文件編號：SPEM51262/21007

發行日期：2003 年 3 月

美國專利字號：5,951,698

Trend Micro ServerProtect 使用手冊介紹本軟體的主要功能，並提供您作業環境的安裝說明。在安裝或使用本軟體前，請先閱讀這本手冊。

如果需要使用軟體特定功能的詳細資訊，請參線上說明和趨勢科技網站的線上資料庫。

趨勢科技將不斷地改良文件的品質。如果您有關於本文件或任何趨勢科技文件的問題、意見或建議，請與我們聯絡，電子郵件信箱為：**docs@trend.com**。我們樂於收到您的任何批評與指教。請於下述網站中填寫您對此份文件之評價：
www.trendmicro.com/download/documentation/rating.asp

目錄

第 1 章

Trend Micro™ ServerProtect™ 入門

ServerProtect 是最新一代用於保護企業網路中檔案伺服器的得獎連連的軟體。它採用最先進的病毒偵測技術，保護您的企業網路完全不受任何病毒侵襲。ServerProtect 可偵測新增檔案和現有檔案中的病毒，以及偵測出可能入侵網路環境中伺服器或工作站的「未知」病毒的活動。

ServerProtect 可讓網路管理員能經由單一可攜式管理主控台輕鬆管理多台 Windows .NET/2000/NT 與 Novell NetWare（NW）伺服器。主控台可供管理員在同一個網域中同時設定多個伺服器，並且整合所有伺服器的病毒事件報告。

透過「管理主控台」，管理員可以設定、監控及維護病毒防護工作。Trend Micro ServerProtect 增強並簡化企業防毒策略的執行以降低病毒防護的成本。

本章內容如下：

- ServerProtect 如何作業
- ServerProtect 架構
- 即時掃瞄或手動掃瞄（立即掃瞄）

- 設定與執行工作
- 當 SeverProtect 發現病毒時 （中毒處理行動）
- 病毒記錄檔
- 部署更新檔
- ServerProtect 病毒偵測技術
- 其他功能

ServerProtect 如何作業

ServerProtect 可監控安裝有 Windows .NET/2000/NT 或 Novell NetWare 伺服器或工作站的所有網路活動。當它偵測到伺服器中的檔案被使用時，就會掃瞄該檔案是否感染病毒。

如果檔案已經中毒，ServerProtect 會發出中毒警訊，並採取已設定好的處理行動。系統中所有的病毒防護動作都會在 ServerProtect 的記錄檔中留下記錄。

ServerProtect 還可自行設計掃瞄設定檔，以節省重複設定的時間。你可以針對不同的工作性質來點選不同的即時掃瞄選項 , 例如 : 在網路效能運作正常的情況下只掃瞄輸入的檔案。

ServerProtect 如何管理伺服器

ServerProtect 以三層式架構 （three-tier architecture）為您的主從架構網路提供安全管理：「管理主控台」、「資料伺服器」（中介軟體）及「一般伺服器」。這三個元件組合在一起後形成一組強大、集中式管理並降低成本的安全防護系統。

「管理主控台」具有容易使用的視窗介面，用來架構系統元件。「管理主控台」的指示會先傳給 「資料伺服器」，再由 「資料伺服器」轉給「一般伺服器」。

通訊方法

「管理主控台」使用 TCP/IP 通訊協定 （傳輸控制 / 網際協定），必須使用密碼才能夠登入 ServerProtect 「資料伺服器」。「資料伺服器」使用 TCP/IP 與 「遠端程序呼叫」（RPC）來連線到 Windows .NET/2000/NT 一般伺服器；以及使用 IPX™ （網際封包交換）、SPX™ （循序封包交換）與 IP 來連線到 Novell NetWare 一般伺服器。

ServerProtect 架構

ServerProtect 以三層式架構（three-tier architecture）為整個網路提供安全管理：「管理主控台」、「資料伺服器」及「一般伺服器」。以下展示這三個元件之間的關係：

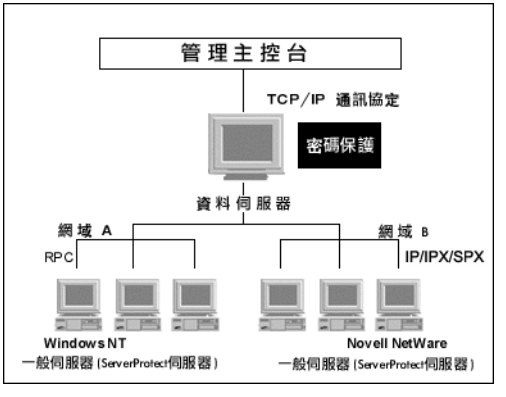


圖 1-1 ServerProtect 三層式架構

管理主控台

ServerProtect「管理主控台」是一個可攜性的主控台，可協助網路管理員集中控管多個網路伺服器及網域。這個主控台可讓您同時設定同一個網域下的伺服器，以及產生所有伺服器病毒事件的整合報告。主控台可分為四個部分：

- 主功能表
- 功能區
- ServerProtect 網域瀏覽目錄
- 設定區

注意：一台「資料伺服器」只由一個「管理主控台」管理，也就是，只要有一個「管理主控台」連線到「資料伺服器」，其他「管理主控台」便無法再與該「資料伺服器」連線。

ServerProtect 的網域瀏覽目錄，可瀏覽安裝在 Windows .NET/2000/NT 與 Novell NetWare 伺服器上的所有 ServerProtect 伺服器，並顯示其狀態。狀態資訊包括病毒碼、掃瞄引擎以及程式檔的版本、作業系統的種類與版本，即時掃瞄的方向等。請注意，管理員可以設定是否顯示上述所有的狀態資料。

秘訣：您可以使用「管理主控台」從遠端安裝一台或多台「一般伺服器」。請參照第 2 章 “安裝一般伺服器”小節。

資料伺服器

「資料伺服器」在「管理主控台」及其所管理的「一般伺服器」之間扮演著通訊樞紐的角色（中介軟體）。管理員可以從遠端站台傳出指示或接收資料，因而簡化了「一般伺服器」的控管作業。

警告！「資料伺服器」本身沒有防衛能力，若要保護「資料伺服器」，必須在同部電腦上安裝「一般伺服器」。

資料伺服器秘訣

- 第一次在網路上安裝 ServerProtect 時，必須將目標伺服器設為「資料伺服器」，再設定將其他「一般伺服器」加入此「資料伺服器」。
- 「資料伺服器」至少要有一個網域成員，以便能夠支援「一般伺服器」。
- 由於「資料伺服器」只不過是資訊的遞送系統，因此，理論上它所能管理的「一般伺服器」總數取決於可用頻寬的大小。但為了

便於管理，指派給「資料伺服器」的「一般伺服器」數量應該適量就好。

- 如果有許多伺服器分散在不同位置，請在每個位置各安裝一台「資料伺服器（IS）」。

注意：根據標竿測試的結果顯示，一台「資料伺服器」可管理多達 500 台「一般伺服器」。此數據僅供參考，實際狀況依可用頻寬而異。

一般伺服器

「一般伺服器」是指網路上安裝有 ServerProtect 的伺服器。在 ServerProtect 架構中，「一般伺服器」是捍衛伺服器的第一道防線，也是一切病毒攻防的戰場。「一般伺服器」負責執行系統的防毒任務，而「一般伺服器」的管理則由「資料伺服器」負責。

ServerProtect 提供數種安裝「一般伺服器」的方法：

- 使用安裝程式。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。
- 使用「管理主控台」。請參照第 2 章 “從管理主控台安裝一般伺服器”小節。
- 使用 Microsoft System Management Server（SMS）。請參照第 2 章 “透過 Microsoft SMS 部署 ServerProtect”小節。
- 使用自動安裝。請參照第 2 章 “自動安裝 ServerProtect”小節。

您可依照公司的需要調整上述每種安裝方式。請參照第 2 章 “安裝一般伺服器”小節。

警告！由於使用安裝程式安裝每一台伺服器非常耗時，趨勢科技建議您從 ServerProtect「管理主控台」安裝伺服器。

ServerProtect 網域

ServerProtect 網域是指「一般伺服器」的虛擬分組，用來簡化伺服器的識別與管理。您可隨時依照網路的需求，建立、重新命名或刪除網域。

網域中的「一般伺服器」只可以被指定給一台「資料伺服器」。另一方面，「資料伺服器」則可以管理數個網域。

管理網路安全最有效的方法是將所有伺服器適當的分類整理成 ServerProtect 網域。例如，您可以建立一個 ServerProtect 網域，取名為 "NW"，即可更有效率地管理 NetWare「一般伺服器」。請參照第 3 章 ServerProtect 網域管理。

警告！ ServerProtect 網域並不同於 Windows .NET/2000/NT 網域；ServerProtect 網域只是將執行 ServerProtect 的「一般伺服器」做邏輯分組。

ServerProtect 網域具有下列特色：

- **網域過濾器**：網路管理員可以對「資料伺服器」設定過濾器，以決定可從「管理主控台」的網域瀏覽目錄中檢視的內容。
- **彈性的網域管理**：登入主控台後，管理員可以依喜好新增、重新命名、移動網域或刪除網域。

即時掃瞄或手動掃瞄（立即掃瞄）

ServerProtect 提供兩個功能強大的掃瞄功能：即時掃瞄與立即掃瞄。

即時掃瞄會在伺服器上持續執行，以提供最嚴密的安全防護。所有輸入與輸出伺服器的檔案都會被監控，並阻止中毒檔案在伺服器間的複製。請參照第 3 章 “使用即時掃瞄”小節。

立即掃瞄即為手動掃瞄（也就是由使用者下命令後立即執行）。立即掃瞄可以立刻檢查可能感染的電腦，或立即取得電腦的相關資訊。請參照第 3 章 “使用立即掃瞄 (手動掃瞄)” 小節。

秘訣：為確保最嚴密的保護，趨勢科技建議您同時使用即時掃瞄與立即掃瞄。

即時掃瞄與立即掃瞄的好處包括：

- **重複的檔案掃瞄**：如果不小心下載或複製中毒檔案，即時掃瞄將阻止執行該動作。但如果即時掃瞄因為某些原因而關閉，您仍可以用立即掃瞄偵測出中毒檔案。
- **有效率的檔案掃瞄**：即時掃瞄的預設值即能可靠地掃瞄檔案，同時又對系統資源所造成的影響減到最小。請參照第 3 章掃瞄病毒。
- **有效且具彈性的檔案掃瞄**：ServerProtect 為管理員提供許多實用的掃瞄設定選項，可根據個別需要自行設定保護網路。

設定與執行工作

ServerProtect 允許管理員建立多項工作，依照需要或預約時間進行部署。

ServerProtect 工作可用來：

- 部署更新檔
- 執行即時掃瞄設定
- 執行立即掃瞄
- 清除、刪除、輸出或列印記錄檔
- 產生病毒掃瞄統計資料

使用 ServerProtect 工作的好處包括：

- 同時部署多項功能

- 自動執行網路防毒工作的例行程序
- 提高防毒管理效率，以及統一防毒政策

工作會被指定給負責維護工作的「工作擁有者」。請參照第 3 章 “工作管理”小節。

在伺服器上安裝 ServerProtect 後，便會產生三項預設工作：立即掃瞄、執行統計與部署，這是管理與監控網路病毒活動的三項必要工作。您可以修改這三項預設工作的目標伺服器及其定義。

當 ServerProtect 發現病毒時 （中毒處理行動）

ServerProtect 可讓您設定對中毒檔案所採取的處理行動。此外，您也可以針對不同病毒設定不同的處理行動。

ServerProtect 可以對中毒檔案採取五種處理行動：

- **不作處置**：手動掃瞄時，ServerProtect 會略過中毒檔案，不採取任何處理行動，只在記錄檔內留下發現病毒的記錄。即時掃瞄時，ServerProtect 會 “禁止存取”中毒檔案，防止檔案進行複製或修改。如需詳細資訊，請參照第 3 章 “定義中毒處理行動”小節。
- **刪除**：刪除中毒檔案。
- **重新命名**：將中毒檔案的副檔名變更為 .vir，以防止執行或開啟該檔案。如果已經有副檔名為 .vir 的同名檔案，則下一個檔案將更名為 .v01、.v02 等，直到 .v99 為止。
- **隔離**：將中毒檔案隔離到指定的資料夾。此外，您可以變更隔離檔案的副檔名，以防止開啟或執行該檔案。
- **清除**：嘗試清除檔案中的病毒。由於清除病毒有時候會破壞檔案，導致檔案變成無法使用，因此您可以先在清除前備份中毒檔案。

所有病毒事件及相關的處理行動都會記錄在記錄檔中。如需詳細資訊，請參閱線上說明中的「檢視中毒記錄檔」主題 ，及定義中毒處理行動。

注意：如果選取「清除」當作中毒處理行動，還可指定清除失敗時的備用處理行動。

病毒記錄檔

集中式防毒系統真正的威力在於能夠從一個主控台記錄及提供有關網路病毒安全防護策略的所有資訊，使管理員在監控網路伺服器時，可以很容易取得各項資訊。

ServerProtect 提供全方位的資訊，包括掃瞄、檔案更新及部署結果等。此外，ServerProtect 將資訊都儲存在記錄檔內，可供您讀取或輸出。例如，您可以分析網路掃毒的統計資料，包括最常見的病毒種類，或是導致網路感染病毒的使用者名稱等資料。不僅如此，您還可以將記錄資料輸出到資料庫或試算表應用程式，做進一步的分析。

記錄檔的預設大小是 8000 筆記錄，或最多 10MB。一旦記錄檔超過 8000 筆記錄或 10MB，ServerProtect 會自動將舊的記錄檔重新命名，再建立新的記錄檔。

您也可以直接從 「掃瞄結果」視窗對中毒檔案採取行動，讓您能夠更方便對中毒事件採取適當的處理行動。如需有關記錄檔的詳細資訊，請參閱 ServerProtect「管理主控台」中的 ServerProtect 線上說明。如需有關病毒記錄檔的詳細資訊，請參閱線上說明的 「檢視記錄檔資訊」與 「檢視資料伺服器記錄檔」主題。

部署更新檔

趨勢科技更新是趨勢科技防毒軟體的昇級與更新部署模組。它簡化了趨勢科技軟體的維護工作，並減少網路病毒安全防護的總成本。因為每個月都會發現許多新病毒，所以成功的病毒安全防護策略必須使用能夠處理最新病毒威脅的病毒碼檔案、程式及掃瞄引擎。

注意：趨勢科技會定期發佈新版本的病毒碼、程式與掃瞄引擎更新，供使用者下載。

ServerProtect 更新功能包括：

- **選擇更新元件：**您可以根據要更新的項目分別更新病毒碼、掃瞄引擎或程式檔案。
- **自動預約更新**：您可以建立預約更新工作，在您休息的時間更新所有的「一般伺服器」。
- **彈性下載檔案**：您可以指定從趨勢科技的更新網站下載更新檔到一台「資料伺服器」，然後讓其他伺服器從這台「資料伺服器」取得更新的檔案。
- **集中更新部署：**您可以從「管理主控台」將更新檔部署到網路上的各個伺服器。
- **相容的防火牆與代理伺服器**：ServerProtect 可以搭配大部分現有的防火牆與代理伺服器一起使用。
- **更新活動記錄**：所有更新活動都記錄在記錄檔內，以作為參考資料。
- **更新還原選項**：若在部署更新時發生錯誤，您可以將已部署的病毒碼、掃瞄引擎或程式檔案還原回先前的版本。

更新 ServerProtect 有兩個步驟：

1. 從趨勢科技的更新伺服器下載更新檔。
2. 將下載的更新檔部署到網路上的其他「一般伺服器」。

這種方式快速有效，既可節省時間，又可將佔用的網路頻寬減到最小。請參照第 4 章 “更新 ServerProtect5 來取得詳細資訊”小節。

秘訣：您可以建立預約的更新工作，將「一般伺服器」的更新部署程序自動化。請參照第 3 章 “建立工作”小節。

ServerProtect 病毒偵測技術

ServerProtect 使用先進的病毒偵測技術。這一節重點介紹支援這項最先進技術的工具，以及如何有利於管理員的管理。

病毒碼比對

ServerProtect 利用「病毒碼比對」的程序，透過大型的病毒碼資料庫來識別已知的病毒樣本。它會檢查可疑檔案的關鍵部分有無病毒碼跡象的字串，再和趨勢科技已經記錄的成千病毒樣本進行比對。

如果是變形或變體病毒，ServerProtect 掃瞄引擎容許可疑的檔案在其內部暫時解碼執行，然後 ServerProtect 再掃瞄整個檔案（包括剛解碼的部分），以識別有無任何變體病毒的可疑字串。

如果找到病毒，ServerProtect 會採取您先前指定的中毒處理行動。ServerProtect 中毒處理行動包括：清除（自動清除）、刪除、不作處置、隔離（移動）或重新命名。您可以自行設定針對開機型病毒與檔案型病毒的中毒處理行動。請參照第 3 章 “掃瞄病毒”小節。

注意：病毒碼檔案永遠保持最新版本是非常重要的，因為每年約有數千種新病毒出現。趨勢科技提供預約下載更新檔，讓您可以方便取得病毒碼更新檔案。如需詳細資訊，請參照第 3 章 “設定預約下載”小節與第 3 章 “設定預約部署”小節。

MacroTrap

ServerProtect 透過趨勢科技取得專利的 MacroTrap 智慧型巨集病毒偵測系統來保護 Microsoft Office 檔案，以防止受到巨集病毒攻擊。巨集病毒是蔓延速度最快的電腦病毒，經由藏匿在電子郵件的附件檔傳送，因此很容易擴大蔓延的範圍。如需有關 MacroTrap 的設定資訊，請參照第 3 章 “設定即時掃瞄”小節。

注意：趨勢科技 MacroTrap 可以防止網路使用者接收與傳送巨集病毒。

MacroTrap 如何作業

MacroTrap 可針對文件附隨儲存的所有巨集程式，進行推理檢查。巨集病毒通常包含在不可檢視的範本（例如 Microsoft Word 的 *.dot）中，並跟隨文件一起移動。MacroTrap 可在文件中搜尋可能具有病毒活動的指令，來檢查有無未知的病毒。例如，將範本的一部分複製到其他範本（繁殖複製），或執行破壞性的指令。

壓縮檔案

壓縮檔（許多個別壓縮檔組成的一個檔案）是透過電子郵件及 Internet 傳送檔案與軟體最常用的方法。不幸的是，壓縮保存的檔案也可能感染病毒。由於有些防毒軟體無法掃瞄這類檔案，因此有心人士有時候會利用壓縮保存檔將病毒「偷渡」進入受保護的網路或電腦。

趨勢科技掃瞄引擎可掃瞄壓縮的檔案。不僅如此，它還可以掃瞄經過壓縮再壓縮的檔案，最多可達 5 層。

ServerProtect 中所用的趨勢科技掃瞄引擎可偵測使用下列演算法所壓縮之檔案中的病毒：

- PKZIP（.zip）與 PKZIP_SFX（.exe）
- LHA（.lzh）與 LHA_SFX（.exe）

- ARJ（.arj）與 ARJ_SFX（.exe）
- CABINET（.cab）
- TAR
- GNU ZIP（.gz）
- RAR（.rar）
- PKLITE（.exe 或 .com）
- LZEXE（.exe）
- DIET（.com）
- UNIX PACKED（.z）
- UNIX COMPACKED（.z）
- UNIX LZW（.Z）
- UUENCODE
- BINHEX
- BASE64

注意：趨勢科技掃瞄引擎目前僅能清除使用 PKZIP 演算法所壓縮的檔案。如果在使用其他演算法的壓縮檔內發現病毒，須在暫存目錄內先將檔案解壓縮後，再清除病毒。

如需壓縮檔的設定資訊，請參照第 3 章 “設定即時掃瞄”小節與第 3 章 “設立即時掃瞄”小節。

木馬殺手

木馬殺手（DCS）會根據檔案行為偵測出特洛伊型病毒，並還原被修改的系統檔案。DCS 也會終止有關特洛伊型病毒的處理程序，並刪除特洛伊型病毒遺留在系統中的檔案。

OLE 層級掃瞄

Microsoft 物件連結與內嵌（OLE）技術讓 Microsoft Office 檔案能夠嵌入 Microsoft Office 檔案中。也就是，您可以將 Microsoft Word 文件放進 Excel 工作表，再將這個 Excel 工作表嵌入 Microsoft™ PowerPoint 簡報內。

OLE 為開發人員提供許多好處，但同時也可能帶來潛在的中毒危險。為了解決這個問題，趨勢科技新研發出一個「OLE 層級掃瞄」功能，使 ServerProtect 先進的病毒安全防護更為完整。請參照第 3 章 “掃瞄病毒”小節。

秘訣：OLE 層級掃瞄提供五層的保護。趨勢科技建議您為立即掃瞄設定 OLE 層級為兩層，在即時掃瞄時則設定一層。設定層級愈小，伺服器效能會愈好。

智慧型掃瞄

智慧型掃瞄是識別哪些檔案需要掃瞄的新方法，它比標準的「掃瞄所有檔案」選項更安全有效。

對於可執行檔（也就是 .zip、.exe），真實的檔案類型由檔案內容來決定。若不是可執行檔（例如 txt），則智慧型掃瞄以檔案標頭來確認真實的檔案類型。請參照第 3 章 “掃瞄病毒”小節。

智慧型掃瞄可以提供管理員許多好處，以下略述一二：

- **效能最佳化**：掃瞄所用的伺服器系統資源將減到最少，所以使用智慧型掃瞄並不影響伺服器上執行的其他重要的應用程式。
- **節省時間**：由於智慧型掃瞄使用真實檔案類型來識別檔案，因此智慧型掃瞄所花費的時間比掃瞄所有檔案要少得多（也就是只掃瞄中毒機會較大的檔案）。若將智慧型掃瞄搭配立即掃瞄使用，節省的時間就會非常明顯。請參照第 3 章 “設定立即掃瞄”小節。

主動式處理行動

主動式處理行動是一組預設的中毒掃瞄行動，您可以針對病毒及其他類型的惡意軟體執行這些預設行動。趨勢科技建議的中毒處理行動是清除病毒。對於特洛伊型病毒與惡作劇程式，則建議刪除檔案。立即掃瞄和即時掃瞄都可以設定主動式處理行動。

何時選擇主動式處理行動

如果您不熟悉中毒處理行動，或不確定對某些病毒應採取哪種最合適的中毒處理行動，建議您選擇主動式處理行動。

不同病毒的差異極大，所以適當的中毒處理行動也會因病毒而異。您必須了解病毒，才能自行設定中毒檔案的處理行動，然而這樣的作法相當繁瑣。因此，趨勢科技建議您使用主動式處理行動。

使用主動式處理行動而不自行設定中毒處理行動的優點如下：

- **節省時間**：不必花時間自行設定中毒處理行動。
- **無須擔心維護工作**：主動式處理行動使用趨勢科技建議的中毒處理行動，所以您可以專心處理其他工作，不必擔心發生錯誤。
- **隨時更新中毒處理行動**：在每一份新的病毒碼，趨勢科技都會附上最新的主動式處理行動設定。因為病毒不斷改變攻擊的方式，所以中毒處理行動當然也要經常修正，以防止任何可能的中毒機會。

如需主動式處理行動的設定資訊，請參照第 3 章 “定義中毒處理行動”小節。

掃瞄連線網路磁碟機

ServerProtect 能夠掃瞄一或多台網路磁碟機，但這些共用的網路資料夾必須先完成連線後，您才能選擇這項功能。它的功用是讓即時掃瞄功能也可以掃瞄及保護連線網路磁碟機，因而減少中毒的危險。請參照第 3 章 “設定即時掃瞄”小節。

其他功能

為提高網路安全防護的彈性，ServerProtect 還提供以下功能。

集中式管理

ServerProtect 提供視窗架構的主控台（管理主控台），以協助您在網路上管理多個 Windows .NET/2000/NT 與 Novell NetWare 伺服器與網域。主控台採可攜式設計，可在任何 32 位元 Windows 電腦上執行（Windows NT 3.51 除外）。

增強安裝時的網路安全防護

安裝「一般伺服器」或「資料伺服器」的過程中，您必須輸入指定目標伺服器的管理員使用者名稱和密碼。

回應病毒爆發更快速

在執行 ServerProtect 的電腦上，如果有病毒嘗試感染共用資料夾內的檔案，便會出現訊息方塊，指出病毒來自哪一台電腦。顯示的資訊包括：掃瞄類型、病毒名稱、中毒檔案名稱、電腦名稱及使用者名稱。此外，它還會顯示針對病毒所採取的行動，以及中毒來源等。請參照第 3 章 “設定通知訊息”小節。

彈性控制中毒檔案

當 ServerProtect 偵測到中毒檔案時，您可以選擇清除病毒後回復檔案、傳送可疑或無法清除病毒的檔案給趨勢科技、刪除清除病毒前留下的備份檔，或將已經清除的檔案傳回給使用者。

NetworkTrap 工具（網路陷阱工具）

某些病毒（例如 PE.FunLove.4099）會尋找共用資料夾，以儘可能感染連線的使用者。NetworkTrap 工具可以讓您分享資料夾，並自動複製誘餌（Bait）資料夾的內容到新建的共用資料夾中（誘餌資料夾包含病毒可能感染的檔案）。此共用資料夾使用新的病毒通知以建立有效的病毒陷阱。如需有關此主題的詳細資訊，請參閱線上說明的「NetworkTrap 工具」一節。

最先進的病毒偵測技術

ServerProtect 新增了主動式處理行動、智慧型掃瞄與 OLE 層級掃瞄等可設定的掃瞄工具，為您提供更快、更有效率的掃瞄。

可檢視掃瞄統計資料

ServerProtect 可讓您有效監控網路病毒安全防護。ServerProtect 可依指定的時間間隔將掃瞄統計資料顯示在畫面上，內容包括發現的病毒總數、發現次數最多的前十名病毒、感染病毒最多的前十名使用者、無法清除的病毒總數等。

相容性

ServerProtect 和 Microsoft Windows .NET、Microsoft Windows 2000、Microsoft Windows NT、Microsoft Cluster Server、Terminal Server 及 Index Server 完全相容。它還可以和許多網路管理工具軟體合併使用，包括 Novell NetWare、Novell NetWare Cluster Service、Computer Associates ARCserve、Veritas Backup Exec、St. Bernard Software Open File Manager、NTP Software Quota Manager、CitrixÆ MetaFrame、Citrix WinFrame，以及 Network File System（NFS）的驅動程式與趨勢科技更新伺服器所需的 SOCKS 4。

第 2 章

安裝 ServerProtect

這一章包含在您的網路上成功安裝 ServerProtect 所需的資訊。

注意：您必須以管理員權限登入，才能安裝「資料伺服器」。

本章內容如下：

- 系統需求
- 安裝方式
- 安裝 ServerProtect
- 移除 ServerProtect

系統需求

ServerProtect 每項元件各有不同的系統需求。

一般伺服器

- 200MHz Intel Pentium III 同級或更快速的處理器
- 作業系統：

  Microsoft Windows

  - Microsoft Windows .NET Server。至少 128MB 記憶體。
  - Microsoft Windows 2000 Professional/Server 含 SP1。至少 128MB 記憶體。
  - Microsoft Windows NT Server/Workstation 4.0 含 SP6 或更新版。至少 64MB 記憶體。

  Novell™ NetWare

  - NetWare 5.1 含 SP4。配備 Pentium II 或更快速處理器的伺服器級個人電腦。至少 128MB 記憶體。
  - NetWare 6.0 含 SP2。配備 Pentium II 或 AMD K7 處理器的伺服器級個人電腦。至少 256MB 記憶體。

  Novell Cluster Services

  - Novell Cluster Services 1.01 for NetWare 5.1。兩台配備 550MHz Pentium III 或更快速處理器的伺服器級個人電腦。至少 1024MB 記憶體。

  注意：NetWare 使用者：要管理 NetWare 伺服器，必須將一台 Windows .NET/2000/NT 電腦安裝成「資料伺服器」。

- 70MB 可用磁碟空間
- 必須安裝下列網路通訊協定與服務：Windows .NET/2000 或 NT Server/Workstation 上必須執行 TCP/IP、Microsoft Network 和 RPC 服務。安裝的 NetWare 伺服器上必須執行 IP、IPX 或 IPX/SPX。

資料伺服器

- 450MHz Intel Pentium III 同級或更快速的處理器
- 作業系統：
  - Microsoft Windows .NET Server
  - Microsoft Windows 2000 Professional/Server（如果要搭配 NetWare「一般伺服器」使用，則需要 Novell Client32™ for Windows .NET/2000/NT）。
  - Microsoft Windows NT Server/Workstation 4.0 含 SP6
- 建議配備 256MB 以上的記憶體
- 70MB 可用磁碟空間
- 90MB 可用磁碟空間（如果含安裝 Control Manager 代理程式）
- 必須安裝下列網路通訊協定與服務：TCP/IP、Microsoft Network、NWLink、IPX、IPX/SPX、NetBIOS Compatible Transport Protocol、NetWare Gateway Service、RPC services for NetWare 及 RPC 服務。

管理主控台

- 作業系統：
  - Windows .NET Server
  - Windows XP Home/Professional
  - Windows 2000 Professional/Server 含 SP1
  - Windows NT 4.0 Server/Workstation 含 SP6
  - Windows Me/98/95
- 1024x 768 或更高解析度的顯示器
- 必須安裝下列網路通訊協定與服務：TCP/IP、Microsoft Network 與 RPC 服務。

安裝方式

這一節將會幫助您選擇最適合在您的網路上安裝 ServerProtect 的方式。以下安裝方式的焦點集中在區域網路（LAN）上，不過您也可以用 TCP/IP 透過廣域網路（WAN）來管理 ServerProtect。請參照第 2 章 “透過廣域網路管理 ServerProtect”小節。

ServerProtect 的安裝方式分為以下幾種：

- 在 Windows .NET/2000/NT 環境下
- 在 NetWare 環境下
- 在 Windows .NET/2000/NT 和 NetWare 雙重環境下

指定您的安裝環境

Trend Micro ServerProtect 支援 Windows .NET/2000/NT 伺服器 / 工作站和 Novell NetWare 伺服器等多種平台。每種安裝方式各有不同的程序。

第一次在網路上安裝 ServerProtect 時，必須將目標伺服器設為「資料伺服器」，再設定將「一般伺服器」加入「資料伺服器」。「資料伺服器」至少要有一個 ServerProtect 網域，才能夠管理其「一般伺服器」。請參照 ServerProtect 網域 。

注意：如果有許多伺服器集中分佈在幾個不同地區，請在每個地區各安裝一台「資料伺服器（IS）」。請參照第 1 章 “資料伺服器秘訣”小節，來獲得有關「資料伺服器」的秘訣。

下表顯示每種 ServerProtect 安裝元件所需的不同安裝環境。

ServerProtect 安裝元件	Windows XP/Me/98/95	Windows.NET/2000/NT	NetWare
資料伺服器	否	是	否
一般伺服器	否	是	是
管理主控台	是	是	否

2-1 ServerProtect 安裝環境

在 Windows .NET/2000/NT 環境下

若是第一次安裝 ServerProtect，而且網路上的所有伺服器都執行 Windows .NET/2000/NT，則安裝程序非常簡單。

要在 Windows .NET/2000/NT 環境下部署 ServerProtect，請執行下列步驟：

1. 安裝「資料伺服器」。請參照第 2 章 “安裝資料伺服器”小節。
2. 在「資料伺服器」電腦上安裝「一般伺服器」。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。
3. 在「資料伺服器」電腦上安裝「管理主控台」。請參照第 2 章 “安裝管理主控台”小節。您可以在網路連線的任何 Windows XP / .NET / 2000 / NT 4.0 / Me / 98 / 95 電腦上安裝其他「管理主控台」。

   秘訣： 不論何時，「資料伺服器」僅能被一個「管理主控台」管理。

4. 更新 ServerProtect 病毒碼、掃瞄引擎與程式檔案。請參照第 3 章 “設定更新”小節。
5. 建立其他 ServerProtect 網域來管理您的「一般伺服器」。請參照第 3 章 “建立 ServerProtect 網域”小節。

6. 使用「管理主控台」安裝其他 .NET/2000/NT「一般伺服器」。請參照第 2 章 “從管理主控台安裝一般伺服器”小節。

最初安裝時，步驟 1、2、3 可以同時執行。

在 NetWare 環境下

若是在 NetWare 環境下安裝 ServerProtect，您還必須有一台 Windows .NET/2000/NT 伺服器 / 工作站，以安裝「資料伺服器」與「管理主控台」。

注意：「一般伺服器」必須能夠找得到負責管理它的「資料伺服器」。所以安裝工作一開始要先在 Windows 伺服器上安裝「資料伺服器」。

要在 NetWare 環境下部署 ServerProtect，請執行下列步驟：

1. 安裝「資料伺服器」。請參照第 2 章 “安裝資料伺服器”小節。
2. 在「資料伺服器」電腦上安裝「一般伺服器」。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。
3. 在「資料伺服器」電腦上安裝「管理主控台」。請參照第 2 章 “安裝管理主控台”小節。
4. 在網路上的 NetWare 伺服器上安裝「一般伺服器」。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。
5. 更新 ServerProtect 病毒碼、掃瞄引擎與程式檔案。請參照第 3 章 “設定更新”小節。
6. 建立其他 ServerProtect 網域來管理您的「一般伺服器」。請參照第 3 章 “建立 ServerProtect 網域”小節。
7. 使用「管理主控台」安裝其他 NetWare「一般伺服器」。請參照第 2 章 “從管理主控台安裝一般伺服器”小節。

最初安裝時，步驟 1、2、3 可以一起執行。等「資料伺服器」安裝完成後再安裝 NetWare「一般伺服器」。

在 Windows .NET/2000/NT 和 NetWare 雙重環境下

若在 Windows .NET/2000/NT 和 NetWare 雙重環境下安裝 ServerProtect，請選擇一台 Windows .NET/2000/NT 伺服器做為「資料伺服器」來管理「一般伺服器」。

以下安裝方式顯示如何將「一般伺服器」分類歸屬於個別的 ServerProtect NT（NT）與 NetWare（NW）網域之下。由下圖可以看出如何運用三層式架構的概念從另一台 Windows 電腦控制 ServerProtect。

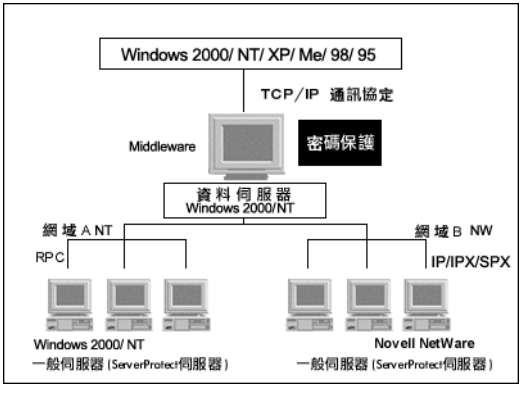


圖 2-1 雙重環境下的設定

要在 Windows .NET/2000/NT 和 NetWare 雙重環境下部署 ServerProtect，請執行下列步驟：

1. 安裝「資料伺服器」。請參照第 2 章 “安裝資料伺服器”小節。
2. 在「資料伺服器」電腦上安裝「一般伺服器」。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。

3. 在「資料伺服器」電腦上安裝「管理主控台」。請參照第 2 章 “安裝管理主控台”小節。您可以在網路連線的任何 Windows XP / .NET / 2000 / NT 4.0 / Me / 98 / 95 電腦上安裝其他「管理主控台」。

注意：在同一時間，「資料伺服器」僅能被一個「管理主控台」管理。

4. 在網路上的 NetWare 伺服器上安裝「一般伺服器」。請參照第 2 章 “從安裝程式安裝一般伺服器”小節。
5. 更新 ServerProtect 病毒碼、掃瞄引擎與程式檔案。請參照第 3 章 “設定更新”小節。
6. 建立其他 ServerProtect 網域來管理您的「一般伺服器」。請參照第 3 章 “建立 ServerProtect 網域”小節。
7. 使用「管理主控台」安裝其他「一般伺服器」（.NET/2000/NT 與 NetWare）。請參照第 2 章 “從管理主控台安裝一般伺服器”小節。

最初安裝時，步驟 1、2、3 可以一起執行。等「資料伺服器」安裝完成後再安裝 NetWare「一般伺服器」。

透過廣域網路管理 ServerProtect

您可以透過 WAN 從多個不同位置管理 ServerProtect，但是為確保適當的網路效能，趨勢科技建議您將「資料伺服器」跟它所管理的「一般伺服器」安裝在網路的同一個實體區段。

例如，如果要從位在德國的「管理主控台」管理位在日本的「一般伺服器」，則管理這台「一般伺服器」的「資料伺服器」最好也在日本。

注意：為確保適當的網路效能，請將 ServerProtect「資料伺服器」跟它所管理的「一般伺服器」安裝在 WAN 的同一個實體區段。

由於「管理主控台」使用 TCP/IP 與「資料伺服器」進行通訊，因此對大部分公司而言，從內部網路內的任一點都可以很容易地管理 ServerProtect。

安裝 ServerProtect 之前

無論安裝伺服器軟體或進行昇級，為了減少安裝本軟體時對使用者造成的影響，建議您在非工作時間以及完整備份後才進行。

另外，先在測試伺服器上安裝本程式也是很好的方法，這樣如果有任何安裝上的問題，可以在問題解決後再真正安裝到生產伺服器。安裝 ServerProtect 之前，必須確定已仔細閱讀「安裝方式」一節。請參照第 2 章 “安裝方式”小節。

注意：您必須以管理員權限登入，才能安裝 ServerProtect。

安裝 ServerProtect

第一次安裝時，趨勢科技建議您安裝完整的 ServerProtect，包括「管理主控台」、「資料伺服器」以及「一般伺服器」。

這一節將引導您完成 ServerProtect 的安裝程序。

安裝完整版的 ServerProtect

要安裝完整的 ServerProtect（包括「管理主控台」、「資料伺服器」以及「一般伺服器」），請在 Windows .NET/2000/NT 伺服器 / 工作站

電腦上執行安裝程式。如果在 Windows XP/98/95/Me 電腦上執行安裝程式，將只能安裝 ServerProtect 「管理主控台」。

請執行下列步驟來安裝完整的 ServerProtect：

1. 插入 Enterprise 光碟片，然後執行 SETUP.EXE，隨即顯示 ServerProtect 歡迎畫面。

圖 2-2 ServerProtect 歡迎畫面

2. 按「下一步」，隨即顯示「軟體授權合約」畫面。您必須同意合約內容，才能繼續執行安裝程式。

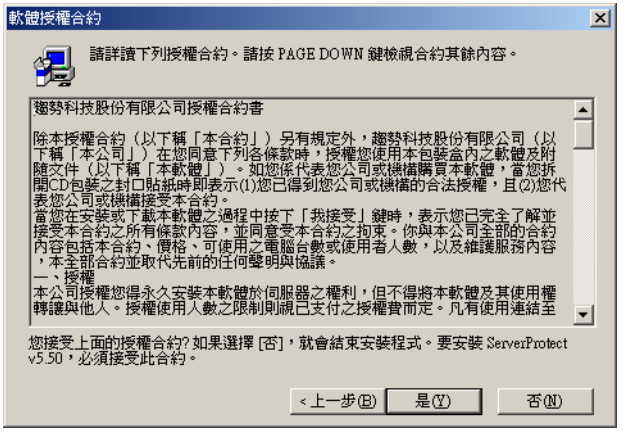


圖 2-3 「軟體授權合約」畫面

3. 按下「是」，ServerProtect 便會檢查啟動磁區是否感染病毒。

圖 2-4 掃瞄結果「資訊」視窗

4. 按下「確定」以繼續安裝。隨即顯示使用者資訊畫面。

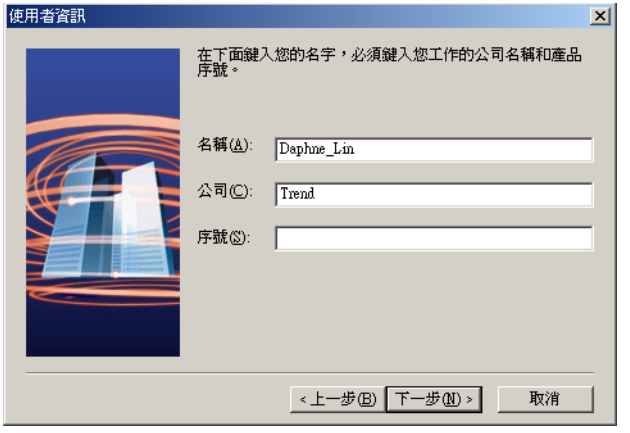


圖 2-5 ServerProtect「使用者資訊」畫面

5. 輸入您的使用者資訊，包括產品序號。

如果沒有產品序號，您可以將欄位保留空白。這樣會安裝 30 天試用版。

6. 按「下一步」繼續執行安裝程式。「選取元件」畫面隨即開啟。

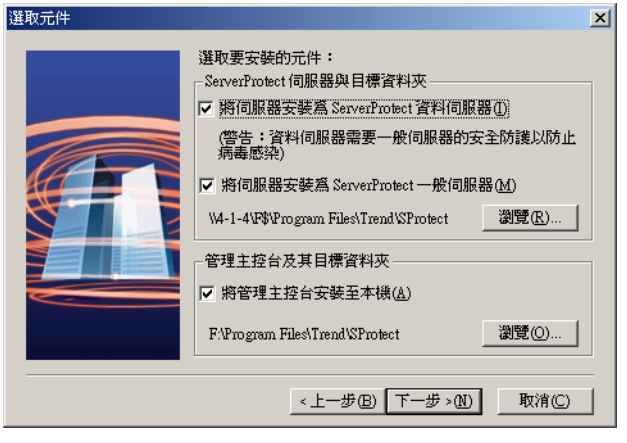


圖 2-6 ServerProtect「選取元件」畫面

7. 在「選取元件」畫面上，您必須選取要安裝的元件。有三個元件（「管理主控台」、「資料伺服器」及「一般伺服器」），請選擇您所需要的元件進行安裝。您可以選擇隱藏的共用磁碟機（如 C$ 或 D$），當作目標資料夾。

   預設的安裝路徑是：

   < 磁碟機 >:\Program Files\Trend\Sprotect

   注意： 為了保護「資料伺服器」，建議您在同一台電腦上安裝「一般伺服器」。

8. 按「下一步」。如果您選擇安裝「一般伺服器」或「資料伺服器」，隨即顯示「輸入登入資訊」畫面。在「登入資訊」下的「網域名稱」、「使用者名稱」、「密碼」及「確認密碼」欄位中輸入正確資料，然後按「下一步」。

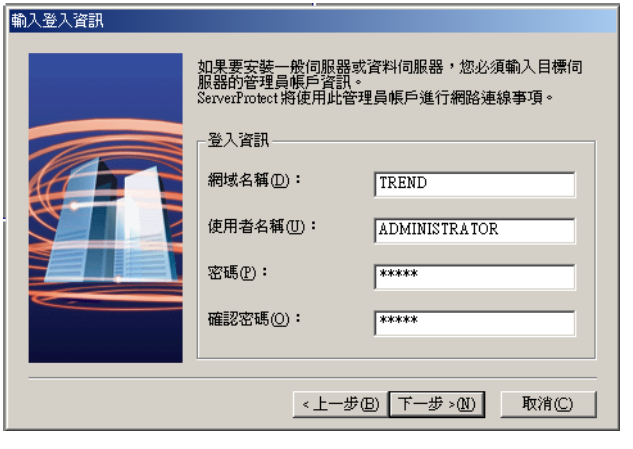


圖 2-7 ServerProtect「輸入登入資訊」畫面

9. 依照每個元件的指示完成 ServerProtect 安裝程式。

安裝管理主控台

管理員可以利用 「管理主控台」從遠端管理 ServerProtect 「一般伺服器」。「管理主控台」是 ServerProtect 與使用者互動的元件，它可以跟「資料伺服器」與 「一般伺服器」安裝在同一台電腦上，也可以安裝在另一台電腦。

安裝 「管理主控台」：

1. 執行安裝程式，同時完成必要的步驟來提供產品資訊。
2. 從 「選取元件」畫面上選取 「將管理主控台安裝至主機」選項方塊。請參閱圖 2-6 您可以按 「瀏覽」按鈕變更本機安裝路徑。「管理主控台」必須安裝在 Windows XP / .NET / 2000 / NT 4.0 / Me / 98 / 95 環境。

注意：趨勢科技不支援遠端安裝 「管理主控台」。

3. 如果想將自己設成唯一可從 Windows 「開始」功能表看到 ServerProtect 程式的人，請按下 「個人程式資料夾」。否則，請按下 「共用程式資料夾」。按下 「確定」，隨即顯示 「開始複製檔案」視窗。
4. 按 「下一步」以繼續執行安裝程式。安裝程式隨即開始複製所有的程式元件，並啟動所有服務。複製完所有程式元件後，安裝程式會顯示 「安裝完成」畫面。

圖 2-8 ServerProtect「安裝完成」畫面

5. 按下「完成」，「Trend ServerProtect 管理主控台 5.5」視窗隨即開啟。

圖 2-9 選取資料伺服器畫面

6. 請以下列方式之一選擇您要「管理主控台」管理的「資料伺服器」：

- 從清單中選取

- 輸入伺服器名稱
- 輸入 IP 位址

注意：如果「資料伺服器」是位於和安裝「管理主控台」不同的網路區段上，清單上則不會顯示該伺服器。

7. 按下「確定」儲存您所做的變更，或按下「取消」來關閉視窗但不儲存變更。

安裝資料伺服器

「資料伺服器」負責管理「一般伺服器」，且回應由「管理主控台」發出的指令。

如果您要安裝「資料伺服器」...

1. 執行安裝程式，同時完成必要的步驟來提供產品資訊。
2. 在「選取元件」畫面上，選取「將伺服器安裝為 ServerProtect 資料伺服器」核取方塊。請參閱圖 2-6。

   如果要從遠端安裝「資料伺服器」，請按「瀏覽」來尋找目標伺服器。隨即顯示「ServerProtect 安裝路徑選項」視窗。

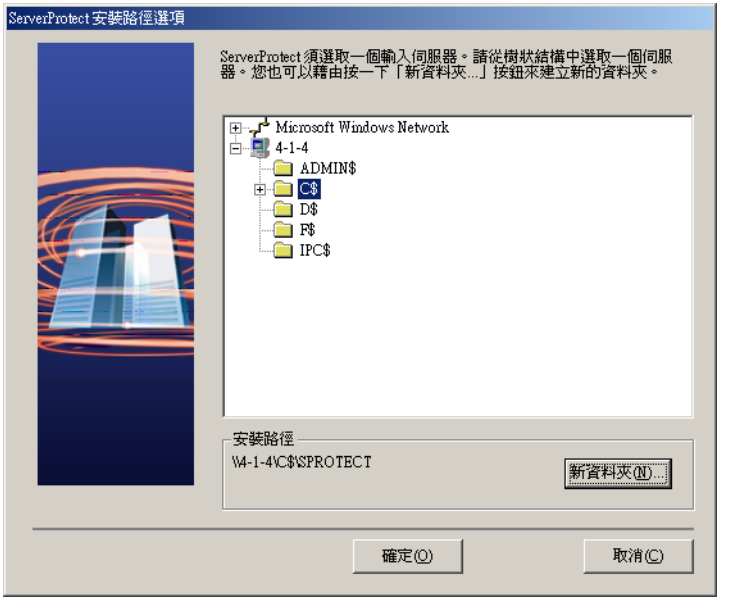


圖 2-10 「ServerProtect 安裝路徑選項」畫面

所有可用的 Windows .NET/2000/NT 伺服器將顯示在畫面上。

3. 在伺服器中按兩下您要的伺服器，接著選擇安裝「ServerProtect 資料伺服器」檔案的路徑。如果要將安裝路徑變更為新資料夾，請按下「新資料夾」，再按「確定」。

4. 在「選取元件」畫面上按「下一步」隨即顯示「輸入登入資訊」畫面。請參閱 圖 2-7。

5. 在「登入資訊」下的「網域名稱」、「使用者名稱」、「密碼」及「確認密碼」欄位中輸入正確資料，然後按「下一步」。
隨即顯示「設定資料伺服器」視窗。

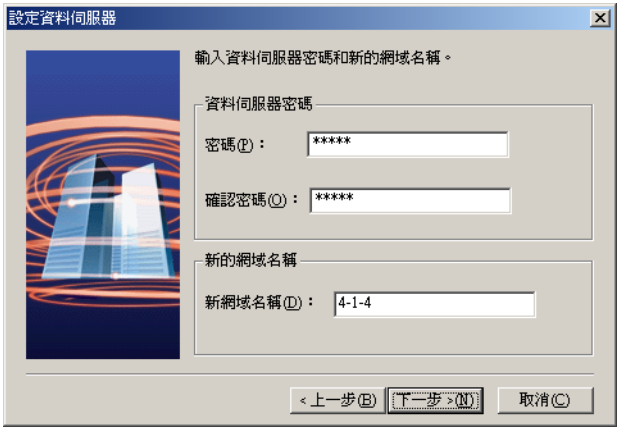


圖 2-11 ServerProtect「設定資料伺服器」畫面

6. 隨即顯示「設定資料伺服器」畫面。您必須輸入密碼，以防未經授權的使用者企圖透過主控台來連到「資料伺服器」。

7. 按「下一步」，隨即顯示「開始複製檔案」視窗。請檢查列在畫面上的資訊。

8. 按「下一步」繼續安裝程式，ServerProtect 現在將開始複製所有的程式元件，並啟動所有服務。如果所有的程式元件都完成複製，同時所有的服務都啟動成功，便會顯示「安裝完成」畫面。

圖 2-12 ServerProtect「安裝完成」畫面

9. 按下「完成」，隨即顯示「立即安裝 Control Management 代理程式」畫面。

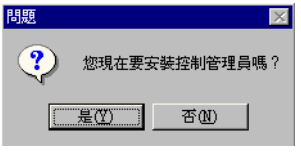


圖 2-13 「Control Manager 代理程式安裝」畫面

10. 按下「是」進行安裝 Control Manager 代理程式，否則按下「否」來關閉安裝程式。

安裝一般伺服器

第一次安裝「一般伺服器」時，要使用安裝程式。之後即可用「管理主控台」安裝其他「一般伺服器」。

從安裝程式安裝一般伺服器

安裝程式可讓您在本機安裝「一般伺服器」，也可以採用遠端安裝。

注意：將 NetWare 伺服器安裝成「一般伺服器」前，必須有可以使用的「資料伺服器」。「資料伺服器」必須安裝在 Windows .NET/2000/NT 電腦上。

如果您要從安裝程式安裝「一般伺服器」...

1. 執行安裝程式，同時完成必要的步驟來提供產品資訊。
2. 在「選取元件」畫面上，選取「將伺服器安裝為 ServerProtect 一般伺服器」核取方塊。請參閱圖 2-6。

   如果要從遠端安裝「一般伺服器」，請按「瀏覽」來尋找目標伺服器。隨即顯示「ServerProtect 安裝路徑選項」畫面。

   按下「新資料夾」來建立新的目標資料夾。

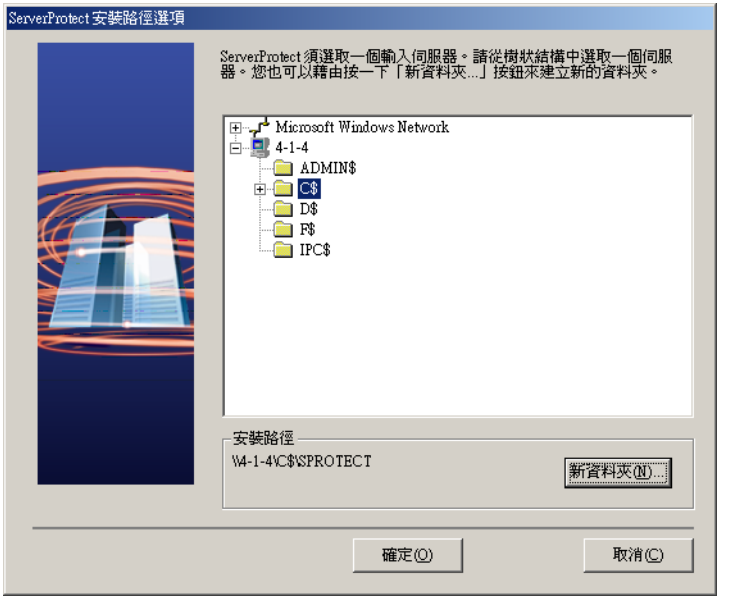


圖 2-14 ServerProtect「安裝路徑選項」畫面

3. 在伺服器中按一下需要的網路以展開樹狀目錄，再按下您要的伺服器。

4. 按下「確定」，隨即顯示「輸入密碼」視窗。

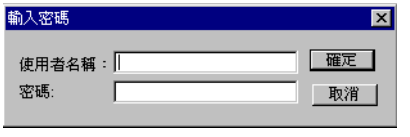


圖 2-15 ServerProtect 目標伺服器登入畫面

5. 輸入目標伺服器的管理員使用者名稱與密碼。樹狀目錄上便會顯示目標伺服器的本機磁碟機。

6. 選擇「一般伺服器」的安裝路徑，再按下「確定」。如果要安裝到新資料夾，請按下「新資料夾」後，再按「確定」。

7. 在「選取元件」畫面上按「下一步」，隨即顯示「輸入登入資訊」畫面。請參閱圖 2-7。
   如果要安裝 NetWare「一般伺服器」，請在「選取元件」畫面中指定通訊協定，再按「下一步」。

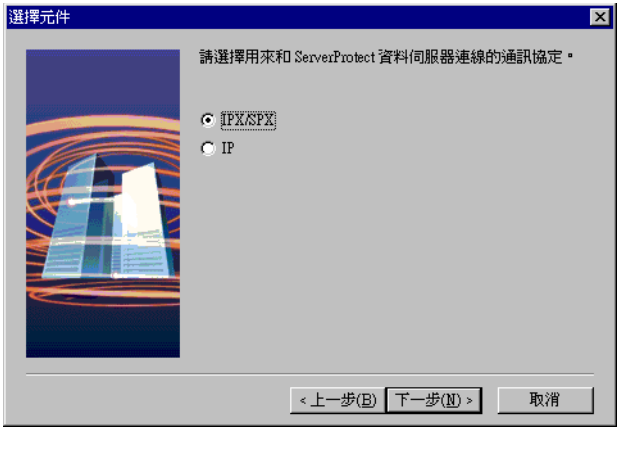


圖 2-16 「選取元件」視窗

注意：如果選取「IP」，請輸入目標伺服器的固定 IP 位址，再按「下一步」。

8. 在「登入資訊」下的「網域名稱」、「使用者名稱」、「密碼」及「確認密碼」欄位中輸入正確資料，然後按「下一步」。

9. 按「下一步」，然後在接下來的視窗中按「確定」以繼續安裝。隨即顯示「ServerProtect 安裝路徑選項」畫面。

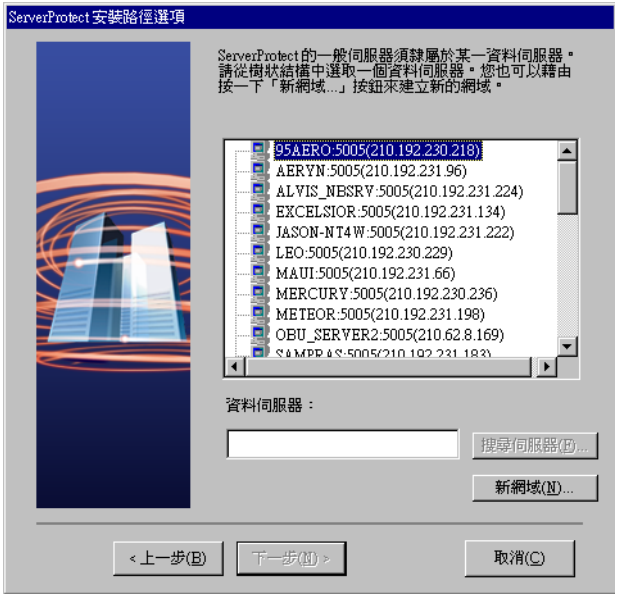


圖 2-17 「ServerProtect 安裝路徑選項」畫面

10. 請以下列方式之一尋找「資料伺服器」：

    - 在瀏覽目錄下的文字方塊中輸入「資料伺服器」的名稱或 IP 位址。按下「搜尋伺服器」按鈕。
    - 在瀏覽目錄中按兩下要當作「資料伺服器」的目標電腦。

    如果要建立新的 ServerProtect 網域，請按「新網域」。

注意：如果「資料伺服器」是位於和「一般伺服器」不同的網路上，則該伺服器可能不會顯示在清單中。這樣一來，您可能必須手動輸入「資料伺服器」的名稱或 IP 位址，來協助安裝程式尋找伺服器。

11. 按「下一步」，隨即顯示「輸入 ServerProtect 資料伺服器密碼」畫面。
12. 輸入「資料伺服器」的密碼。這是您在安裝「資料伺服器」時指定的密碼。

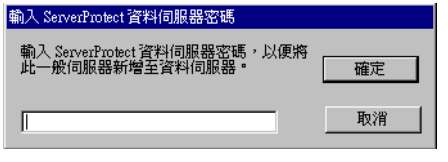


圖 2-18 「輸入 ServerProtect 資料伺服器密碼」視窗

13. ServerProtect 便會複製所有程式元件，並啟動所有服務。隨即顯示「安裝完成」畫面。請參閱圖 2-12。
14. 按下「完成」，Windows 工作列上便會新增一個 ServerProtect 圖示（ ），提醒您掃瞄程式已經安裝成功並且已經啟動。

從管理主控台安裝一般伺服器

「管理主控台」所登入的「資料伺服器」應該至少負責管理一台「一般伺服器」。因為 ServerProtect 將使用現有的伺服器當作安裝新的「一般伺服器」的來源，所以該伺服器必須與即將安裝的伺服器屬於同一類型。例如，安裝 NetWare 伺服器就需要 NetWare 來源的 ServerProtect 伺服器。

在伺服器樹狀目錄所顯示的伺服器中，如果只有一台「一般伺服器」與即將安裝的伺服器同類型，便會自動選擇這台伺服器當作來源伺服器。

如果您要從「管理主控台」安裝「一般伺服器」...

1. 在網域瀏覽目錄中選取要將伺服器加入的網域。
2. 執行下列任一種方式：
   - 從主功能表選取「網域 | 安裝新的 SPNT」或「網域 | 使用 IPX 安裝新的 SPNW」（使用 IP 安裝新的 SPNW）
   - 在上個步驟所選取的網域上按滑鼠右鍵，並在即現式功能表上按「安裝新的 SPNT」或「使用 IPX 安裝新的 SPNW」（使用 IP 安裝新的 SPNW）

   「選擇來源伺服器」視窗隨即開啟。
3. 從清單方塊中選取一台現有的「一般伺服器」，再按「確定」，隨即顯示確認視窗。
4. 按下「確定」，「新增伺服器至網域」視窗隨即開啟。
5. 使用下列任一種方式將伺服器新增至網域：
   - 在左邊的清單方塊中選取伺服器名稱
   - 在「伺服器名稱」中輸入伺服器名稱
6. 按下「新增」，將伺服器名稱加入在右邊的清單方塊中。
7. 重複步驟 5，直到您將所有要加入新網域的伺服器都加到右邊的清單方塊中為止。如果要移除先前加入的伺服器，請反白選取右邊清單方塊中的名稱，再按「移除」按鈕。按下「全部移除」按鈕會清除右邊的清單方塊。
8. 按下「確定」儲存您所做的變更，或按下「取消」來關閉對話方塊而且不新增伺服器。

注意：新增與安裝「一般伺服器」是兩個不同作業。新增只是將現有的「一般伺服器」從一台「資料伺服器」移到另一台「資料伺服器」；安裝則是從遠端安裝軟體，以登錄新的「一般伺服器」。

透過 Microsoft SMS 部署 ServerProtect

您可以透過 Windows .NET/2000/NT 平台上的 Microsoft Systems Management Server （SMS）版本 1.2/2.0 來安裝 Trend Micro ServerProtect。

注意：您必須在 Windows .NET/2000/NT 伺服器上安裝 Microsoft Systems Management Server （SMS）軟體，才能透過這種方式部署用戶端軟體。請先確定 Windows 系統目錄中含有 MSVCRT20.DLL 檔，以便可以從 SMS 軟體配送站台成功部署 ServerProtect。

以下列出透過 Microsoft SMS 版本 1.2 來部署 ServerProtect 的部署程序步驟說明。Microsoft SMS 版本 2.0 的部署程序完全相同，但顯示的畫面可能稍有差異。

要透過 Microsoft SMS 部署 ServerProtect，請執行下列步驟：

1. 開啟 Microsoft SMS 管理員。
2. 在 SMS 管理員的圖示列上按「套裝軟體」。
3. 在主功能表上按「檔案 | 開啟新檔」，「套裝軟體內容」視窗隨即開啟。

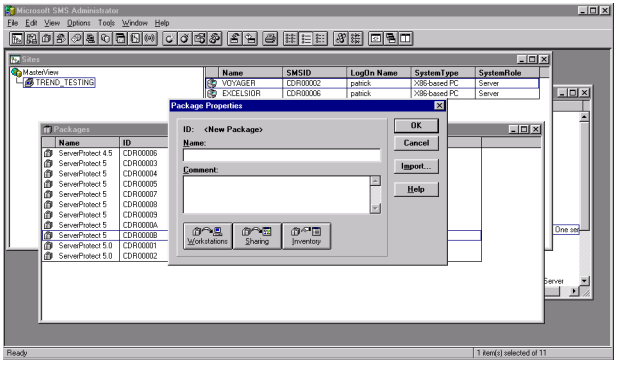


圖 2-19 Microsoft SMS 管理員視窗

4. 按下「匯入」按鈕。瀏覽到安裝 ServerProtect 軟體的 PDF 檔（套裝軟體說明檔）所在目錄。按下 setup.pdf 檔，再按「確定」。ServerProtect 軟體的預設目錄如下：

   < 磁碟機 >:\program files\Trend\Sprotect\SMS\

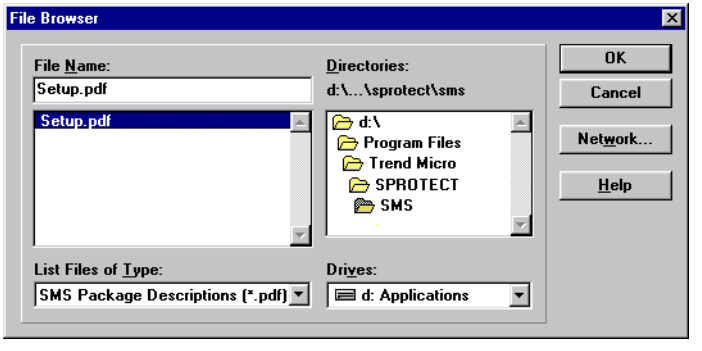


圖 2-20 「檔案瀏覽器」視窗

PDF 檔的說明在「SMS 管理員套裝軟體內容」視窗中將顯示為「ServerProtect 5」。

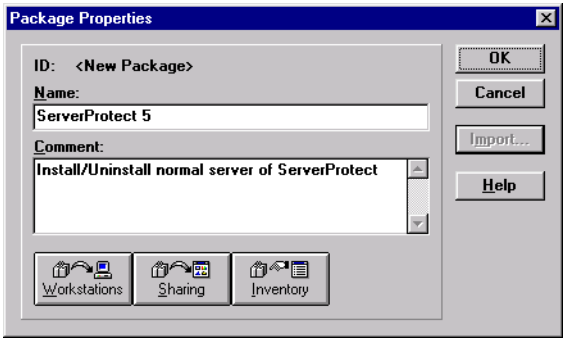


圖 2-21 SMS 管理員套裝軟體內容設定視窗

5. 在 SMS 管理員中輸入安裝檔案的來源。在「SMS 管理員套裝軟體內容」設定視窗中按「工作站」按鈕，接著瀏覽到安裝來源檔的網路位置。

< 磁碟機 >:\< 資料伺服器目錄 >\SMS

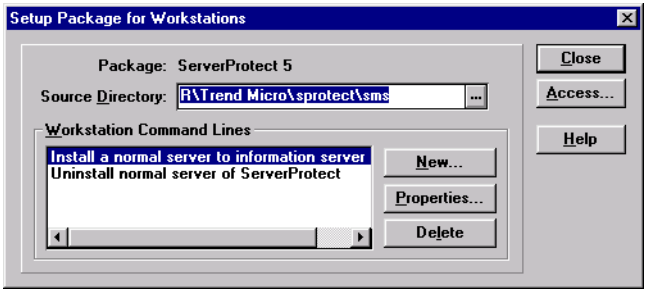


圖 2-22 「Setup Package for Workstations」視窗

6. 按下「確定」，回到「SMS 管理員套裝軟體內容」設定視窗，再按下「關閉」按鈕。接下來的工作便是選擇要安裝軟體的伺服器 / 工作站。

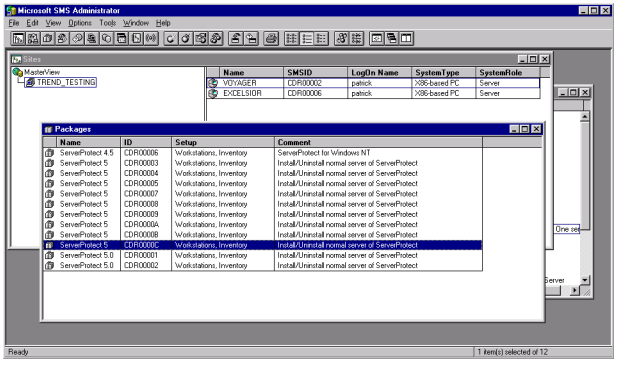


圖 2-23 顯示新建立之套裝軟體的 SMS 管理員套裝軟體視窗

注意： SMS 管理員視窗中有一個瀏覽視窗。請將您剛建立的 SMS 套裝軟體拖曳到目標伺服器 / 工作站上。「工作詳細資料」設定視窗隨即開啟。

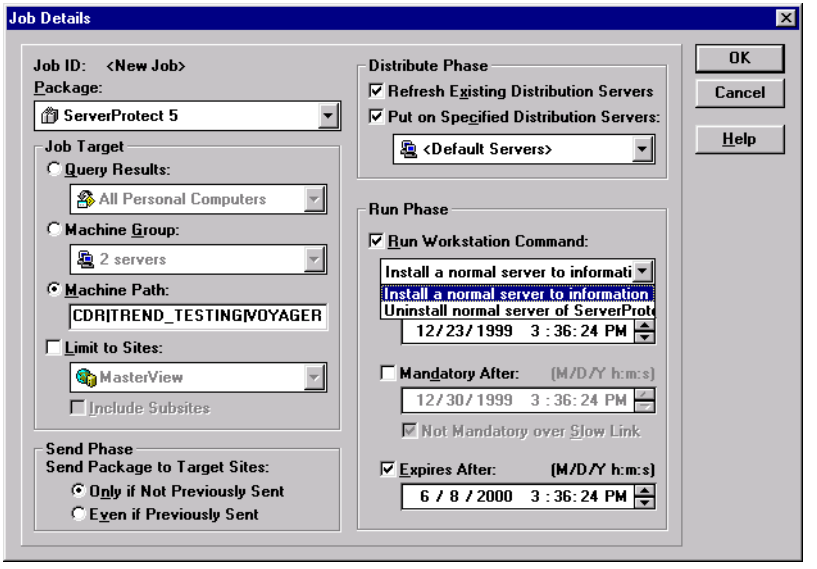


圖 2-24 工作詳細資料設定視窗

7. 設定工作詳細資料，來自訂軟體安裝 / 移除。「執行階段」欄中的設定可讓您預約軟體的安裝 / 移除。

成功設定好工作後，安裝 / 移除會暫停，而且會出現在 SMS 管理員的「工作」視窗中。

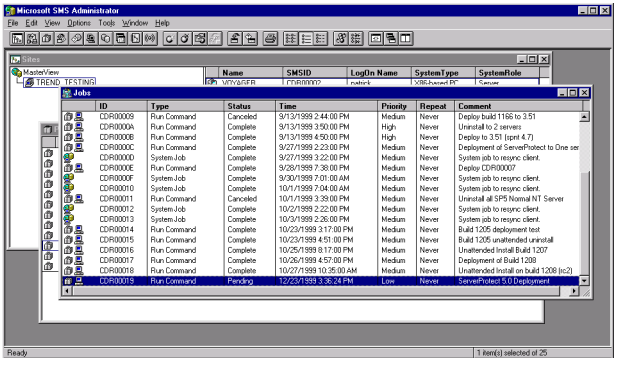


圖 2-25 SMS 管理員工作視窗

自動安裝 ServerProtect

從遠端安裝 Windows .NET/2000/NT 「一般伺服器」時，自動安裝 ServerProtect 的功能相當有用。

要自動安裝 Windows .NET/2000/NT 的 ServerProtect，請執行下列步驟：

1. 安裝 「資料伺服器」。請參照第 2 章 “安裝資料伺服器”小節。
2. 切換到 「資料伺服器」的 SMS 資料夾，將資料夾分享出來。並確認要安裝 「一般伺服器」的伺服器能存取此資料夾。如果您要執行自動安裝到多台伺服器，請將 SMS 資料夾連線到目標伺服器。
3. 在目標伺服器上，開啟 DOS 提示字元，切換到 「資料伺服器」的 SMS 資料夾或磁碟機，並輸入下列指令：

   < 磁碟機 >:\setup -SMS -s -m"SPNT5"

例如：

a. 在目標伺服器上，將 SMS 資料夾連線到磁碟機 "M"。
b. 開啟 DOS 提示字元。
c. 鍵入 "M:"，以便將磁碟機切換到 M:
d. 鍵入指令：M:\setup -SMS -s -m"SPNT5"
e. 按 「Enter」鍵。

自動安裝會開始執行，並將目標電腦登錄到 「資料伺服器」。

如果用自動安裝，「一般伺服器」會被安裝在 SMS 網域。在執行自動安裝時，無法變更網域。但您可以先安裝所有的 「一般伺服器」，然後將 SMS 網域重新命名。

您也可以指定路徑，以自動安裝 ServerProtect。例如，如果要將 ServerProtect 安裝到 「D:\UtilityAntiVirus\Sprotect」這個路徑，請執行下列步驟：

1. 找到來源資料夾內的 Setup.ini 檔。
2. 新增下列各行：

   [CommonSection]

   ServerTargetUNCPath=D$\Utility\AntiVirus\Sprotect

   其中：

   ServerTargetUNCPath：設定「一般伺服器」的安裝位置。

若要授與產品序號給安裝的「一般伺服器」，請將下列各行新增到來源資料夾內的 Setup.ini 檔。

[CommonSection]

ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX

其中：

XXXX-XXXX-XXXX-XXXX-XXXX：代表合法的產品序號。

您可能無法在 SMS 網域底下登錄「一般伺服器」，這是由「資料伺服器」上使用的網域控制器所造成的問題。如果要解決這個問題，請在使用自動安裝之前設定 IP 位址。

要設定 IP 位址，請執行下列步驟：

1. 開啟 SMS 資料夾中的 Setup.ini 檔。
2. 將 AgentName 旁的主機名稱換成它的 IP 位址，然後儲存檔案。

移除 ServerProtect

由於 ServerProtect 由三個元件組成，三個元件可一起或分別移除。以下幾節將說明個別移除的詳細內容。

移除一般伺服器

每種環境各有不同的移除程序

移除 Windows .NET/2000/NT 的一般伺服器

在 Windows .NET/2000/NT 環境下，有兩種方法可移除「一般伺服器」：

要從遠端移除 Windows .NET/2000/NT 的「一般伺服器」，請執行下列步驟：

1. 在「管理主控台」上選取「一般伺服器」。
2. 在主功能表上按「網域 | 解除安裝 ServerProtect」。

   所有選取的伺服器都將以遠端方式移除。

要在本機移除 Windows .NET/2000/NT 的「一般伺服器」，請執行下列步驟：

1. 按下「開始 | 設定 | 控制台 | 新增 / 移除程式」。
2. 按下 ServerProtect 5.xx 項目（xx 代表次要版本編號，也就是 5.0、5.35），再按「新增 / 移除」。

移除 NetWare 的一般伺服器

在 NetWare 環境下，有兩種方法可移除「一般伺服器」：

要從遠端移除 NetWare 的「一般伺服器」，請執行下列步驟：

1. 在「管理主控台」上選取「一般伺服器」。
2. 在主功能表上按「網域 | 解除安裝 ServerProtect」。

所有選取的伺服器都將以遠端方式移除。

要在本機移除 NetWare 的「一般伺服器」，請執行下列步驟：

1. 在 ServerProtect 監控畫面上按「ESC」鍵，再按下「是」來卸載 ServerProtect 模組。
2. 用 Novell Client for Windows 刪除下列項目：

   SYS:SYSTEM\SPNW.NCF

   SYS:LOGIN\SPROTECT

   <Volume>:Sprotect 目錄
3. 從 ServerProtect「資料伺服器」刪除下列系統登錄內容：

   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\CurrentVersion\InformationServer\（指定的 ServerProtect 一般伺服器）

   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\CurrentVersion\NW\（指定的 ServerProtect 一般伺服器）

移除資料伺服器

ServerProtect 只容許您在本機移除「資料伺服器」服務。

要移除 Windows .NET/2000/NT 的「資料伺服器」，請執行下列步驟：

1. 按下「開始 | 控制台 | 新增 / 移除程式」。
2. 按下「ServerProtect 資料伺服器」，再按「新增 / 移除」。

移除管理主控台

ServerProtect 只容許您在本機移除「管理主控台」。

要從 Windows XP/.NET/2000/NT/98/95/Me 移除「管理主控台」，請執行下列步驟：

1. 按下「開始 | 控制台 | 新增 / 移除程式」。
2. 按下「ServerProtect 管理主控台」，再按「新增 / 移除」。

第 3 章

管理 ServerProtect

這一章介紹管理 ServerProtect 不可或缺的工具。其他管理工具請參閱「管理主控台」的線上說明。

本章內容如下：

- 使用管理主控台
- ServerProtect 網域管理
- 資料伺服器管理
- 一般伺服器管理
- 部署更新檔
- 工作管理
- 設定通知訊息
- 掃瞄病毒
- 使用即時掃瞄
- 使用立即掃瞄（手動掃瞄）
- 預約掃瞄

使用管理主控台

ServerProtect 可讓您在 32 位元 Windows 電腦上，透過單一且具有可攜性的「管理主控台」，管理多台 Windows .NET/2000/NT/NetWare 伺服器與工作站。透過密碼保護，主控台可確保只有授權的管理員能夠修改 ServerProtect 設定。

開啟管理主控台

您可以從網路上任何 32 位元的 Windows 電腦執行「管理主控台」。

要執行「管理主控台」：

1. 按下「開始 | Trend Micro ServerProtect 管理主控台」。系統便會提示輸入管理員密碼來登入選取的「資料伺服器」。

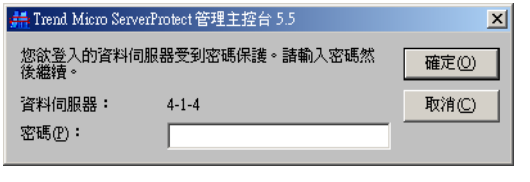


圖 3-1 「Trend Micro ServerProtect 管理主控台」登入視窗

注意：如果您管理的「資料伺服器」不止一台，ServerProtect 會提示您從清單中選擇其一，然後才能繼續下去。

2. 輸入您在「資料伺服器」安裝期間所設定的管理密碼，再按「確定」。請注意，密碼區分大小寫，而且一次只能登入一台「資料伺服器」。
3. 按下「確定」，「Trend Micro ServerProtect 管理主控台 5.5」視窗隨即開啟。

管理主控台的主畫面

ServerProtect「管理主控台」直覺式的使用者介面，讓您輕鬆使用所有設定及管理 ServerProtect 有關的功能。

圖 3-2 管理主控台的構成部分

「管理主控台」包含下列四部分：

- 主功能表
- 功能區
- 網域瀏覽目錄
- 設定區

主功能表

主功能表包含下面六個項目：

- **資料伺服器**：設定 「資料伺服器」的相關資訊，例如，備份或回復 「資料伺服器」的資訊，以及選取或移動網路上的 「資料伺服器」。
- **網域**：變更顯示在網域瀏覽目錄中的網域及伺服器組織。
- **設定**：修改掃瞄與記錄檔設定，以及設定主控台重新整理頻率。
- **檢視**：檢視 ServerProtect 記錄檔、掃瞄結果與趨勢科技病毒百科全書。
- **執行**：建立或修改工作、執行手動掃瞄、更新或還原病毒碼、掃瞄引擎或程式檔、變更 「資料伺服器」的密碼、尋找網域或伺服器等。
- **說明**：存取線上說明系統以及 ServerProtect 產品資訊。

功能區

功能區在 ServerProtect 畫面左邊，其中包含七組項目。按一下功能區中的捷徑可快速開啟功能的設定區。

- **工作群組**

  
  新工作：建立新工作

  
  現有工作：開始執行、停止、修改、移除或檢視現有的工作

- **立即掃瞄群組**

  
  立即掃瞄：設定手動 （立即）病毒掃瞄

- **掃瞄結果群組**

  
  即時掃瞄：檢視即時掃瞄的結果

  
  立即掃瞄：檢視手動掃瞄的結果


預約掃瞄：檢視由預約執行的掃瞄結果

- **更新群組**


更新：下載並部署更新檔到網路上的「一般伺服器」


還原：將網路上執行的部署動作還原到前一版

- **檢視記錄檔群組**


檢視記錄檔：檢視網路上發生之防毒事件的歷史記錄資訊

- **設定掃瞄選項群組**


即時掃瞄：設定針對網路執行的即時病毒掃瞄


例外清單：定義 ServerProtect 不掃瞄的檔案、目錄或病毒


防寫清單：防止特定檔案或目錄被修改

- **設定通知群組**


一般警訊：設定當伺服器上偵測到預設狀況時發出的一般警訊


病毒爆發警訊：設定當一定時間內發生大量的病毒爆發時發出的病毒爆發警訊

網域瀏覽目錄

網域瀏覽目錄顯示受到本軟體保護的網路元件，包括根目錄（ServerProtect 產品圖示）、分枝（網域）以及節點（ServerProtect 一般伺服器）。網域瀏覽目錄中可看到四個主要項目：

- 欄標題
- 資料伺服器
- 網域
- 一般伺服器

欄標題

網域瀏覽目錄上方的欄位顯示作業系統、病毒碼版本、掃瞄引擎版本、程式版本、即時掃瞄方向等。

在 ServerProtect 主控台以滑鼠右鍵按一下瀏覽目錄的圖示，即可為選取的元件變更設定。您可以變更網域瀏覽目錄窗格的大小。

資料伺服器

「資料伺服器」負責處理該網域的主要資料及通訊。而且「資料伺服器」還將網域連結在一起。

 資料伺服器

網域

網域是指 ServerProtect 網路上伺服器的分組。屬於相同網域的「一般伺服器」可以集中管理。ServerProtect 網域和 Windows NT 網域不同。

 ServerProtect 網域

 ServerProtect 網域上有一台中毒的一般伺服器

一般伺服器

「一般伺服器」是網路上任何安裝 ServerProtect 的伺服器。在 ServerProtect 架構中，「一般伺服器」是由「資料伺服器」來管理。

 Windows .NET/2000/NT 一般伺服器

 Novell NetWare 一般伺服器

 中毒的 Windows .NET/2000/NT 一般伺服器

 中毒的 Novell NetWare 一般伺服器

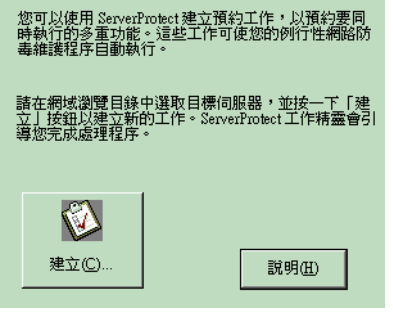
已經中斷連線或無法連線的一般伺服器

處於「病毒爆發防範策略」模式中的一般伺服器

處於「病毒爆發防範策略」模式中的中毒一般伺服器

設定區

ServerProtect 畫面右側是設定區，這裏可用來鍵入設定資料，以及檢視有關企業網路的資訊。



ServerProtect 網域管理

ServerProtect 網域是指「一般伺服器」的虛擬分組，用來簡化伺服器的識別與管理。您可隨時依照網路的需求，建立、重新命名或刪除網域。

注意：如果某個網域下有伺服器中毒，則該網域的圖示會改變，而且中毒伺服器的圖示會呈著火狀。這是要提醒您掃瞄中毒的伺服器，以防止病毒散播到整個網路。如果要移除中毒圖示，您必須將「管理主控台」中「掃瞄結果」底下的所有記錄項目全部清除乾淨。

建立 ServerProtect 網域

透過 ServerProtect 的安裝程式建立預設網域後，您可以從「管理主控台」建立新的網域。

網域名稱的長度上限是 50 個單位元組字元或 25 個雙位元組字元（用於中文、日文或韓文）。

要建立 ServerProtect 網域：

1. 執行下列一項：
   - 在主功能表上按「網域 | 新增新網域」
   - 在網域瀏覽目錄的「資料伺服器」圖示上按滑鼠右鍵，再按下「新增新網域」

   「建立新網域」視窗隨即開啟。

圖 3-3 「建立新網域」視窗

2. 在「網域名稱」文字方塊中輸入新網域的名稱。
3. 指明要新增到網域的伺服器。執行下列一項：
   - 在左邊的清單中選取伺服器
   - 在「輸入伺服器名稱」文字方塊中輸入伺服器名稱
4. 按下「新增」。
5. 重複步驟 3 和 4，直到右邊清單方塊中顯示所有您要加到新網域的伺服器為止。如果要移除伺服器，請在右邊清單方塊中選取伺服器，再按「移除」。按下「全部移除」可刪除右邊清單中的所有伺服器。
6. 按下「確定」儲存您所做的變更，或按下「取消」來關閉視窗但不建立新網域。

更改 ServerProtect 網域名稱

安裝 ServerProtect 時，安裝程式會建立一個名稱為「預設值」的網域。您可依需要從「管理主控台」變更任何現有網域的名稱。

要變更 ServerProtect 網域名稱：

1. 在網域瀏覽目錄中按一下要重新命名的網域。

2. 執行下列一項：

   - 在選取的網域上按滑鼠右鍵，再按「更改網域名稱」。
   - 在主功能表上選取「網域 | 更改網域名稱」，「更改網域名稱」視窗隨即開啟。
   - 按鍵盤上的「F2」鍵。

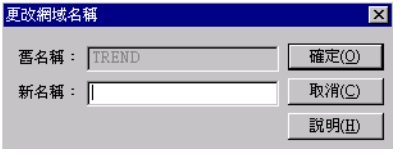


圖 3-4 「更改網域名稱」視窗

3. 在「新網域名稱」文字方塊中輸入新的網域名稱，再按「確定」。按下「取消」可關閉視窗但不儲存變更。

刪除 ServerProtect 網域

您可以刪除任何不再需要的空網域（網域內沒有任何「一般伺服器」），但不可以刪除含有「一般伺服器」的網域。

要刪除 ServerProtect 網域：

1. 在網域瀏覽目錄中選取要刪除的網域。
2. 執行下列一項：
   - 在網域上按滑鼠右鍵，再按「刪除網域」
   - 在主功能表上按「網域 | 刪除網域」
   - 按鍵盤上的「Delete」鍵

注意：您不可以刪除含有任何「一般伺服器」的網域。

在網域之間移動一般伺服器

為了加強管理，有時候您必須將「一般伺服器」從現有的網域移動到另一個網域。請在網域瀏覽目錄中選取某個網域底下的「一般伺服器」，然後將該「一般伺服器」拖曳到其他網域後放下即可。

另一種方法是在建立 ServerProtect 網域的時候移動「一般伺服器」。請參照第 3 章 “建立 ServerProtect 網域” 小節。

資料伺服器管理

「資料伺服器」負責儲存資料，以及將資料傳進與傳出各個「一般伺服器」。

如果用「資料伺服器」管理 NetWare「一般伺服器」，它還要負責傳送警訊。但是 Windows .NET/2000/NT「一般伺服器」會自行負責傳送警訊。

由於「資料伺服器」只不過是資訊的遞送系統，因此，理論上它所能管理的伺服器總數取決於可用頻寬的大小。

秘訣：對於 WAN 這一類大型網路，建議您在每個網路區段各安裝一台「資料伺服器」，以免影響網路流量。

選取資料伺服器

通常，當您開啟「管理主控台」時，ServerProtect 會提示您輸入您要登入之「資料伺服器」的使用者名稱及密碼。請注意，「資料伺服器」只容許一個「管理主控台」登入。如果您無法登入「資料伺服器」，請確定網路上沒有任何「管理主控台」連上該「資料伺服器」。

要選取「資料伺服器」：

1. 在主功能表上按「資料伺服器 | 選擇資料伺服器」，「選擇資料伺服器」視窗隨即開啟。
2. 執行下列一項：
   - 輸入「資料伺服器」的名稱或 IP 位址
   - 從清單中選取資料伺服器

     如果需要重新整理清單中的伺服器，請按下「重新整理」。

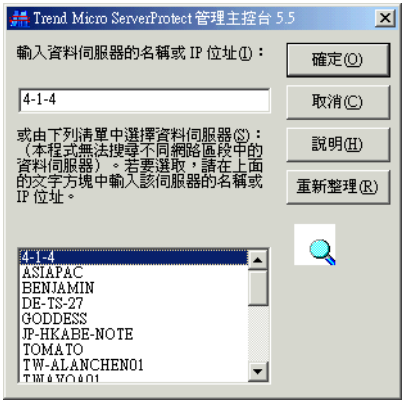


圖 3-5 Trend ServerProtect「管理主控台」視窗

3. 按下「確定」儲存您所做的變更，或按下「取消」來關閉視窗但不儲存變更。

一般伺服器管理

在 ServerProtect 架構中，「一般伺服器」是防毒的第一道防線，並由「資料伺服器」管理。「一般伺服器」位於 ServerProtect 結構最底層。下面說明 「一般伺服器」的管理方式。

在網域之間移動一般伺服器

要將 「一般伺服器」從一個 ServerProtect 網域移到另一個網域，請在網域瀏覽目錄中選取 「一般伺服器」，然後將該 「一般伺服器」拖曳到其他網域後放下即可。

在資料伺服器之間移動一般伺服器

ServerProtect 可讓您將 「一般伺服器」移到別的 「資料伺服器」。這對於減輕 「資料伺服器」的負載特別有用。

要在 「資料伺服器」之間移動 「一般伺服器」：

1. 執行下列一項：
   - 用滑鼠右鍵按一下要移動的 「一般伺服器」，再按 「將 NS 搬移到其他 IS」。
   - 按一下要移動的 「一般伺服器」，然後在主功能表上按 「網域 | 將 NS 搬移到其他 IS」

   隨即顯示 「選擇目的資料伺服器」。
2. 在 「目的資料伺服器」視窗中選取目標 「資料伺服器」。
3. 按下 「確定」，隨即顯示警告視窗。如果確定要將 「一般伺服器」移到選取的 「資料伺服器」，按下 「確定」。

設定更新

趨勢科技的更新伺服器可讓您更新 ServerProtect 的各項元件。更新程序包括下載與部署更新檔。

更新元件

ServerProtect 可下載更新的元件包括病毒碼、掃瞄引擎以及程式昇級檔案。以下說明這三個元件：

- 程式昇級：趨勢科技會不定期發行「一般伺服器」、「資料伺服器」與「管理主控台」的更新版本，以提供新功能、使用者介面的改進以及舊版程式問題的修正。
- 病毒碼檔案：病毒碼檔案是病毒特徵的集合（資料庫）。由於每個月都會出現很多新的病毒，因此這個元件會是最常更新的元件。
- 掃瞄引擎：掃瞄引擎是實際執行檔案掃瞄的軟體元件。

下載與部署的流程

下面說明 ServerProtect 如何在其網路上進行下載與部署的作業。

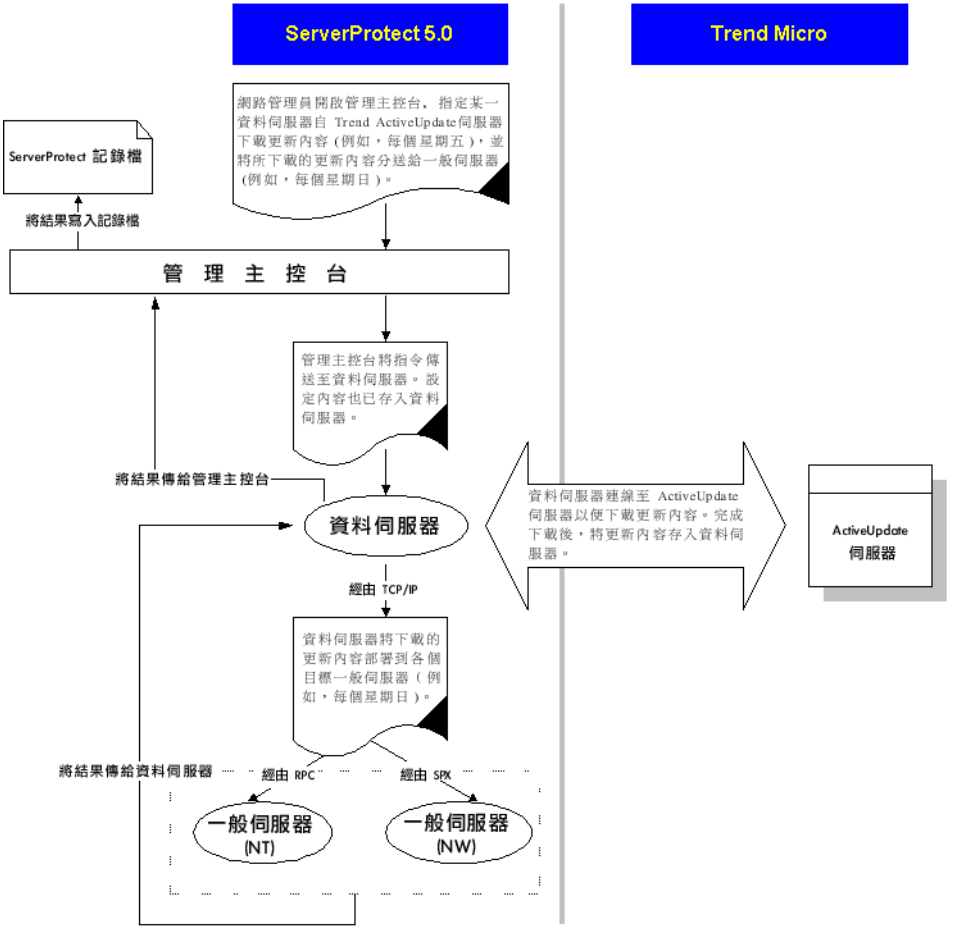


圖 3-6 下載與部署的流程圖

檢視更新檔的目前版本

您隨時可以檢查目前「資料伺服器」所使用的病毒碼檔案、掃瞄引擎、程式檔案版本。

執行下列任一步驟以檢視目前的版本：

- 在功能區中按「更新 | 更新」
- 在主功能表上按「執行 | 更新」

圖 3-7 Trend Micro ServerProtect 更新的主畫面

「更新」畫面上半部顯示儲存在網路上「資料伺服器」的病毒碼檔案、掃瞄引擎、程式檔案目前的版本資訊。

第一次安裝 ServerProtect 後，便會顯示版本欄位，請按下「開始下載」按鈕，從趨勢科技的更新伺服器下載更新檔案。更新成功後，ServerProtect 會顯示更新的版本資訊。

下載更新檔

建議您定期從趨勢科技的更新伺服器下載更新檔，以確保可以持續擁有偵測新病毒的能力。趨勢科技每週都會發行幾次病毒碼更新檔。程式與掃瞄引擎的更新頻率則相對的較不頻繁。

從趨勢科技的更新伺服器下載更新檔之後，您可以指定一台網路磁碟機做為網路上其他「資料伺服器」的下載來源，以避免重複下載。

有多台「資料伺服器」的大型網路（例如企業內部網路）最適合採用從網路磁碟機下載更新檔的方式。嘗試從別的伺服器下載更新檔之前，必須確定來源伺服器已經有更新的檔案。

設定下載來源

您可以從趨勢科技的更新伺服器下載更新檔，也可以從網路上的某個位置複製檔案。如果要從網路上的某個位置複製檔案，您必須建立一個下載來源資料夾。

要將趨勢科技的更新伺服器設為下載來源：

1. 執行下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 在「下載」群組中按「設定」，以開啟「下載選項」視窗。
3. 按下「Internet」，然後輸入下列 URL 來從趨勢科技的更新伺服器下載更新檔：

   serverprotect-t.activeupdate.trendmicro.com/activeupdate
4. 按下「確定」，下載的檔案將會儲存在「資料伺服器」的下列目錄中：

   \ProgramFiles\Trend\Sprotect\spntshare

要將本機或網路磁碟機設為下載來源：

1. 執行下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 在「下載」底下按「設定」，「下載選項」視窗隨即開啟。
3. 按下「從本機或網路磁碟機」。

4. 以 UNC 路徑輸入檔案位置，來從網路上的其他伺服器下載更新檔。請使用 UNC 格式，而不是伺服器名稱的連線網路磁碟機格式來下載更新檔。

   例如：

   \\ 伺服器名稱 \ 資料夾名稱

5. 輸入「使用者名稱」及「密碼」來存取來源伺服器。來源伺服器上必須已經先下載一份更新檔。

6. 按下「確定」，

警告！從本機或網路磁碟機開始下載之前，您必須先建立下載來源資料夾。請參閱下述程序建立下載來源。

要建立下載來源資料夾：

1. 按「開始下載」按鈕從 Internet 執行更新。

2. 執行下列一項：

   - 將指定的「資料伺服器」中 \ProgramFiles\Trend\Sprotect\ 底下的 SpntShare 資料夾設成共用資料夾
   - 在網路伺服器上建立一個共用資料夾，再將 SpntShare 資料夾中的所有檔案複製到這個共用資料夾

如果下載來源不是設成 SpntShare 資料夾，每次從 Internet 下載更新檔之後，都必須將指定的「資料伺服器」中 SpntShare 資料夾的所有檔案內容複製到這個共用資料夾。

使用開始下載

當趨勢科技發行新的病毒碼時，您可以設定讓 ServerProtect 立即從趨勢科技的更新伺服器或其他網路上的「資料伺服器」下載最新版的病毒碼。

要使用「開始下載」：

1. 執行下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 在「更新」主畫面上按「開始下載」。隨即出現進度列，指示剩餘的下載時間。

注意：初次使用「開始下載」之前，必須先設定下載選項，否則按下「開始下載」時，您可能會遭遇 “HTTP 一般錯誤” 或 “HTTP 認證錯誤” 訊息。請參照第 3 章 “下載設定” 小節。

ServerProtect 將事件記錄在「資料伺服器」的記錄檔中。

設定預約下載

您可以設定讓 ServerProtect 從趨勢科技或網路上的其他伺服器預約下載最新版的更新檔。

要設定預約下載：

1. 選擇下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 在「下載」底下按「設定」，「下載選項」視窗隨即開啟。
3. 按下「預約設定」標籤。

圖 3-8 下載選項 -- 預約設定視窗

4. 在「預約」下的「頻率」清單中，選擇下載頻率。您可以選取無、每天或每週。如果不想預約下載，請按下「無」。如果選每週一次，請在「星期」清單中選一天。

5. 在「時間」方塊中，輸入或選取您要更新元件的時間，再按「上午」或「下午」。

6. 選取「重試」核取方塊，來要求 ServerProtect 在下載作業失敗時重新連線到下載伺服器。在「次數」和「間隔」方塊中，輸入或選取重試的頻率。

7. 按下「確定」，下載檔案將儲存在下列目錄中：

   Program File\Trend\Sprotect\spntshare

下載設定

以下描述如何下載最新版的更新檔

要設定下載設定：

1. 執行下列一項：

   - 在功能區中按「更新 | 更新」

- 在主功能表上按「執行 | 更新」

2. 在「更新」畫面上按「設定」來變更下載設定，「下載選項」視窗隨即開啟。

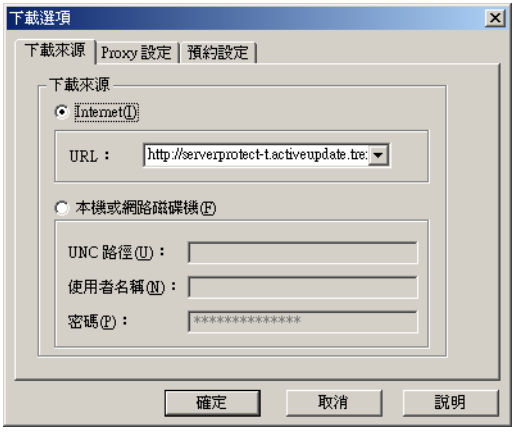


圖 3-9 「下載選項」視窗

設定 Proxy 伺服器設定

您可以設定 ServerProtect 在連線到 Internet 時使用您的 Proxy 伺服器設定。

要設定 Proxy 伺服器設定：

1. 選擇下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 在「下載」底下按「設定」，「下載選項」視窗隨即開啟。
3. 按下「Proxy 設定」標籤。

圖 3-10 下載選項 --Proxy 設定視窗

4. 選取「透過 Proxy 伺服器連線至 Internet」核取方塊。
5. 在「通訊協定」清單中，按一下用來下載的通訊協定。ServerProtect 支援兩種通訊協定：HTTP 和 SOCKS 4。
6. 在「Proxy 設定」下執行下列動作：
   - 在「Proxy 伺服器」和「連接埠」文字方塊中輸入使用的伺服器名稱和連接埠。
   - 在「使用者名稱」和「密碼」文字方塊中輸入 Proxy 伺服器的使用者名稱和密碼。
7. 按下「確定」。

部署更新檔

當「資料伺服器」要將更新檔部署到「一般伺服器」時，它會傳送指令到每一台「一般伺服器」（一次一台），要求它們從「資料伺服器」取得更新檔複本。ServerProtect 同時會將連線及部署程序資料記錄在記錄檔中。

部署之前

「開始部署」功能是用來將存在「資料伺服器」上的更新檔部署到「一般伺服器」。

要部署更新檔：

1. 執行下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 按下「開始部署」，隨即顯示確認視窗。按下「是」來繼續手動更新部署，「部署」視窗隨即開啟。

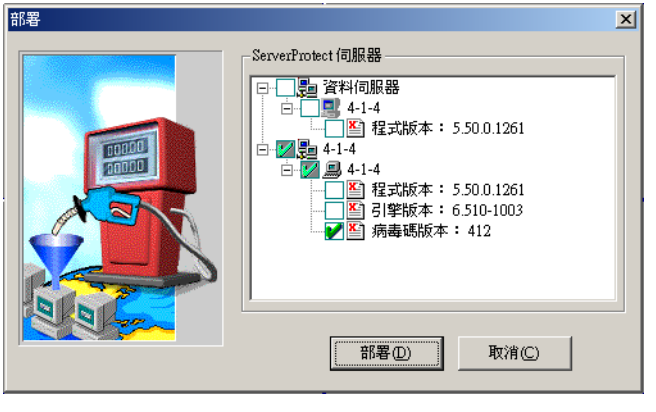


圖 3-11 「部署」視窗

伺服器樹狀結構中顯示每個伺服器元件目前的版本，並預設選取「病毒碼版本」核取方塊。

3. 選取要更新之元件的核取方塊。如果要更新「一般伺服器」中的所有元件，請選取該伺服器的核取方塊。
4. 按下「部署」來啟動部署程序，或按下「取消」來停止部署。

注意：「管理主控台」必須與「資料伺服器」安裝在同一台電腦上，它的程式檔案才會更新。

設定預約部署

以預約方式下載更新檔之後，請設定預約部署，以便將最新的更新檔部署到「一般伺服器」。

ServerProtect 會建立一個預設的部署工作。第 3 章 “預設工作”小節。

請參閱第 3 章 “建立工作”小節以取得如何設定預約工作的詳細資訊。

秘訣：當您設定下載與部署的時間時，請務必將部署時間設在下載時間之後。

要設定預約部署：

1. 執行下列一項：
   - 在功能區中按「更新 | 更新」
   - 在主功能表上按「執行 | 更新」
2. 按下「部署」群組中的「設定」按鈕，「部署設定」視窗隨即開啟。

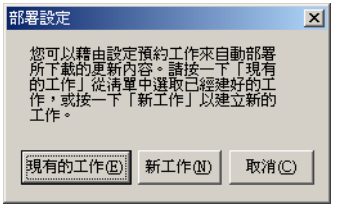


圖 3-12 「部署設定」視窗

3. 執行下列一項：

- 按下「新工作」來建立工作
- 按下「現有的工作」來編輯工作

  關於如何建立或編輯工作的詳細資訊，請參照第 3 章 “建立工作”小節和第 3 章 “修改現有的工作”小節。

還原上一個部署動作

ServerProtect 容許您還原已部署的更新動作，將系統的更新檔還原為之前的版本，包括病毒碼、掃瞄引擎以及程式檔案。這只有在發生軟體不相容問題，或是更新檔下載不完全時，才需要這樣做。

注意：如果已將病毒碼及掃瞄引擎部署到「一般伺服器」，您必須將兩者皆還原。

要還原上一版的部署更新：

1. 執行下列任一項步驟：

- 在功能區中按「更新 | 還原」
- 在主功能表上按「執行 | 還原」

  隨即顯示「還原」畫面。

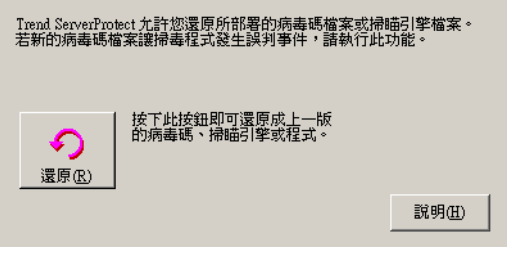


圖 3-13 還原設定視窗

2. 按下「還原」，ServerProtect「還原」視窗隨即開啟。

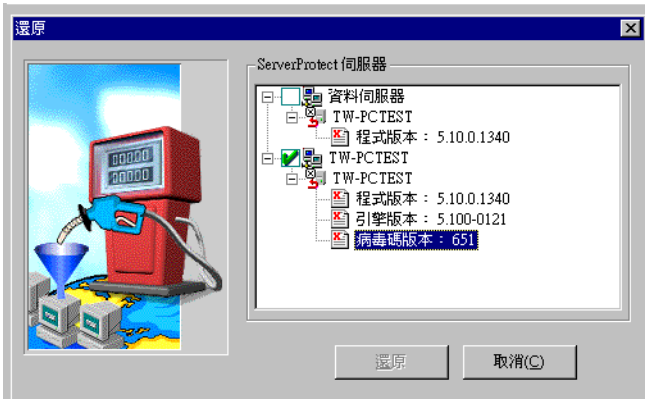


圖 3-14 「還原」視窗

此畫面會顯示目前 Trend Micro ServerProtect 使用的病毒碼檔案、掃瞄引擎、程式檔案資訊、個別版本及組建編號。

3. 選取您要還原的項目，再按下「還原」。

注意：您無法將病毒碼或掃瞄引擎還原到前一版之前的版本。

工作管理

工作可讓您預約設定「一般伺服器」同時執行多項功能。使用工作設定可自動執行網路防毒工作的例行程序，如此可以提高防毒管理效率以及統一防毒策略。

您可以將工作定義成一次執行多個工作項目，就如同使用巨集功能自動執行文書處理程式，或使用指令檔（script）自動執行網路管理工作一般。

每項工作都有指定的「工作擁有者」，由這個人負責維護該工作。

使用 ServerProtect 工作精靈

ServerProtect 的「工作精靈」提供直覺式的使用者介面，讓您能夠簡單地定義工作。您可以加到工作中的工作項目如下：

- **即時掃瞄設定**：你可以針對不同的工作性質來點選不同的即時掃瞄選項 , 例如 : 在網路效能運作正常的情況下只掃瞄輸入的檔案
- **立即掃瞄**：檢查伺服器的檔案是否感染病毒
- **清除記錄檔**：定義要從記錄檔清除的記錄種類。您可以設定自動清除指定時間之前的記錄。
- **匯出記錄檔**：將記錄輸出成 CSV 檔供其他應用程式使用
- **列印記錄檔**：選擇網路印表機來列印符合所設定條件的記錄
- **執行統計**：列印或匯出伺服器病毒掃瞄的統計資料
- **部署**：定義將病毒碼檔案、掃瞄引擎或程式的更新檔部署或配送到網路上其他 ServerProtect 伺服器的時間

圖 3-15 「工作精靈」視窗

預設工作

ServerProtect 會在每個「一般伺服器」建立預設工作。當您第一次安裝 ServerProtect，ServerProtect 會自動建立三個預設的工作：立即掃瞄、執行統計與部署。您可以編輯這三個預設工作，但不可以修改工作名稱和工作擁有者。

建立工作

新工作可讓您設定例行維護及設定程序。

要建立工作：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：
   - 在主功能表上按「執行 | 新工作」

- 在功能區中按「工作 | 新工作」

3. 按下「建立」，「建立新工作」視窗隨即開啟。

圖 3-16 「建立新工作」視窗

4. 在「現有工作」清單中選取您要加到工作中的工作項目。
5. 按下「新增第 n 個工作項目」將選取的工作項目加到「指定工作」清單。您可以繼續選擇其他工作項目，或移除先前選取的工作項目。(n 是數字)

秘訣： 您可以按「指定工作」旁的上移和下移箭頭來變更工作的執行順序，但「部署」一定要是清單中的最後一項。

如果您想將這個工作排定為預約執行，請選取「建立預約工作」核取方塊。您可以將工作排定成每小時執行一次。

6. 按下「建立」按鈕來啟動精靈，協助您建立具有所選工作項目的工作。按下「取消」可關閉「建立新工作」視窗但不儲存變更。

建立預約工作

建立預約工作不僅容易設定，而且可以幫您節省時間。

要建立預約工作：

1. 依照第 3 章 “建立工作” 小節的步驟 1 到 6 執行。必須確定已選取「預約工作」下的「建立預約工作」核取方塊，請參閱圖 3-16。「工作精靈」視窗隨即開啟。
2. 按「下一步」，「預約設定」視窗隨即開啟。

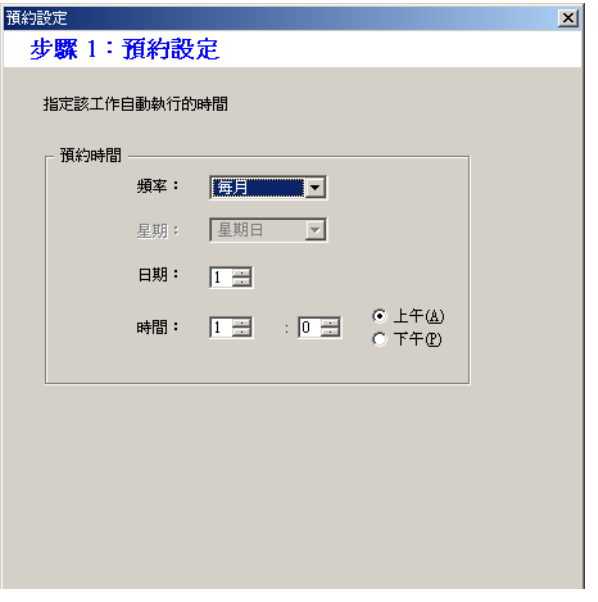


圖 3-17 「預約設定」視窗

3. 在「預約時間」下的「頻率」清單中，選擇下載頻率。您可以選取每月、每週、每日或每小時執行一次。如果選每週一次，請在「星期」清單中選一天。如果選每月一次，請在「日期」清單中選一天。
4. 在「時間」方塊中，輸入或選取您要更新元件的時間 ，再按「上午」或「下午」。
5. 按「下一步」以繼續執行工作精靈設定。

指定手動掃瞄的目標

掃瞄工作必須在特定磁碟機上執行。定義磁碟機時，一開始您可以選擇要掃瞄所有本機磁碟機，或只掃瞄特定磁碟機和目錄。後一種選項可讓您掃瞄網路上的另一台磁碟機。

圖 3-18 「新增磁碟機及 / 或目錄」視窗

建立預設工作

工作精靈的最後一個畫面是「工作資訊」視窗，您可以在這裏定義工作的名稱和擁有者。預設工作會影響一台「資料伺服器」所管轄的所有「一般伺服器」，所以如果新增「一般伺服器」的話，它將會繼承現有的預設工作。

圖 3-19 「工作資訊」視窗

檢視現有工作清單

「現有工作」清單顯示所有已定義之工作的相關資訊。您可以使用「現有工作」清單來執行、修改、移除或檢視工作定義。

要檢視現有的工作，請執行下列一項：

- 在功能區中按「工作 | 現有工作」
- 在主功能表上按「執行 | 現有工作」

「現有工作」清單是具有下列欄位的表格。您可以按下每一個欄位的標頭來排序清單項目。

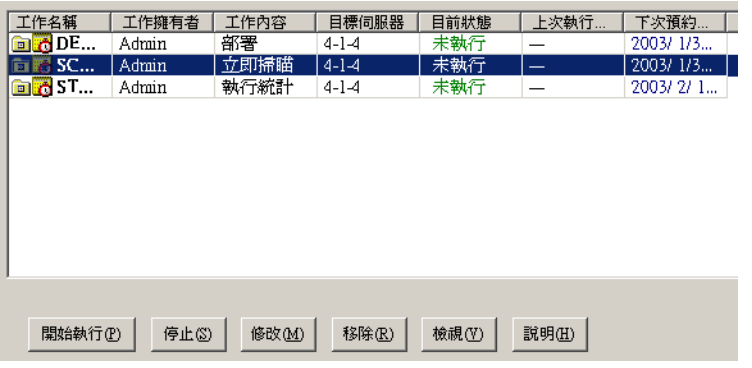


圖 3-20 檢視現有工作表格

注意：管理多個跨時區伺服器的使用者應該記住，「上次執行時間」和「下次預約執行時間」欄位中顯示的值是每台伺服器當地的時間。

執行現有的工作

「現有工作」清單顯示所有已定義之工作的相關資訊。您可以使用「現有工作」清單來執行工作。

要執行現有的工作：

1. 執行下列一項：
   - 在功能區中按「工作 | 現有工作」
   - 在主功能表上按「執行 | 現有工作」

   「現有工作」清單隨即顯示 ServerProtect 中目前所有已定義的工作。
2. 選取您要執行的工作，再按「立即執行」。

修改現有的工作

修改現有的工作可以為您省下寶貴的設定時間，讓您不必花時間設定新的工作。

要修改現有的工作：

1. 執行下列一項：
   - 在功能區中按「工作 | 現有工作」
   - 在主功能表上按「執行 | 現有工作」

   隨即顯示「現有工作」清單。
2. 在「現有工作」清單中選取要修改的工作。
3. 按下「修改」，「修改工作」視窗隨即開啟。

圖 3-21 「修改工作」視窗

4. 執行下列一項：
   - 選取「修改目標伺服器」核取方塊可變更設定之工作執行對象的伺服器
   - 選取「修改工作定義」核取方塊可變更用來定義工作的程序
5. 按下「確定」。

要修改現有工作的目標伺服器：

1. 在「選擇要套用工作的伺服器」視窗上，選取要執行此工作的每台伺服器。
2. 按下「新增」。

圖 3-22 「選擇要套用工作的伺服器」視窗

3. 按下「套用」，或按下「取消」來關閉視窗但不儲存變更。

要修改現有工作的工作定義：

1. 在「現有工作」清單中選取您要加到工作中的工作項目。

圖 3-23 「修改工作」視窗

2. 按下「新增第 n 個工作項目」將您選取的工作項目加到「指定工作」清單。(n 是數字)

如果您想將這個工作排定為預約執行，請選取「建立預約工作」核取方塊。

秘訣：您可以按「指定工作」旁的上移和下移箭頭來變更工作的執行順序，但「部署」一定要是清單中的最後一項。

3. 按下「修改」按鈕來啟動精靈，協助您建立具有您所選工作項目的工作。按下「取消」可關閉「修改工作」視窗但不儲存變更。

檢視現有工作的詳細資訊

您可從「現有工作」視窗檢視任何現有工作的定義。這使您可以在執行前知道工作的確實執行內容。

要檢視現有的工作：

1. 執行下列一項：
   - 在主功能表上按「執行 | 現有工作」
   - 在功能區中按「工作 | 現有工作」
2. 在「現有工作」清單中選取要檢視的工作。
3. 按下設定區下方的「檢視」。或者，您也可以按兩下「現有工作」表中的工作記錄項目。便會顯示「檢視工作資訊」視窗。

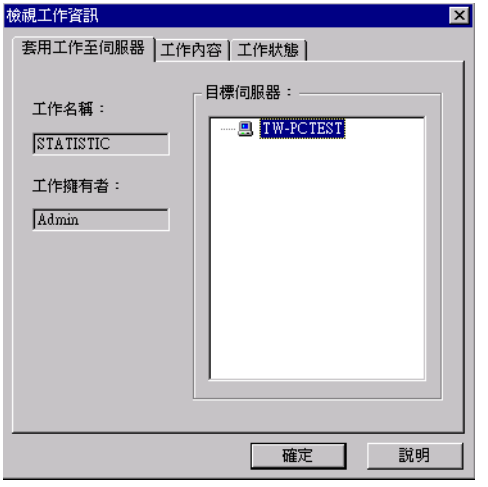


圖 3-24 檢視工作視窗

這個畫面上有「套用工作至伺服器」、「工作內容」及「工作狀態」三個標籤。

- 套用工作至伺服器：「工作名稱」與「工作擁有者」顯示在標籤的左邊。「目標伺服器」顯示網路上將做為工作執行對象的所有伺服器。
- 工作內容：顯示組成該工作的所有工作項目。按下「工作順序」清單中的工作項目，工作項目定義將顯示在右邊的工作定義表中。
- 工作狀態：「目標伺服器」顯示網路上將做為工作執行對象的所有伺服器。「目前狀態」、「上次執行時間」與「下次預約執行時間」欄位顯示工作的狀態及最後執行的時間。

4. 按下「確定」來關閉「檢視工作資訊」視窗。

移除現有的工作

「現有工作」清單顯示所有已定義之工作的相關資訊。您可以使用「現有工作」清單來刪除現有工作。

要移除現有的工作：

1. 執行下列一項：
   - 在主功能表上按「執行 | 現有工作」
   - 在功能區中按「工作 | 現有工作」
2. 在「現有工作」清單中選擇要移除的工作。
3. 按下「移除」。

設定通知訊息

好用的防毒軟體必須能夠在找到病毒時主動通知使用者或管理員。ServerProtect 可以讓您設定中毒通知，以及誰可以收到通知。

ServerProtect 通知訊息分為一般警訊和病毒爆發警訊。傳送警訊的方法有多種。請參照第 3 章 “設定警訊方式”小節了解所有可用的傳送選項。

一般警訊

當指定的伺服器偵測到設定的狀況時，便會產生一般警訊。您可以在通知訊息中加入其他文字。

中毒通知事件

您可以設定 ServerProtect 在發生以下事件時送出通知。

- **中毒**：在伺服器上偵測到中毒檔案
- **嘗試變更防寫檔案**：企圖修改防寫檔案
- **變更即時掃瞄設定**：變更即時掃瞄的組態設定
- **服務程式（NLM）載入 / 卸載**：NetWare 服務停止
- **病毒碼過期**：病毒碼檔案已經過期

要設定一般警訊：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：
   - 在主功能表上按「設定 | 通知 | 一般警訊」
   - 在功能區中按「設定通知 | 一般警訊」

   隨即顯示「一般警訊」畫面。

圖 3-25 ServerProtect「一般警訊」設定視窗

3. 選取事件類型的核取方塊。
4. 按下所選事件種類的「設定訊息」按鈕，「設定警示訊息」視窗隨即開啟。
5. 輸入您要的設定，再按「確定」來關閉視窗。
6. 按下「設定警訊方式」來選取通知的方式。請參考第 3 章 “設定警訊方式”小節來取得詳細資訊。

7. 按下「套用」儲存您所做的變更。

注意：如需有關設定警示訊息的詳細資訊，請參閱線上說明中的相關主題。

病毒爆發警訊

病毒爆發極可能在網路上造成重大破壞。當病毒事件數目超過臨界值時，便會發出病毒爆發警訊通知系統管理員。

這樣一來，只要發生病毒爆發，系統管理員或相關人員保證會收到通知，以便採取必要的措施。您可以自行指定病毒爆發警訊的訊息內容。

要設定病毒爆發警訊：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：
   - 在功能區中按「設定通知 | 病毒爆發警訊」
   - 在主功能表上按「設定 | 通知 | 病毒爆發警訊」

   「病毒爆發警訊」畫面隨即開啟。

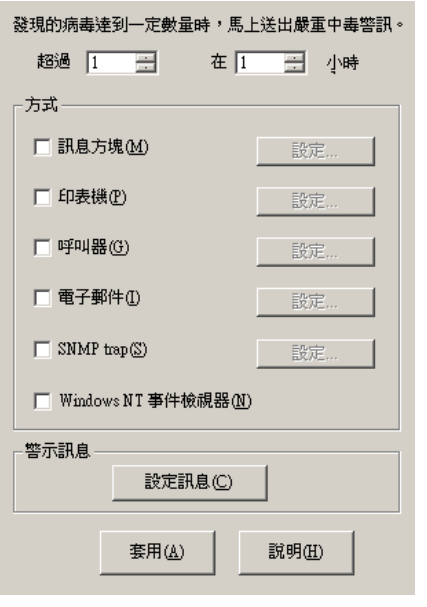


圖 3-26 ServerProtect「病毒爆發警訊」設定視窗

3. 定義病毒爆發臨界值。在方塊中指定超出的病毒數目，以及時間範圍。
4. 選取發出警訊的方法。
5. 按下「設定」可修改所選警訊方式的通知設定。有關修改警訊方式，請參照第 3 章 “設定警訊方式”小節以取得詳細資料。
6. 在「警示訊息」下按「設定訊息」來修改發生病毒爆發時顯示的訊息。
7. 按下「套用」儲存您所做的變更。

設定警訊方式

當偵測到病毒爆發時，ServerProtect 可以用下列方式通知系統管理員：

- **訊息方塊**：管理員的電腦上顯示標準的 Windows 即現訊息方塊
- **印表機**：傳送文件到本機或網路印表機

- **呼叫器**：傳送訊息到呼叫器，此功能要有與趨勢科技 ServerProtect 伺服器相連結的數據機
- **電子郵件**：當偵測到病毒或病毒爆發事件時傳送電子郵件訊息
- **SNMP Trap**：透過 SNMP 傳送警示郵件給網路管理員。此功能可和您公司使用的其他 SNMP 相容管理工具整合在一起
- **NT 事件檢視器**：將病毒偵測寫到 Windows NT 事件檢視器

您可以同時設定一個或多個中毒通知方法。以下說明如何設定電子郵件通知。如需其他通知方式的資訊，請參閱線上說明。

要設定透過 Internet 電子郵件傳送中毒警訊：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：

   要設定一般警訊：

   - 在功能區中按「設定通知 | 一般警訊」
   - 在主功能表上按「設定 | 通知」，再按「一般警訊」

   設定病毒爆發警訊：

   - 在主功能表上按「設定 | 通知 | 病毒爆發警訊」，再按「設定警訊方式」
   - 在功能區中按「設定通知 | 病毒爆發警訊」，再按「設定警訊方式」
3. 選取「電子郵件」核取方塊，再按「設定」，「設定 Internet 電子郵件警訊」視窗隨即開啟。

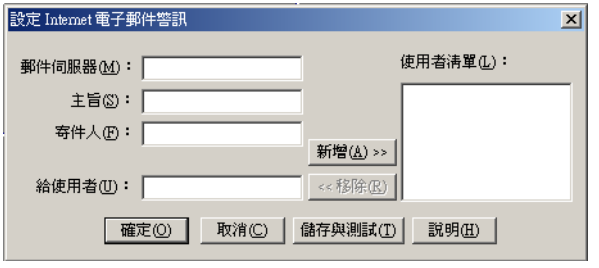


圖 3-27 「設定 Internet 電子郵件警訊」視窗

4. 執行下列動作：
   - 在「郵件伺服器」文字方塊中輸入郵件伺服器的名稱
   - 在「主旨」文字方塊中輸入訊息的主旨
   - 在「寄件人」文字方塊中輸入寄件人的名稱（只可輸入英文字）
5. 在「給使用者」文字方塊中輸入接收這個電子郵件訊息的人，再按「新增」。您可以選取使用者，再按「移除」來移除收件者。
6. 按下「儲存與測試」以確定組態設定可以正常運作。如果成功，您指定的收件者便會收到一封測試電子郵件。
7. 按下「確定」來儲存組態變更，同時回到「設定警訊方式」視窗。

注意：如需有關設定警示訊息的詳細資訊，請參閱線上說明中的相關主題。

掃瞄病毒

ServerProtect 提供三種病毒掃瞄模式：即時掃瞄、立即掃瞄（手動掃瞄）以及預約掃瞄。

即時掃瞄可檢查所有輸入與輸出伺服器的檔案是否感染病毒。手動掃瞄是靠使用者下指令來執行，讓您可以立即檢查電腦是否感染病毒。預約掃瞄可在指定的時間，自動檢查網路上選取的 ServerProtect 伺服器是否中毒。

針對中毒檔案，ServerProtect 有五種中毒處理行動：不作處置、刪除、重新命名、隔離以及清除病毒。

您可以執行下列動作：

- 選擇要掃瞄的檔案種類
- 使用「防寫清單」防止使用者修改或刪除特定目錄或檔案。如需有關設定「防寫清單」的詳細資訊，請參閱線上說明中的相關主題。

注意：每次掃瞄的結果都記錄在掃瞄結果記錄檔中。您可以從「掃瞄結果」視窗直接對中毒檔案採取處理行動，讓您能夠更方便對中毒事件採取適當的處理行動。如需詳細資訊，請參閱線上說明的「檢視掃瞄結果資訊」主題。

定義中毒處理行動

ServerProtect 可讓您設定即時掃瞄或立即掃瞄期間在網路上發現中毒檔案時所採取的處理行動。

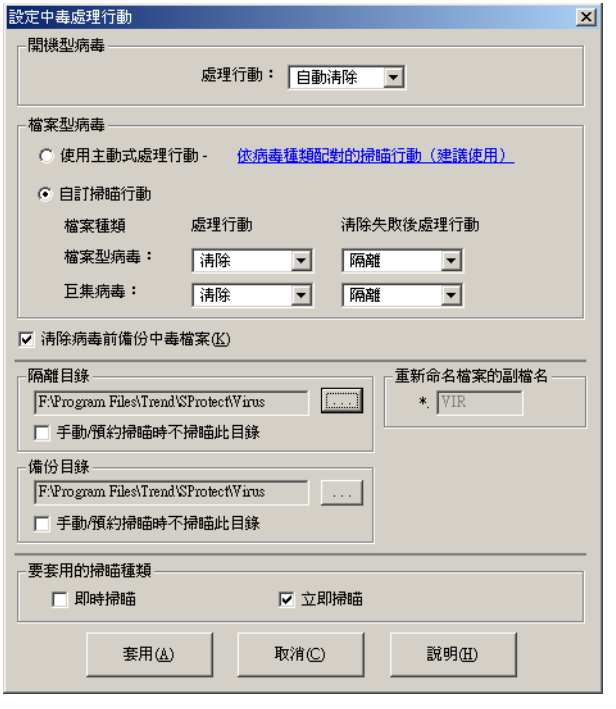


圖 3-28 「設定中毒處理行動」視窗

要定義中毒處理行動：

1. 在 「立即掃瞄」或「即時掃瞄」設定區中按「設定行動」，「設定中毒處理行動」視窗隨即開啟。
2. 在「開機型病毒」下的「處理行動」清單中，選取 ServerProtect 發現開機型病毒時所應採取的中毒處理行動。您可以選擇 「自動清除」或「不作處置」。
3. 在「檔案型病毒」下執行下列一項：
   - 按下「使用主動式處理行動」來設定趨勢科技建議的中毒處理行動
   - 按下「自訂掃瞄行動」，在「處理行動」和「清除失敗後處理行動」清單中選取對中毒檔案和巨集病毒採取的適當處理

行動。請參照第 1 章 “當 ServerProtect 發現病毒時 (中毒處理行動)”小節。如需有關主動式處理行動的詳細資訊，請參閱第 1 章 “智慧型掃瞄”小節。

注意：如果選取「清除」，建議您選取「清除病毒前備份中毒檔案」核取方塊。有時候，清除病毒的處理行動可能會破壞檔案，使檔案不可使用。

您可以選取不要掃瞄備份和隔離目錄。如需詳細資訊，請參閱線上說明的「例外目錄清單」主題。選取的掃瞄種類顯示在「要套用的掃瞄種類」底下。

4. 按下「套用」來開始使用這些設定。

注意：NetWare「一般伺服器」無法使用主動式處理行動和「開機型病毒」功能。

設定掃瞄設定檔

即時掃瞄和立即掃瞄設定可以儲存成設定檔，供您用來建立或修改工作。您也可以刪除不再需要的設定檔。設定立即掃瞄和即時掃瞄工作時都可以套用掃瞄設定檔。如需詳細資訊，請參閱線上說明的「選擇掃瞄設定檔」。

如果是預約掃瞄，您可以選擇現有的設定檔，也可以建立您要的設定掃瞄選項。請參照第 3 章 “修改現有的工作”小節。

要儲存掃瞄設定檔：

1. 設定即時掃瞄或立即掃瞄的掃瞄選項。請參照第 3 章 “設定即時掃瞄”小節和第 3 章 “設定立即掃瞄”小節。
2. 按下「儲存為 / 刪除設定檔」，隨即顯示「儲存 / 刪除設定檔」視窗。

圖 3-29 「儲存 / 刪除設定檔」視窗

3. 在「設定檔名稱」文字方塊中輸入設定檔的名稱。
4. 按下「儲存」來儲存新設定檔。或按「關閉」來關閉視窗但不儲存設定檔。

要刪除掃瞄設定檔：

1. 執行下列一項：
   - 在功能區中按「立即掃瞄 | 立即掃瞄」
   - 在主功能表上按「執行 | 立即掃瞄」
   - 在功能區中按「設定掃瞄選項 | 即時掃瞄」
   - 在主功能表上按「設定 | 掃瞄選項 | 即時掃瞄」
2. 按下「儲存為 / 刪除設定檔」，隨即顯示「儲存 / 刪除設定檔」視窗。
3. 在「現有設定檔」清單中選取要刪除的設定檔。
4. 按下「刪除」來刪除設定檔。或按「關閉」來關閉視窗但不刪除設定檔。

使用即時掃瞄

即時掃瞄可持續掃瞄所有存取的檔案，在背景提供伺服器強大的病毒保護。所有輸入與輸出的檔案都受到監控，因此中毒檔案無法複製自或複製至該伺服器。

設定即時掃瞄

以下介紹即時掃瞄專用的掃瞄選項：

- **開機時掃瞄磁片**：電腦開機時掃瞄軟碟機及軟碟機中的磁片。
- **關機時掃瞄磁片**：電腦關機時掃瞄軟碟機及軟碟機中的磁片，以防使用者使用有毒的磁片開機。
- **掃瞄磁片啟動區**：這個選項可掃瞄電腦的磁片啟動區，以防止「Master Boot Record」病毒。
- **MacroTrap**：啟用趨勢科技取得專利的 MacroTrap™ 智慧型巨集病毒偵測系統來保護 Microsoft Office 檔案，以防止受到巨集病毒攻擊。
- **掃瞄 OLE 層級**：這個選項可掃瞄內嵌的檔案。OLE 層級掃瞄功能可提供五層的保護。如需詳細資訊，請參照第 1 章 “OLE 層級掃瞄” 小節。
- **掃瞄連線網路磁碟機**：這個選項可掃瞄任何連線的網路磁碟機。必須已有現存的連線網路磁碟機，這個選項才有作用。

要設定即時掃瞄：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：
   - 在功能區中按「設定掃瞄選項 | 即時掃瞄」
   - 在主功能表上按「設定 | 掃瞄選項 | 即時掃瞄」

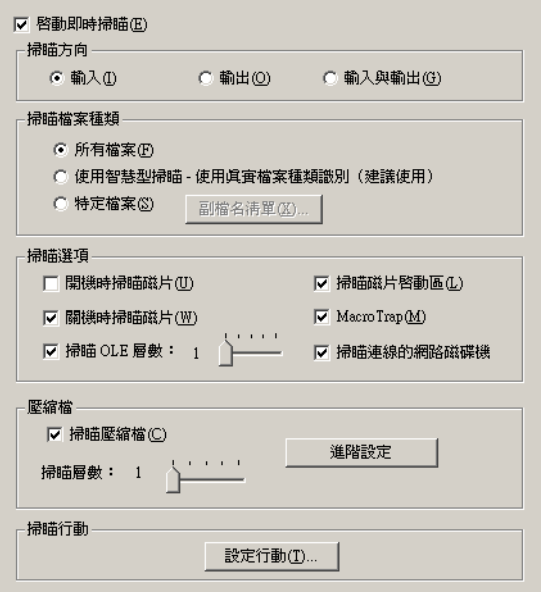


圖 3-30 「即時掃瞄」設定視窗

3. 選取「啟動即時掃瞄」核取方塊。
4. 在「掃瞄方向」下選擇下列一項：
   - 輸入：掃瞄複製到伺服器的檔案
   - 輸出：掃瞄從伺服器複製出去的檔案
   - 輸入與輸出：掃瞄伺服器上所有輸入與輸出的檔案
5. 在「掃瞄檔案種類」下選擇下列一項：
   - 所有檔案：掃瞄所有檔案種類
   - 智慧型掃瞄：使用真實檔案種類識別來掃瞄檔案。請參照第 1 章 “智慧型掃瞄”小節。

注意：NetWare「一般伺服器」無法使用 智慧型掃瞄 功能。

- 特定檔案：只掃瞄指定的檔案。如果選擇「特定檔案」，請按「副檔名清單」來定義要掃瞄的檔案種類。請參照第 3 章“選取要掃瞄的檔案種類”小節。

6. 在「掃瞄選項」下單選或複選下列核取方塊：

- 開機時掃瞄磁片
- 關機時掃瞄磁片
- 掃瞄 OLE 層數
- 掃瞄磁片啟動區
- MacroTrap
- 掃瞄連線的網路磁碟機

  請參閱第 3 章 “設定即時掃瞄”小節以取得各個掃瞄選項的詳細資訊。

注意： 設定 NetWare「一般伺服器」時，只能選用 MacroTrap 功能。

---

7. 選取「掃瞄壓縮檔」核取方塊來掃瞄壓縮檔，然後移動「掃瞄層數」滑塊設定要掃瞄的壓縮層數。如需有關進階設定的詳細資訊，請參閱線上說明的「壓縮檔掃瞄」主題。

注意： 如果您在步驟 5 選擇掃瞄指定檔案格式，請務必將壓縮檔的副檔名（如 ZIP）加到清單中。

---

8. 按下「設定行動」來設定 ServerProtect 所採取的中毒處理行動。請參照第 3 章 “定義中毒處理行動”小節。

注意：如果您選取含有 NetWare 伺服器的網域，或您選取的伺服器是 NetWare 伺服器，請在「NetWare 設定」下按「NetWare 選項」來設定 MAC 檔案掃瞄選項。

9. 按下「套用」儲存您所做的變更，或按下「儲存為 / 刪除設定檔」，以便以後可以存取您的組態設定。

使用立即掃瞄（手動掃瞄）

立即掃瞄會在使用者下指令時開始執行掃瞄。如果您懷疑伺服器可能已經中毒，便可以使用立即掃瞄。

設定立即掃瞄

立即掃瞄可設定的選項包括：

- 掃瞄目標
- 掃瞄檔案種類
- 掃瞄選項
- 壓縮檔掃瞄
- 掃瞄優先順序
- 掃瞄行動

要設定立即掃瞄：

1. 在網域瀏覽目錄中選取「資料伺服器」、「網域」或「一般伺服器」。
2. 執行下列一項：
   - 在功能區中按「立即掃瞄 | 立即掃瞄」
   - 在主功能表上按「執行 | 立即掃瞄」

圖 3-31 「立即掃瞄」設定視窗

3. 在「掃瞄目標」下選擇下列一項：

- 所有本機磁碟機：掃瞄伺服器的所有磁碟機
- 特定磁碟機 / 目錄：掃瞄伺服器上的特定磁碟機或目錄。按下「瀏覽」，「新增磁碟機及 / 或目錄」視窗隨即開啟。選取要掃瞄之磁碟機或目錄的核取方塊，再按 「確定」來關閉視窗。

圖 3-32 「新增磁碟機及 / 或目錄」視窗

4. 在「掃瞄檔案種類」下選擇下列一項：

   - 所有檔案：掃瞄所有檔案
   - 使用智慧型掃瞄：使用真實檔案種類識別來掃瞄檔案。請參照第 1 章 “智慧型掃瞄”小節。

   注意：NetWare「一般伺服器」無法使用智慧型掃瞄功能。

   - 特定檔案：只掃瞄指定的檔案。按下「副檔名清單」來定義要掃瞄的檔案種類。請參照第 3 章 “選取要掃瞄的檔案種類”小節。

5. 在「掃瞄選項」下選取「掃瞄 OLE 層級」。移動「掃瞄 OLE 層數」滑塊來設定 OLE 層級。您最多可以掃瞄五層。

   注意：只有 Windows .NET/2000/NT 伺服器可以使用「掃瞄 OLE 層級」功能。

6. 在「壓縮檔掃瞄」下選取「掃瞄壓縮檔」核取方塊。移動「掃瞄層數」滑塊來設定要掃瞄的壓縮層數。如需有關進階設定的詳細資訊，請參閱線上說明的「壓縮檔掃瞄」主題。NetWare「一般伺服器」無法選取進階設定。

注意：如果您在步驟 4 選擇掃瞄指定檔案格式，請務必將壓縮檔的副檔名（如 ZIP）加到清單中。

7. 在「掃瞄優先順序」下選取低、中或高優先順序。高優先順序會耗用較多的 CPU 資源，但可以較快完成掃瞄工作。

8. 按下「設定行動」來設定 ServerProtect 所採取的中毒處理行動。請參照第 3 章 “定義中毒處理行動”小節。

注意：如果您選取含有 NetWare 伺服器的網域，或您選取的伺服器是 NetWare 伺服器，請在「NetWare 設定」下按「NetWare 選項」來設定 MAC 檔案掃瞄選項。

9. 按下「套用」儲存您所做的變更，或按下「儲存為 / 刪除設定檔」，以便以後可以存取您的組態設定。

在 Windows 一般伺服器上執行立即掃瞄工具

使用「立即掃瞄工具」可以直接掃瞄 Windows .NET/2000/NT 伺服器，不必經由「管理主控台」。「立即掃瞄工具」會依據「管理主控台」上的「立即掃瞄」設定來執行掃瞄（例如，掃瞄目標、掃瞄檔案種類等）。

要執行「立即掃瞄工具」：

1. 在「一般伺服器」上按「開始 | 程式集 | 附屬應用程式 | Windows 檔案總管」，隨即開啟「Windows 檔案總管」視窗。

2. 按下 ServerProtect 的安裝目錄。預設位置為：

   C:\Program Files\Trend\SProtect

3. 按兩下 ScanNow.EXE，立即掃瞄隨即開始執行。

要停止「立即掃瞄工具」：

1. 在「一般伺服器」上按「開始 | 執行」，「執行」視窗隨即開啟。
2. 按下「瀏覽」，尋找 ScanNow.EXE 檔案（預設位置在 C:\Program Files\Trend\SProtect）。
3. 執行「立即掃瞄工具」並加上 “stop” 參數：

   C:\Program Files\Trend\SProtect\ScanNow.exe /STOP

4. 按下「確定」，立即掃瞄隨即停止。

注意： 檔名與 Stop 參數之間需空一格。

預約掃瞄

預約掃瞄會依照設定的頻率在指定的時間掃瞄檔案。使用預約掃瞄可以將「一般伺服器」的例行掃瞄工作自動化。您可以用預約工作建立預約的立即掃瞄或即時掃瞄。

設定預約掃瞄

您可以利用預約工作來設定預約的立即掃瞄或即時掃瞄。如需詳細資訊，請參閱第 3 章 “建立工作” 小節。

注意： 安裝好 ServerProtect 伺服器後，ServerProtect 會自動對伺服器套用掃瞄工作。預設掃瞄工作設成每週五掃瞄所有的本機目錄是否中毒。

如果現有工作不符合您的需要，您可以修改預設工作，或自行建立新工作。ServerProtect 工作精靈將指引您完成整個作業。

選取要掃瞄的檔案種類

設定即時掃瞄、立即掃瞄或預約掃瞄（工作掃瞄）時，ServerProtect 可讓您控制要掃瞄的檔案種類。由於只有某些種類的檔案可能含有病毒，因此您可以設定只掃瞄這種檔案，來減少伺服器負荷。

要新增要掃瞄的副檔名：

1. 在「即時掃瞄」或「立即掃瞄」設定區中，在「掃瞄檔案種類」下按「特定檔案」，再按「副檔名清單」來定義要掃瞄的檔案種類。隨即顯示「選擇欲掃瞄的檔案」視窗。

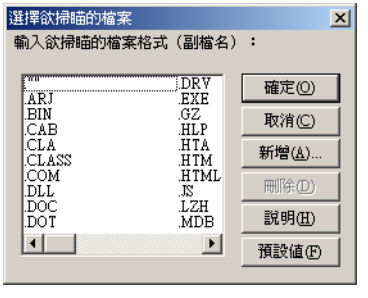


圖 3-33 「選擇欲掃瞄的檔案」視窗

2. 執行下列一項：

   - 按下「新增」，隨即顯示「新增檔案副檔名」視窗。

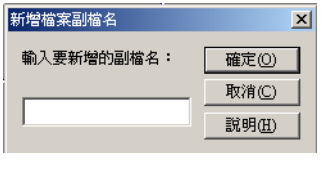


圖 3-34 「新增檔案副檔名」視窗

在文字方塊中輸入要新增的副檔名，再按「確定」將副檔名新增到清單中。按下「取消」可關閉視窗但不儲存變更。最後再按「確定」來關閉「選擇欲掃瞄的檔案」視窗。

- 按下「預設值」來新增所有預設的副檔名，再按「確定」來關閉「選擇欲掃瞄的檔案」視窗。任何自訂的副檔名都將消失不見。

  預設值已足夠為大部分的環境提供安全防護。預設的檔案副檔名包括：

.ARJ	.BIN	.CAB	.CLA
.CLASS	.COM	.DLL	.DOC
.DOT	.DRV	.EXE	.GZ
.HLP	.HTA	.HTM	.HTML
.JS	.LZH	.MDB	.MPP
.MPT	.MSG	.OCX	.OFT
.OVL	.PIF	.POT	.PPS
.PPT	.RAR	.RTF	.SCR
.SHS	.SYS	.TAR	.VBS
.VSD	.VST	.XLA	.XLS
.XLT	.Z	.ZIP	

- 選取要刪除的檔案副檔名，再按「刪除」。

第 4 章

昇級 ServerProtect 軟體

ServerProtect 支援從舊版昇級與更新。舊版本的設定大部份都可以轉移到新版本。此外，會沿用舊版的安裝路徑。

當您執行 ServerProtect 安裝程式時，安裝程式會偵測是否已安裝舊版的 ServerProtect 並進行昇級或更新。

「昇級」和「更新」的區別如下：

- 昇級：這是指從 ServerProtect 的一個主要版本昇級到另一個主要版本，例如從 ServerProtect 4.x 昇級到 ServerProtect 5.x。
- 更新：這是指將特定元件從 ServerProtect 的一個主要版本昇級到一個次要版本，例如從 ServerProtect 5.35 昇級到 ServerProtect 5.5。

注意：如果要檢查須更新還是昇級，請參照第 3 章 “檢視更新檔的目前版本”小節。

要昇級 ServerProtect 的元件，請參照第 4 章 “昇級計劃”小節。

要更新 ServerProtect 5.x 的元件，請參照第 4 章 “更新 ServerProtect5”小節。

本章內容如下：

- 昇級計劃
- 從管理主控台昇級
- 更新 ServerProtect 5

昇級計劃

以下說明透過網路來昇級 ServerProtect 的方式：

- 當一台「資料伺服器」管理一台「一般伺服器」時
- 當一台「資料伺服器」管理多台「一般伺服器」時

當一台「資料伺服器」管理一台「一般伺服器」時

如果您的網路「資料伺服器」只管理一台「一般伺服器」，您可以用安裝程式來昇級「資料伺服器」和「一般伺服器」。請參照第 2 章 “安裝 ServerProtect” 小節。

注意：如果要從安裝程式昇級，您必須安裝完整的 ServerProtect。

當一台「資料伺服器」管理多台「一般伺服器」時

如果您的網路「資料伺服器」負責管理多台「一般伺服器」（ServerProtect 網域），則要先安裝完整的 ServerProtect（「資料伺服器」、「一般伺服器」和「管理主控台」）。請參照第 2 章 “安裝完整版的 ServerProtect” 小節。等安裝完成後，再用「管理主控台」昇級「一般伺服器」。請參照第 4 章 “從管理主控台昇級” 小節。

從管理主控台昇級

您可以透過「ServerProtect 管理主控台」，將現有的 ServerProtect 4.x 或 ServerProtect for NetWare 3.x「一般伺服器」昇級到最新版的 ServerProtect。

注意：您只能從「管理主控台」昇級「一般伺服器」。

要從「管理主控台」昇級「一般伺服器」：

1. 在網路上安裝完整的 ServerProtect。
2. 開啟「管理主控台」。
3. 執行下列一項：

   NT 一般伺服器

   - 在網域瀏覽目錄中，於 ServerProtect 網域上按滑鼠右鍵，然後選擇「從 SPNT 4.x 昇級為 5.x」。
   - 在網域瀏覽目錄中按一下 ServerProtect 網域，然後在主功能表上按「網域 | 從 SPNT 4.x 昇級為 5.x」。

   NetWare 一般伺服器

   - 在網域瀏覽目錄中，於 ServerProtect 網域上按滑鼠右鍵，然後選擇「安裝新的 SPNW」（使用 IPX 或 IP）
   - 按下「網域」，然後選擇一個 SPNW 安裝選項
   - 參考第 2 章 “從管理主控台安裝一般伺服器”小節選擇安裝或昇級的來源伺服器。

注意：NetWare 一般伺服器的安裝選項也可用來昇級。

「昇級舊版的 ServerProtect 伺服器」視窗隨即開啟。

圖 4-1 「昇級舊版的 ServerProtect 伺服器」視窗

4. 執行下列動作：

- 在「資料伺服器」中輸入「資料伺服器」的名稱，來昇級它所管理的「一般伺服器」
- 在「使用者名稱」中輸入用來存取「資料伺服器」的使用者名稱
- 在「密碼」中輸入這個使用者名稱的密碼

5. 按下「搜尋伺服器」。如果找到「資料伺服器」，該伺服器管理的所有「一般伺服器」會顯示在左邊清單中。

圖 4-2 資料伺服器所管理的伺服器視窗

6. 在左邊清單中按一下要昇級的伺服器，再按「新增 >」，或按「全部新增 >>」來新增所有伺服器。如果想移除之前選取的伺服

器，請在右邊清單中按一下該伺服器，再按「< 移除」，或按「全部移除」來移除之前選取的所有伺服器。

7. 按下「昇級」，「登入目標伺服器」視窗隨即開啟。

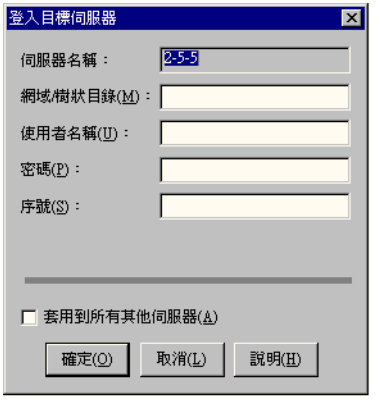


圖 4-3 「登入目標伺服器」視窗

8. 在「序號」中輸入有效的產品序號。如果您輸入的資訊適用於其他執行 ServerProtect 的伺服器，請選取「套用到所有其他伺服器」核取方塊。否則，取消選取核取方塊，再按「確定」。「昇級伺服器」視窗隨即開啟。

圖 4-4 「昇級伺服器清單」視窗

9. 選取伺服器，再按「移除」將伺服器從清單中移除。如果要修改伺服器的昇級資訊，請選取伺服器，再按「修改」。

10. 按下「開始」來昇級伺服器。昇級程序隨即開始執行。ServerProtect 首先檢查遠端環境，接著將必要的檔案複製到目標伺服器。複製好檔案後，ServerProtect 隨即啟動目標伺服器的遠端服務。

圖 4-5 「遠端昇級進度」視窗

隨即出現一個「通知」視窗，列出已經完成昇級的伺服器名稱。

圖 4-6 「通知」視窗

11. 按下「確定」來關閉「通知」視窗。

注意：從舊版移轉時，所有的掃瞄設定檔（即時與手動掃瞄）都會保存下來，並複製到新安裝的 ServerProtect 伺服器。

更新 ServerProtect 5

如果您之前已經安裝 ServerProtect 版本 5.0 或更新版，您有兩種方法可以更新現有的 ServerProtect 元件（程式檔案、掃瞄引擎和病毒碼檔案），比較有效率的方法是利用「管理主控台」，但您也可以利用新版 ServerProtect 隨附的安裝程式。

注意：更新過程中會停止所有執行中的工作。

要更新 ServerProtect 5 元件：

- 透過管理主控台：

  1.下載已有的更新檔。請參照第 3 章 “下載更新檔”小節來規劃下載更新檔的方式。

  2.部署更新檔。請參照第 3 章 “部署更新檔”小節來規劃部署更新檔的方式。

- 透過安裝程式：

  1.從光碟執行新版 ServerProtect 的安裝程式。安裝程式將會偵測之前安裝的 ServerProtect 版本。

  2.更新 ServerProtect。請參照第 2 章 “安裝 ServerProtect”小節來取得詳細指示。

第 5 章

使用 Trend Micro Control Manager™ 管理 ServerProtect

Trend Micro Control Manager (TMCM) 是一套集中式網路病毒與內容安全防護管理系統，利用功能強大的單一窗口設計，企業可以集中管理、監控與部署各項病毒與內容安全防護策略，以提高管理效率。

由於 Control Manager 採用 Web 介面，因此只要能執行 Microsoft™ Internet Explorer 的電腦都可以使用這套軟體。不同於「管理主控台」的是，Control Manager 的 Web 主控台可讓您同時管理多台「資料伺服器」，使病毒安全防護策略的管理更嚴密也更具彈性。

ServerProtect「資料伺服器」只能管理在該伺服器註冊的「一般伺服器」。但是 Control Manager 可以管理多台「資料伺服器」，進而能夠管理這幾台「資料伺服器」所屬的「一般伺服器」，因而簡化了大型網路的管理。

本章內容如下：

- 何謂 Trend Micro Control Manager
- 安裝與移除 Control Manager 代理程式 ServerProtect 版

- Control Manager 代理程式 ServerProtect 版的功能
- 病毒爆發防範服務

何謂 Trend Micro Control Manager

Control Manager 使管理員能置身於系統的中央位置，以便集中控管病毒與內容安全防護程式，且不受限於程式的實際位置以及所採用的平台，因此簡化了企業病毒與內容安全防護策略的管理。

Control Manager 以易於了解的圖形來顯示完整的網路架構，讓您輕鬆了解如何部署趨勢科技的產品與服務（包括 ServerProtect），並建立有效而目標明確的病毒安全防護策略。

Control Manager 可與更新伺服器連線，以提供 TrendLabs™ 所研發的最新資訊與服務，管理員能夠隨時掌握最新的病毒活動情形，並主動出擊，防堵任何可能的威脅。

遭受病毒攻擊時，Trend Micro Control Manager Web 主控台可以做為中央「指揮中心」，監控病毒擴散的情況，並實施遏阻策略、部署最新下載的病毒碼及管理病毒清除任務。只要能有效遏阻病毒的擴散，便能夠減少病毒對員工生產力的影響，並縮短收拾善後的時間。

Control Manager 是趨勢科技企業安全防護策略的重要元件。趨勢科技企業安全防護策略（TM EPS）為企業建構具調節性的防護體系，以因應不同階段的病毒爆發生命週期。

病毒爆發的活動方式分成三個主要階段：病毒爆發防範、病毒碼產生與部署以及損害評估與清除。為滿足企業全方位病毒安全防護的需求，TM EPS 採用極具彈性的架構，提供可擴充性、多平台服務與產品，以及集中式的管理與知識等功能。

TM EPS 將傳統單點式的病毒安全防護策略，透過網路上部署病毒爆發防範、偵測、保護與清除策略的集中式管理，轉換成企業全方位的安全防護策略。

Control Manager 具有以下優點：

- 主動式病毒爆發防範
- 安全的通訊基礎架構
- 工作委派
- 指令追蹤
- 即時的產品控管
- 集中式安裝的代理程式
- 集中式的更新控管
- 集中式的環境設定
- 集中式的記錄報表

安裝與移除 Control Manager 代理程式 ServerProtect 版

安裝 CM 代理程式 ServerProtect 版需要兩個步驟：

1. 從 Control Manager 伺服器取得公開金鑰。
2. 在「資料伺服器」上安裝代理程式。

部署代理程式之前，您需要以下資訊：

- Control Manager 伺服器的 Fully Qualified Domain Name (FQDN) 或 IP 位址
- 目標 ServerProtect「資料伺服器」上至少有一台共用磁碟機，用來安裝代理程式
- 具備 Control Manager 伺服器管理權限的使用者 ID
- 將用來註冊代理程式的 Control Manager 公開金鑰所在位置

取得公開金鑰

安裝 Control Manager 代理程式的第一個步驟是取得公開金鑰。

取得安裝所需的公開金鑰：

1. 請以下列方式開啟 Control Manager 主控台：

   http:// **電腦名稱** /ControlManager

   此處「電腦名稱」是 Control Manager 伺服器的 IP 位址或主機名稱。Control Manager 主控台隨即開啟。

2. 在「使用者 ID」和「密碼」欄位中輸入使用者 ID 和密碼。使用者 ID 必須有 Control Manager 主控台存取權限的 Operator、Power User 或 Administrator。
3. 在功能表上按「Products」。
4. 在左邊的功能表上按「Add/Remove Product Agents」。

5. 在「public encryption key」連結上按滑鼠右鍵後，選取「另存新檔」。將公開金鑰儲存在準備安裝代理程式的伺服器位置。

安裝代理程式

第二個步驟是，在所有 ServerProtect「資料伺服器」上安裝 Control Manager 代理程式。

安裝代理程式：

1. 須使用具備網域管理員權限的 Windows .NET/2000/NT 管理員帳號登入「資料伺服器」電腦。
2. 按兩下 ServerProtect 光碟上 CMAgent 資料夾中的 Setup.exe 來啟動安裝程序。「Trend Micro Control Manager 代理程式 ServerProtect 版安裝」畫面隨即開啟。
3. 在「歡迎」畫面上按「下一步」。請仔細閱讀授權合約，您必須同意合約內容，才能繼續執行安裝程式。按「下一步」，「安裝 Control Manager 代理程式」畫面隨即開啟。
4. 在「使用者 ID」中輸入管理員帳號。請務必保留這個帳號。一旦刪除這個帳號，將再也無法管理代理程式。

   注意： 此使用者 ID 應該已事先建立，而且具備 Control Manager 伺服器的管理員權限。

5. 當「設定訊息遞送路徑」畫面出現時，設定輸入與輸出訊息的路徑。可以直接傳送輸出的訊息，也可以經由 Proxy 伺服器傳送。選擇任一項後，按「下一步」。「註冊 Control Manager 代理程式」畫面隨即開啟。

   接收輸入訊息的方式包括：

   - 任何主機：接受來自任何來源的訊息
   - IP 連接埠轉送：輸入供 Control Manager 通訊使用的映射 IP 位址和連接埠號碼

- Proxy 伺服器：選取「Proxy 伺服器通訊」核取方塊，來指定 Proxy 伺服器的 IP 位址、連接埠號碼和類型（HTTP 或 SOCKS 4）。如果您的 Proxy 伺服器需要認證，請選取「需要認證」核取方塊，並在「使用者名稱」和「密碼」欄位中指定正確的使用者名稱和密碼。

6. 按下「匯入」來設定與 Control Manager 伺服器的安全通訊。尋找要註冊代理程式之 Control Manager 伺服器的公開金鑰 E2EPublic.dat。

7. 依照畫面上的安裝指示完成安裝步驟。

移除代理程式

將 Control Manager 代理程式從 ServerProtect「資料伺服器」上移除的方法很簡單。

要移除 Trend Micro Control Manager 代理程式 ServerProtect 版：

1. 在「資料伺服器」電腦上按「開始｜設定｜控制台｜新增 / 移除程式」。

2. 按下「Trend Micro Control Manager 代理程式 ServerProtect 版」，再按「移除」，隨即出現一訊息方塊。

3. 按下「是」來移除 Control Manager 代理程式 ServerProtect 版。

4. 按下「關閉」來完成移除。

Control Manager 代理程式 ServerProtect 版的功能

Control Manager 代理程式 ServerProtect 版包含以下功能以管理 ServerProtect。

注意：ServerProtect「管理主控台」的功能只有一部分可在 Control Manager Web 主控台上使用。

工作

Control Manager 工作跟 ServerProtect 工作不同。ServerProtect 工作是您自行設定之後儲存起來供未來使用，而 Control Manager 工作則是已預先定義而且可以立即執行。

ServerProtect 和 Control Manager 工作可以同時執行，彼此不會互相干擾。

Control Manager 的 Web 主控台可用來執行下列 Control Manager 工作：

- 執行手動掃瞄（立即掃瞄）
- 啟動即時掃瞄
- 部署病毒碼檔案
- 部署掃瞄引擎檔案
- 部署程式檔案

記錄檔

您可以用 Control Manager 的 Web 主控台查閱下列記錄檔：

- 事件記錄檔
- 安全防護記錄檔

Outbreak Commander

Outbreak Commander 針對各種病毒攻擊類型提供不同的資訊和防範策略，幫助企業在病毒碼發佈之前迴避、隔離及遏阻病毒攻擊。

趨勢科技對所有發佈的病毒碼實施嚴格的品保測試，所以在完成病毒分析之後，還需要一小段時間才會正式發佈病毒碼。在病毒碼正式發佈之前，Outbreak Commander 可讓您獲得完整的資料分析。

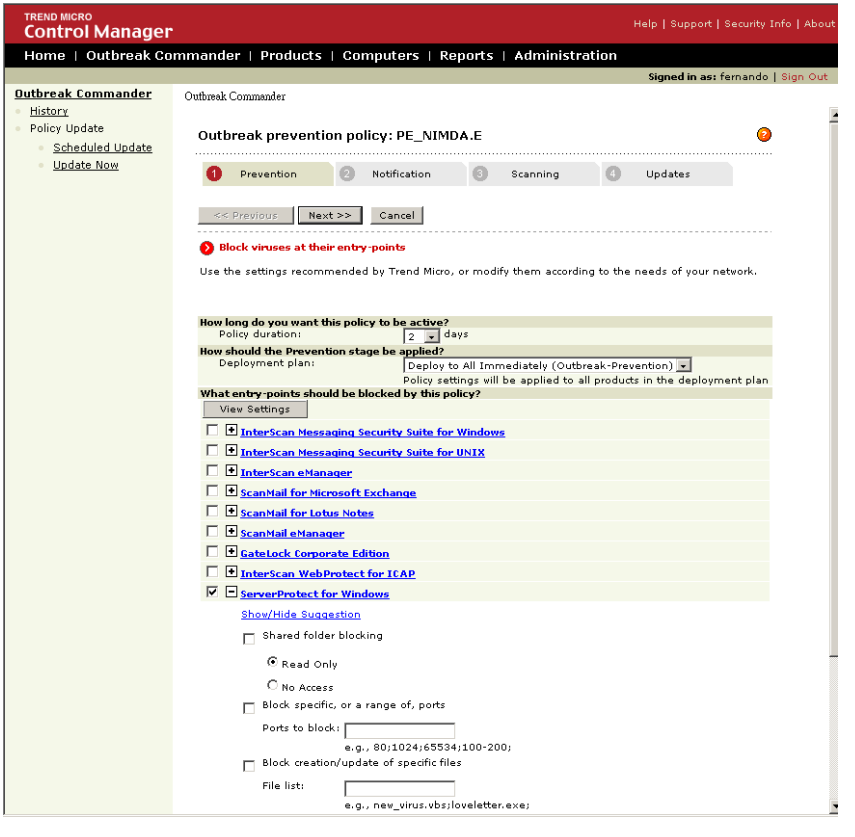


圖 5-1 Outbreak Commander 設定畫面

Outbreak Commander 是您與趨勢科技病毒爆發防範服務之間的主要介面，也是實施病毒爆發防範策略的主要方式。

病毒爆發防範策略（OPP）

病毒爆發防範策略（OPP）是由多項設定所組合而成的，使用者可利用 Outbreak Commander 直接將此策略套用到 ServerProtect 上。這些設定是由趨勢科技公司因應病毒爆發所建立的策略，並提供給 Control Manager 使用者作為病毒爆發防範服務的一部分。

這些設定是為了保護您的網路免於病毒爆發而設計的，而且只適用於相關產品。例如，對於只透過電子郵件散播的病毒，其防範策略中便只有針對訊息系統作設定。

病毒爆發防範服務

在所需要的病毒碼正式發佈之前，您可以透過 Control Manager 使用趨勢科技提供的「病毒爆發防範服務」（OPS），以主動防範新病毒的威脅。即使在收到警訊和病毒碼之間有一小段時間間隔，也能夠迅速遏阻病毒擴散，將系統損害降到最低，並縮短工作停擺的時間。

OPS 是趨勢科技企業安全防護策略（EPS）的重要元件，以創新的方式協助企業找出最有效的實務作法，並預防病毒攻擊時可能造成的損壞，或將其影響降到最小，以因應傳統安全保護措施所無法防禦的新一代威脅（例如 CodeRed 與 Nimda）。

注意：如需其他企業安全防護策略的資訊，請參考趨勢科技 Web 網站，網址：www.trendmicro.com.tw。

OPS 可提供：

- 針對新病毒的威脅提供即時通知
- 持續且全面性地更新病毒爆發狀態

- 針對特定病毒提供遏阻方式的建議
- 立即傳送針對特定病毒所制定的產品設定，稱為「策略」

第 6 章

註冊與聯絡技術支援

這一章說明如何註冊 ServerProtect 及聯絡技術支援。

本章內容如下：

- 技術支援資訊
- 趨勢科技網路安全百科
- 註冊 Trend Micro ServerProtect
- 使用 SolutionBank
- 上傳病毒給趨勢科技
- TrendLabs

技術支援資訊

取得趨勢科技防毒軟體的使用授權後，您就有權獲得趨勢科技或授權經銷商所提供的病毒碼檔案更新與技術支援，為期一年。之後，您必須每年依照趨勢科技最新的維護費用來更新維護內容，才有權繼續得到這些服務。

您可以從趨勢科技網站下載趨勢科技所有產品的試用版。

如需技術支援，請參考以下線上資源：

電子郵件：support@antivirus.com.tw

網站支援：www.trend.com.tw/corporate/solutionbank/

常見問題集：www.trend.com.tw/corporate/solutionbank/

病毒情報中心：www.trendmicro.com.tw/vinfo/

趨勢科技網路安全百科

在趨勢科技的 Internet 網站上，我們的 「網路安全百科」提供易於了解的網路安全資訊：

www.trendmicro.com.tw/vinfo/

使用 「網路安全百科」可獲得如下資訊：

- 病毒黑名單
- 病毒氣象台
- 病毒教室
- 趨勢科技病毒百科全書
- 電腦病毒的基本說明
- 基本防毒概念的專題報導
- 產品詳細資料與白皮書

您也可以從 「管理主控台」查閱趨勢科技病毒百科全書。請在主功能表上按 「檢視 > 檢視病毒百科全書」。

註冊 Trend Micro ServerProtect

趨勢科技或授權經銷商為所有註冊使用者提供為期一年的技術支援、病毒碼下載及程式更新，一年之後，您必須支付最新的維護費用，才能繼續得到這些服務。

要註冊 ServerProtect，請瀏覽下列網站：

www.trendmicro.com/support/registration.asp

使用 SolutionBank 常見問題集

趨勢科技在網站上有一個名為 SolutionBank 的線上資料庫，提供一般問題的解答。例如發生錯誤訊息時，您就可以利用 SolutionBank 尋求解決的方法。

www.trend.com.tw/corporate/solutionbank/

SolutionBank 的內容會不斷更新，每天都會加入解決的方法。但是如果您找不到解答，您可以將問題直接傳送給趨勢科技，TrendLabs 的技術支援工程師將會為您提供解答，如需進一步的資訊，工程師將會跟您聯絡。

上傳病毒給趨勢科技

ServerProtect 使用病毒碼比對（比較掃瞄檔與已知病毒的「指紋」）以及智慧型分析（監控檔案是否有和病毒類似的行為）方式偵測中毒檔案。雖然這兩種方法對大多數使用者而言已經足夠，但您仍可以向趨勢科技的防毒工程師尋求支援。

如果您發現可疑檔案（ServerProtect 未發現病毒，但檔案有明顯的異常行為），或您發現檔案會造成「錯誤警訊」（您知道檔案未中毒，但 ServerProtect 認為含有病毒），歡迎您將檔案上傳給趨勢科技防毒工程師做進一步分析。

要上傳檔案給趨勢科技的「病毒醫生」：

1. 在網域瀏覽目錄上選取一台「一般伺服器」。
2. 在主功能表上按「執行 > 上傳檔案」，隨即顯示「上傳檔案給趨勢科技的病毒醫生」畫面。
3. 在適當的文字欄位中輸入您的姓名、公司、電話號碼和電子郵件地址。
4. 寫下問題的簡短描述。
5. 輸入您要使用的 SMTP 伺服器名稱。
6. 按下「瀏覽」來選取您要當作附件傳送的檔案。「選擇檔案」視窗隨即開啟。
7. 選取您要上傳的檔案，再按「確定」。
8. 按下「上傳」來傳送訊息。

趨勢科技的病毒工程師將會詳細分析您傳送的檔案，找出可能感染的任何病毒及其特徵，並將清除病毒的檔案回傳給您，一般是在 48 小時內。

TrendLabs

TrendLabs 是趨勢科技客服基本架構的骨幹，這個全球防毒研發暨產品支援中心擁有超過 250 名以上的工程師，負責為趨勢科技客戶提供每天 24 小時全年無休的服務，以迅速回應全球各地發生的任何電腦病毒威脅。TrendLabs 設在菲律賓 Metro Manila 的總部已獲得 ISO 9002 品質認證，另外在東京、巴黎、加州、台北、慕尼黑等地也都設有服務中心。

附 錄 A

將試用版昇級為正式版

如果不輸入產品序號，您可以安裝有效期 30 天的 ServerProtect 試用版。試用版擁有完整的功能，但病毒掃瞄功能會在 30 天後關閉。屆時，您應該購買使用授權，或移除試用版。

購買使用授權後，請參閱下列主題更新產品序號。

本章內容如下：

- 「軟體試用期限」視窗
- 檢視產品序號清單
- 更新產品序號

「軟體試用期限」視窗

安裝 ServerProtect 試用版之後，每次開啟 「管理主控台」時，都會顯示 「軟體試用期限」視窗。「軟體試用期限」視窗會顯示網路上哪些「一般伺服器」使用試用版，以及到期天數。

圖 A-1 「軟體試用期限」視窗

檢視產品序號清單

您可以用「管理主控台」檢視所有 ServerProtect「一般伺服器」的序號。

要檢視產品序號清單，請執行下列步驟：

1. 在主功能表上按「說明 > 關於 ServerProtect」，隨即顯示「關於 ServerProtect 管理主控台」視窗。

圖 A-2 「關於 ServerProtect 管理主控台」視窗

2. 按下「序號」，隨即開啟「序號清單」視窗，顯示網路上所有的 ServerProtect「一般伺服器」，以及個別的序號。

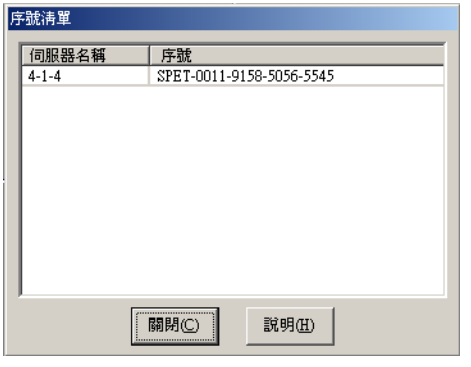


圖 A-3 ServerProtect「序號清單」視窗

3. 按下「關閉」以關閉「序號清單」視窗，再按「確定」以關閉「關於 ServerProtect 管理主控台」視窗。

更新產品序號

購買 ServerProtect 的使用授權後，就可以直接從「管理主控台」更新安裝的 ServerProtect 產品序號，而不須重新安裝 ServerProtect。

要更新產品序號，請執行下列步驟：

1. 在網域瀏覽目錄中選取要更新產品序號的「一般伺服器」。
2. 在主功能表上按「執行 > 更新序號」，隨即開啟「輸入新的序號」視窗。

圖 A-4 「輸入新的序號」視窗

3. 在「新序號」文字方塊中輸入新的序號。
4. 按下「確定」，否則，按「取消」以關閉視窗。

索引