McAfee Total Protection for Endpoint
試用指南

McAfee®

著作權

Copyright © 2009 McAfee, Inc. 保留一切權利。

未經 McAfee, Inc. 或其供應商或附屬公司書面許可，不得以任何形式、任何方式複製、傳播、改錄本出版品的任何內容，也不得將任何內容儲存於檢索系統或翻譯成任何語言。

商標特性

AVERT、EPO、EPOLICY ORCHESTRATOR、FOUNDSTONE、GROUPSHIELD、INTRUSHIELD、LINUXSHIELD、MAX (MCAFEE SECURITYALLIANCE EXCHANGE)、MCAFEE、NETSHIELD、PORTALSHIELD、PREVENTSYS、SECURITYALLIANCE、SITEADVISOR、TOTAL PROTECTION、VIRUSSCAN 與 WEBSHIELD 是 McAfee, Inc. 及/或其附設公司在美國及/或其他國家地區的註冊商標或商標。與安全性相關的紅色是 McAfee 產品特有的代表色。此處提及的其他所有註冊和未註冊商標都是其各擁有者的自有資產。

授權資訊

授權合約

所有使用者請注意：請仔細閱讀與您所購買之授權相應的適當法律合約，該合約提供了使用授權軟體的一般條款及條件。如果您不知道所取得的授權類型，請洽詢銷售人員，並查閱其他相關授權或您的軟件包裝中隨附、或作為購買的一部份另外收到的購買訂單文件 (如手冊、產品 CD 上的檔案或從下載軟體套裝的網站上獲得的檔案)。如果您不完全同意合約中提出的條款，請勿安裝軟體。如果適合，您可以將所購買的產品退至 MCAFEE 或購買地點，以取得全額退款。

授權和歸屬聲明

請參照產品的版本資訊。

目錄

McAfee Total Protection for Endpoint 簡介 4
安裝前的工作 6
伺服器需求 6
作業系統語言支援 7
安裝 McAfee Total Protection for Endpoint 套件 8
登入 ePolicy Orchestrator 9
設定 ePolicy Orchestrator 伺服器 10
新增要管理的系統 12
設定端點原則 14
設定電子郵件伺服器原則 20
設定端點工作 25
部署 McAfee Agent 27
使用儀表板和查詢 30
摘要 32
參考 33

McAfee Total Protection for Endpoint 簡介

歡迎使用 McAfee® Total Protection® for Endpoint。本解決方案整合了最佳且最完整的 McAfee 安全性，可為端點、電子郵件、網頁與資料做好保護。相較於購買與維護來自多家廠商的多種安全性元件，McAfee Total Protection for Endpoint 不只節省您的時間與金錢，還能針對企業所知與未知的威脅提供威力更強大的整合型防禦機制。

本指南的編排方式旨在讓您在一個測試環境中試用 McAfee Total Protection for Endpoint，該測試環境包含一部 ePolicy Orchestrator® (ePO™) 伺服器及一些用戶端電腦。本指南涵蓋一些基本的步驟，當您快速安裝 ePolicy Orchestrator、設定基本原則與工作，以及部署下列 McAfee 產品以提供用戶端保護時，需要使用這些步驟：

- VirusScan® Enterprise 8.7i
- AntiSpyware Enterprise 8.7
- Host Intrusion Prevention 7.0
- SiteAdvisor® Enterprise Plus 2.0
- GroupShield® 7.0

本指南提供的真實步驟範例可讓您應用在真實部署環境中，但不涵蓋每種可能的部署情況，也沒有對每一項功能都進行檢驗。如需 Total Protection for Endpoint 內附的所有產品面向完整資訊，請參閱個別產品指南。

如需完整的產品說明文件，請參閱 McAfee 知識庫。

在 [閱讀支援] 下方，按一下 [產品說明文件] 並選擇產品與版本，然後選擇文件。

產品說明

Total Protection for Endpoint 中的產品可以分為以下幾個類別：

- 管理解決方案
- 端點保護
- 電子郵件伺服器保護

管理解決方案

Total Protection for Endpoint 提供下列產品做為管理解決方案。

產品	說明
McAfee ePolicy Orchestrator	ePolicy Orchestrator 是領先業界的企業級系統安全性管理解決方案。它能針對惡意威脅與攻擊提供整合式的主動防禦系統。ePolicy Orchestrator 整合了無與倫比的全域原則控制、單一代理程式、中央主控台和自訂報告功能，讓您輕鬆管理自己的系統安全性環境。
McAfee Agent	McAfee Agent 這套用戶端架構支援 McAfee 安全性管理基礎架構。它能在端點產品與 ePolicy Orchestrator 之間，以及本機服務和端點產品之間提供安全的通訊功能。McAfee Agent 架構能夠讓端點產品專注在強制執行原則，同時提供包含記錄、通訊與原則儲存等廣泛的服務。

端點保護

Total Protection for Endpoint 提供下列產品做為端點保護用途。

產品	說明
McAfee VirusScan® Enterprise 8.7i	VirusScan Enterprise 是一個在安全領域頗受信賴的產品，它是個人電腦及伺服器進階主動保護方面的領導者。在病毒發作時，企業可以依賴 VirusScan Enterprise 的以下主要功能：清除記憶體、Rootkit、登錄及檔案，以及防止惡意程式碼傳播到其他系統。 VirusScan Enterprise 還包含防毒、入侵防禦及防火牆的功能，以保護系統免遭已知及不明攻擊的侵害。
McAfee AntiSpyware Enterprise 8.7	AntiSpyware Enterprise Module 是最主要之企業級防間諜軟體的軟體解決方案，它使用真正的常駐掃描來識別、主動封鎖及安全消除可能不需要的程式 (PUP)，以便讓商業可用性達到最佳。透過 ePolicy Orchestrator 的集中管理，McAfee AntiSpyware Enterprise Module 能夠與 VirusScan Enterprise 完美整合，直接減少因為威脅與 PUP 緣故所產生的干擾。
McAfee Host Intrusion Prevention 7.0	Host Intrusion Prevention 結合了簽章、行為式防護以及系統防火牆，藉此監控與封鎖入侵的行為。對資產進行保護，改善業務流程的可用性、機密性及完整性。單一代理程式可以讓部署、設定及管理變得更加輕鬆，同時減少修補的頻率，並降低修補的緊迫性。
McAfee SiteAdvisor® Enterprise Plus 2.0	SiteAdvisor Enterprise Plus 能夠完全封鎖間諜軟體、廣告軟體、網路釣魚詐騙等等的惡意行為，讓您的員工安全自在地瀏覽與搜尋網頁。已經整合至 McAfee 解決方案的 SiteAdvisor Enterprise 技術，能夠將網頁安全性加入到您的全方位保護機制中，藉此引導並保護使用者免於線上威脅。

電子郵件伺服器保護

Total Protection for Endpoint 提供下列產品做為電子郵件伺服器保護用途。

產品	說明
McAfee GroupShield® 7.0	GroupShield 能夠在電子郵件與其他文件進出您的 Microsoft Exchange 和 Lotus Domino 伺服器之際加以保護。 GroupShield 會主動掃描病毒、自動管理爆發的病毒，並阻止惡意程式碼干擾您的系統。 GroupShield 的內容篩選功能會封鎖或隔離包含違反內容規則之特定單字及片語的郵件。
McAfee Anti-Spam for GroupShield 7.0	Anti-Spam for GroupShield 會封鎖來自您 Microsoft Exchange 和 Lotus Domino 郵件伺服器的垃圾郵件。這樣不但會增加員工生產力，還能阻止網路釣魚詐騙活動，藉此保護機密資料免於遭到員工外洩。Anti-Spam 整合了 McAfee GroupShield，可針對忙碌的郵件伺服器減少資源使用率。

當您準備將產品部署到環境中時，例如 VirusScan Enterprise 或 Host Intrusion Prevention，您會用到 ePolicy Orchestrator 和 McAfee Agent 來處理部署與更新作業。McAfee 建議您使用下列章節中的工作流程來開始使用解決方案。

安裝前的工作

安裝 McAfee Total Protection for Endpoint 軟體之前，請先驗證每個元件都符合下方所列的最低系統需求。

伺服器需求

硬體與網路最低需求

- 可用磁碟空間 - 最少 1GB；建議使用 2GB。
- 記憶體 - 1GB 可用 RAM；建議使用 2-4GB。
- 處理器 - Intel Pentium III 或更高等級；1 GHz 或更快速度。
- 顯示器 - 1024x768、256 色、VGA 顯示器。
- NIC - 網路介面卡；100MB 或更高。
- 檔案系統 - 建議採用 NTFS (NT 檔案系統) 分割區。
- IP 位址 - McAfee 建議針對 ePolicy Orchestrator 伺服器使用靜態 IP 位址。

軟體需求

- 伺服器等級的作業系統
  - Windows 2000 Server (含 Service Pack 4 或更新版本)。
  - Windows 2000 Advanced Server (含 Service Pack 4 或更新版本)。
  - Windows Server 2003 Enterprise (含 Service Pack 1 或更新版本)。
  - Windows Server 2003 Standard (含 Service Pack 1 或更新版本)。
  - Windows Server 2003 Web (含 Service Pack 1 或更新版本)。
  - Windows Server 2003 R2 Enterprise。
  - Windows Server 2003 R2 Standard。
  - Windows Server 2008。
- 瀏覽器
  - Microsoft Internet Explorer 6.0 Service Pack 1 或更新版本。
  - Microsoft Internet Explorer 7.0
  - 若使用 Proxy，請略過 Proxy 伺服器：

  1 在 Internet Explorer 中，選取 [工具] 功能表中的 [網際網路選項]。
  2 選取 [連線] 索引標籤，然後按一下 [區域網路設定]。
  3 選取 [在您的區域網路使用 Proxy 伺服器]，然後選取 [近端網址不使用 Proxy]。
  4 依需要按一下 [確定] 以關閉 [網際網路選項]。

- 網域控制站 - ePolicy Orchestrator 軟體可以管理工作群組或 Windows 網域中的系統。以下的安裝說明將會使用後者，因此伺服器必須是您 Windows 網域的成員。如需指示說明，請參閱 Microsoft 產品說明文件。
- 安全保護軟體
  - 在 ePolicy Orchestrator 伺服器上安裝和/或更新防毒軟體並掃描病毒。

    注意：若要安裝 ePolicy Orchestrator 的系統上執行的是 VirusScan Enterprise 8.5i 或 8.7i，則您必須確定在 ePO 安裝期間停用 VSE 存取保護規則，否則安裝將會失敗。

  - 在 ePolicy Orchestrator 伺服器上安裝和/或更新防火牆軟體。

資料庫考慮事項

必須先安裝資料庫，才可以安裝 ePO。依預設，安裝程式會先安裝 SQL Server 2005 Express 資料庫，然後在同一部伺服器上安裝 ePolicy Orchestrator 軟體。請注意，也可以選擇將 ePO 和其他資料庫搭配使用，例如 MSDE 2000、SQL 2000 或 SQL 2005 Server。如需詳細資訊，請參閱《ePO 4.0 安裝指南》。

其他軟體需求

軟體	附註
MSXML 6.0	若先前並未安裝，安裝精靈會自動安裝。
Internet Explorer 6 SP1 或更新版本	必須取得並安裝。
.NET Framework 2.0	若先前並未安裝，安裝精靈會自動安裝。
MDAC 2.8	若先前並未安裝，安裝精靈會自動安裝。
SQL Server 2005 Backward Compatibility	若先前並未安裝，安裝精靈會自動安裝。

作業系統語言支援

此版本的 McAfee Total Protection for Endpoint 可以在所支援之作業系統的以下語言版本上執行：

- 中文 (簡體)
- 中文 (繁體)
- 英文
- 法文 (標準)
- 韓文
- 西班牙文
- 德文 (標準)
- 日文

安裝 McAfee Total Protection for Endpoint 套件

本節會指引您使用預設的選項來安裝 McAfee Total Protection for Endpoint 套件。McAfee Total Protection for Endpoint 套件安裝程式將會安裝 ePO 伺服器，同時將端點軟體簽入 ePO 存放庫。

工作

1 從 McAfee 官方網站下載並解壓縮 McAfee Total Protection for Endpoint 軟體的內容，存放到 ePO 伺服器或要使用之管理伺服器的暫存目錄。

2 連按兩下 [setup.exe]。[歡迎使用 Total Protection for Endpoint 套件的 McAfee ePolicy Orchestrator 安裝程式] 頁面便會出現。

3 按 [下一步]。[試用] 頁面便會出現。

4 按一下 [確定]。[使用者授權合約] 頁面便會出現。

5 接受 [使用者授權合約]，然後按一下 [確定]。[選擇要評估的軟體] 頁面便會出現並顯示下列選項 (預設為啟用)：

- 基本安裝
- Host Intrusion Prevention
- GroupShield for Email Servers

6 按 [下一步]。[設定管理員資訊] 頁面便會出現。

7 輸入要用於 ePolicy Orchestrator 管理員帳戶的使用者名稱和密碼，然後按 [下一步]。[選擇安裝類型] 頁面便會出現。

附註：稍後需使用此相同的認證來登入 ePolicy Orchestrator。

8 選取 [預設]，使用預設的位置和設定來安裝 ePolicy Orchestrator 和 Microsoft SQL 2005 Express，然後按 [下一步]。螢幕上會出現確認對話方塊。

9 按一下 [確定] 以安裝 Microsoft SQL 2005 Express。[設定資料庫資訊] 頁面便會出現。

10 識別 ePolicy Orchestrator 伺服器用來存取資料庫的帳戶類型與驗證詳細資料。

- 從 [資料庫伺服器認證] 欄位下拉式清單選取 Windows 網域，輸入網域使用者名稱和密碼，然後按 [下一步]。[開始複製檔案] 頁面便會出現。

附註：依預設會啟用 Windows 驗證，因為 SQL Express 不允許 SA 驗證。

11 按 [下一步] 開始安裝。[InstallShield 精靈完成] 頁面便會出現，依預設會啟用下列選項：

- 選取 [是，我要檢視 ReadMe 檔] 以檢視 Readme。
- 選取 [是，我要立即啟動 McAfee ePolicy Orchestrator] 以啟動 ePolicy Orchestrator 使用者介面。

附註：安裝期間系統可能會提示您變更一或多個預設連接埠號碼，以避免發生任何衝突。

12 按一下 [完成]。

登入 ePolicy Orchestrator

您可以使用此工作登入 ePolicy Orchestrator。您必須具備有效認證才能執行此作業。

工作

1 若要啟動 ePolicy Orchestrator 軟體，請開啟網際網路瀏覽器並前往該伺服器的 URL (例如：https://<伺服器名稱>:8443)。[登入 ePolicy Orchestrator] 對話方塊便會出現。

   附註：您也可以連按兩下桌面上的 McAfee ePolicy Orchestrator 圖示來啟動 ePolicy Orchestrator。

2 輸入在 < 安裝 McAfee Total Protection for Endpoint 套件 > 章節的步驟 7 中建立之有效帳戶的 [使用者名稱] 和 [密碼]。

   附註：密碼必須區分大小寫。

3 選取您要軟體顯示的 [語言]。

4 按一下 [登入]。

設定 ePolicy Orchestrator 伺服器

ePolicy Orchestrator 存放庫可集中放置所有 McAfee 產品安裝程式、更新與簽章套件。ePolicy Orchestrator 的模組化設計可以「延伸模組」方式新增產品。這些項目包括新的或更新版本的 McAfee 產品，例如 VirusScan Enterprise 與非 McAfee 產品 (來自 McAfee 合作夥伴)。「套件」指的是可以簽入主存放庫，然後部署到用戶端系統的元件。

如需延伸模組與套件的詳細資訊，請參閱《ePolicy Orchestrator 產品指南》中的下列主題：

- 延伸模組及其功能
- 部署產品和更新的套件

依據您在安裝期間的選擇，Total Protection for Endpoint 用戶端軟體應該已經新增到您的 ePO 主存放庫中。若要驗證安裝，請移至主存放庫。

設定存放庫提取工作

為了讓 ePolicy Orchestrator 將您的用戶端系統保持在最新狀態，您必須設定「存放庫提取工作」以便在指定時間間隔內從 McAfee 網站 (HTTP 或 FTP) 擷取更新。

附註：系統會在安裝期間自動為您建立存放庫提取工作。

工作

您可以使用此工作建立存放庫提取工作，以新增並更新用戶端軟體。

1 移至 [自動處理 | 伺服器工作]。

2 在清單中，找到名為 [更新主存放庫] 的工作，然後按一下 [動作] 欄位中的 [編輯] 以開啟 [伺服器工作產生器]。

3 在 [說明] 頁面上，將 [排程狀態] 設為 [已啟用]，然後按 [下一步]。

4 在 [動作] 頁面上，標示為 1 的頁面說明底下會有一條灰色列。從下拉式清單中選取 [存放庫提取]。

5 選取 [將現有的套件移至舊版分支]，然後按 [下一步]。

   附註：簽入此選項可讓 ePolicy Orchestrator 保有一天以上的簽章檔。下一次執行提取工作時，今日的更新就會移至名為「舊版」的伺服器目錄中。這可讓您在必要時回復更新。

6 在 [排程] 頁面上，選擇您想要 ePolicy Orchestrator 檢查 McAfee 網站上更新檔的時間。
   - 將工作排程為 [每日] 執行，而且 [沒有結束日期]。
   - 將 [排程] 設為 [介於] 早上 9:00 到下午 11:00。
   - 將 [每] 設為二或三小時。

   提示：McAfee 建議每天檢查更新數次，確保您擁有最新的內容。

7 按 [下一步]。

8 在 [摘要] 頁面，按一下 [儲存]。主控台便會回到 [伺服器工作] 頁面。

9 尋找 [更新主存放庫] 工作，然後在 [動作] 欄位底下，按一下 [執行]。此時會立即擷取目前的更新，並開啟 [伺服器工作記錄]。

檢查提取工作狀態

[伺服器工作記錄] 可用來顯示 McAfee 提取工作狀態。您可以使用此工作，驗證「更新主存放庫」工作已經完成從 McAfee 網站提取更新的動作。

工作

1 移至 [報告 | 伺服器工作記錄]。

2 在工作清單中，找到 [更新主存放庫] 工作。

3 當 [狀態] 欄位報告 [已完成]，表示工作已完成。

新增要管理的系統

ePolicy Orchestrator 系統樹狀目錄可以將受管理系統組織為多個單元，以便進行監視、指派原則、排程工作及採取動作。這些單元叫做「群組」，是由全域管理員或具有適當權限的使用者建立與管理，而且可以同時包括系統與其他群組。在開始為網路中的用戶端系統管理端點原則之前，您必須先將這些系統新增到您的系統樹狀目錄。

組織與填入系統樹狀目錄的方法有以下幾種：

- 建立自己的群組並新增個別系統，以手動組織自己的系統樹狀目錄結構。
- 同步處理 Active Directory 或 NT 網域以做為系統來源。在使用 Active Directory 的案例中，同步化作業也會提供系統樹狀目錄結構。
- 依據 IP 範圍或子網路建立自己的群組。這項程序稱為「準則型分類」。
- 從文字檔案匯入群組和系統

本節中的工作流程將使用手動方式建立簡單的結構以供評估。在真實網路中部署 ePolicy Orchestrator 時使用此方法可能會很緩慢，但在測試網路中新增少量的系統就很好用。當您對 ePolicy Orchestrator 比較熟悉之後，就可以嘗試其他方法。

建立您的系統樹狀目錄群組

您可以使用此工作，將群組新增到系統樹狀目錄。針對本練習，我們將建立兩個群組，亦即 Servers 群組和 Workstations 群組。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [群組]。

2 反白 [我的組織]，然後按一下 [新增子群組]。

3 輸入 Test Group，然後按一下 [確定]。新群組會出現在系統樹狀目錄中。

4 反白 [Test Group] 並按一下 [新增子群組]，然後輸入 Servers 並按一下 [確定]。

5 重複步驟 4，但是輸入 Workstations 做為群組名稱。回到 [群組] 頁面後，反白 [Test Group]。您的 Servers 與 Workstations 群組現在已經列在 [群組] 頁面中了。其分類次序應該與您建立群組時的次序一致。

新增系統至您的系統樹狀目錄群組

您可以使用此工作，手動將一些測試系統新增至您的 ePO 系統樹狀目錄。

1 在系統樹狀目錄中，反白 [工作站] 群組並按一下 [新增系統]。

2 在 [如何新增系統] 中，選取 [將系統新增至目前的群組，但不部署代理程式]。

3 在 [要新增的系統] 中，將每個系統的 NetBIOS 名稱輸入文字方塊中，並以逗號、空格或換行符號來加以分隔。您也可以按一下 [瀏覽] 來選取系統。

4 驗證已停用 [系統樹狀目錄分類]。

5 按一下 [確定]。

6 視需要重複以上步驟，將更多系統新增至 [Servers] 群組中。

將新系統組織到群組中

由於您在先前幾節中已經執行了一些工作，您的系統樹狀目錄中現在包含好幾個群組與系統。在真實的生產環境中，新的系統會連絡 ePolicy Orchestrator 伺服器，而且需要放到系統樹狀目錄中。當您在新的系統上安裝 McAfee Agent (透過 Rogue System Detection 或另一種方法) 時，就會出現這種情況。不管是哪一種情況，系統都會放在 [遺失與發現] 群組中。

ePolicy Orchestrator 內建功能強大的群組分類功能，可讓您設定當系統第一次連絡 ePO 伺服器時，如何將自己歸類到系統樹狀目錄中。如需此功能的詳細資訊，請參閱《ePolicy Orchestrator 4.0 版產品指南》中的 < 準則型分類 > 。

在本練習當中，您會依據標記建立系統分類規則。ePolicy Orchestrator 會建立兩個預設標記供您使用，分別是「伺服器」和「工作站」。分類規則必須等到不屬於系統樹狀目錄中的某個系統呼叫 ePO 伺服器時才會開始產生作用。您也可以排程分類規則，或手動加以執行。

工作

您可以使用此工作，依據預設標記建立分類規則。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [群組]。
2 反白 [Test Group]。
3 在 [群組] 頁面上方，找到 [分類準則] 標籤，然後按一下 [編輯]。
4 選取 [符合以下任何準則的系統 (IP 位址和/或標記)]。此時頁面會展開並顯示額外的選項。
5 按一下 [新增標記]。
6 從下拉式功能表中，選取 [伺服器] 並按一下加號 (+)，然後選取 [工作站]。
7 按一下 [儲存]。
8 在 [系統樹狀目錄] 中，反白 [我的組織]。
9 在 [分類次序] 清單中，找到 [Test Group] 項目。在 [動作] 欄位中，按一下 [上移]，直到群組移至清單的最上層。如此一來，當您將新的系統放到系統樹狀目錄中時，此群組會是首先評估的項目。

使用系統樹狀目錄詳細資訊

您可以使用許多群組類型來組織您的系統樹狀目錄。

除了群組之外，您可以將標記新增到系統中，以便透過依據系統內容的特徵進一步加以識別。

設定端點原則

您可以透過原則，針對用戶端系統上執行的各式 Total Protection for Endpoint 產品 (例如 McAfee Agent 和 VirusScan Enterprise) 進行設定。

為了讓您的原則反映所需的各種設定與例外項目，McAfee 建議您在進行原則指派之前，先建立相關原則。為了方便使用，您可以將原則依據其功能來命名。建立自己的「具名原則」可讓您依據系統的角色或功能輕鬆套用原則。

本節將逐步帶領您完成幾項原則變更，供您應用在 McAfee Agent、 VirusScan Enterprise、Host Intrusion Prevention 和 SiteAdvisor Enterprise 之類的生產環境。這些工作代表建議的基本原則設定。一旦您更熟悉套件的使用之後，還有更多額外的原則選項可供您考慮。

如果您已在 Total Protection for Endpoint 中安裝所有產品，McAfee 建議您執行本節中所述的所有工作。

建立 McAfee Agent 的原則

評估 McAfee Total Protection for Endpoint 時，變更 McAfee Agent 原則以在用戶端系統上顯示系統匣圖示會有所幫助。這麼做可讓您檢視「代理程式狀態監視器」。

當您與遠端辦公室的 WAN 連線太慢，或是受管理的節點太多時，您可能需要變更 McAfee Agent 原則。

例如，您可以決定使用慢速連線進行通訊的系統應該每隔 180 分鐘連絡 ePolicy Orchestrator 一次，亦即一天 8 次，而不是預設的 24 次。在此情況下，您可以建立名為「低頻寬」或「3 小時輪詢一次」的原則，並將 [代理程式與伺服器連線間隔] 選項從預設的 60 分鐘改為 180 分鐘。

工作

您可以使用此工作，建立可在用戶端系統上顯示 McAfee Agent 的原則：

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [McAfee Agent]。

3 在列出 [McAfee Default] 的那行，按一下 [複製]。

4 在 [名稱] 中，輸入 Show Agent Icon，然後按一下 [確定]。

5 在列出新原則的那行，按一下 [編輯]。

6 選取 [顯示 McAfee 系統匣圖示] 旁邊的方塊，然後按一下 [儲存]。

ePolicy Orchestrator 會提供您選項，讓您從遠端存取每一個系統上的 McAfee Agent 記錄。如需這項好用的疑難排解工具詳細資料，請參閱《ePolicy Orchestrator 產品指南》。

建立 VirusScan Enterprise 的原則

本節將以三個 VirusScan Enterprise 原則的範例來說明。第一個範例的設計可預防使用者對各自受管理系統上的 VirusScan 設定進行變更。第二個範例可在伺服器上建立資料庫例外項目。第三個範例會暫時修改「不需要的程式原則」。

鎖定本機 VirusScan 主控台

您可以使用此工作修改預設的 [VirusScan Enterprise 使用者介面原則]，預防使用者竄改本機 VirusScan 介面。 VirusScan Enterprise 會同時在工作站與伺服器上執行；因此， VirusScan 原則對於個別平台會採用不同的設定。在本例中，您只需要對工作站設定進行變更。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。

3 從 [類別] 下拉式功能表中，選取 [使用者介面原則]。

4 在列出 [McAfee Default] 的那行，按一下 [複製]。

5 在 [名稱] 中，輸入 Lock VSE Console，然後按一下 [確定]。

6 在列出新的 [Lock VSE Console] 原則的那行，按一下 [編輯]。

7 在功能表列上，按一下 [密碼選項]。

8 確定 [設定] 選項已設為 [工作站]。

9 在 [使用者介面密碼] 中，選取 [以密碼保護所有列出的項目]。

10 在提供的方塊中輸入密碼，然後按一下 [儲存]。

在伺服器上建立檔案例外項目

您可以使用此工作建立 VirusScan 原則，以排除伺服器上兩個假設的資料庫檔案。您常常會在許多資料庫與郵件伺服器上，建立這些類型的掃描例外項目。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。

2 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。

3 展開 [Test Group]，然後按一下您的 [Servers] 群組。您可以先設定此原則，再將系統加入此群組中。

4 在 [常駐掃描預設處理程序原則] 右側，按一下 [編輯指派]。

5 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。

6 在 [指派原則] 中，按一下 [新增原則]。

7 在 [建立新原則] 對話方塊中，輸入 Database AV Exclusions，然後按一下 [確定]。這麼做會開啟原則編輯器。

8 從 [設定] 下拉式功能表中，選取 [伺服器]。

9 在功能表列上，按一下 [排除]。

10 在 [不掃描的項目] 中，按一下 [新增]。

11 在對話方塊中，選取 [依圖樣]，然後輸入 data.mdf，接著按一下 [確定]。再按一下 [新增]，然後輸入 data.ldf 做為另一項例外，接著按一下 [確定]。

此工作只會指定檔案名稱。在真實環境中，您可以指定完整路徑以縮小排除範圍。

12 一旦列出兩項例外，請按一下 [儲存]。

13 從 [指派原則] 下拉式功能表中，選取 [Database AV Exclusions]，然後按一下 [儲存]。

以 Microsoft Exchange Server 為例，以下連結可在您執行 Exchange 2007 的檔案層級防毒掃描時，引導您設定 Microsoft 建議的例外項目：

http://technet.microsoft.com/zh-tw/library/bb332342.aspx。

在 Microsoft Exchange Server 的 VirusScan 原則中，儘管需要設定的例外項目數量較多，但設定方法大致上與本例所示相差不遠。

建立 AntiSpyware Enterprise 模組的原則

AntiSpyware 模組安裝完畢後，會立即啟用並清除或刪除所找到的任何可能不需要的程式 (PUP)。儘管它會偵測並清除間諜軟體和廣告軟體，但還是有一些您不想要清除的 PUP，例如 IT 部門的

管理工具。舉例來說，公司裡的 IT 員工可能會使用一些遠端管理工具、連接埠掃描程式或是密碼破解公用程式。這些工具大部分都是系統管理員合法用在網路上的。

本節將說明偵測網路上 PUP 的方法，藉此搜尋存在的項目、針對任何合法用途的項目建立例外，然後設定掃描程式來封鎖剩餘項目。

此工作會修改 VirusScan 常駐掃描設定以記錄找到的 PUP，但不會加以刪除。 VirusScan 會持續偵測並清除病毒、蠕蟲、特洛伊木馬程式與其他威脅。此工作目的是以「稽核模式」檢查存在數天或一週的 PUP、檢查 ePolicy Orchestrator 中的 PUP 偵測報告，並識別所需的例外項目。

之後您會變更原則指派以便再次清除 PUP。

工作

您可以使用此工作修改預設的 VirusScan 常駐掃描原則，以便稽核受管理系統上的 PUP。

1 移至 [系統 | 原則目錄]。
2 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。
3 在 [類別] 欄位中，選取 [常駐掃描預設處理程序原則]。
4 在列出 [McAfee Default] 的那行，按一下 [複製]。
5 在 [名稱] 中，輸入 Audit for PUPs，然後按一下 [確定]。
6 在列出新原則的那行，按一下 [編輯]。
7 從 [設定] 下拉式功能表中，選取 [工作站]。
8 在功能表列上，按一下 [動作]。
9 在 [找到不需要的程式時] 中，針對要執行的第一個動作，從下拉式功能表中選取 [允許存取檔案]。此動作會停用第二個動作。
10 按一下 [儲存]。

建立 SiteAdvisor Enterprise Plus 的原則

在本節中，您會建立 SiteAdvisor Enterprise Plus 評等動作原則與強制訊息原則。

建立評等動作原則

您可以使用此工作建立新的原則，以阻止使用者存取包含威脅的網站，或是警告使用者有關網站上的潛在威脅。

「評等動作」原則中的選項可讓您使用 SiteAdvisor 評等 (綠色、黃色、紅色或未評等) 來決定使用者是否可存取某個網站或網站的資源，例如下載檔案等。

- 對每個黃色、紅色或未評等的網站，您可指定是否允許、警告或是封鎖該網站。
- 對每個黃色、紅色或未評等的下載檔案，您可指定是否允許、警告或是封鎖該下載項目。對於可能對具有整體綠色評等的網站產生威脅的個別檔案，這項機制可讓您提供使用者更精細的保護。
- 對每個網路釣魚網頁，您可指定是否要封鎖或允許存取。對於可能對具有整體綠色評等的網站使用網路釣魚技巧的網頁，這項機制可讓您提供使用者更精細的保護。

工作

1 移至 [系統 | 原則目錄]。
2 從 [產品] 下拉式功能表中，選取 [SiteAdvisor Enterprise Plus]。
3 從 [類別] 下拉式功能表中，選取 [評等動作]。
4 在列出 [McAfee Default] 的那行，按一下 [複製]。
5 在 [名稱] 中，輸入 Rating Actions Policy，然後按一下 [確定]。
6 在列出新原則的那行，按一下 [編輯]。

7 針對 [網站瀏覽評等動作]，請對黃色網站設定 [警告]，對紅色網站設定 [封鎖]，並對未評等網站設定 [警告]。

8 按一下 [儲存]。

建立強制訊息原則

您可以使用此工作建立新的原則，自訂使用者嘗試存取某個您已關聯評等動作的網站時，要向使用者顯示的訊息。此訊息會以安全氣球方式顯示，並顯示在 [警告] 或 [封鎖] 頁面。

工作

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [SiteAdvisor Enterprise Plus]。

3 從 [類別] 下拉式功能表中，選取 [強制訊息]。

4 在列出 [McAfee Default] 的那行，按一下 [複製]。

5 在 [名稱] 中，輸入 Enforcement Messaging Policy，然後按一下 [確定]。

6 在列出新原則的那行，按一下 [編輯]。

7 按一下 [網站] 索引標籤。

8 選擇一種語言。

9 在以下情況中，輸入長度上限為 50 個字元的訊息：

- 至於您已設為 [警告] 的網站，輸入警告訊息。
- 至於您已設為 [封鎖] 的網站，輸入「封鎖存取」訊息。
- 至於您已設為 [允許] 的網站，輸入「允許存取」訊息。

10 按一下 [儲存]。

指派原則給系統

您現在已有數個原則，可以指派給系統樹狀目錄中的系統。在本練習中，您將從 [系統樹狀目錄] 介面指派所有原則。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。

2 反白 [Test Group]。

3 指派 McAfee Agent 原則：

- 從 [產品] 下拉式功能表中，選取 [McAfee Agent]。
- 在列出 [My Default] 的那行，按一下 [編輯指派]。
- 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。
- 從 [指派原則] 下拉式功能表中，選取 [顯示代理程式圖示]。
- 按一下 [儲存]。

4 指派 SiteAdvisor Enterprise Plus 原則：

- 從 [產品] 下拉式功能表中，選取 [SiteAdvisor Enterprise Plus]。
- 在列出 [評等動作] 的那行，按一下 [編輯指派]。
- 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。
- 從 [指派原則] 下拉式功能表中，選取 [Rating Actions Policy]。
- 按一下 [儲存]。
- 在列出 [強制訊息] 的那行，按一下 [編輯指派]。
- 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。
- 從 [指派原則] 下拉式功能表中，選取 [Enforcement Messaging Policy]。

- 按一下 [儲存]。

5 指派 VirusScan Enterprise 原則：

附註：在您建立好 [Database AV Exclusions] 原則時，會一併將其指派給 [Servers] 群組。

- 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。
- 在列出 [使用者介面原則] 的那行，按一下 [編輯指派]。
- 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。
- 從 [指派原則] 下拉式功能表中，選取 [Lock VSE Console]。
- 按一下 [儲存]。
- 從 [指派原則] 下拉式功能表中，選取 [常駐掃描預設處理程序原則]，然後選取 [Audit for PUPs]。
- 按一下 [儲存]。當您回到 [原則] 頁面時，會看到 [常駐掃描預設處理程序原則] 在 [中斷繼承] 欄位內有一個項目。這是因為您已將 [Database AV Exclusions] 原則指派給 [Servers] 群組。

Host Intrusion Prevention 原則

McAfee Host Intrusion Prevention 會提供三種保護類型：IPS、防火牆及應用程式封鎖。在預設的安裝中，IPS 防護會設為 [防止高嚴重性入侵]，並停用防火牆與應用程式封鎖原則。此原則除了提供立即的防護之外，還會延伸 VirusScan Enterprise 緩衝區溢位的基本功能，同時保護您免於許多 Microsoft 弱點的威脅，但不會影響到您的企業運作。

本節一開始將說明基本防火牆原則，並針對您可以套用或調整的其他規則提供說明。防火牆規則原則包含「允許」與「封鎖」規則，用以管理受保護電腦上的流量。McAfee 可讓您將幾個預先設定的原則納入 Host Intrusion Prevention，讓您輕鬆使用端點防火牆保護功能。

您可以使用「一般公司環境」原則做為基準防火牆原則。這項功能完整的原則可以滿足大多數組織的需求。請以此原則做為開始，然後整合套用適應模式後的結果，藉此學習與驗證其他額外規則。相較於現有的預設防火牆原則，在適應模式中這項原則應該會產生較少的用戶端學習規則。

當您第一次部署防火牆原則時，可能會想讓用戶端針對受保護的電腦瞭解各項應用程式的通訊需求。這個學習程序稱為「適應模式」。在此模式中，防火牆會自動將規則附加到原則中以允許流量通過，但這已經超出防火牆規則原則所能處理的範圍。這項動作會自動完成，而不會提示使用者。在每個代理程式與伺服器通訊期間，McAfee Agent 會將在用戶端電腦上學習到的任何規則傳送給 ePolicy Orchestrator。您可以進入介面中的 [報告 | Host IPS]，檢閱這些「用戶端學習到的規則」。透過這個畫面，您可以看到 Host Intrusion Prevention 用戶端已經新增哪些規則，以及升級為原則的規則有哪些。

如需在預設值之外調整 IPS 功能的詳細指南，請參閱《採用 McAfee Host Instrusion Prevention：快速上手最佳實務》白皮書 (可透過您的 McAfee 支援或銷售連絡人取得)。

請使用下列工作，依據一般公司環境範本設定防火牆規則，並將防火牆選項設為使用適應模式。

指派防火牆規則原則

1 移至 [系統 | 系統樹狀目錄]，然後從功能表列選取 [原則]。

2 在 [系統樹狀目錄] 中，展開 [Test Group]，然後反白 [Workstations] 群組。

3 從 [產品] 下拉式功能表中，選取 [Host Intrusion Prevention 7.X.X:Firewall]。

4 在 [類別] 欄位中，找到 [防火牆規則 (Windows)]，然後按一下 [編輯指派]。

5 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。

6 從 [指派原則] 下拉式功能表中，選取 [一般公司環境]。

7 按一下 [編輯原則]，然後檢閱現有的規則設定。

8 按一下 [取消]，結束原則的編輯頁面。

9 當您回到 [原則指派] 頁面時，按一下 [儲存]。

如果您想要變更 [一般公司環境] 原則中的規則設定，可以加以複製然後再調整內容。

設定防火牆選項

1 移至 [系統 | 系統樹狀目錄]，然後從功能表列選取 [原則]。

2 在 [系統樹狀目錄] 中，展開 [Test Group]，然後反白 [Workstations] 群組。

3 從 [產品] 下拉式功能表中，選取 [Host Intrusion Prevention 7.X.X:Firewall]。

4 在 [類別] 欄位中，找到 [防火牆選項 (Windows)]，然後按一下 [編輯指派]。

5 在 [繼承自] 中，選取 [取消繼承並在下方指定原則和設定]。

6 從 [指派原則] 下拉式功能表中選取 [適應]，讓防火牆針對尚未由防火牆規則原則處理的流量建立相關規則。

7 按一下 [儲存]。

如需管理 Host Intrusion Prevention 防火牆的詳細資訊，請參閱《Host Intrusion Prevention 產品指南》。< 參考 > 一節包含技術簡報與其他說明文件的連結。

設定電子郵件伺服器原則

McAfee GroupShield 可為您的 Microsoft Exchange 和 Lotus Domino 伺服器提供保護。它能保護您免於各種病毒、不需要的內容、可能不需要的程式、禁止的檔案類型/郵件的威脅，並支援在電子郵件訊息中的內容篩選功能。

GroupShield 同時支援透過附加套件對內送郵件提供防垃圾郵件與防網路釣魚的功能。它會以大量規則來比對每封電子郵件，然後計算出整體的垃圾郵件分數。

GroupShield Exchange 原則

在下列幾節中，您會針對禁止的內容、防垃圾郵件與防網路釣魚掃描程式建立 GroupShield for Microsoft Exchange 範例原則。McAfee 建議您使用預設的已定義防毒原則。一開始請使用預設的防垃圾郵件原則，接著視需要微調閾值。此處所列範例僅供說明之用。

設定禁止的內容原則

本節提供示範篩選禁止內容的範例。您可以使用此工作建立一項原則，藉此要求任何在文件附件中使用「Company Confidential」字樣的電子郵件都以警示來取代該郵件，並發送通知給系統管理員。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [GroupShield for Exchange 7.0.0]。

3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。

4 在列出 [My Default] 的那行，按一下 [複製]。

5 在 [名稱] 中，輸入 My Exchange Policy，然後按一下 [確定]。

6 在列出 [My Exchange Policy] 的那行，按一下 [編輯]。

7 在 [原則管理員] 底下，按一下 [共用資源]。

8 按一下 [篩選規則] 索引標籤。

9 若要建立新的內容掃描程式規則類別，按一下 [新類別]。

10 在 [名稱] 中，輸入 Content，然後按一下 [確定]。

11 若要建立類別的新規則，在 [內容掃描程式規則] 底下按一下 [建立新規則]。

12 在 [規則名稱] 中，輸入 Blocked content。

13 提供說明，並勾選 [將此規則新增至此類別的規則群組]。

14 選取 [單字或片語] 索引標籤。在 [找到下列單字或片語時，會觸發此規則] 文字方塊中，輸入 Company Confidential。

15 選取 [檔案格式] 索引標籤。取消勾選 [全部] 選項。在 [檔案類別] 底下，選取 [文件]。在 [子類別] 底下，選取 [全部]。

16 按一下 [儲存]。

17 在 [共用資源] 頁面上，再次按下 [儲存]。

18 在 [原則管理員] 底下，按一下 [常駐]。

19 按一下 [主原則]。

20 在 [核心掃描程式] 底下，針對 [內容掃描] 選取 [使用中]。在 [名稱] 欄位中，按一下 [內容掃描]。

21 選取 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [內容掃描]。

22 在 [選項] 底下，勾選 [內容掃描中包括文件和資料庫格式] 和 [掃描所有附件中的文字]。

23 當您收到有關導致高 CPU 使用率的警告時，按一下 [確定]。

24 在 [內容掃描程式規則與相關動作] 區段中，按一下 [新增規則]。

25 從 [選取規則群組] 下拉式功能表中，選取 [Content]。[從此群組選取規則] 選項應該會包含「Blocked content」。

26 從 [一旦偵測到，便採取下列動作] 下拉式功能表中，選取 [以警告取代項目]。在 [以及] 區段中，選取 [通知系統管理員]。

27 按一下 [儲存]。

28 在 [常駐] 頁面上，再次按下 [儲存]。

設定防垃圾郵件掃描程式原則

您可以使用此工作設定一項原則，要求對任何一封獲得高分的「垃圾郵件」加以拒絕。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [GroupShield for Exchange 7.0.0]。

3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。

4 在列出 [My Exchange Policy] 的那行，按一下 [編輯]。

5 在 [原則管理員] 底下，按一下 [閘道]。

6 按一下 [主原則]。

7 按一下 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [反垃圾郵件]。

8 在 [偵測到垃圾郵件時要採取的動作] 區段，按一下 [編輯]。

9 按一下 [高分類別] 索引標籤。

10 從 [執行以下動作] 下拉式功能表中，選取 [拒絕郵件]。在 [以及] 區段中，取消選取 [隔離訊息]。

11 按一下 [儲存]。

12 在 [閘道] 頁面上，再次按下 [儲存]。

設定防網路釣魚掃描程式原則

您可以使用此工作，設定可記錄任何網路釣魚郵件的原則。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [GroupShield for Exchange 7.0.0]。

3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。

4 在列出 [My Exchange Policy] 的那行，按一下 [編輯]。

5 在 [原則管理員] 底下，按一下 [閘道]。

6 按一下 [主原則]，或者假如您仍在 [My Exchange Policy] 頁面上，從 [原則] 下拉式功能表中選取 [主原則]。

7 按一下 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [防網路釣魚]。

8 在 [動作] 區段中，按一下 [編輯]。

9 在 [以及] 區段中，選取 [記錄]。

10 按一下 [儲存]。

11 在 [閘道] 頁面上，再次按下 [儲存]。

指派原則給 Exchange 伺服器

您可以使用此工作，將您設定的原則指派給 Microsoft Exchange 伺服器。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。
2 展開 [Test Group]，然後反白 [Servers]。
3 從 [產品] 下拉式功能表中，選取 [GroupShield for Exchange 7.0.0]。
4 在 [掃描程式設定] 的那行，按一下 [編輯指派]。
5 選取 [取消繼承並在下方指定原則和設定]。
6 從 [指派原則] 下拉式功能表中，選取 [My Exchange Policy]。
7 按一下 [儲存]。
8 按一下功能表列上的 [系統]。
9 按一下 [更多動作]，然後選取 [喚醒代理程式]。
10 在 [喚醒 McAfee Agent] 底下，將 [隨機] 時間設為零分鐘。
11 按一下 [確定]。

GroupShield Domino 原則

在下列幾節中，您會針對禁止的內容、防垃圾郵件與防網路釣魚掃描程式建立 GroupShield for IBM Lotus Domino 範例原則。McAfee 建議您使用預設的已定義防毒原則。一開始請使用預設的防垃圾郵件原則，接著視需要微調閾值。此處所列範例僅供說明之用。

設定禁止的內容原則

本節提供示範篩選禁止內容的範例。您可以使用此工作建立一項原則，藉此要求任何在文件附件中使用「Company Confidential」字樣的電子郵件都以警示來取代該郵件，並發送通知給系統管理員。

1 移至 [系統 | 原則目錄]。
2 從 [產品] 下拉式功能表中，選取 [GroupShield for Lotus Domino 7.0.0]。
3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。
4 在列出 [My Default] 的那行，按一下 [複製]。
5 在 [名稱] 中，輸入 My Domino Policy，然後按一下 [確定]。
6 在列出 [My Domino Policy] 的那行，按一下 [編輯]。
7 在 [原則管理員] 底下，按一下 [共用資源]。
8 按一下 [篩選規則] 索引標籤。
9 若要建立新的內容掃描程式規則類別，按一下 [新類別]。
10 在 [名稱] 中，輸入 Content，然後按一下 [確定]。
11 若要建立類別的新規則，在 [內容掃描程式規則] 底下按一下 [建立新規則]。
12 在 [規則名稱] 中，輸入 Blocked content。
13 提供說明，並勾選 [將此規則新增至此類別的規則群組]。
14 選取 [單字或片語] 索引標籤。在 [找到下列單字或片語時，會觸發此規則] 文字方塊中，輸入 Company Confidential。
15 選取 [檔案格式] 索引標籤。取消勾選 [全部] 選項。在 [檔案類別] 底下，選取 [文件]。在 [子類別] 底下，選取 [全部]。
16 按一下 [儲存]。

17 在 [共用資源] 頁面上，再次按下 [儲存]。

18 在 [原則管理員] 底下，按一下 [外部郵件]。

19 按一下 [主原則]。

20 在 [核心掃描程式] 底下，針對 [內容掃描] 選取 [使用中]。在 [名稱] 欄位中，按一下 [內容掃描]。

21 選取 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [內容掃描]。

22 在 [選項] 底下，勾選 [內容掃描中包括文件和資料庫格式] 和 [掃描所有附件中的文字]。

23 當您收到有關導致高 CPU 使用率的警告時，按一下 [確定]。

24 在 [內容掃描程式規則與相關動作] 區段中，按一下 [新增規則]。

25 從 [選取規則群組] 下拉式功能表中，選取 [Content]。[從此群組選取規則] 選項應該會包含「Blocked content」。

26 從 [一旦偵測到，便採取下列動作] 下拉式功能表中，選取 [以警告取代項目]。在 [以及] 區段中，選取 [通知系統管理員]。

27 按一下 [儲存]。

28 在 [外部郵件] 頁面上，再次按下 [儲存]。

設定防垃圾郵件掃描程式原則

您可以使用此工作設定一項原則，要求對任何一封獲得高分的「垃圾郵件」加以拒絕。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [GroupShield for Lotus Domino 7.0.0]。

3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。

4 在列出 [My Domino Policy] 的那行，按一下 [編輯]。

5 在 [原則管理員] 底下，按一下 [外部郵件]。

6 按一下 [主原則]。

7 按一下 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [反垃圾郵件]。

8 在 [偵測到垃圾郵件時要採取的動作] 區段，按一下 [編輯]。

9 按一下 [高分類別] 索引標籤。

10 從 [執行以下動作] 下拉式功能表中，選取 [拒絕郵件]。在 [以及] 區段中，取消選取 [隔離訊息]。

11 按一下 [儲存]。

12 在 [外部郵件] 頁面上，再次按下 [儲存]。

設定防網路釣魚掃描程式原則

您可以使用此工作，設定可記錄任何網路釣魚郵件的原則。

1 移至 [系統 | 原則目錄]。

2 從 [產品] 下拉式功能表中，選取 [GroupShield for Lotus Domino 7.0.0]。

3 從 [類別] 下拉式功能表中，選取 [掃描程式設定]。

4 在列出 [My Domino Policy] 的那行，按一下 [編輯]。

5 在 [原則管理員] 底下，按一下 [外部郵件]。

6 按一下 [主原則]，或者假如您仍在 [My Domino Policy] 頁面上，從 [原則] 下拉式功能表中選取 [主原則]。

7 按一下 [檢視設定] 索引標籤。從 [選項] 下拉式功能表中，選取 [防網路釣魚]。

8 在 [動作] 區段中，按一下 [編輯]。
9 在 [以及] 區段中，選取 [記錄]。
10 按一下 [儲存]。
11 在 [閘道] 頁面上，再次按下 [儲存]。

指派原則給 IBM Lotus Domino 伺服器

您可以使用此工作，將您設定的原則指派給 IBM Lotus Domino 伺服器。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。
2 展開 [Test Group]，然後反白 [Servers]。
3 從 [產品] 下拉式功能表中，選取 [GroupShield for Lotus Domino 7.0.0]。
4 在 [掃描程式設定] 的那行，按一下 [編輯指派]。
5 選取 [取消繼承並在下方指定原則和設定]。
6 從 [指派原則] 下拉式功能表中，選取 [My Domino Policy]。
7 按一下 [儲存]。
8 按一下功能表列上的 [系統]。
9 按一下 [更多動作]，然後選取 [喚醒代理程式]。
10 在 [喚醒 McAfee Agent] 底下，將 [隨機] 時間設為零分鐘。
11 按一下 [確定]。

設定端點工作

您現在已建立了系統樹狀目錄、新增一些用戶端系統、簽入軟體並設定相關原則。接下來，您將排程 VirusScan Enterprise 與其他安全性產品的部署作業。您可以透過 McAfee Agent 所擷取與執行的用戶端工作來完成產品部署。您也可以使用用戶端工作來排程掃描與更新。

完成本節中的建立部署和更新工作後，請建立一個 VirusScan Enterprise 按指定掃描工作。請按一下本連結，遵照線上說明中的步驟進行。

建立部署工作

在本節，您會建立一個用戶端工作，用以將一或多個產品部署到系統群組中。本工作假設您在安裝期間已簽入所有端點產品。如果沒有的話，產品清單 (步驟 5) 中只會顯示您簽入的產品。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [用戶端工作]。

2 反白 [我的組織]，然後按一下 [新增工作]。

3 在 [名稱] 中，輸入 McAfee Deployment。

4 在 [類型] 中，從下拉式功能表中選取 [產品部署 (McAfee Agent)]，然後按 [下一步]。

5 在 [設定] 頁面的 [產品及元件] 下方，選取您的端點產品。使用加號 (+) 來新增額外的行。針對每個產品，將 [動作] 設為 [安裝] 並將 [語言] 設為用戶端系統上使用的語言。從 [產品] 下拉式清單中：

- 選取 [VirusScan Enterprise 8.7.0.xxx]，然後按一下 +。
- 選取 [AntiSpyware Enterprise Module 8.7.0.xxxx]，然後按一下 +。
- 選取 [Host Intrusion Prevention 7.0.0.xxx]，然後按一下 +。
- 選取 [SiteAdvisor Enterprise Plus 2.0.0.xxx]。

6 選取 [在每次原則強制時執行]，然後按 [下一步]。

7 在 [排程] 頁面上，設定下列選項，然後按 [下一步]：

排程狀態	啟用
排程類型	立即執行

8 在 [摘要] 頁面，按一下 [儲存]。

當您部署到生產環境中的大量系統時，McAfee 建議您使用 [排程] 頁面上的 [隨機] 選項。工作隨機處理可協助防止用戶端系統將大量同時發生的要求傳送給伺服器。一般來說，在真實環境裡，您可能想要將部署作業排程在一天的特定時段執行。將排程設為 [立即執行] 可加速部署程序以供評估。

建立更新工作

在本節中，您會建立一項用戶端工作，用以更新 VirusScan 引擎和 DAT，以及 Host Intrusion Prevention 內容。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [用戶端工作]。

2 反白 [Test Group]，然後按一下 [新增工作]。

3 在 [名稱] 中，輸入 Daily Update。

4 在 [類型] 中，從下拉式功能表中選取 [更新 (McAfee Agent)]，然後按 [下一步]。

5 在 [設定] 頁面上，依序選取 [引擎]、[DAT] 和 [Host Intrusion Prevention 內容]，然後按 [下一步]。

6 在 [排程] 頁面上，將 [排程類型] 設為 [每日]。

附註：如果您正在更新大量的系統，McAfee 建議您指定一些隨機時間來錯開用戶端要求。

7 在 [選項] 中，選取 [執行錯過的工作]。

8 將 [排程] 設為 [重複，介於]，並將時間值設為 [早上 7:00]、[早上 6:59] 和 [每 4 小時]。

9 在 [摘要] 頁面，按一下 [儲存]。

排程的時間範圍僅做為範例參考。一般來說，在真實環境裡，您會想要將用戶端系統排程為一天檢查更新數次。排程選項可讓您設定所需的任何排程。

與網路暫時中斷連線的系統 (例如筆記型電腦) 會繼續執行指派的更新工作。在此情況下，當筆記型電腦位於飯店或是具有網際網路連線能力的任何位置，就會從 McAfee 網站擷取更新 (而不是從 ePO 伺服器)。

部署 McAfee Agent

McAfee Agent 是 ePolicy Orchestrator 的分散式元件，必須安裝在網路中每一個您想要管理的系統上。代理程式不但會負責收集並傳送資訊到 ePO 伺服器，還會安裝並更新端點產品，然後套用您的端點原則。若要透過 ePolicy Orchestrator 管理系統，您必須先安裝 McAfee Agent。

在部署 McAfee Agent 之前，最好驗證伺服器與系統之間的通訊，看看是否能夠存取預設的管理員共用目錄。同時，您可能需要建立防火牆例外。

1 檢查是否可以依據名稱來 Ping 用戶端系統。這麼做可確定伺服器可以將用戶端名稱解析為 IP 位址。

2 檢查是否可存取用戶端系統上的預設 Admin$ 共用：在 Windows 介面中，按一下 [開始 | 執行]，然後輸入 \\computer-name\admin$。若系統已正確連線至網路，您的認證有足夠的權限且 Admin$ 共用資料夾存在，便會開啟 Windows [檔案總管] 對話方塊。

3 如果任何一部使用中的用戶端系統正在執行防火牆，則請建立 Framepkg.exe 例外。ePolicy Orchestrator 會將此檔案複製到您要管理的系統中。

部署代理程式

您可以使用此工作，將 McAfee Agent 部署到用戶端系統。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [系統]。

2 反白 [Test Group]。如果此群組未包含任何系統，但是卻在系統中擁有子群組，請按一下 [層級篩選] 下拉式功能表，然後選取 [此群組與所有子群組]。

3 從清單中選取一或多個系統，然後按一下 [更多動作 | 部署代理程式]。

4 輸入有權在用戶端系統上安裝軟體的認證，例如「網域管理員」，然後按一下 [確定]。

您需要等候幾分鐘，讓 McAfee Agent 完成安裝，並讓用戶端系統順利擷取並執行端點產品的安裝套件。首次安裝時，代理程式會決定一個隨機時間 (10 分鐘內)，用以連線至 ePO 伺服器來擷取相關原則和工作。

您還可以透過其他許多種方式部署 McAfee Agent (請參閱 ePolicy Orchestrator 說明文件或線上說明)。

驗證代理程式與 ePolicy Orchestrator 的通訊

建立好代理程式和伺服器之間的初始通訊後，代理程式預設每隔 60 分鐘就會輪詢一次伺服器。這項程序稱為「代理程式與伺服器通訊間隔時間」或「ASCI」。每次執行這項程序時，代理程式就會擷取原則變更，並在本機強制執行相關原則。

根據預設 ASCI 規定，在 15 分鐘前剛輪詢完伺服器的代理程式，在接下來的 45 分鐘之內不會收取任何一項新的原則。但是，您可以強迫系統使用「代理程式喚醒呼叫」來輪詢伺服器。當您需要在下一次通訊程序開始之前強迫執行原則變更時，喚醒呼叫就會很有用。這可讓您強迫用戶端執行一些工作，例如立即更新。

您可以使用此工作，驗證用戶端系統是否正與 ePolicy Orchestrator 通訊。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [系統]。

2 反白您的 [Servers] 或 [Workstations] 群組。

3 如果列出 IP 位址和使用者名稱，就表示用戶端系統上的代理程式正與伺服器通訊。

4 如果經過了 5 到 10 分鐘之後，系統還是沒有列出任何 IP 位址和使用者名稱，請選取 [更多動作 | 喚醒代理程式]。

如果傳送一則喚醒呼叫仍舊無法擷取任何 IP 位址和使用者名稱，則可能是因為其他環境因素導致初始代理程式部署作業失敗。如果發生這種情況，請複製代理程式安裝程式 Framepkg.exe (從 ePO 伺服器)，然後在用戶端系統上加以執行。

驗證用戶端軟體安裝

依據您所部署的產品數量而定，用戶端安裝程序可能需要一點時間來完成。您可以透過 ePO 伺服器，或是在用戶端系統上的 McAfee 系統匣圖示上按一下滑鼠右鍵，來驗證用戶端安裝。

您可以使用此工作，透過 ePO 伺服器驗證用戶端安裝。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [系統]。

2 反白您的 [Servers] 或 [Workstations] 群組。

3 使用核取方塊來選取個別系統，或是使用 [在此頁面中全選] 或 [在所有頁面中全選] 來選取。

4 按一下 [更多動作 | 喚醒代理程式]。

5 如果您要喚醒大量的系統，新增幾分鐘的「隨機」時間會很有用。按一下 [確定]。

6 幾分鐘之後，按一下個別系統。[系統詳細資料] 頁面會提供系統相關資訊，包括已安裝的 McAfee 軟體。

重新造訪 PUP 稽核 VirusScan 原則

此時，軟體安裝用戶端工作應該已經執行，或是正在執行，而且您於先前工作中建立的所有原則應該已經下載完畢。如果您的測試系統包含全新安裝的乾淨作業系統，您可能不會看到任何 PUP 偵測項目。針對本練習，假定您的用戶端已偵測到下列項目：

- 遠端管理工具 Tight VNC。
- 名為 SuperScan 的連接埠掃描程式。

偵測到的大多數 PUP 同時包含應用程式系列與名稱。例如，名為 SuperScan 的連接埠掃描程式會被偵測為 PortScan-SuperScan，而 TightVNC 則被偵測為 RemAdm-TightVNC。ePO 報告與本機用戶端記錄檔中的「偵測名稱」就是使用這種基本的命名規則。

完成您的 PUP 稽核作業之後，您可以使用此工作並依據現有的「不需要的程式原則」原則來建立新的原則，並新增想要的例外項目。以下使用 SuperScan 與 Tight VNC 來示範此工作。您現在不需要輸入這些例外項目；您可以在需要建立實際的例外項目時再回來參考此範例。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。

2 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。

3 反白 [Test Group]。

4 按一下 [不需要的程式原則] 右側的 [編輯指派]。

5 選取 [取消繼承並在下方指定原則和設定]。

6 按一下 [新增原則]。

7 輸入原則名稱，例如 PUP exclusions for IT staff，然後按一下 [確定]。[原則編輯器] 隨即開啟。

8 在 [不需要的程式排除] 區域，輸入 PortScan-SuperScan，然後按一下右側的加號 (+)。

9 輸入 RemAdm-TightVNC，再按一下 + 並輸入 Reg-TightVNC。

TightVNC 同時針對此應用程式要求在 Windows 登錄項目中加入 Reg 例外項目。此動作會指示掃描程式不要清理與此程式相關的登錄項目。SuperScan 不會要求加入 Reg 排除項目，因為它只是獨立的執行檔。

10 按一下 [儲存]。

11 從 [指派原則] 下拉式功能表中，選取 [PUP exclusions for IT staff] 原則，然後按一下 [儲存]。

比較安全的作法是只排除使用的工具，而不要取消選取整個類別。例如，關於遠端管理工具，您可能需要針對正常操作情況排除幾項工具，但是您可能同時想要知道 McAfee AntiSpyware 模組是否已經在網路中找到任何一項與此相關但尚未核准的未管轄工具。

完成 PUP 稽核作業之後，請務必將 VirusScan 設定改回 [清除]，然後建立包含例外的原則。如果您沒有將原則更改為原本的清除 PUP 設定，您將無法移除間諜軟體。

重設常駐掃描原則

您在之前練習中建立一個新的原則，指示常駐掃描程式偵測 PUP 但不加以清除。您可以使用此工作重新套用預設的掃描程式原則，進而啟用清除功能。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [原則]。

2 從 [產品] 下拉式功能表中，選取 [VirusScan Enterprise 8.7.0]。

3 反白 [Test Group]。

4 在 [常駐掃描預設處理程序原則] 右側，按一下 [編輯指派]。

5 從 [指派原則] 下拉式功能表中，選取 [My Default]。

6 選取 [Audit for PUPs] 原則的選項按鈕，此原則可能是 [全域根] 或 [我的組織] (取決於您先前的設定)。

7 按一下 [儲存]。

驗證按指定掃描工作

在先前的練習當中，您已針對用戶端系統排程週期性掃描。在該設定當中，我們指示掃描程式暫時只偵測 PUP，而不要加以清除。您可以使用此工作重設選項，啟用排程掃描期間的清除功能。

1 移至 [系統 | 系統樹狀目錄]，然後按一下功能表列上的 [用戶端工作]。

2 反白 [Test Group]。

3 找到您所建立的掃描工作，然後按一下 [動作] 欄位底下的 [編輯]。

4 在工作精靈的第一頁，按 [下一步]。

5 在 [設定] 頁面，按一下 [動作]，然後在 [找到不需要的程式時] 下拉式功能表中，選取 [清除檔案]。

6 按一下 [儲存]。

VirusScan 現在會清除您未明確指定排除的所有 PUP。下次當用戶端系統輪詢伺服器時，就會下載您的設定變更。

使用儀表板和查詢

儀表板和查詢可針對您的環境提供各種類型的狀態資訊。Total Protection for Endpoint 套件中的每一項產品都包含預先定義的查詢。此套件包含數個預先定義的儀表板。您也可以建立自訂的儀表板與查詢。

根據預設，安裝完畢後唯一一項作用中的儀表板為 ePO 摘要儀表板。在本節中，您將啟用第二個儀表板、變更其中一項監視器、執行預先定義的查詢，以及建立自訂查詢。

啟用儀表板

為了讓儀表板成為 [儀表板] 頁面索引標籤列上使用中集合的一部份，您需要加以啟用。

1 移至儀表板，按一下 [選項]，然後選取 [管理儀表板]。[管理儀表板] 頁面便會出現。

2 從 [儀表板] 清單中，反白 [HIP 儀表板]，然後按一下 [啟用]。

3 看到提示時按一下 [確定]，然後按一下 [關閉]。

[HIP 儀表板] 現在會顯示在索引標籤列上。請花一點時間檢視此儀表板及內含的資訊。

變更儀表板監視器

大部分預設儀表板都包含六個監視器。如果預設監視器無法提供您想要的資訊，您可以變更監視器集合，而無需建立新的儀表板。若要檢視 VirusScan Enterprise 與可能不需要的程式相關資訊，您需要先進行複製，然後修改 [VSE: 目前偵測數量] 儀表板。

1 移至儀表板，按一下 [選項]，然後選取 [管理儀表板]。[管理儀表板] 頁面便會出現。

2 從 [儀表板] 清單中，反白 [VSE: 目前偵測數量]，然後按一下 [複製]。

3 在 [名稱] 中，輸入 VSE: Detections (custom)，然後按一下 [確定]。

4 按一下 [編輯]。

5 找到名為 [VSE: 過去 24 小時所偵測到的威脅] 監視器，然後按一下 [刪除]。

6 按一下 [新增監視器]。

7 從 [類別] 清單中，選取 [查詢]。

8 從 [監視器] 清單中，選取 [VSE: DAT 部署]，然後按一下 [確定]。

9 找到名為 [VSE: 過去 7 天所偵測到的威脅] 監視器，然後按一下 [刪除]。

10 按一下 [新增監視器]。

11 從 [類別] 清單中，選取 [查詢]。

12 從 [監視器] 清單中，選取 [VSE: 前 10 個違反的存取保護規則]，然後按一下 [確定]。

13 按一下 [儲存]。

14 按一下 [啟用]，然後在收到提示時按一下 [確定]。

15 按一下 [關閉]。

16 在 [儀表板] 索引標籤列上，按一下 [VSE: Detections (custom)]。

您新增的兩個監視器會顯示一個圓形圖 (DAT 部署) 與一個摘要表格 (前 10 個違反的存取保護規則)。在您建立自己的查詢時，請考慮您要檢視的資料類型以及顯示方式。

執行預先定義的查詢

您在上一項工作中應該已經發現，查詢可以是儀表板監視器所顯示的來源資料。您也可以個別執行查詢。

若要驗證用戶端系統上的 VirusScan Enterprise 安裝，您可以執行 [VSE: 8.7 版符合性] 查詢。

1 移至 [報告 | 查詢]。

2 在查詢清單中，捲動至 [VSE: 8.7 版符合性] 並加以反白。

3 按一下 [執行]。

結果會以圓形圖來顯示，告訴您系統是否相容。此查詢會依據以下準則定義符合性：

- VirusScan® Enterprise 8.7i 已安裝。
- 掃描引擎版本至少是 5200。
- 用戶端上的防毒簽章檔 (DAT) 版本符合 ePO 主存放庫中三個簽章檔版本其中一個。

無法通過上述任一準則的系統，就會標示為不相容。如需某些準則的更詳細資訊 (例如不同用戶端上的 DAT 版本)，請執行 [VSE: DAT 部署] 查詢。

若要檢查 Host Intrusion Prevention 是否已安裝，並具有正確的程式版本，請執行 [HIP: 用戶端版本] 查詢。若要檢查這些用戶端是否具有最新的更新，請執行 [HIP: 內容版本] 查詢。您也可以將這些查詢新增為儀表板監視器。

建立自訂查詢

您可以使用此工作，建立顯示所有 PUP 偵測項目的查詢。

1 移至 [報告 | 查詢]。

2 按一下 [新增查詢]。

3 從清單中，選取 [事件]，然後按 [下一步]。

4 選取下列項目，然後按 [下一步]：

用途...	請選取這項...
顯示結果為	長條圖
長條圖標籤為	威脅名稱
長條圖值為	事件數

5 再按 [下一步] 略過 [欄位] 頁面。

6 在 [篩選器] 頁面上，從 [可用的內容] 之 [事件] 區段中：

- 按一下 [偵測產品名稱]，然後將 [比較] 設為 [等於]。在 [值] 中，輸入 VirusScan Enterprise 8.7。
- 按一下 [事件 ID]，然後將 [比較] 設為 [大於]。在 [值] 中，輸入 20000。
- 按一下 [威脅名稱]，然後將 [比較] 設為 [不包含]。在 [值] 中，輸入 Cookie。

7 按一下 [執行]。

8 結果出現之後，按一下 [儲存]。在 [查詢名稱] 中，輸入 VSE: All PUP Detections，然後按一下 [儲存]。

當自訂查詢儲存完畢後，就會依據英文字母順序新增到所有查詢清單中。您現在隨時可以執行此查詢，或是把它當作儀表板監視器來使用。如果您想要專注在 PUP 偵測項目的特定期間，可以複製此查詢，然後將「事件產生時間」內容新增為額外的篩選器。

摘要

恭喜。當您完成本指南，即表示您已完成多項用來建立與維護安全網路環境的常見工作。

以下列出您已完成的項目：

1 完成安裝 Total Protection for Endpoint 套件。

2 完成啟用與執行從 McAfee 網站更新 ePO 主存放庫的工作。

3 完成建立系統樹狀目錄結構，並將測試系統新增至群組。

4 完成建立與套用新的 McAfee Agent 原則，能在受管理系統上顯示系統匣圖示。

5 完成建立與套用端點產品的新原則，包括：

- 數個 VirusScan 原則，包括用以稽核 PUP 的原則。
- 一個 SiteAdvisor Enterprise Plus 原則。
- 一個 Host Intrusion Prevention 原則。

6 完成建立部署工作以在用戶端系統上安裝 VirusScan、Host Intrusion Prevention 和 SiteAdvisor Plus。

7 完成建立與套用保護電子郵件的原則。

8 完成建立用戶端更新工作以讓用戶端保持在最新狀態。

9 完成部署 McAfee Agent。

10 完成確認代理程式與伺服器的通訊，並傳送代理程式喚醒呼叫以確保受管理系統成功擷取新的原則。

11 完成修改包含例外的 PUP 稽核原則。

12 完成重新套用預設的常駐掃描原則，並重設按指定掃描工作以清除 PUP。

13 完成啟用第二個儀表板、變更儀表板上的監視器，並執行預先定義的查詢。

14 完成建立可列出 PUP 偵測項目的自訂查詢。

參考

請使用本節中的連結存取更多資訊。

閱讀支援

搜尋 McAfee 屢獲獎賞的知識庫，尋找更多問題解答。

搜尋知識庫

如需 Total Protection for Endpoint 的詳細資訊，請參閱下列產品說明文件：

ePolicy Orchestrator 4.0

- ePolicy Orchestrator 4.0 試用指南
- ePolicy Orchestrator 4.0.2 產品指南
- ePolicy Orchestrator 4.0 安裝指南
- ePolicy Orchestrator 4.0 硬體評估及頻寬使用指南
- ePolicy Orchestrator 4.0 快速參考卡
- 使用記錄檔疑難排解 ePolicy Orchestrator 4.0 中的問題
- ePolicy Orchestrator 4.0 - 版本支援文章主清單

VirusScan Enterprise 8.7i

- VirusScan Enterprise 8.7i 安裝指南
- VirusScan Enterprise 8.7i 產品指南
- VirusScan Enterprise 8.7i 快速參考卡
- McAfee VirusScan Enterprise 與 Host Intrusion Prevention 存取保護 - 白皮書

AntiSpyware Enterprise 8.7

- AntiSpyware Enterprise 8.7 產品指南
- AntiSpyware Enterprise 8.7 版本說明

McAfee Host Intrusion Prevention 7.0

- Host Intrusion Prevention 7.0.0 安裝指南
- 採用 Host Intrusion Prevention - 快速上手最佳實務
- Host Intrusion Prevention 7.0.0 for ePO 4.0 產品指南
- Host Intrusion Prevention 7.0 防火牆通訊協定支援
- Host Intrusion Prevention 7.x 多槽式原則與其有效的原則
- Host Intrusion Prevention 防火牆：連線識別群組
- Host Intrusion Prevention 7.x 適應模式
- McAfee VirusScan Enterprise 與 Host Intrusion Prevention 存取保護 - 白皮書

SiteAdvisor Enterprise Plus 2.0

- SiteAdvisor Enterprise Plus 2.0 產品指南
- 白皮書：再度造訪惡意網站分布圖
- 白皮書：預防勝於治療
- McAfee SECURE™ 購物入口網站
- 網站擁有者與消費者的資源

GroupShield 7.0 for Microsoft Exchange

- GroupShield 7.0.1 for Microsoft Exchange 最佳實務指南
- GroupShield 7.0 for Microsoft Exchange 使用者指南
- GroupShield 7.0.1 for Microsoft Exchange 使用者指南補遺

GroupShield 7.0 for Lotus Domino

- GroupShield 7.0 for Lotus Domino - ePolicy Orchestrator - 設定指南
- GroupShield 7.0 for Lotus Domino - 安裝指南
- GroupShield 7.0 for Lotus Domino - 產品指南
- GroupShield 7.0 for Lotus Domino 最佳實務指南

影片支援

檢視教學課程

檢視解決一般問題的影片教學課程

實作支援

下載軟體更新

取得最新的防毒定義、產品安全性更新與產品版本。若要取得產品修補程式與維護版本，您必須登入 ServicePortal。

全球支援實驗室

在真實的測試環境中，設定並逐步解決一般問題。