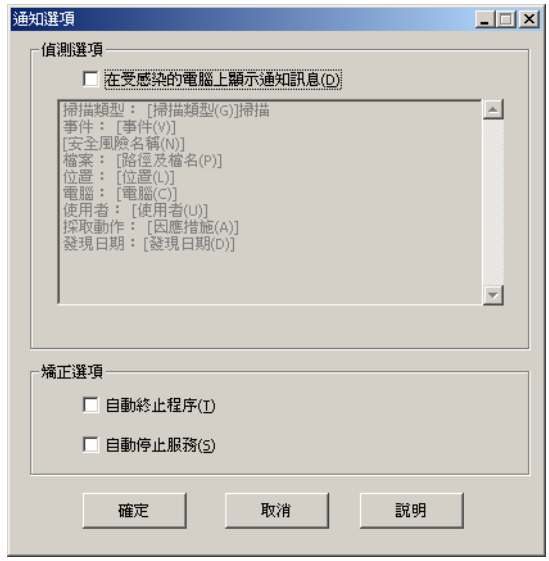
這個程序「完整掃描」作為架構範例，但您架構其它掃描時，可用相同方式架構通知。

架構病毒與安全風險的通知

1　在左窗格中，展開「**掃描**」，然後按下「**完整掃描**」。

2　在右窗格中，按下「**選項**」。

3 在「掃描選項」視窗中，按下「通知」。



4 若想在掃描發現病毒或安全風險時顯示訊息，可在「通知選項」視窗的「偵測選項」下，勾選「在受感染的電腦上顯示訊息」。

5 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：

- 按下此選項來輸入或編輯文字。
- 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」。

6 若您架構的是「檔案系統自動防護」的通知，那麼在訊息方塊下方還有一個額外選項。若想在「自動防護」發現病毒或安全風險時，隱藏包含結果的對話方塊，取消勾選「在受感染的電腦上顯示自動防護結果」。

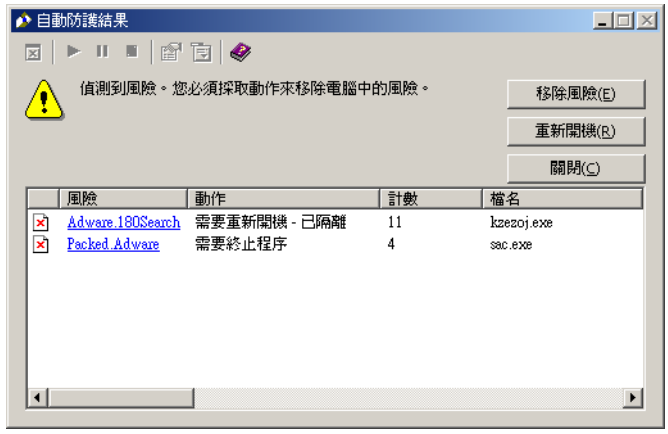
7 在「矯正選項」下，勾選您要設定的選項。選項如下所示：

自動中止程序	若勾選此選項，Symantec AntiVirus 會在需要時自動中止程序，以移除或修復病毒或安全風險。中止程序前，Symantec AntiVirus 不會提示您儲存資料。
自動停止服務	若勾選此選項，Symantec AntiVirus 會在需要時自動停止服務時，以移除或修復病毒或安全風險。停止服務前，Symantec AntiVirus 不會提示您儲存資料。

8 按下「確定」，直到您返回 Symantec AntiVirus 主視窗，然後按下「掃描」。

與通知進行互動

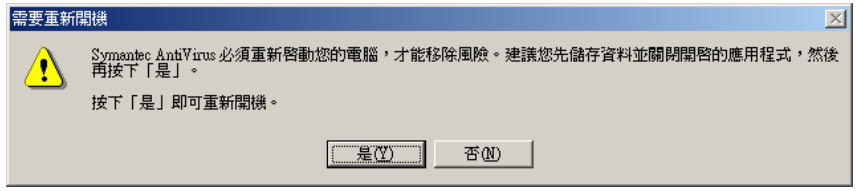
若您採用預設值，那麼在 Symantec AntiVirus 發現病毒或安全風險時，會發出通知。此時會出現「自動防護結果」對話方塊：



若 Symantec AntiVirus 需要中止程序或應用程式，或停止服務，「移除風險」按鈕便會啟用。按下「移除風險」時，會出現如下訊息：

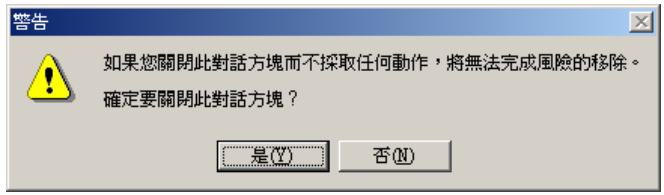
若您尚未儲存工作並關閉開啟的應用程式，它讓您有機會完成這些事。儲存資料後，您可以回到此訊息方塊，然後按下「是」，完成移除或修復。

若 Symantec AntiVirus 需要重新啟動電腦以完成移除或修復，「重新開機」按鈕便會啟用。按下「重新開機」時，會出現如下訊息：



若您尚未儲存工作並關閉開啟的應用程式，它讓您有機會完成這些事。儲存資料後，您可以回到此訊息方塊，然後按下「是」，重新啟動電腦。若按下「否」，並關閉訊息方塊而不重新啟動，那麼直到您下一次重新啟動電腦後，移除或修復才會完成。

最後，若您選擇關閉訊息方塊，而不採取動作完成移除或修復，會出現以下訊息：



若按下「是」，關閉對話方塊而不採取任何動作，則威脅可在稍後，以下列方式移除或修復：

- 您可以開啟「威脅記錄」，在威脅上按下滑鼠右鍵，然後執行動作。
- 您可以執行掃描重新偵測該威脅，然後重新開啟結果對話方塊。

可採取的動作取決於針對發現的特定類型病毒或安全風險所架構的動作。

若按下「否」，您可回到結果對話方塊，以執行適當的動作。

解析掃描結果

每當執行手動、排程、開機或使用者定義的掃描時，Symantec AntiVirus 都會顯示掃描進度對話方塊來報告進度，但您必須進行架構才行。

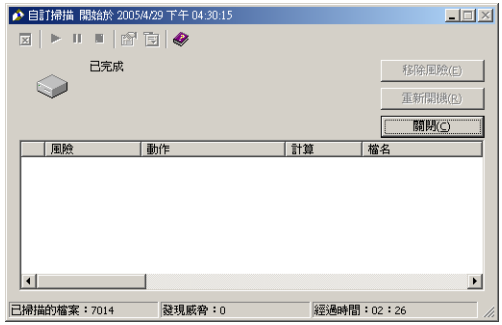
請參閱第 46 頁的「起始手動掃描」。

請參閱第 48 頁的「建立排程掃描」。

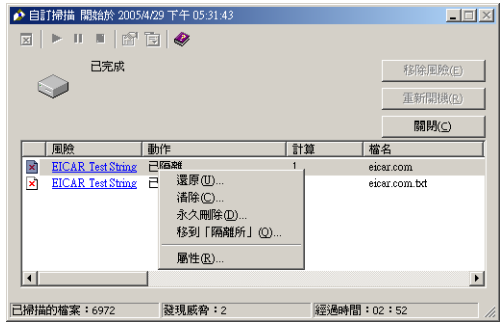
請參閱第 50 頁的「建立開機掃描」。

請參閱第 51 頁的「建立使用者定義的掃描」。

若您架構 Symantec AntiVirus 以顯示掃描進度對話方塊，您可以暫停、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」。



如果在掃描期間偵測到病毒或安全風險，掃描進度對話方塊包含受感染檔案的名稱、病毒或安全風險的名稱和所採取的動作。根據預設，偵測到病毒或安全風險時會發出通知。



請參閱第 65 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「掃描進度」對話方塊中。同樣地，您的管理員可能會選擇遇到病毒或安全風險時不要顯示警示。

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 AntiVirus 會將未感染病毒的檔案誤判為已受到感染。

如果 Symantec AntiVirus 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安全風險的軟體，例如廣告軟體，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 13 頁的「關於安全風險」。

針對以下每一種掃描類型分別設定排除項目：「自動防護」、開機、使用者定義、排程或手動，包括「自訂掃描」、「快速掃描」，或「完整掃描」。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 AntiVirus 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「**檔案系統自動防護**」。
   - 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. 在右窗格或「掃描選項」對話方塊中，勾選排除的檔案與資料夾選項。
3. 按下「**排除**」，然後按下「**檔案 / 資料夾**」，選取要排除的檔案。
4. 按下「**確定**」。
5. 按下「**副檔名**」。
6. 指定要排除的檔案類型，然後按下「**確定**」。
   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「**確定**」，直到返回 Symantec AntiVirus 主視窗。

Chapter 4

發現病毒或安全風險時要執行什麼動作

本章包含下列主題：

對受感染的檔案採取的動作

Symantec AntiVirus 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」。若是安全風險，預設是隔離受感染的檔案，並且移除或修復其副作用，若無法修復，則記錄該項偵測動作。

如果受病毒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。如果受安全風險感染的檔案已被隔離且被移除或修復，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「掃描進度」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。

您可以稍後再從「威脅記錄」或「隔離所」中處理受病毒或安全風險感染的檔案。

請參閱第 69 頁的「重新掃描隔離所內的檔案是否有病毒」。

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「掃描進度」對話方塊中。同樣地，您的管理員可能會選擇遇到病毒或安全風險時不要顯示警示。

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「掃描進度」對話方塊中，選取您所要的檔案。
- 在 Symantec AntiVirus 的左窗格中，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：

- 還原：如果可以，請改採前一個回應動作。
- 清除 (僅病毒)：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。
  針對安全風險，請謹慎使用此動作，因為在某些情況下，刪除安全風險會導致應用程式失去功能。
- 移到隔離所：將受安全風險感染的檔案放置於「隔離所」中，並嘗試移除或修復所造成的副作用。
- 屬性：顯示有關病毒或安全風險的資訊。

根據預設的病毒或安全風險偵測的動作，Symantec AntiVirus 可能無法執行您所選取的動作。

關於病毒造成的損壞

如果檔案受到感染之後迅速被發現，之前受感染的檔案或許將完全有作用。然而，在某些情形下，Symantec AntiVirus 可能會清除已被病毒損壞的受感染檔案。例如，如果 Symantec AntiVirus 在受感染的文件檔中發現 Word.Wazzu 巨集病毒，Symantec AntiVirus 會移除這個病毒，但不會移除病毒置入受感染文件中的單字 wazzu。在這個情況下，Symantec AntiVirus 便無法修復受感染檔案中已造成的損害。

關於隔離所

有時候 Symantec AntiVirus 會偵測到目前其病毒定義檔無法排除的未知病毒，或者您認為某個檔案已經受到感染，但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。

將受到病毒感染的檔案移動到隔離所

將受病毒感染的檔案移動到「隔離所」中，可徹底減少病毒自我複製，因此而感染其它檔案的機會。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。

將受病毒感染的檔案移動至「隔離所」可防止病毒的散播。但是，它並不會清除病毒，因此病毒仍將留在您的電腦中，直到病毒被清除或是檔案被刪除為止。對受檔案病毒與巨集病毒感染的檔案來說，將受感染的檔案移動至「隔離所」是一個有用的執行動作，但是對開機型病毒感染則沒有用。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」。

請參閱第 13 頁的「關於主要開機記錄」。

請參閱第 12 頁的「開機病毒」。

在檔案被移動至「隔離所」後，您可以嘗試清除這個檔案、永久刪除檔案，或將它還原至原始的位置。您也可以檢視受感染檔案的內容。當病毒定義檔被更新時，您可以重新掃描「隔離所」中受病毒感染的檔案。

請參閱第 69 頁的「重新掃描隔離所內的檔案是否有病毒」。

讓受到安全風險感染的檔案留在隔離所中

您可以將因為安全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，直到您確定電腦上的應用程式未遺漏任何功能為止。

刪除隔離所中受到病毒感染的檔案

如果您刪除「隔離所」中的檔案，Symantec AntiVirus 便會永久將它從您的電腦硬碟上刪除。

刪除受到病毒感染的檔案可減少病毒藉由移除檔案 (因此移除病毒) 而散播的威脅。對於檔案病毒與巨集病毒來說，刪除受感染的檔案相當有用。

由於病毒會破壞檔案的一部份，因此刪除受感染的檔案並以乾淨的備份檔來取代可能比清除受感染的檔案更好。

您可以在受感染的檔案被移動至「隔離所」後，手動執行這個動作。刪除「隔離所」中受感染的檔案是從無法清除病毒的可任意處理檔案中移除病毒的一種有效方式。

警告：只有在您擁有決定要掃描檔案的乾淨備份時，才能使用這個選項。您不得使用這個選項在「自動防護」或排程掃描期間，做為檔案掃描的主要動作。

刪除隔離所中受到安全風險感染的檔案

如果您刪除與某個安全風險相關的檔案，而電腦上的應用程式若已與您所刪除的檔案有關聯，則可能會無法適當地運作。「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：一旦您執行了與安全風險相關的應用程式，並且確定沒有喪失功能，則您可能會想要刪除檔案以節省磁碟空間。

管理隔離所

您可以將受病毒或安全風險感染的檔案放置在「隔離所」中。

檔案被置入「隔離所」的方式有兩種：

- Symantec AntiVirus 會根據其設定，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 AntiVirus 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」。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 Symantec AntiVirus 的左窗格中，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. 尋找並選取檔案，然後按下「**新增**」。
5. 按下「**關閉**」。

在隔離所中檢視檔案及檔案的細節

您可以檢視已被置入「隔離所」中的檔案，以及檔案的詳細資料，例如病毒名稱、發現檔案的電腦名稱等等。

在隔離所中檢視檔案及檔案的細節

1. 在 Symantec AntiVirus 的「檢視」功能表上，按下「**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」，請即更新您的定義檔。根據管理員架構「隔離所」的方式，在更新定義檔之後，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。

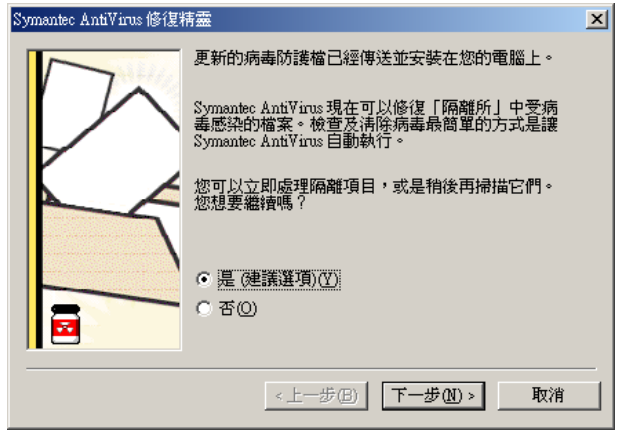
如果在 Symantec AntiVirus 重新掃描「隔離所」中的檔案之後，仍無法移除病毒，請將受感染的檔案傳送給 Symantec Security Response (賽門鐵克安全機制應變中心) 進行分析。

請參閱第 73 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」內的檔案是否有病毒，但不能重新掃描是否有安全風險。

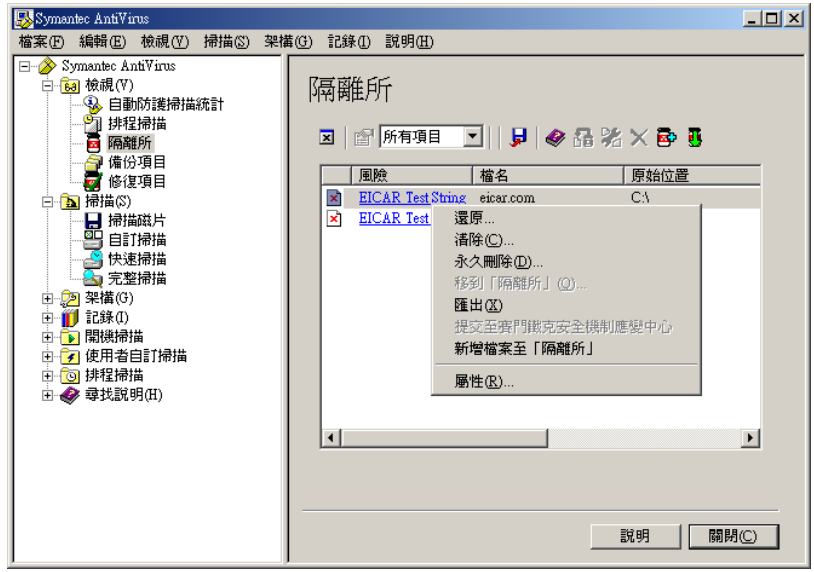
手動重新掃描「隔離所」中的檔案是否有病毒

1 更新您的定義檔。
請參閱第 29 頁的「更新病毒和安全風險防護定義檔」。

2 在 Symantec AntiVirus 的左窗格中，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 AntiVirus 的左窗格中，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 AntiVirus 在嘗試清除或修復之前，預設會被架構為先備份受病毒和安全風險感染的檔案，作為資料安全防護的屏障。在某個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 73 頁的「自動清除隔離所、備份項目和修復項目中的檔案」。

手動清除備份項目

1. 在 Symantec AntiVirus 的左窗格中，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 73 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 AntiVirus 的左窗格中，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 AntiVirus 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 AntiVirus 的左窗格中，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. 按下工具列最右邊的「清除」圖示。
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**」。

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 AntiVirus 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。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 Internet 連線，才能傳送樣本。

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」的管理員負責處理。在此情況下，您的 Symantec AntiVirus 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 AntiVirus 的左窗格中，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。

檢視事件日誌

「事件日誌」包含您電腦上有關病毒和安全風險防護相關活動的每日記錄，包括架構變更、錯誤以及病毒和安全風險定義檔資訊。這些記錄稱為事件，會以清單格式，和其它相關資訊一起顯示。

使用「事件日誌」內的資訊可讓您追蹤電腦上，與病毒和安全風險相關的趨勢。如果您的電腦由許多人使用，您可能可以識別誰傳入最多的病毒或安全風險，並協助這個人使用更好的預防措施。

檢視事件日誌

- 在 Symantec AntiVirus 的「記錄」功能表上，按下「事件日誌」。

過濾事件日誌中的項目

您可以依所記錄的「日期」、「事件」、「電腦」、「使用者」或「掃描類型」，來過濾「事件日誌」中記錄事件的事件。您也可以依事件的日期或是類別過濾，讓您可以檢視幾天前或是最近幾年的資訊。

依日期過濾項目

您可以依日期過濾顯示在「威脅記錄」、「掃描記錄」、「事件日誌」和「竄改記錄」中的項目。

Symantec AntiVirus 預設會在「事件日誌」中，以事件發生的順序輸入事件。從安裝 Symantec AntiVirus 之後，所有發生在電腦上的事件都會被儲存。

當您變更日期範圍時，Symantec AntiVirus 不會刪除資訊。例如，若您變更出現在「今日」的資訊，則其它資訊會繼續存在，但不會出現在記錄或日誌中。

依日期過濾項目

1 在「記錄」功能表上，按下「事件日誌」。

2 按下「所有項目」(或是日期範圍)下拉式清單方塊。

3 選取一個過濾器。

4 如果您按下「選取的範圍」，請選取開始日期與結束日期，然後按下「確定」。

依事件類別來過濾事件日誌：

在您已顯示您要在「事件日誌」中檢視的資訊之後，您可以用逗號分隔 (.csv) 的檔案儲存資料，如同它在您電腦上所顯示一般。

在「事件日誌」中，事件被分為下列幾種類別：

- 架構變更
- 啟動 / 關閉 Symantec AntiVirus
- 病毒定義檔
- 掃描省略
- 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
- 授權
- 用戶端管理與漫遊
- 日誌轉送
- 未經授權通訊 (拒絕存取) 警告
- 登入與憑證管理

您可以透過只顯示特定的事件類別，來減少出現在「事件日誌」中的事件數目。

例如，如果您只想要檢視錯誤事件，您可以只選取「架構變更」類別。當 Symantec AntiVirus 要在其它的類別中繼續記錄事件時，那些事件就不會出現在「事件日誌」中。

依事件類別來過濾「事件日誌」

1. 在 Symantec AntiVirus 的「記錄」功能表上，按下「事件日誌」。
2. 按下「過濾事件」。
3. 選取一個或多個事件類別。
4. 按下「確定」。

關於從事件日誌清除項目

您無法從 Symantec AntiVirus 內的「事件日誌」中，永久移除事件記錄。

若要永久刪除「事件日誌」記錄，您必須刪除包含事件記錄的 .log 檔。一週中每天的事件都會記錄在 Symantec AntiVirus Logs 目錄下的 .log 檔中。這些檔案會依據建立的日期來命名。不建議刪除 .log 檔，因為您將會永久遺失包含在其中的歷史病毒防護資料。

將資料匯出至 .csv 檔

您可以將資訊匯出至逗號分隔 (.csv) 的格式。這個共同的檔案格式被大多數的試算表與資料庫程式用來匯入資料。一旦在其它的程式中，您可以使用資料來建立簡報、圖表或是結合資料與其它資訊來建立複雜的報告。

您可以只匯出所顯示的資料。例如，如果您變更 Symantec AntiVirus 設定來顯示最近七天的資訊，只有最近七天的資訊會出現在 .csv 檔中。

將資料匯出至 .csv 檔

1. 在「威脅記錄」、「掃描記錄」或「事件日誌」視窗中，確認您想要儲存的資料有被顯示出來。
2. 按下「匯出」。
3. 在「另存新檔」對話方塊中，找出您想要儲存檔案的目錄，然後輸入檔案名稱。
4. 按下「存檔」。

索引

九劃

十劃

十一劃

十二劃