HP ProtectTools
使用指南

第一版：2009 年 10 月

文件編號：572661-AB1

目錄

1 安全性簡介

HP ProtectTools 安全管理員 (HP ProtectTools Security Manager) 軟體提供安全性功能，協助防止未經授權存取電腦、網路及重要資料。HP ProtectTools Security Manager 的管理是透過「管理主控台」功能提供。

本機管理員可以使用主控台執行下列工作：

- 啓用或停用安全功能
- 爲此電腦的使用者註冊指紋
- 設定智慧卡
- 指定所需的驗證認證
- 管理電腦的使用者
- 調整裝置特定的參數
- 設定已安裝的安全管理員 (Security Manager) 應用程式
- 新增其他的 Security Manager 應用程式

您電腦所適用的軟體模組可能會隨著您的機型而有所不同。

您可以預先安裝、預先載入，或從 HP 網站下載 HP ProtectTools 軟體模組。如需詳細資訊，請造訪 http://www.hp.com。

附註： 本指南的說明內容係預設使用者已安裝適用的 HP ProtectTools 軟體模組。

HP ProtectTools 功能

下列表格詳細說明 HP ProtectTools 模組的主要功能。

模組	重要功能
HP ProtectTools 認證管理員 (HP ProtectTools Credential Manager)	• 密碼管理員 (Password Manager) 作爲個人密碼的保管庫，透過「單一登入」功能自動記住並套用使用者的認證，以簡化登入程序。 • 「單一登入」同時還藉由要求不同安全性技術的組合（例如 Java ™ 卡和生物測定），爲使用者驗證提供額外的保護。 • 密碼儲存透過軟體加密保護，同時可以透過使用安全性裝置驗證（例如 Java Card 或生物測定）來加強。 **附註：** 認證管理員 (Credential Manager) 功能可以在 HP ProtectTools Security Manager 的 Password Manager 選項中找到。
HP ProtectTools 磁碟機解密（HP ProtectTools Drive Encryption，僅限特定機型）	• 磁碟機解密 (Drive Encryption) 提供完整、全磁碟區的硬碟加密。 • Drive Encryption 強制執行開機前驗證，才能解密和存取資料。
HP ProtectTools 隱私管理員（HP ProtectTools Privacy Manager，僅限特定機型）	• 隱私管理員 (Privacy Manager) 使用進階的登入技術，以在使用電子郵件、Microsoft® Office 文件或即時傳訊 (IM) 時，驗證通訊的來源、完整性和安全性。
HP ProtectTools 檔案清理工具 (HP ProtectTools File Sanitizer)	• 檔案清理工具 (File Sanitizer) 允許您安全拆解電腦上的數位資產（包括應用程式檔案、歷程記錄或 Web 相關內容，以及其他機密資料等敏感性資訊），並定期清理硬碟。
HP ProtectTools 裝置存取管理員（HP ProtectTools Device Access Manager，僅限特定機型）	• 裝置存取管理員 (Device Access Manager) 可讓 IT 管理員依據使用者設定檔來控制裝置存取權。 • 裝置存取管理員 (Device Access Manager) 能夠預防未獲授權的使用者，經由外部儲存媒體來移除資料或將病毒帶入系統中。 • 管理員可以爲特定的個人或使用者群組，停用可寫入裝置的存取權限。

達成重要的安全性目標

各個 HP ProtectTools 模組可以協同運作以針對各種安全性問題提供解決方案，包括下列重要的安全性目標：

- 防止發生針對性偷竊事件
- 限制存取敏感性資料
- 防止未獲授權的使用者從內部或外部位置進行存取
- 建立不易破解的密碼政策
- 因應法規的安全規範

防止鎖定目標的竊取

鎖定目標的竊取範例之一是在機場安全檢查點竊取包含機密資料和客戶資訊的電腦。下列功能可協助防止鎖定目標的竊取：

- 預先開機驗證功能一旦啓用，就可以協助預防存取作業系統。請參閱下列程序：
  - Security Manager
  - Drive Encryption

限制存取敏感性資料

假設一位合約的稽核人員正在現場工作，且已被授權存取電腦以檢閱敏感性的財務資料，您不希望此稽核人員能夠列印檔案或將檔案儲存在可寫入的裝置（例如 CD）中。下列功能可協助限制存取資料：

- HP ProtectTools Device Access Manager 可以讓 IT 管理員限制存取可寫入裝置，如此敏感性的資訊便無法被列印或從硬碟複製到抽取式媒體中。

防止未獲授權的使用者從內部或外部位置進行存取

未經授權就可以存取未受保護的企業電腦，代表企業的網路資源（例如財務服務、高階主管或研發團隊的資訊）以及私人資訊（例如病歷記錄或個人財務記錄）存在非常明顯的風險。以下功能有助於防止未經授權的存取：

- 預先開機驗證功能一旦啓用，就可以協助預防存取作業系統。請參閱下列程序：
  - Password Manager
  - Drive Encryption
- Password Manager 可協助確保未獲授權的使用者無法取得密碼或存取受密碼保護的應用程式。
- HP ProtectTools Device Access Manager 可以讓 IT 管理員限制存取可寫入裝置，如此便無法從硬碟複製敏感性的資訊。
- DriveLock 可協助確保資料無法被存取，即使硬碟被取出並安裝在不安全的系統中亦然。

建立強式密碼原則

如果強制規定數十個 Web 架構的應用程式和資料庫都需要使用強式密碼原則，則 Security Manager 可提供受保護的密碼存放庫以及「單一登入」的方便性。

其他的安全性要素

指定安全性角色

管理電腦安全性（特別是大型組織時）時，在各種管理員和使用者類型之間分割責任和權利，是實務中很重要的一環。

附註： 在小型的組織或個人用戶中，同一個人可能會兼具不同角色。

對於 HP ProtectTools，可將安全性責任和權限分割成下列角色：

- 安全性主管 — 定義公司或網路的安全性等級，並決定要部署的安全性功能，例如 Java™ 卡、生物測定讀取器或 USB Token 等裝置。

  附註： 安全性主管可與 HP 合作，自訂 HP ProtectTools 的許多功能。如需詳細資訊，請參閱 HP 網站，網址爲：http://www.hp.com。

- IT 管理員 — 套用和管理安全性主管所定義的安全性功能。也能啓用和停用部份功能。例如，若安全主管已決定部署 Java 卡，IT 管理員就能啓用 Java 卡 BIOS 安全性模式。

- 使用者 — 使用安全性功能。例如，若安全性主管和 IT 管理員已啓用系統的 Java 卡，則使用者可設定 Java 卡 PIN 碼並使用該卡進行驗證。

注意： 建議管理員依照限制終端使用者權限和限制使用者存取的「最佳實務」進行。

未獲授權的使用者不應授與管理權限。

管理 HP ProtectTools 密碼

大多數 HP ProtectTools 安全管理員 (HP ProtectTools Security Manager) 功能是利用密碼來保護的。下表列出常用的密碼、設定了密碼的軟體模組，和密碼功能。

這個表格也指示了只能由 IT 管理員設定和使用的密碼。一般的使用者或管理員可設定其他所有密碼。

HP ProtectTools 密碼	在此 HP ProtectTools 模組中設定	功能
Security Manager 登入密碼	Security Manager	這個密碼可提供 2 個選項： • 登入 Windows 後，它可以作爲 Security Manager 登入以存取 Security Manager。 • 它可以用來允許同時存取 Windows 和 Security Manager。
Security Manager 復原檔案密碼	Security Manager，由 IT 管理員設定	保護 Security Manager 復原檔案的存取。
Java™ Card PIN 碼	Java 卡安全性 (Java Card Security)	保護對 Java 卡內容的存取，並驗證 Java 卡使用者。當用於開機驗證時，Java 卡 PIN 碼也可以保護對電腦設定公用程式和電腦內容的存取。 如果選擇使用 Java 卡 Token 的話，就會驗證磁碟機加密 (Drive Encryption) 機制的使用者。
Windows 登入密碼	Windows® 控制台	可使用於手動登入或儲存在 Java 卡上。

建立安全密碼

建立密碼時，您必須先遵循程式設定的所有規格。不過，您通常應該考慮使用下列指導方針，以協助您建立不易破解的密碼，並降低密碼被竊取的機會：

- 使用超過 6 個字元的密碼，最好有 8 個以上。
- 請在密碼中混用大小寫字母。
- 可能的話，請混用英數字元並加入特殊字元和驚嘆號。
- 替代關鍵字中的特殊字元或數字。例如，您可以使用數字 1 代表字母 I 或 L。
- 組合使用 2 或多種語言的字。
- 以數字或特殊字元分割字或詞的中央，例如 "Mary2-2Cat45"。
- 請勿使用字典裏有的字做爲密碼。
- 請勿使用您的名稱當做密碼，或其他任何個人資訊，如生日、寵物名稱或母親的本姓，即使是倒著用也一樣。
- 定期變更密碼。您只能變更增加的一組字元。
- 如果您記下密碼，請不要將它放在電腦旁很容易看到的地方。
- 請不要將密碼儲存在電腦的檔案中，如電子郵件。
- 請勿與他人共用帳戶，或將帳戶告訴他人。

備份和還原 HP ProtectTools 認證

您可以使用 HP ProtectTools Drive Encryption 選取並備份 HP ProtectTools 認證。

2 快速入門

附註： 管理 HP ProtectTools 需要管理權限。

HP ProtectTools 設定精靈會引導您完成 Security Manager 最常用功能的設定。但是，透過 HP ProtectTools 管理主控台還可以使用更多其他功能。精靈中所找到的相同設定以及其他安全性功能，都可以透過主控台進行設定，它可以從 Windows® 的「開始」功能表中存取。這些設定會套用於此電腦和共用此電腦的所有使用者。

1. 在「歡迎」頁面中，您可以選取下列其中一個選項以停用進一步的精靈顯示畫面。
2. 設定電腦一週後，或當擁有管理權限的使用者第一次在指紋讀取器上掃過指紋時，HP ProtectTools 設定精靈會自動啟動以引導您完成設定程式的基本步驟。設定電腦的視訊教學課程會自動啟動。
3. 遵照畫面上的指示完成設定程序。

如果沒有完成精靈程序，便會自動啟動兩次。之後，便可以從工作列通知區附近所出現的通知汽球存取精靈（除非您已依上方步驟 2 所述之方式停用精靈）。

若要使用 HP ProtectTools Security Manager 應用程式，可從「開始」功能表啟動 HP ProtectTools Security Manager，或是在工作列最右邊通知區中的 Security Manager 圖示上按一下滑鼠右鍵。所有共用這部電腦的使用者都可以使用 HP Security Manager 管理主控台及其應用程式。

開啓 HP ProtectTools 管理主控台

對於設定系統原則或設定軟體之類的管理工作，可依下列步驟開啓主控台：

▲ 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。

－ 或 －

在 Security Manager 的左窗格中，按一下「**管理**」。

對於註冊指紋或使用 Security Manager 之類的使用者工作，可依下列步驟開啓主控台：

▲ 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools Security Manager**」。

－ 或 －

在工作列最右端的通知區域中，連按兩下 **HP ProtectTools Security Manager** 圖示。

啓用安全功能

設定精靈會要求您驗證身份。

1. 閱讀「歡迎」畫面，然後按「**下一步**」。
2. 輸入 Windows 密碼（如果尚未註冊指紋）或使用指紋讀取器掃描指紋，以驗證您的身分。按「**下一步**」。

   如果沒有 Windows 密碼，會要求您建立一組密碼。需要 Windows 密碼，才能確保經過授權的人員存取 Windows 帳戶，並使用 HP ProtectTools Security Manager 功能。

設定精靈會引導您完成啓用安全性功能的程序，此安全性功能會套用於此電腦的所有使用者：

- Windows 登入安全性會藉由要求使用特定的認證進行存取，以保護您的 Windows 帳戶。
- Drive Encryption 藉由硬碟加密，使未獲授權人士無法讀取資訊的方式，保護您的資料。
- Pre-Boot Security 藉由禁止未獲授權人士在啓動 Windows 之前存取電腦的方式，保護您的電腦。

若要啓用安全功能，請選取對應的核取方塊。選取的功能愈多，電腦的安全性就愈高。

附註： Pre-Boot Security 若不受 BIOS 支援便無法使用。

註冊指紋

如果您已選取「指紋」，並且電腦有內建或連接的指紋讀取器，您將被引導逐步完成設定或「註冊」指紋的程序。

1. 此時會顯示兩個手掌的輪廓。已註冊的手指會顯示爲綠色。按一下輪廓的手指。

   附註： 若要刪除先前註冊的指紋，請按一下對應的手指。

2. 選取要註冊的手指後，會提示您掃描指紋，直到成功註冊爲止。已註冊的手指會在輪廓中顯示爲綠色。

3. 您必須至少註冊兩支手指，最好是食指和中指。對於另一隻手指，請重複步驟 1 至 3。

4. 按「**下一步**」。

附註： 透過「快速入門」程序註冊手指時，必須按「**下一步**」，才會儲存指紋資訊。如果電腦閒置一段時間或關閉 Dashboard，則不會儲存您的變更。

設定智慧卡

如果您選取「智慧卡」且智慧卡讀取器已內建或連接於您的電腦，則 HP ProtectTools 設定精靈會提示您設定智慧卡的 PIN 碼（個人識別碼）。

若要設定智慧卡 PIN：

1. 在「設定智慧卡」頁面上，輸入並確認 PIN。

   您也可以變更 PIN。提供您的舊 PIN，然後選擇新的 PIN。

2. 若要繼續，請按「**下一步**」。

使用管理主控台

HP ProtectTools 管理主控台是管理 HP ProtectTools Security Manager 功能和應用程式的中央位置。

主控台包含下列元件：

- **工具** － 顯示下列用來設定電腦安全性的類別：
  - **首頁** － 讓您選取要執行的安全性工作。
  - **系統** － 讓您設定使用者和裝置的安全功能和驗證。
  - **應用程式** － 顯示 HP ProtectTools Security Manager 和 Security Manager 應用程式的一般設定。
  - **資料** － 提供連結至可保護您的資料的 Security Manager 應用程式的展開式功能表。
- **管理工具** － 提供其他工具的資訊。以下面板顯示下列選項：
  - **HP ProtectTools 設定精靈** — 引導您完成 HP ProtectTools Security Manager 的設定。
  - **說明** — 顯示「說明」檔，提供關於 Security Manager 和其預先安裝之應用程式的資訊。您可能新增之應用程式的「說明」會在這些應用程式中提供。
  - **關於** － 顯示 HP ProtectTools Security Manager 相關資訊，例如版本號碼和著作權公告。
- **主要區域** — 顯示特定應用程式的畫面。

若要開啓 HP ProtectTools 管理主控台，請依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。

3 設定系統

從 HP ProtecTools 管理主控台畫面左側的「工具」功能表面板可存取「系統」群組。您可以使用此群組中的應用程式，管理用於電腦、電腦使用者及其裝置的原則和設定值。

「系統」群組中包含下列應用程式：

- **安全性** – 管理支配使用者與這部電腦之互動方式的功能、驗證和設定值。
- **使用者** – 設定、管理和註冊這部電腦的使用者。
- **裝置** – 管理電腦內建或連接的安全裝置設定值。

設定電腦適用的驗證

在驗證應用程式內，您可以選取這部電腦應執行哪些安全功能，設定支配電腦存取的原則，以及設定其他進階設定值。您可以指定在使用者工作階段登入 Windows 或登入網站和程式時驗證各個等級使用者所需的認證。

若要在您電腦上設定驗證：

1. 在「安全性」面板功能表中，按一下「**驗證**」。
2. 若要設定登入驗證，請按「**登入原則**」標籤，進行變更，然後按「**套用**」。
3. 若要設定工作階段驗證，請按「**工作階段原則**」標籤，進行變更，然後按「**套用**」。

登入原則

若要定義支配登入 Windows 時驗證使用者所需之認證的原則：

1. 在「工具」功能表中，按一下「**安全性**」，然後按「**驗證**」。
2. 在「**登入原則**」標籤上按一下使用者類別。
3. 指定選定的使用者類別所需的驗證認證。您至少必須指定一個認證。
4. 選擇驗證使用者時需要「任何」（僅一個）指定的認證，還是需要「所有」指定的認證。您也可以防止任何使用者存取電腦。
5. 按一下「**套用**」。

工作階段原則

若要定義支配 Windows 工作階段期間存取 HP ProtectTools 應用程式所需之認證的原則：

1. 在「工具」功能表中，按一下「**安全性**」，然後按「**驗證**」。
2. 在「**工作階段原則**」標籤上按一下使用者類別。
3. 指定選定的使用者類別所需的驗證認證。
4. 選擇驗證使用者時需要「任何」（僅一個）指定的認證，還是需要「所有」指定的認證。您也可以要求無需驗證即可存取 HP ProtectTools 軟體。
5. 按一下「**套用**」。

設定

您可以允許下列一項或多項安全性設定值：

- **允許一步登入** － 如果在 BIOS 加密磁碟層級執行驗證，允許此電腦的使用者略過 Windows 登入。
- **允許 Windows 登入的 HP SpareKey 驗證** － 不論 Security Manager 需要什麼驗證原則，都允許此電腦的使用者使用 HP SpareKey 功能登入 Windows。

若要編輯設定值：

1. 按一下以啓用或停用特定的設定值。
2. 按一下「**套用**」以儲存您所做的變更。

管理使用者

在使用者應用程式內，可監視和管理這部電腦的 HP ProtectTools 使用者。

所有 HP ProtectTools 使用者都會列出，並對照 Security Manager 設定的原則逐一驗證，確認他們是否已經註冊使其符合那些原則的適當認證。

若要新增其他使用者，請按「**新增**」。

若要刪除使用者，可按一下該使用者，然後按「**刪除**」。

若要註冊指紋或設定使用者的其他認證，可按一下該使用者，然後按「**註冊**」。

若要檢視特定使用者的原則，請選取該使用者，然後按「**檢視原則**」。

指定裝置設定值

在裝置應用程式內，可指定 HP ProtectTools Security Manager 認可之任何內建或連接的安全裝置的可用設定值。

指紋

「指紋」頁面有三個標籤：註冊、敏感度和進階。

註冊

您可選擇使用者可以註冊的指紋數上限和下限。

您也可以清除指紋讀取器的所有資料。

⚠ **警告!** 所有使用者的所有指紋資料（包括管理員）都會清除。如果「登入原則」只要求指紋，則所有使用者都無法登入此電腦。

敏感度

若要調整指紋讀取器掃描指紋時所使用的敏感度，請移動滑桿。

如果指紋識別度不夠穩定，則可能需要設定較低的敏感度。較高的設定值可提高指紋掃描的變異敏感度，並降低錯誤接受的可能性。中高設定值提供了結合安全性和方便性的好處。

進階

當電腦使用電池電源運作時，您可以設定指紋讀取器以保存電力。

智慧卡

您可以設定電腦在取出智慧卡時自動鎖定。然而，只有在登入 Windows 時將智慧卡當成驗證認證使用時，電腦才會鎖定。取出未用來登入 Windows 的智慧卡，則不會鎖定電腦。

▲ 選取核取方塊以啓用或停用取出智慧卡時自動鎖定電腦的功能。

4 設定應用程式

從 HP ProtecTools 管理主控台左側的「安全性應用程式」功能表面板可存取「應用程式」群組。您可以使用「設定」來自訂目前已安裝之 HP ProtectTools Security Manager 應用程式的行爲。

若要編輯應用程式設定值：

1. 在「工具」功能表中，在「**應用程式**」群組按一下「**設定**」。
2. 按一下以啓用或停用特定的設定值。
3. 按一下「**套用**」以儲存您所做的變更。

一般標籤

「一般」標籤上有下列設定可供使用：

- **不針對管理員自動啓動設定精靈** — 選取此選項即可防止在登入時自動開啓精靈。
- **不針對使用者自動啓動快速入門精靈** — 選取此選項即可防止使用者設定在登入時自動開啓。

應用程式標籤

此處顯示的設定值在 Security Manager 增加新的應用程式時即可變更。預設的最小設定如下所示：

- **Security Manager** — 爲電腦的所有使用者啓用 Security Manager 應用程式。
- **啓用「詳細搜尋」按鈕** — 允許此電腦的所有使用者按一下「**[+] 詳細搜尋**」按鈕，就可以爲 HP ProtectTools Security Manager 新增應用程式。

若要使所有應用程式回復出廠設定，請按「**還原預設值**」按鈕。

5 新增管理工具

另有可爲 Security Manager 新增管理工具的其他應用程式可供使用。此電腦的管理員可以透過「設定」應用程式停用此功能。

若要新增其他管理工具，請按「**[+] 管理工具**」。

您可以存取 DigitalPersona 網站以搜尋新的應用程式，或可設定自動更新的排程。

6 HP ProtectTools Security Manager

HP ProtectTools Security Manager 可以讓您大幅增加電腦的安全性。

您可以使用預先載入的 Security Manager 應用程式，以及可從網站立即下載的其他應用程式：

- 管理您的登入和密碼
- 輕鬆變更 Windows® 作業系統密碼
- 設定程式偏好設定
- 使用指紋強化安全性並提升便利性
- 設定智慧卡進行驗證
- 備份和還原程式資料
- 新增更多應用程式

設定程序

快速入門

HP ProtectTools 設定精靈會在 HP ProtectTools Security Manager 中以預設頁面自動顯示，直到設定完成爲止。

如果設定 Security Manager，請依照下列步驟執行：

附註： 如果沒有指紋讀取器或智慧卡可供使用，則僅執行步驟 1、5 和 6。

1. 在「歡迎」頁面中，按「**下一步**」。
2. 下頁列出此電腦可用的驗證方法。按「**下一步**」以繼續。
3. 在「驗證您的身分」頁面上輸入 Windows 密碼，然後按「**下一步**」。
4. 視您電腦的組態而定，參閱下列一項或多項主題。
   - 如果有指紋讀取器可供使用，請參閱 22 頁的註冊指紋。
   - 如果有智慧卡可供使用，請參閱 23 頁的設定智慧卡。
5. 如果沒有指紋讀取器或智慧卡可供使用，則會要求您輸入 Windows 密碼。未來只要需要驗證，您就必須使用此密碼。
6. 在精靈的最後一頁上，按一下「**完成**」。

   此時會顯示 Security Manager Dashboard。

註冊認證

您可以使用「我的身份」頁面，來註冊各種驗證方法或認證。註冊完成後，您可以使用這些方法登入 Security Manager。

註冊指紋

如果您的電腦有內建或連接的指紋讀取器，HP ProtectTools 設定精靈會引導您完成設定程序或「註冊」您的指紋。

1. 閱讀「歡迎」畫面，然後按「**下一步**」。
2. 輸入 Windows 密碼（如果尚未註冊指紋）或使用指紋讀取器掃描指紋，以驗證您的身分。按「**下一步**」。

   如果沒有 Windows 密碼，會要求您建立一組密碼。需要 Windows 密碼，才能確保經過授權的人員存取 Windows 帳戶，並使用 HP ProtectTools Security Manager 功能。
3. 此時會顯示兩個手掌的輪廓。已註冊的手指會顯示爲綠色。按一下輪廓的手指。

   附註： 若要刪除先前註冊的指紋，請按對應的指紋。
4. 選取要註冊的手指後，會提示您掃描指紋，直到成功註冊爲止。已註冊的手指會在輪廓中顯示爲綠色。
5. 您必須至少註冊兩支手指，最好是食指和中指。對於其他手指，重複進行步驟 3 和 4。
6. 按「**下一步**」。

附註： 透過「快速入門」程序註冊手指時，必須按「**下一步**」，才會儲存指紋資訊。如果電腦閒置一段時間或關閉 Dashboard，則不會儲存您的變更。

變更 Windows 密碼

Security Manager 能夠使得變更 Windows 密碼的程序比透過 Windows 控制台進行更簡單快速。

若要變更 Windows 密碼，請依照下列步驟執行：

1. 從 Security Manager Dashboard 按一下「**我的身分**」、「**認證**」，然後按一下「**密碼**」。
2. 在「**目前的 Windows 密碼**」文字方塊中，輸入您目前的密碼。
3. 在「**新的 Windows 密碼**」文字方塊中輸入新密碼，然後在「**確認新的密碼**」文字方塊中再次輸入新密碼。
4. 按一下「**變更**」便會立即將目前的密碼變更爲您輸入的新密碼。

設定智慧卡

如果電腦內建或連接智慧卡讀取器，Security Manager 會提示您設定智慧卡 PIN（個人識別碼）。

- 若要設定智慧卡 PIN 碼 — 在「設定智慧卡」頁面上，輸入並確認 PIN。
- 若要變更 PIN — 先輸入舊的 PIN，然後選擇新的 PIN。

使用 Security Manager Dashboard

Security Manager Dashboard 是方便存取 Security Manager 功能、應用程式和設定的集中位置。

Dashboard 包含下列元件：

- **識別卡** — 顯示 Windows 使用者名稱與用以識別登入使用者帳戶的圖片。
- **安全性應用程式** — 顯示設定下列類型的安全性時所使用的連結展開清單：
  - **我的身分**
  - **我的資料**
  - **我的電腦**
- **詳細搜尋** — 開啓可找到其他應用程式的頁面，以提升您身分、資料和通訊的安全性。
- **主要區域** — 顯示特定應用程式的畫面。
- **管理** — 開啓 HP ProtectTools 管理主控台。
- **「說明」按鈕** — 顯示目前畫面的資訊。
- **進階** — 允許您存取下列選項：
  - **偏好設定** — 允許您將 Security Manager 設定個人化。
  - **備份和還原** — 允許您備份或還原資料。
  - **關於** — 顯示 Security Manager 的版本資訊。

若要開啓 Security Manager Dashboard，請依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools Security Manager**」。

開啓 HP ProtectTools Security Manager

您可以利用下列的任何一種方式開啓 HP ProtectTools Security Manager：

- 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools Security Manager**」。
- 在工作列最右端的通知區域中，連按兩下 **HP ProtectTools** 圖示。
- 在「**HP ProtectTools**」圖示上按一下滑鼠右鍵，然後按一下「**開啓 HP ProtectTools Security Manager**」。
- 按一下 Windows 資訊看板上的「**Security Manager 識別卡**」小工具。
- 按下快速鍵組合 ctrl+alt+h，開啓 Security Manager 快速連結功能表。

一般工作

此群組包含的應用程式可協助您管理數位身分的不同層面。

- **Security Manager** — 建立並管理「快速連結」，可以讓您藉由驗證您的 Windows 密碼、指紋或智慧卡來啓動並登入網站和程式。
- **認證** — 可用來變更 Windows 密碼、註冊指紋或設定智慧卡。

若要新增更多應用程式，請按一下 Dashboard 左下角的 [+]「**進一步搜尋**」按鈕。管理員可能已停用此按鈕。

密碼管理員

使用密碼管理員是更輕鬆安全登入 Windows、網站和應用程式的方式。您可以用來建立強式密碼，完全不需要寫下或記憶，然後便能夠使用指紋、智慧卡或 Windows 密碼輕鬆快速登入。

密碼管理員提供下列選項：

- 從「管理」標籤新增、編輯或刪除登入。
- 使用已設定的快速連結來啓動您的預設瀏覽器，並登入任何網站或程式。
- 使用拖放的方式，將快速連結分類。
- 檢視您任何的密碼是否有安全性風險，並自動產生可用於新網站的複雜強式密碼。

出現網頁或程式登入畫面時，會顯示密碼管理員圖示，其中提供多項密碼管理員功能。按一下圖示可顯示內容功能表，您可以從中選擇下列選項。

對於尚未建立登入的網頁或程式

下列選項會顯示在內容功能表中：

- **將 [somedomain.com] 新增至密碼管理員** — 允許您新增目前登入畫面的登入。
- **開啓密碼管理員** — 啓動密碼管理員。
- **圖示設定** — 允許您指定顯示密碼管理員圖示的條件。
- **說明** — 顯示密碼管理員軟體說明。

對於已經建立登入的網頁或程式

下列選項會顯示在內容功能表中：

- **填入登入資料** — 將您的登入資料填入登入欄位，然後提交頁面（如果建立或最後編輯登入時已指定提交的內容）。
- **編輯登入** — 允許您編輯此網站的登入資料。
- **新增帳戶** — 允許您將帳戶新增至登入。
- **開啓密碼管理員** — 啓動密碼管理員應用程式。
- **說明** — 顯示密碼管理員軟體說明。

附註： 此電腦的管理員可能已經設定 Security Manager 在驗證您的身分時要求多個認證。

新增登入

您只要輸入登入資訊一次，即可新增網站或程式的登入。從此以後，密碼管理員就會自動爲您輸入資訊。您可以在瀏覽到網站或程式後使用這些登入，也可以從「**登入**」功能表按一下登入，讓密碼管理員開啓網站或程式，並且將您登入。

若要新增登入：

1. 開啓網站或程式的登入畫面。
2. 按一下「**密碼管理員**」圖示的箭頭，然後根據出現的是網站或程式的登入畫面，按下列其中一項：
   - 對於網站，按一下「**將 [somedomain.com] 新增至密碼管理員**」。
   - 對於程式，按一下「**此登入畫面新增至密碼管理員**」。
3. 輸入您的登入資料。畫面的登入欄位以及對話方塊的對應欄位，都會以較粗的橘色邊框表示。您可以按一下「**密碼管理員管理**」標籤的「**新增登入**」。某些選項需視連接電腦的安全性裝置而定，例如，使用 ctrl+alt+H 快速鍵、掃描指紋或插入智慧卡。
   - 若要在登入欄位中填入其中一個預先格式化的選項，按一下欄位右側的箭頭。
   - 若要將其他欄位從畫面新增至您的登入，請按「**選擇其他欄位**」。
   - 若要填入登入欄位但不提交，請清除「**提交登入資料**」核取方塊。
   - 若要檢視此登入的密碼，請按「**顯示密碼**」。
4. 按一下「**確定**」。

   密碼管理員圖示的加號會消失，以通知您已建立登入。

每次您存取網站或開啓程式時，都會顯示密碼管理員圖示，以指示您可以使用已註冊的認證進行登入。

編輯登入

若要編輯登入，請依照下列步驟執行：

1. 開啓網站或程式的登入畫面。
2. 若要顯示您可以編輯您登入資訊的對話方塊，請按「**密碼管理員**」圖示的箭頭，然後按一下「**編輯登入**」。畫面的登入欄位以及對話方塊的對應欄位，都會以較粗的橘色邊框表示。

   您可以按一下「**密碼管理員管理**」標籤的「**編輯所需的登入**」。
3. 編輯您的登入資訊。
   - 若要在登入欄位中填入其中一個預先格式化的選項，按一下欄位右側的箭頭。
   - 若要將其他欄位從畫面新增至您的登入，請按「**選擇其他欄位**」。
   - 若要填入登入欄位但不提交，請清除「**提交登入資料**」核取方塊。
   - 若要檢視此登入的密碼，請按「**顯示密碼**」。
4. 按一下「**確定**」。

使用登入功能表

若要啓動您已經建立登入的網站和程式，密碼管理員是快速簡便的方式。連按兩下「**登入**」功能表的程式或網站登入，或按一下「**密碼管理員**」的「**管理**」標籤，然後填入您的登入資料。

建立登入時，會自動新增至「密碼管理員登入」功能表。

若要顯示登入功能表：

1. 按下「**密碼管理員**」快速鍵組合。ctrl+alt+h 是原廠設定。若要變更快速鍵組合，請按「**密碼管理員**」，然後按一下「**設定**」。
2. 掃描您的指紋（從內建或連接指紋讀取器的電腦進行）。

將登入分類

建立一項或多項分類，即可使用分類來整理您的登入。然後即可將登入拖放到所需的分類。

若要新增分類：

1. 從 Security Manager Dashboard 中，按一下「**密碼管理員**」。
2. 按一下「**管理**」標籤，然後按一下「**新增分類**」。
3. 輸入分類的名稱。
4. 按一下「**確定**」。

若要將登入新增至分類：

1. 將滑鼠指標指向所需的登入。
2. 按住滑鼠左鍵。
3. 將登入拖放到分類的清單中。當您將滑鼠指向分類時，分類便會反白顯示。
4. 當所需的分類反白顯示時，放開滑鼠按鈕。

您的登入不會移至分類，只會複製到選取的分類中。您可以將相同的登入新增至多個分類中，也可以按一下「**全部**」來顯示所有的登入。

管理您的登入

密碼管理員是管理登入名稱、密碼和多個登入帳戶等登入資訊的集中位置。

您的登入會列在「管理」標籤中。如果已針對相同網站建立多個登入，則各個登入會列在網站名稱下，並且在登入清單中縮排。

若要管理您的登入：

從 Security Manager Dashboard 中，按一下「**密碼管理員**」，然後按一下「**管理**」標籤。

- **新增登入** — 按一下「**新增登入**」，並按照畫面上的指示進行。
- **編輯登入** — 按一下登入，並按一下「**編輯**」，然後變更登入資料。
- **刪除登入** — 按一下登入，然後按一下「**刪除**」。

若要新增網站或程式的其他登入：

1. 開啓網站或程式的登入畫面。
2. 按一下「**密碼管理員**」圖示，以顯示捷徑功能表。
3. 按一下「**新增其他登入**」，然後按照畫面上的指示進行。

評估密碼強度

使用強式密碼登入網站和程式，是防護您身分的重要層面。

密碼管理員會立即自動分析登入網站和程式所用的各組密碼強度，以監控和提升您的安全性。

密碼管理員圖示設定

密碼管理員會嘗試識別網站和程式的登入畫面。當密碼管理員偵測出您尚未建立登入的登入畫面時，會顯示含有「+」符號的密碼管理員圖示，以提示您新增該畫面的登入。

按一下圖示箭頭，然後按一下「**圖示設定**」以自訂「**密碼管理員**」處理可能登入網站的方式。

- **提示新增登入畫面的登入** — 按一下此選項後，當登入畫面顯示尚未設定登入時，密碼管理員會提示您新增登入。
- **排除此畫面** — 選取此核取方塊，密碼管理員便不再提示您爲此登入畫面新增登入。

若要存取其他密碼管理員設定，請按一下「**密碼管理員**」，然後按一下 Security Manager Dashboard 上的「**設定**」。

設定

您可以指定將 HP ProtectTools Security Manager 個人化的設定：

1. **提示爲登入畫面新增登入** — 只要偵測到網站或程式的登入畫面，含有加號的密碼管理員圖示就會出現，指示您可以將此畫面的登入新增至密碼保存庫。若要停用此功能，請在「**圖示設定**」對話方塊中，清除「**提示爲登入畫面新增登入**」旁的核取方塊。
2. **使用 ctrl+alt+H 開啓密碼管理員** — 開啓密碼管理員快速連結功能表的預設快速鍵是 ctrl+alt+H。若要變更快速鍵，請按一下此選項，然後輸入新的組合鍵。組合鍵可能包含下列一個或多個按鍵： ctrl、alt 或 shift，以及任何英文字母或數字鍵。
3. 按一下「**套用**」以儲存變更。

認證

您可以使用 Security Manager 認證來驗證您的身分正確無誤。此電腦的本機管理員可以設定哪些認證可用在您登入到 Windows 帳戶、網站或程式時證明您的身分。

可用的認證會因爲電腦內建或連接的安全性裝置而有所不同。各個支援的認證都會列在「**我的身分、認證**」群組中。

其中會列出可用的認證、需求和目前狀態，並且可能包含下列項目：

- 指紋
- 密碼
- 智慧卡

若要註冊或變更認證，按一下連結並按照畫面上的指示進行。

您個人的識別卡

您的識別卡可證明您確實是此 Windows 帳戶的擁有者，其中會顯示您的姓名及選擇的圖片。這會顯明出現在 Security Manager 頁面的左上角及「Windows 資訊看板」小工具中。

按一下「Windows 資訊看板」中的識別卡，是快速存取 Security Manager 的其中一種方式。

您可以變更圖片以及顯示姓名的方式。預設會顯示您在 Windows 設定期間選取的完整 Windows 使用者名稱和圖片。

若要變更顯示的名稱：

1. 從 Security Manager Dashboard 按一下左上角的「**識別卡**」。
2. 按一下顯示 Windows 中輸入帳戶名稱的方塊。系統將會顯示這個帳戶的 Windows 使用者名稱。
3. 若要變更名稱，請輸入新的名稱，然後按一下「**儲存**」按鈕。

若要變更顯示的圖片：

1. 從 Security Manager Dashboard 按一下「**我的身分**」，然後按一下左上角中的「**識別卡**」。
2. 按一下「**選擇圖片**」按鈕，按一下影像，然後按一下「**儲存**」按鈕。

設定您的偏好設定

您可以將 HP ProtectTools Security Manager 設定個人化。從 Security Manager Dashboard 中，按一下「**進階**」，然後按一下「**偏好設定**」。有兩個標籤會顯示可用的設定：「一般」和「指紋」。

一般

「一般」標籤上有下列設定可供使用：

外觀 － 在工作列上顯示圖示

若要在工作列上顯示圖片，請選取此核取方塊。

若不要在工作列上顯示圖片，請清除此核取方塊。

指紋

「指紋」標籤上有下列設定可供使用：

快速動作 — 使用「快速動作」可選取掃描指紋期間按下指定按鍵時要執行的 Security Manager 工作。

若要將快速動作指派給其中一個列出的按鍵：

- 按一下「**（按鍵）+指紋**」選項，然後從功能表中按一下其中一個可用的工作。

指紋掃描回應 — 只有在有指紋讀取器時才會顯示。使用此設定可調整掃描指紋時出現的回應。

- **啓用聲音回應** — 掃描指紋後，Security Manager 會發出聲音回應，對於特定的程式事件會發出不同的聲音。透過 Windows 控制台的「聲音」標籤，您可以將新的聲音指派給這些事件，也可以清除此選項，停用聲音回應。
- **顯示掃描品質回應** — 只有指紋掃描的品質不足以驗證您的身分，Security Manager 預設會顯示含有問號的指紋影像。您可以清除此選項，以停用此影像的顯示。

備份和還原資料

建議您定期備份 Security Manager 資料。備份的頻率可視資料變更的頻率而定。例如，如果您每天都會新增登入，則應該每天備份資料。

備份也可用來從一部電腦轉移到另一部電腦，也就是所謂的匯入和匯出。

附註： 此功能只會備份資料。

要用來接收備份資料的任何電腦都必須安裝 HP ProtectTools Security Manager，才能從備份檔案還原資料。

若要備份資料：

1. 在左側面板上，按一下「**進階**」，然後按一下「**備份和還原**」。
2. 按一下「**備份資料**」。
3. 選取您要包含在備份中的模組。在多數情況下，都會全部選取。
4. 輸入儲存檔的名稱。根據預設，此檔案會儲存到您的文件資料夾。按一下「**瀏覽**」以指定不同的位置。
5. 輸入密碼以保護檔案。
6. 驗證您的身分。
7. 按一下「**完成**」。

若要還原資料：

1. 在左側面板上，按一下「**進階**」，然後按一下「**備份和還原**」。
2. 按一下「**還原資料**」。
3. 選取之前建立的儲存檔。您可以在提供的欄位中輸入路徑，或按一下「**編輯**」。
4. 輸入用來保護檔案的密碼。
5. 選取您要還原其資料的模組。通常會是所有列出的模組。
6. 按一下「**完成**」。

新增應用程式

另有提供此程式新功能的其他應用程式可供使用。

從 Security Manager Dashboard 中，按一下「**[+] 詳細搜尋**」，以瀏覽其他應用程式。

附註： 如果 Dashboard 的左下方沒有「**[+] 詳細搜尋**」連結，則表示此電腦的管理員已停用此連結。

安全性應用程式狀態

Security Manager 應用程式狀態頁面顯示已安裝安全性應用程式的整體狀態。這會顯示已安裝的應用程式，以及各個應用程式的設定狀態。開啓 Security Manager Dashboard 或按一下「**安全性應用程式**」時，會自動顯示摘要。

7 HP ProtectTools Drive Encryption（僅限特定機型）

△ **注意：** 如果您決定要解除安裝 Drive Encryption 模組，您必須先將所有加密的磁碟機解密。若沒有將磁碟機解密，除非您已經註冊 Drive Encryption 復原服務，否則您將無法存取加密磁碟機中的資料。重新安裝 Drive Encryption 模組並不能讓您存取加密的磁碟機。

HP ProtectTools Drive Encryption 可透過加密電腦硬碟，提供完整的資料保護。啟用 Drive Encryption 時，您必須在 Windows® 作業系統啟動之前所顯示的 Drive Encryption 登入畫面中登入 Drive Encryption。

HP ProtectTools 設定精靈允許 Windows 管理員啟用 Drive Encryption、備份加密金鑰、新增及移除使用者，以及停用 Drive Encryption。如需詳細資訊，請參閱 HP ProtectTools Security Manager 軟體「說明」。

Drive Encryption 可執行下列工作：

- 加密管理
  - 加密或解密個別磁碟機

    附註： 僅能加密內建硬碟。
- 復原
  - 建立備份金鑰
  - 執行復原

設定程序

開啓 Drive Encryption

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Drive Encryption**」。

一般工作

啓用 Drive Encryption

使用 HP ProtectTools 設定精靈來啓用 Drive Encryption。

附註： 此精靈也可用於新增和移除使用者。

－ 或 －

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」，然後按一下「**功能**」。
3. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。
4. 在「**要加密的磁碟機**」下方，選取在您要加密的硬碟核取方塊。
5. 將儲存裝置插入適當的插槽。

   附註： 若要儲存加密金鑰，您必須使用具有 FAT32 格式的 USB 儲存裝置來儲存加密金鑰。
6. 在「**儲存加密金鑰的外接式儲存裝置**」下，選取即將儲存加密金鑰的儲存裝置核取方塊。
7. 按一下「**套用**」。

   磁碟機加密隨即開始。

如需詳細資訊，請參閱 HP ProtectTools Security Manager 軟體「說明」。

停用 Drive Encryption

使用 HP ProtectTools 設定精靈來停用 Drive Encryption。如需詳細資訊，請參閱 HP ProtectTools Security Manager 軟體「說明」。

－ 或 －

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」，然後按一下「**功能**」。
3. 清除「**Drive Encryption**」核取方塊，然後按一下「**套用**」。

   磁碟機解密隨即開始。

在啓用 Drive Encryption 之後登入

當您在啓用 Drive Encryption 並註冊使用者帳戶之後開啓電腦時，就必須在 Drive Encryption 登入畫面進行登入：

附註： 如果 Windows 管理員已經在 HP ProtectTools Security Manager 中啓用「預先開機安全性」功能，您就會在電腦開啓後立刻登入電腦，而不是在 Drive Encryption 登入畫面登入。

1. 按一下您的使用者名稱，然後輸入 Windows 密碼或 Java™ 卡 PIN，或者用已註冊的手指掃過。
2. 按一下「**確定**」。

附註： 如果您在 Drive Encryption 登入畫面中以復原金鑰登入，這時系統也會提示您在 Windows 登入畫面選取 Windows 使用者名稱並輸入密碼。

將硬碟加密以保護資料

使用 HP ProtectTools 設定精靈將硬碟加密以保護資料：

1. 在 Security Manager 中，按一下「**快速入門**」，然後按一下「**Security Manager 設定**」圖示。說明 Security Manager 功能的示範隨即開始 （您也可以從「Drive Encryption」頁面啓動 Security Manager）。
2. 在左側窗格中，按一下「**Drive Encryption**」，然後按一下「**加密管理**」。
3. 按一下「**變更加密**」。
4. 選取要加密的磁碟機。

附註： 強烈建議您加密硬碟。

顯示加密狀態

使用者可從 HP ProtectTools Security Manager 顯示加密狀態。

附註： 必須使用「HP ProtectTools 管理主控台」變更磁碟機加密狀態。

1. 開啓「**HP ProtectTools Security Manager**」。
2. 在「**我的資料**」之下按「**加密狀態**」。

   如果磁碟機狀態是「作用中」，則磁碟機狀態會顯示下列其中一個狀態代碼：

   - 作用中
   - 非作用中
   - 未加密
   - 已加密
   - 加密
   - 解密

   如果正在加密或解密硬碟，進度列會顯示完成加密或解密的百分比，以及完成加密或解密的剩餘時間。

進階工作

管理 Drive Encryption（管理員工作）

「加密管理」頁面可讓管理員檢視和變更 Drive Encryption 的狀態（作用中或非作用中），以及檢視電腦上所有硬碟的加密狀態。

- 如果狀態是「非作用中」，表示 Windows 管理員尚未啓用 HP ProtectTools Security Manager 中的 Drive Encryption，因此目前並沒有在保護硬碟。使用 HP ProtectTools Security Manager 安裝精靈來啓用 Drive Encryption。
- 如果狀態是「作用中」，表示 Drive Encryption 已啓用並已設定。磁碟機會處於下列其中一種狀態：
  - 未加密
  - 已加密
  - 加密
  - 解密

加密或解密個別磁碟機

如果要加密電腦上一個或多個硬碟，或是解密已加密過的磁碟機，請使用「變更加密」功能：

1. 開始「**HP ProtectTools 管理主控台**」，按一下「**Drive Encryption**」，然後按「**加密管理**」。
2. 按一下「**變更加密**」。
3. 在「變更加密」對話方塊中，選取或清除要加密或解密之個別硬碟旁邊的核取方塊，然後按一下「**確定**」。

附註： 在磁碟機進行加密或解密時，進度列會在目前工作階段過程中顯示完成處理所剩餘的時間。如果電腦在加密處理期間關機或啓動「睡眠」或「休眠」，之後又重新啓動，雖然「剩餘時間」顯示會重設爲從頭開始，但是實際加密會從上次停止處繼續進行。剩餘時間和進度顯示的變化會更快速，以反映之前的進度。

備份與復原（管理員工作）

「復原」頁面可讓管理員備份及復原加密金鑰。

「**本機磁碟加密金鑰備份**」— 可讓您在 Drive Encryption 啓用期間將加密金鑰備份至抽取式媒體。

建立備份金鑰

您可以將已加密磁碟機的加密金鑰備份至抽取式儲存裝置：

注意： 請確定將含有備份金鑰的儲存裝置存放在安全的地方，因爲如果忘記密碼或遺失 Java 卡，就只能透過此裝置提供的資料來存取硬碟。

1. 開啓「**HP ProtectTools 管理主控台**」，按一下「**Drive Encryption**」，然後按「**復原**」。
2. 按一下「**備份金鑰**」。
3. 在「選取備份磁碟」頁面上，選取要備份加密金鑰的裝置核取方塊，然後按「**下一步**」。

4. 閱讀下一頁所顯示的資訊，然後按「**下一步**」。這樣加密金鑰就會儲存至選定的存放裝置。
5. 當出現確認對話方塊時，按一下「**完成**」。

執行復原

如果忘記密碼，若要執行復原，請依照下列步驟進行：

1. 開啓電腦。
2. 插入包含您的備份金鑰的抽取式儲存裝置。
3. 當「HP ProtectTools Drive Encryption」登入對話方塊開啓時，按一下「**取消**」。
4. 按一下螢幕左下角的「**選項**」，然後按一下「**復原**」。
5. 選取含有您備份金鑰的檔案，或按一下「**瀏覽**」搜尋該檔案，然後按「**下一步**」。
6. 當出現確認對話方塊時，按一下「**確定**」。

   電腦隨即啓動。

附註： 在執行復原之後，強烈建議您重設密碼。

8 HP ProtectTools Privacy Manager（僅限特定機型）

HP ProtectTools Privacy Manager 可供您使用進階的安全登入（驗證）方法，以在使用電子郵件、Microsoft® Office 文件或即時通訊 (IM) 時驗證通訊的來源、完整性與安全性。

Privacy Manager 運用 HP ProtectTools Security Manager 提供的安全性基礎架構，其中包括下列安全登入法：

- 指紋驗證
- Windows® 密碼
- HP ProtectTools Java™ 卡

您可以在 Privacy Manager 中使用上述的任何安全登入法。

Privacy Manager 需要下列項目：

- HP ProtectTools Security Manager 5.00 或更高版本
- Windows® 7、Windows Vista® 或 Windows XP 作業系統
- Microsoft Outlook 2007 或 Microsoft Outlook 2003
- 有效的電子郵件帳戶

附註： 在您存取安全性功能之前，必須從 Privacy Manager 之中申請並安裝 Privacy Manager 憑證（一種數位憑證）。如需申請 Privacy Manager 憑證的詳細資訊，請參閱 38 頁的申請並安裝 Privacy Manager 憑證。

設定程序

開啓 Privacy Manager

若要開啓 Privacy Manager：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools Security Manager**」。
2. 按一下「**Privacy Manager**」。

－ 或 －

以滑鼠右鍵按一下工作列最右側通知區域中的「**HP ProtectTools**」圖示，按一下「**Privacy Manager**」，然後按一下「**組態 (Configuration)**」。

－ 或 －

在 Microsoft Outlook 電子郵件訊息的工具列上，按一下「**安全地傳送**」旁邊的向下箭頭，然後按一下「**憑證**」或「**信任的連絡人**」。

－ 或 －

在 Microsoft Office 文件的工具列上，按一下「**登入與加密**」旁邊的向下箭頭，然後按一下「**憑證**」或「**信任的連絡人**」。

管理 Privacy Manager 憑證

Privacy Manager 憑證使用一種名爲公開金鑰基礎架構 (Public Key Infrastructure，PKI) 的密碼編譯技術，保護資料和郵件。PKI 要求使用者取得密碼編譯金鑰和憑證授權單位 (CA) 簽發的 Privacy Manager 憑證。不像多數資料加密及驗證軟體僅要求您定期驗證，Privacy Manager 在您每次使用密碼編譯金鑰簽署電子郵件訊息或 Microsoft Office 文件時都會要求驗證。Privacy Manager 確保您儲存和傳送重要資訊的過程安全無虞。

您可以執行下列工作：

- 申請並安裝 Privacy Manager 憑證
- 檢視 Privacy Manager 憑證詳細資料
- 更新 Privacy Manager 憑證
- 當有多重憑證可使用時，請設定 Privacy Manager 使用的預設 Privacy Manager 憑證
- 刪除並撤銷 Privacy Manager 憑證（進階）

申請並安裝 Privacy Manager 憑證

在您使用 Privacy Manager 功能之前，必須使用有效的電子郵件地址以申請並安裝 Privacy Manager 憑證（在 Privacy Manager 中執行）。此電子郵件地址必須在您申請 Privacy Manager 憑證的相同電腦上，設定爲 Microsoft Outlook 中的一個帳號。

申請 Privacy Manager 憑證

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下「**申請 Privacy Manager 憑證**」。

3. 閱讀「歡迎」頁面上的文字，然後按「**下一步**」。
4. 閱讀「授權合約」頁面上的授權合約內容。
5. 務必選取「**勾選此處以授受此授權合約的條款**」旁邊的核取方塊，然後按「**下一步**」。
6. 在「您的憑證詳細資料」頁面上，輸入必要的資訊，然後按「**下一步**」。
7. 在「接受憑證要求」頁面上，按一下「**完成**」。
8. 按一下「**確定**」即可關閉憑證。

您將在 Microsoft Outlook 中收到一封附加 Privacy Manager 憑證的電子郵件。

取得預先指定的 Privacy Manager 公司憑證

1. 在 Outlook 中，開啓您所收到通知您已被預先指派公司憑證的相關電子郵件。
2. 按一下「**取得**」。
3. 您將在 Microsoft Outlook 中收到一封附加 Privacy Manager 憑證的電子郵件。
4. 若要安裝憑證，請參閱 39 頁的安裝 Privacy Manager 憑證。

安裝 Privacy Manager 憑證

1. 當您收到附加 Privacy Manager 憑證的電子郵件時，可開啓此電子郵件，並在 Outlook 2007 郵件右下角或在 Outlook 2003 左上角按一下「**設定**」按鈕。
2. 使用您選擇的安全登入法進行驗證。
3. 在「已安裝憑證」頁面上，按「**下一步**」。
4. 在「憑證備份」頁面上，輸入備份檔案的位置及名稱，或按一下「**瀏覽**」以搜尋位置。

△ **注意：** 務必將此檔案儲存在硬碟以外的地方，並收藏在安全處所。這個檔案僅供您個人使用，在還原 Privacy Manager 憑證和相關金鑰時需要用到。

5. 輸入並確認密碼，然後按「**下一步**」。
6. 使用您選擇的安全登入法進行驗證。
7. 如果您選擇開始進行「信任的連絡人」邀請程序，請依照螢幕上的指示進行，從 42 頁的使用 Microsoft Outlook 通訊錄新增信任的連絡人主題的步驟 2 開始。

   － 或 －

   如果您按一下「**取消**」，稍後請參閱 42 頁的新增信任的連絡人以取得新增「信任的連絡人」的詳細資訊。

檢視 Privacy Manager 憑證詳細資料

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下「Privacy Manager 憑證」。
3. 按一下「**憑證詳細資料**」。
4. 當您檢視完畢詳細資料後，按一下「**確定**」。

更新 Privacy Manager 憑證

當 Privacy Manager 憑證即將到期時，您將收到更新通知：

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下「**更新憑證**」。
3. 請依照螢幕上的指示，購買新的 Privacy Manager 憑證。

附註： Privacy Manager 憑證更新程序不會取代舊的 Privacy Manager 憑證。您需要購買新的 Privacy Manager 憑證，並使用如 38 頁的申請並安裝 Privacy Manager 憑證所示之相同程序來安裝。

設定預設的 Privacy Manager 憑證

即使您的電腦已安裝其他憑證授權單位簽發的憑證，在 Privacy Manager 內也只能看到 Privacy Manager 憑證。

如果您的電腦由 Privacy Manager 內安裝了一個以上的 Privacy Manager 憑證，您可以指定其中一個做爲預設憑證：

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下要當做預設值使用的 Privacy Manager 憑證，然後按「**設定預設值**」。
3. 按一下「**確定**」。

附註： 您不需要使用預設的 Privacy Manager 憑證。由各種 Privacy Manager 功能中，可以選取任何 Privacy Manager 憑證來使用。

刪除 Privacy Manager 憑證

如果刪除 Privacy Manager 憑證，您將無法開啓或檢視任何以該憑證加密的檔案或資料。如果不小心刪除了 Privacy Manager 憑證，您可以使用安裝憑證時所建立的備份檔案加以還原。如需詳細資訊，請參閱 40 頁的還原 Privacy Manager 憑證。

若要刪除 Privacy Manager 憑證：

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下您要刪除的 Privacy Manager 憑證，然後按「**進階**」。
3. 按一下「**刪除**」。
4. 當確認對話方塊開啓時，按一下「**是**」。
5. 按一下「**關閉**」，然後按「**套用**」。

還原 Privacy Manager 憑證

安裝 Privacy Manager 憑證期間，需要建立憑證的備份副本。您也許可以從「轉移」頁面建立備份副本。當要轉移至另一部電腦，或要將憑證還原至相同電腦時，即可使用此備份副本。

1. 開啓 Privacy Manager，並按一下「**轉移**」。
2. 按一下「**還原**」。

3. 在「轉移檔案」頁面上，按一下「**瀏覽**」以搜尋您在備份過程中所建立的 .dppsm 檔案，然後按「**下一步**」。
4. 輸入建立備份時所使用的密碼，然後按「**下一步**」。
5. 按一下「**完成**」。
6. 按一下「**確定**」。

如需詳細資訊，請參閱 39 頁的安裝 Privacy Manager 憑證或 54 頁的備份 Privacy Manager 憑證和信任的連絡人。

撤銷 Privacy Manager 憑證

如果您對 Privacy Manager 憑證的安全性已經產生疑慮，即可撤銷您自己的憑證：

附註： 撤銷的 Privacy Manager 憑證並未刪除。該憑證仍可用來檢視加密的檔案。

1. 開啓 Privacy Manager，並按一下「**憑證**」。
2. 按一下「**進階**」。
3. 按一下您要撤銷的 Privacy Manager 憑證，然後按「**撤銷**」。
4. 當確認對話方塊開啓時，按一下「**是**」。
5. 使用您選擇的安全登入法進行驗證。
6. 請依照螢幕上的說明繼續執行。

管理信任的連絡人

「信任的連絡人」是與您交換 Privacy Manager 憑證的使用者，您可以與他們安全地彼此通訊。

「受信任連絡人管理員」可讓您執行下列工作：

- 檢視信任的連絡人詳細資料
- 刪除信任的連絡人
- 檢查「信任的連絡人」（進階）的撤銷狀態

新增信任的連絡人

新增「信任的連絡人」是一個 3 步驟的程序：

1. 首先，傳送一封電子郵件邀請給「信任的連絡人」收件者。
2. 「信任的連絡人」收件者回應此電子郵件。
3. 您收到「信任的連絡人」收件者的電子郵件回應，然後按「**接受**」。

您可以傳送「信任的連絡人」電子郵件邀請給個別收件者，或者傳送邀請函給所有在您 Microsoft Outlook 通訊錄中的連絡人。

請參閱下列章節以新增「信任的連絡人」。

附註： 若要回應您的邀請以成爲「信任的連絡人」，「信任的連絡人」收件者必須在其電腦上安裝 Privacy Manager，或者安裝替代用戶端程式。如需安裝替代用戶端程式的詳細資訊，請造訪 DigitalPersona 網站，網址是：http://DigitalPersona.com/PrivacyManager。

新增信任的連絡人

1. 開啓 Privacy Manager，按一下「**受信任連絡人管理員**」，然後按「**邀請連絡人**」。

   － 或 －

   在 Microsoft Outlook 的工具列上，按一下「**安全地傳送**」旁邊的向下箭頭，然後按「**邀請連絡人**」。

2. 如果開啓了「選取憑證」對話方塊，按一下您要使用的 Privacy Manager 憑證，然後按「**確定**」。

3. 當出現「信任的連絡人邀請」對話方塊時，請閱讀文字，然後按「**確定**」。

   接著將自動產生一封電子郵件。

4. 輸入一個或多個您要新增爲「信任的連絡人」的收件者電子郵件地址。

5. 編輯文字，並簽署您的名字（選用）。

6. 按一下「**傳送**」。

附註： 如果您尚未取得 Privacy Manager 憑證，將會有訊息通知您必須具有 Privacy Manager 憑證才能傳送「信任的連絡人」要求。按一下「**確定**」以啓動「憑證要求精靈」。如需詳細資訊，請參閱 38 頁的申請並安裝 Privacy Manager 憑證。

7. 使用您選擇的安全登入法進行驗證。

附註： 當「信任的連絡人」收件者收到電子郵件後，收件者必須開啓電子郵件，並按一下電子郵件右下角的「**接受**」，然後在確認對話方塊開啓時按一下「**確定**」。

8. 當您收到收件者接受邀請成爲「信任的連絡人」的電子郵件回應後，按一下電子郵件右下角的「**接受**」。

   對話方塊隨即開啓，確認收件者已經成功地新增到您的「信任的連絡人」清單。

9. 按一下「**確定**」。

使用 Microsoft Outlook 通訊錄新增信任的連絡人

1. 開啓 Privacy Manager，按一下「**受信任連絡人管理員**」，然後按「**邀請連絡人**」。

   － 或 －

   在 Microsoft Outlook 的工具列上，按一下「**安全地傳送**」旁邊的向下箭頭，然後按「**邀請所有我的 Outlook 連絡人**」。

2. 當「信任的連絡人邀請」頁面開啓時，選取您要新增爲「信任的連絡人」的電子郵件地址，然後按「**下一步**」。

3. 當「傳送邀請」頁面開啓時，按一下「**完成**」。

   接著將會自動產生一封列出選定 Microsoft Outlook 電子郵件地址的電子郵件。

4. 編輯文字，並簽署您的名字（選用）。

5. 按一下「**傳送**」。

附註： 如果您尚未取得 Privacy Manager 憑證，將會有訊息通知您必須具有 Privacy Manager 憑證才能傳送「信任的連絡人」要求。按一下「**確定**」以啓動「憑證要求精靈」。如需詳細資訊，請參閱 38 頁的申請並安裝 Privacy Manager 憑證。

6. 使用您選擇的安全登入法進行驗證。

附註： 當「信任的連絡人」收件者收到電子郵件後，收件者必須開啓電子郵件，並按一下電子郵件右下角的「**接受**」，然後在確認對話方塊開啓時按一下「**確定**」。

7. 當您收到收件者接受邀請成爲「信任的連絡人」的電子郵件回應後，按一下電子郵件右下角的「**接受**」。

   接著對話方塊開啓，確認收件者已經成功地新增到您的「信任的連絡人」清單。

8. 按一下「**確定**」。

檢視信任的連絡人詳細資料

1. 開啓 Privacy Manager，按一下「**信任的連絡人**」。
2. 按一下「信任的連絡人」。
3. 按一下「**連絡人詳細資料**」。
4. 當您檢視完畢詳細資料後，按一下「**確定**」。

刪除信任的連絡人

1. 開啓 Privacy Manager，按一下「**信任的連絡人**」。
2. 按一下要刪除的「信任的連絡人」。
3. 按一下「**刪除連絡人**」。
4. 當出現確認對話方塊時，請按一下「**是**」。

檢查信任的連絡人的撤銷狀態

若要查看「信任的連絡人」是否已撤銷他們的 Privacy Manager 憑證：

1. 開啓 Privacy Manager，按一下「**信任的連絡人**」。
2. 按一下「信任的連絡人」。
3. 按一下「**進階**」按鈕。

   「進階的受信任連絡人管理」對話方塊隨即開啓。

4. 按一下「**檢查撤銷**」。
5. 按一下「**關閉**」。

一般工作

您可以在下列 Microsoft 產品中使用 Privacy Manager：

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

在 Microsoft Outlook 中使用 Privacy Manager

安裝 Privacy Manager 後，「隱私權」按鈕會顯示在 Microsoft Outlook 工具列上，而且「安全地傳送」按鈕也會顯示在每一封 Microsoft Outlook 電子郵件訊息的工具列上。當您按一下「**隱私權**」或「**安全地傳送**」旁邊的向下箭頭後，可以由下列選項中選擇：

- 簽署與傳送（僅限「安全地傳送」按鈕）— 此選項會在電子郵件中新增數位簽章，並在使用您選擇的安全登入法進行驗證後傳送電子郵件。
- 爲信任的連絡人密封並傳送（僅限「安全地傳送」按鈕）— 此選項會新增數位簽章、加密電子郵件，並在使用您選擇的安全登入法進行驗證後傳送電子郵件。
- 邀請連絡人 — 此選項可以讓您傳送「信任的連絡人」邀請。如需詳細資訊，請參閱 42 頁的新增信任的連絡人。
- 邀請 Outlook 連絡人 — 此選項可以讓您傳送「信任的連絡人」邀請給您 Microsoft Outlook 通訊錄中的所有連絡人。如需詳細資訊，請參閱 42 頁的使用 Microsoft Outlook 通訊錄新增信任的連絡人。
- 開啓 Privacy Manager 軟體 —「憑證」、「信任的連絡人」和「設定」選項可以讓您開啓 Privacy Manager 軟體，以新增、檢視或變更目前的設定。如需詳細資訊，請參閱 44 頁的爲 Microsoft Outlook 設定 Privacy Manager。

爲 Microsoft Outlook 設定 Privacy Manager

1. 開啓 Privacy Manager，按一下「**設定**」，然後按一下「**電子郵件**」標籤。

   - 或 -

   在 Microsoft Outlook 的主工具列上，按一下「**安全地傳送**」旁邊的向下箭頭（Outlook 2003 中請按一下「**隱私權**」），然後按一下「**設定**」。

   - 或 -

   在 Microsoft 電子郵件訊息的工具列上，按一下「**安全地傳送**」旁邊的向下箭頭，然後按一下「**設定**」。

2. 選取您在傳送安全的電子郵件時執行的動作，然後按一下「**確定**」。

簽署與傳送電子郵件訊息

1. 在 Microsoft Outlook 中，按一下「**新增**」或「**回覆**」。
2. 輸入您的電子郵件訊息。

3. 按一下「**安全地傳送**」旁邊的向下箭頭（Outlook 2003 中請按一下「**隱私權**」），然後按一下「**簽署與傳送**」。

4. 使用您選擇的安全登入法進行驗證。

密封並傳送電子郵件訊息

經過數位簽署並密封（加密）的密封電子郵件訊息，只能由您從「信任的連絡人」清單中選擇的人檢視。

若要密封並傳送電子郵件訊息給「信任的連絡人」：

1. 在 Microsoft Outlook 中，按一下「**新增**」或「**回覆**」。

2. 輸入您的電子郵件訊息。

3. 按一下「**安全地傳送**」旁邊的向下箭頭（Outlook 2003 中請按一下「**隱私權**」），然後按一下「**爲信任的連絡人密封並傳送**」。

4. 使用您選擇的安全登入法進行驗證。

檢視密封的電子郵件訊息

當您開啓密封的電子郵件訊息時，安全性標籤會顯示在電子郵件的標題中。此安全性標籤提供下列資訊：

- 使用哪一個認證來驗證簽署這封電子郵件者的身份
- 用來驗證簽署這封電子郵件者之認證的產品

在 Microsoft Office 2007 文件中使用 Privacy Manager

附註： Privacy Manager 僅能用於搭配 Microsoft Office 2007 文件。

安裝 Privacy Manager 憑證後，「簽署與加密」按鈕會顯示在所有 Microsoft Word、Microsoft Excel 和 Microsoft PowerPoint 文件的工具列右側。當您按「**簽署與加密**」旁邊的向下箭頭後，您可以由下列選項中選擇：

- 簽署文件 — 此選項會在文件中新增您的數位簽章。
- 在簽署前新增簽章線（僅限 Microsoft Word 和 Microsoft Excel）— 根據預設，當 Microsoft Word 或 Microsoft Excel 文件簽署或加密時會新增簽章線。若要關閉這個選項，請按一下「**新增簽章線**」以移除此核取標記。
- 加密文件 — 此選項會新增您的數位簽章並加密文件。
- 移除加密 — 此選項會移除文件的加密。
- 開啓 Privacy Manager 軟體 —「憑證」、「信任的連絡人」和「設定」選項可以讓您開啓 Privacy Manager 軟體，以新增、檢視或變更目前的設定。如需詳細資訊，請參閱 38 頁的管理 Privacy Manager 憑證、41 頁的管理信任的連絡人或 46 頁的爲 Microsoft Office 設定 Privacy Manager。

爲 Microsoft Office 設定 Privacy Manager

1. 開啓 Privacy Manager，按一下「**設定**」，然後按一下「**文件**」標籤。

   - 或 -

   在 Microsoft Office 文件的工具列上，按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**設定**」。

2. 選取您要設定的動作，然後按一下「**確定**」。

簽署 Microsoft Office 文件

1. 在 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 中，建立並儲存文件。
2. 按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**簽署文件**」。
3. 使用您選擇的安全登入法進行驗證。
4. 當確認對話方塊開啓時，請閱讀文字，然後按一下「**確定**」。

如果您稍後決定要編輯此文件，請依照下列步驟進行：

1. 按一下畫面左上角的「**Office**」按鈕。
2. 按一下「**準備**」，然後按一下「**標示爲最終版本**」。
3. 當確認對話方塊開啓時，按一下「**是**」並繼續工作。
4. 在完成編輯後，再次簽署文件。

簽署 Microsoft Word 或 Microsoft Excel 文件時新增簽章線

Privacy Manager 可讓您在簽署 Microsoft Word 或 Microsoft Excel 文件時，新增簽章線：

1. 在 Microsoft Word 或 Microsoft Excel 中，建立並儲存文件。
2. 按一下「**首頁**」功能表。
3. 按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**在簽署前新增簽章線**」。

   附註： 選取此選項後，「在簽署前新增簽章線」旁邊會顯示核取標記。此選項預設爲啓用。

4. 按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**簽署文件**」。
5. 使用您選擇的安全登入法進行驗證。

新增建議的簽署者至 Microsoft Word 或 Microsoft Excel 文件

您可以藉由指定建議的簽署者新增一個以上的簽章線至文件中。建議的簽署者是由 Microsoft Word 或 Microsoft Excel 文件的所有者指定，新增簽章線至文件中的使用者。建議的簽署者可以是您或是另一位您要其簽署文件的人。例如，如果您準備的文件需要由部門的所有成員簽署，您可以爲那些使用者在文件最後一頁的底部加上簽章線，並附上在特定日期前簽署的指示。

若要新增建議的簽署者至 Microsoft Word 或 Microsoft Excel 文件：

1. 在 Microsoft Word 或 Microsoft Excel 中，建立並儲存文件。
2. 按一下「**插入**」功能表。

3. 在工具列上的「**文字**」群組中，按一下「**簽章線**」旁邊的箭頭，然後按一下「**Privacy Manager 簽章提供者 (Privacy Manager Signature Provider)**」。

   「簽章設定」對話方塊隨即開啓。

4. 在「**建議的簽署者**」底下的方塊中，輸入建議的簽署者姓名。

5. 在「**給簽署者的指示**」底下的方塊中，輸入給這位建議的簽署者的訊息。

   附註： 此訊息將出現在職稱處，而且此文件一經簽署，便無法由使用者的職稱刪除或取代。

6. 選取「**在簽章線顯示簽署日期**」核取方塊以顯示日期。

7. 選取「**在簽章線顯示簽署者職稱**」核取方塊以顯示職稱。

   附註： 因爲文件的所有者爲他或她的文件指定了建議的簽署者，如果「**在簽章線顯示簽署日期**」和/或「**在簽章線顯示簽署者職稱**」的核取方塊未被選取，那麼即使建議的簽署者的文件做這樣的設定，建議的簽署者也無法在新增簽章線中顯示日期和/或職稱。

8. 按一下「**確定**」。

新增建議的簽署者的簽章線

當建議的簽署者開啓文件時，他們將看見自己的名字出現在括號中，表示需要他們的簽章。

若要簽署文件：

1. 連按兩下適當的簽章線。

2. 使用您選擇的安全登入法進行驗證。

   簽章線將根據文件所有者所指定的設定顯示。

加密 Microsoft Office 文件

您可以爲您和您的「信任的連絡人」加密 Microsoft Office 文件。當您加密文件並關閉後，您和您從清單所選取的「信任的連絡人」在開啓文件前必須先進行驗證。

若要加密 Microsoft Office 文件：

1. 在 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 中，建立並儲存文件。

2. 按一下「**首頁**」功能表。

3. 按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**加密文件**」。

   「選取信任的連絡人」對話方塊隨即開啓。

4. 按一下能夠開啓文件並檢視其內容之「信任的連絡人」姓名。

   附註： 若要選取多個「信任的連絡人」姓名，請按住 ctrl 鍵並按一下個別名稱。

5. 按一下「**確定**」。

如果您稍後決定要編輯此文件，請依照 48 頁的從 Microsoft Office 文件中移除加密中的步驟進行。移除加密後，您就可以編輯文件了。請依照本節所述之步驟，再次加密文件。

從 Microsoft Office 文件中移除加密

在您從 Microsoft Office 文件中移除加密後，您和您的「信任的連絡人」就不再需要經過驗證來開啓和檢視文件內容。

若要從 Microsoft Office 文件中移除加密：

1. 開啓加密的 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 文件。
2. 使用您選擇的安全登入法進行驗證。
3. 按一下「**首頁**」功能表。
4. 按一下「**簽署與加密**」旁邊的向下箭頭，然後按一下「**移除加密**」。

傳送加密的 Microsoft Office 文件

您可以將已加密的 Microsoft Office 文件附加於電子郵件訊息中，無需簽署或加密電子郵件本身。若要這麼做，只要依照您通常傳送帶有附件的一般電子郵件的方式，建立並傳送帶有簽署或加密文件的電子郵件即可。

然而，爲達到最佳的安全性，建議您在附加簽署或加密的 Microsoft Office 文件時，加密該電子郵件。

若要傳送附加簽署和/或加密的 Microsoft Office 文件的密封電子郵件，請依照下列步驟進行：

1. 在 Microsoft Outlook 中，按一下「**新增**」或「**回覆**」。
2. 輸入您的電子郵件訊息。
3. 附加 Microsoft Office 文件。
4. 如需進一步指示，請參閱 45 頁的密封並傳送電子郵件訊息。

檢視簽署的 Microsoft Office 文件

附註： 您不需具備 Privacy Manager 憑證，就能夠檢視已經簽署的 Microsoft Office 文件。

當簽署的 Microsoft Office 文件開啓後，「數位簽章」圖示會顯示在文件視窗最底下的狀態列中。

1. 按一下「**數位簽章**」圖示以切換「簽章」對話方塊的顯示，即顯示簽署文件的所有使用者名稱及每位使用者簽署的日期。
2. 若要檢視每個簽章的其他詳細資料，以滑鼠右鍵按一下「簽章」對話方塊中的名稱，然後選取「簽章詳細資料」。

檢視加密的 Microsoft Office 文件

若要從其他電腦檢視加密的 Microsoft Office 文件，就必須在該電腦上安裝 Privacy Manager。此外，您必須還原用來加密該檔案的 Privacy Manager 憑證。

若「信任的連絡人」想要檢視加密的 Microsoft Office 文件，就必須具備 Privacy Manager 憑證，並在電腦上安裝 Privacy Manager。此外，加密的 Microsoft Office 文件所有者必須選取該「信任的連絡人」。

在 Windows Live Messenger 中使用 Privacy Manager

Privacy Manager 將以下安全通訊功能新增至 Windows Live Messenger：

- **安全聊天** — 訊息是使用 SSL/TLS（安全通訊端層/傳輸層安全性）透過 XML 通訊協定傳輸，與確保電子商務交易安全性的技術相同。
- **收件者識別** — 在傳送訊息前，您可以驗證個人的狀態和身份。
- **簽署的訊息** — 您可以以電子的方式簽署訊息。如果此訊息被竄改，則當收件者收到時，訊息將被標示爲無效。
- **隱藏/顯示功能** — 您可以在 Privacy Manager Chat 視窗隱藏任何或所有訊息。您也可以傳送隱藏內容的訊息。訊息顯示前需要經過驗證。
- **安全聊天歷程記錄** — 聊天工作階段的記錄在儲存前會加密，且需要驗證才能檢視。
- **自動鎖定/解除鎖定** — 您可以鎖定和解除鎖定 Privacy Manager Chat) 視窗，或設定成超過一段指定的無活動期間後自動鎖定。

啓動 Privacy Manager Chat 工作階段

附註： 爲了使用 Privacy Manager Chat，雙方均須安裝 Privacy Manager 和 Privacy Manager 憑證。如需安裝 Privacy Manager 憑證的詳細資訊，請參閱 38 頁的申請並安裝 Privacy Manager 憑證。

1. 若要在 Windows Live Messenger 中啓動 Privacy Manager Chat，請執行下列程序之一：

   a. 以滑鼠右鍵按一下 Live Messenger 中的線上連絡人，然後選取「**啓動活動 (Start an Activity)**」。

   b. 按一下「**啓動聊天 (Start Chat)**」。

   - 或 -

   a. 連按兩下 Live Messenger 中的線上連絡人，然後選取「**查看活動清單 (See a list of activities)**」功能表。

   b. 按一下「**動作 (Action)**」，然後按一下「**啓動聊天 (Start Chat)**」。

   - 或 -

   a. 在通知區域中的「HP ProtectTools」圖示上按一下滑鼠右鍵，按一下「**HP ProtectTools Privacy Manager**」，然後選取「**啓動聊天 (Start Chat)**」。

   b. 在 Live Messenger 中，按一下「**動作：啓動活動 (Actions: Start an Activity)**」，然後選取「**Privacy Manager Chat**」。

   附註： 每位使用者都必須在 Live Messenger 中處於線上狀態，且使用者必須顯示在彼此的 Live Messenger 線上視窗中。按一下以選取一位線上使用者。

   Privacy Manager 會傳送邀請至連絡人，以啓動 Privacy Manager Chat。當受邀的連絡人接受後，Privacy Manager Chat 視窗就會開啓。如果受邀的連絡人沒有 Privacy Manager，就會出現提示要求他或她下載。

2. 按一下「**啓動 (Start)**」以開始安全聊天。

爲 Windows Live Messenger 設定 Privacy Manager

1. 在 Privacy Manager Chat 中，按一下「**設定**」按鈕。

   - 或 -

   在 Privacy Manager 中，按一下「**設定**」，然後按一下「**聊天**」標籤。

   - 或 -

   在 Privacy Manager Chat 歷程記錄檢視器中，按一下「**設定**」按鈕。

2. 若要指定「隱私權管理員交談 (Privacy Manager Chat)」在鎖定您的工作階段前等候的時間，請在「**無活動 _ 分鐘後鎖定工作階段 (Lock session after _ minutes of inactivity)**」方塊中選取一個數字。

3. 若要爲您的聊天工作階段指定歷程記錄資料夾，請按一下「**瀏覽**」以搜尋資料夾，然後按一下「**確定**」。

4. 若要在關閉前先自動加密並儲存您的工作階段，請選取「**自動儲存安全聊天歷程記錄**」核取方塊。

5. 按一下「**確定**」。

在 Privacy Manager Chat 視窗中聊天

在啓動 Privacy Manager Chat 後，Privacy Manager Chat 視窗會在 Windows Live Messenger 中開啓。使用 Privacy Manager Chat 與使用基本的 Windows Live Messenger 類似，只不過 Privacy Manager Chat 視窗中多了下列幾個其他功能可用：

- **儲存** — 按一下此按鈕可以將您的聊天工作階段儲存在組態設定中所指定的資料夾內。您也可以設定 Privacy Manager Chat 在關閉時自動儲存每個工作階段。
- **全部隱藏**和**全部顯示** — 按一下適當的按鈕可以展開或摺疊顯示於「安全通訊」視窗中的訊息。您也可以藉由按一下訊息標題來隱藏或顯示個別訊息。
- **在嗎？** — 按一下此按鈕可以要求連絡人驗證。
- **鎖定** — 按一下此按鈕可以關閉 Privacy Manager Chat 視窗並返回「聊天入口」視窗。若要再次顯示「安全通訊」視窗，請按一下「**繼續工作階段 (Resume the session)**，然後使用您選擇的安全登入法進行驗證。
- **傳送** — 按一下此按鈕可以傳送加密的訊息給您的連絡人。
- **簽署傳送** — 選取此核取方塊會以電子方式簽署並加密訊息。如果此訊息被竄改，則當收件者收到時，訊息將被標示爲無效。每次傳送簽署的訊息時都必須驗證。
- **隱藏傳送** — 選取此核取方塊會加密訊息，並以僅顯示訊息標題的方式傳送。您的連絡人必須驗證才能閱讀訊息內容。

檢視聊天歷程記錄

Privacy Manager Chat:Live Messenger 歷程記錄檢視器會顯示加密的 Privacy Manager Chat 工作階段檔。您可以在 Privacy Manager Chat 視窗中按一下「**儲存**」，或者在 Privacy Manager 中的「聊天」標籤上設定自動儲存，以儲存工作階段。在檢視器中，每個工作階段都會顯示（已加密）「連絡人螢幕名稱」，以及工作階段開始和結束的日期和時間。根據預設，工作階段會顯示在所有您已經設定的電子郵件帳戶上。您可以使用「**顯示下列所屬的歷程記錄**」功能表，只選取要檢視的特定帳戶。

檢視器可讓您執行下列工作：

- 51 頁的顯現所有工作階段
- 51 頁的爲特定帳戶顯現工作階段
- 52 頁的檢視工作階段 ID
- 52 頁的檢視工作階段
- 52 頁的搜尋工作階段的特定文字
- 52 頁的刪除工作階段
- 52 頁的新增或移除欄
- 53 頁的篩選顯示的工作階段

若要啓動 Live Messenger 歷程記錄檢視器：

▲ 以滑鼠右鍵按一下工作列最右側通知區域中的「**HP ProtectTools**」圖示，按一下「**Privacy Manager:for HP ProtectTools**」，然後按一下「**Live Messenger 歷程記錄檢視器**」。

– 或 –

▲ 在「聊天」工作階段，按一下「**歷程記錄檢視器**」或「**歷程記錄**」。

顯現所有工作階段

顯現所有工作階段會顯示目前所選取的工作階段，和相同帳戶中所有工作階段之已解密「連絡人螢幕名稱」。

若要顯現所有已儲存的聊天歷程記錄工作階段：

1. 在「Live Messenger 歷程記錄檢視器」中，以滑鼠右鍵按一下任何工作階段，然後選取「**顯現所有工作階段**」。
2. 使用您選擇的安全登入法進行驗證。

   「連絡人螢幕名稱」已經過解密。
3. 連按兩下任何工作階段，即可檢視其內容。

爲特定帳戶顯現工作階段

顯現工作階段會顯示目前所選取工作階段之已解密「連絡人螢幕名稱」。

若要顯現特定聊天歷程記錄工作階段：

1. 在「Live Messenger 歷程記錄檢視器」中，以滑鼠右鍵按一下任何工作階段，然後選取「**顯現工作階段**」。
2. 使用您選擇的安全登入法進行驗證。

   「連絡人螢幕名稱」已經過解密。
3. 連按兩下顯現的工作階段，即可檢視其內容。

附註： 其他使用相同憑證加密的工作階段會顯示未鎖定的圖示，表示您可以在任意工作階段上連按兩下，不需要其他驗證就能檢視它們。以不同憑證加密的工作階段會顯示鎖定的圖示，表示在檢視「連絡人螢幕名稱」或內容前，那些工作階段需要進一步的驗證。

檢視工作階段 ID

若要檢視工作階段 ID：

- 在「Live Messenger 歷程記錄檢視器」中，以滑鼠右鍵按一下任何顯現的工作階段，然後選取「**檢視工作階段 ID**」。

檢視工作階段

檢視工作階段會開啓檔案以供檢視。如果工作階段先前尚未顯現（顯示已解密「連絡人螢幕名稱」），則會同時顯現工作階段。

若要檢視 Live Messenger 歷程記錄工作階段：

1. 在「Live Messenger 歷程記錄檢視器」中，以滑鼠右鍵按一下任何工作階段，然後選取「**檢視**」。
2. 如果出現提示，請使用您選擇的安全登入法進行驗證。

   工作階段內容已經過解密。

搜尋工作階段的特定文字

您只能搜尋顯示在檢視器視窗中已顯現（已解密）工作階段中的文字。這些工作階段的「連絡人螢幕名稱」是以純文字顯示。

若要搜尋聊天歷程記錄工作階段中的文字：

1. 在「Live Messenger 歷程記錄檢視器」中，按一下「**搜尋**」按鈕。
2. 輸入搜尋文字，設定任何需要的搜尋參數，然後按一下「**確定**」。

   檢視器視窗中會反白顯示包含文字的工作階段。

刪除工作階段

1. 選取聊天歷程記錄工作階段。
2. 按一下「**刪除**」。

新增或移除欄

根據預設，最常使用的 3 個欄會顯示在「Live Messenger 歷程記錄檢視器」中。您可以新增其他欄到顯示畫面，也可以由顯示畫面移除欄。

若要新增欄到顯示畫面：

1. 在任何欄標題上按一下滑鼠右鍵，然後選取「**新增/移除欄 (Add/Remove Columns)**。
2. 在左側面板中選取欄標題，然後按一下「**新增 (Add)**」將它移至右側面板。

若要從顯示畫面移除欄：

1. 在任何欄標題上按一下滑鼠右鍵，然後選取「**新增/移除欄 (Add/Remove Columns)**。
2. 在右側面板中選取欄標題，然後按一下「**移除 (Remove)**」將它移至左側面板。

篩選顯示的工作階段

在「Live Messenger 歷程記錄檢視器」中顯示一份所有帳戶的工作階段清單。您也可以爲下列項目篩選顯示的工作階段：

- 特定帳戶。如需詳細資訊，請參閱 53 頁的顯示特定帳戶的工作階段。
- 日期範圍。如需詳細資訊，請參閱 53 頁的顯示某日期範圍的工作階段。
- 不同的資料夾。如需詳細資訊，請參閱 53 頁的顯示儲存在預設資料夾以外之資料夾中的工作階段。

顯示特定帳戶的工作階段

▲ 在「Live Messenger 歷程記錄檢視器」中，從「**顯示下列所屬的歷程記錄**」功能表選取帳戶。

顯示某日期範圍的工作階段

1. 在「Live Messenger 歷程記錄檢視器」中，按一下「**進階篩選**」圖示。

   「進階篩選」對話方塊隨即開啓。

2. 選取「**僅顯示指定日期範圍內的工作階段 (Display only sessions within specified date range)**」核取方塊。
3. 在「**開始日期 (From date)**」和「**結束日期 (To date)**」方塊中，輸入日、月和/或年，或者按一下行事曆旁邊的向下箭頭選取日期。
4. 按一下「**確定**」。

顯示儲存在預設資料夾以外之資料夾中的工作階段

1. 在「Live Messenger 歷程記錄檢視器」中，按一下「**進階篩選**」圖示。
2. 選取「**使用替代歷程記錄檔案資料夾 (Use an alternate history files folder)**」核取方塊。
3. 輸入資料夾位置，或者按一下「**瀏覽**」以搜尋資料夾。
4. 按一下「**確定**」。

進階工作

移轉 Privacy Manager 憑證和信任的連絡人至不同電腦

您可以安全地轉移 Privacy Manager 憑證和信任的連絡人至另一部電腦，或是將資料備份起來以安全保存該資料。若要這麼做，可將資料備份爲受密碼保護的檔案，並儲存到網路位置或任何抽取式儲存裝置，然後將檔案還原至新電腦。

備份 Privacy Manager 憑證和信任的連絡人

您可以遵循下列步驟，將 Privacy Manager 憑證和信任的連絡人備份至受密碼保護的檔案：

1. 開啓 Privacy Manager，並按一下「**轉移**」。
2. 按一下「**備份**」。
3. 在「選取資料」頁面上，選取要包含在轉移檔案中的資料類別，然後按「**下一步**」。
4. 在「轉移檔案」頁面上，輸入檔案名稱或按一下「**瀏覽**」以搜尋位置，然後按「**下一步**」。
5. 輸入並確認密碼，然後按「**下一步**」。

附註： 將此密碼儲存在安全處所，因爲當您還原轉移檔案時需要使用此檔案。

6. 使用您選擇的安全登入法進行驗證。
7. 在「已儲存轉移檔案」頁面上，按一下「**完成**」。

還原 Privacy Manager 憑證和信任的連絡人

您可以遵循下列步驟，將 Privacy Manager 憑證和信任的連絡人還原至不同電腦（當作還原程序的一部分），或還原至相同電腦：

1. 開啓 Privacy Manager，並按一下「**轉移**」。
2. 按一下「**還原**」。
3. 在「轉移檔案」頁面上，按一下「**瀏覽**」以搜尋檔案，然後按「**下一步**」。
4. 輸入建立備份檔案時所使用的密碼，然後按「**下一步**」。
5. 在「轉移檔案」頁面上，按一下「**完成**」。

Privacy Manager 的集中管理

Privacy Manager 安裝可以當成集中安裝的一部分，概由您的管理員自訂。下列之一項或多項功能可以啓用或停用：

- **憑證使用原則** – 限制您使用 Comodo 簽發的 Privacy Manager 憑證，或准許您使用其他憑證授權單位簽發的數位憑證。
- **加密原則** – 加密功能可以在 Microsoft Office 或 Outlook 以及在 Windows Live Messenger 中個別啓用或停用。

9 HP ProtectTools File Sanitizer

File Sanitizer 這項工具可供您安全拆解電腦上的資料資產（個人資訊或檔案、歷程或網路相關資料或其他資料元件），並且定期清空硬碟。

附註： 這個 File Sanitizer 版本僅支援系統硬碟。

拆解

拆解不同於標準 Windows® 刪除（亦即所謂的 File Sanitizer 簡單刪除），因爲當您使用 File Sanitizer 拆解資產時，會呼叫隱藏資料的演算法，以免他人取得原始資產。Windows 簡單刪除可在硬碟上保留完整的檔案（或資產），或者保留以討論之方法復原檔案（或資產）的狀態。

當您選擇拆解設定檔（「高安全性」、「中安全性」或「低安全性」）時，會自動選取用來進行拆解的預先定義資產清單和清除方法。您也可以自訂拆解設定檔，以指定拆解週期數、拆解哪些資產、拆解前需先確認的資產，以及不拆解哪些資產。如需詳細資訊，請參閱 59 頁的選取或建立拆解設定檔。

您可以設定自動拆解排程，也可以在任何時候手動拆解資產。如需詳細資訊，請參閱 58 頁的設定拆解排程、62 頁的手動拆解一項資產或 62 頁的手動拆解所有選取的項目。

附註： 只要是移到資源回收筒，即表示已從系統拆解並移除 .dll 檔。

可用空間清理

刪除 Windows 中的資產並非完全移除硬碟中的資產內容。Windows 僅刪除資產的參照內容。資產的內容仍保留在硬碟上，直到另一個資產以新資訊覆寫硬碟上的相同區域。

可用空間清理功能可供您安全地在刪除的資產上寫入任意資料，以避免使用者檢視刪除資產的原始內容。

附註： 可用空間清理功能適用於使用 Windows「資源回收筒」刪除或手動刪除的資產。可用空間清理功能並未提供受拆解資產額外的安全性。

您可以設定自動可用空間清理排程，或者使用工作列最右邊通知區中的「**HP ProtectTools**」圖示，啓動可用空間清理功能。如需詳細資訊，請參閱 58 頁的設定可用空間清理排程或 62 頁的手動啓用可用空間清理。

設定程序

開啓 File Sanitizer

若要開啓 File Sanitizer：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools Security Manager**」。
2. 按一下「**File Sanitizer**」。

－ 或 －

▲ 連按兩下桌面上的「**File Sanitizer**」圖示。

－ 或 －

▲ 在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，再按一下「**File Sanitizer**」，然後按一下「**開啓 File Sanitizer**」。

設定拆解排程

附註： 如需有關選取預先定義的拆解設定檔或建立拆解設定檔的詳細資訊，請參閱 59 頁的選取或建立拆解設定檔。

附註： 如需手動拆解資產的資訊，請參閱 62 頁的手動拆解一項資產。

1. 開啓 File Sanitizer，然後按一下「**拆解**」。
2. 選取拆解選項：
   - **Windows 關機** － 選擇這個選項，即可在 Windows 關機時拆解所有選定的資產。

     附註： 選取這個選項時，會在關機時顯示對話方塊，詢問您是否要繼續拆解所選定的資產，或者是否要略過該程序。按一下「**是**」以略過拆解程序，或者按一下「**否**」以繼續拆解。
   - **Web 瀏覽器開啓** － 選擇這個選項，即可在您開啓 Web 瀏覽器時拆解所有選定的 Web 相關資產，例如瀏覽器 URL 歷程記錄。
   - **Web 瀏覽器結束** － 選擇這個選項，即可在您關閉 Web 瀏覽器時拆解所有選定的 Web 相關資產，例如瀏覽器 URL 歷程記錄。
   - **按鍵順序** － 選擇這個選項，即可使用按鍵順序起始拆解。
   - **排程器** － 選取「**啓用排程器**」核取方塊，輸入您的 Windows 密碼，然後輸入要拆解選定之資產的日期和時間。

   附註： 只要是移到資源回收筒，即表示已從系統拆解並移除 .dll 檔。
3. 按一下「**套用**」，然後按一下「**確定**」。

設定可用空間清理排程

附註： 可用空間清理功能適用於使用 Windows「資源回收筒」刪除或手動刪除的資產。可用空間清理並未提供拆受拆解資產額外的安全性。

若要設定可用空間清理排程：

1. 開啓 File Sanitizer，然後按一下「**可用空間清理**」。
2. 選取「**啓動排程器**」核取方塊，輸入您的 Windows 密碼，然後輸入清理硬碟的日期和時間。
3. 按一下「**套用**」，然後按一下「**確定**」。

附註： 可用空間清理作業要耗費很長的時間。即使在背景中執行可用空間清理，您的電腦還是可能因爲處理器使用量增加而執行得慢一點。

選取或建立拆解設定檔

您可以藉由選取預先定義的設定檔或建立自己的設定檔的方式，指定清除方法及選取要拆解的資產。

選取預先定義的拆解設定檔

當您選擇預先定義的拆解設定檔（高安全性、中安全性或低安全性），便會自動選取預先定義的清除方法和資產清單。您可以按一下「**檢視詳細資料**」按鈕，以檢視所選取要進行拆解的預先定義資產清單。

若要選取預先定義的拆解設定檔：

1. 開啓 File Sanitizer，然後按一下「**設定**」。
2. 按一下預先定義的拆解設定檔。
3. 按一下「**檢視詳細資料**」以檢視所選取要拆解的資產清單。
4. 在「**拆解下列項目**」下方，選取您要在拆解前確認的各項資產旁邊的核取方塊。
5. 按一下「**套用**」，然後按一下「**確定**」。

自訂拆解設定檔

在建立拆解設定檔時，您可以指定拆解週期的數目，哪些資產需要拆解，哪些資產拆解前需要先確認，以及哪些資產要排除拆解：

1. 開啓 File Sanitizer，按一下「**設定**」，按一下「**進階安全性設定**」，然後按一下「**檢視詳細資料**」。
2. 指定拆解週期的數目。

附註： 每一項資產的拆解動作都會以選定的拆解週期數來執行。例如，若您選擇 3 個拆解週期，隱藏資料的演算法就會分別執行 3 次。若您選擇較高的安全性拆解週期，拆解動作就會花費相當長的時間。不過，指定的拆解週期數越高，擷取資料的可能性越低。

3. 選取您要拆解的資產：
   a. 在「**可用的拆解選項**」下方，按一下該資產，然後按一下「**新增**」。
   b. 若要新增自訂資產，請按一下「**新增自訂選項**」，然後瀏覽或輸入檔案名稱或資料夾的路徑。按一下「**開啓**」，然後按一下「**確定**」。在「**可用的拆解選項**」下，按一下自訂資產，然後按一下「**新增**」。

附註： 若要從可用的拆解選項中移除資產，請按一下該資產，然後按一下「**刪除**」。

4. 在「**拆解下列項目**」下方，選取您要在拆解前確認的各項資產旁邊的核取方塊。

附註： 若要從拆解清單中移除資產，請按一下該資產，然後按一下「**移除**」。

5. 若要保護檔案或資料夾免於自動拆解，請在「**請勿拆解下列項目**」下，按一下「**新增**」，然後瀏覽或輸入檔案名稱或資料夾的路徑。按一下「**開啓**」，然後按一下「**確定**」。

附註： 若要從排除清單中移除資產，請按一下該資產，然後按一下「**刪除**」。

6. 當您完成設定拆解設定檔後，按一下「**套用**」，然後按一下「**確定**」。

自訂單純刪除設定檔

簡單的刪除設定檔會執行標準資產刪除，而不進行拆解動作。當您自訂簡單刪除設定檔時，可指定簡單刪除要包含哪些資產、執行簡單刪除之前要先確認哪些資產，以及哪些資產要排除於簡單刪除之外。

附註： 如果您使用「單純刪除」選項，可針對手動刪除的資產偶爾執行「可用空間清理」功能，或可使用 Windows「資源回收筒」執行該功能。

若要自訂簡單刪除設定檔：

1. 開啓 File Sanitizer，按一下「**設定**」，按一下「**單純刪除設定**」，然後按一下「**檢視詳細資料**」。
2. 選取您要刪除的資產：
   a. 在「**可用的刪除選項**」下方，按一下該資產，然後按一下「**新增**」。
   b. 若要新增自訂資產，請按一下「**新增自訂選項**」，輸入檔案名稱或資料夾名稱，然後按一下「**確定**」。按一下自訂資產，然後按一下「**新增**」。

附註： 若要從可用刪除選項中刪除資產，請按一下該資產，然後按一下「**刪除**」。

3. 在「**刪除下列項目**」下方，選取在您要在刪除前確認的各項資產旁邊的核取方塊。

附註： 若要從可用刪除清單中移除資產，請按一下該資產，然後按一下「**移除**」。

4. 在「**請勿刪除下列項目**」下方，按一下「**新增**」以選取您要排除在拆解之外的特定資產。

附註： 若要從排除清單中移除資產，請按一下該資產，然後按一下「**刪除**」。

5. 當您完成設定單純刪除設定檔，請按一下「**套用**」，然後按一下「**確定**」。

一般工作

您可以使用 File Sanitizer 執行下列工作：

- 使用按鍵順序啓動拆解 — 此功能可以讓您建立按鍵順序（例如，ctrl+alt+s）以啓動拆解。如需詳細資訊，請參閱 61 頁的使用按鍵順序啓動拆解。
- 使用 File Sanitizer 圖示啓動拆解 — 此功能類似於 Windows 中的拖放功能。如需詳細資訊，請參閱 61 頁的使用 File Sanitizer 圖示。
- 手動拆解特定資產或所有選取資產 — 此功能可以讓您手動拆解項目，無需等待定期的拆解排程啓動。如需詳細資訊，請參閱 62 頁的手動拆解一項資產或62 頁的手動拆解所有選取的項目。
- 手動啓用可用空間清理 — 此功能可以讓您手動啓用可用空間清理。如需詳細資訊，請參閱 62 頁的手動啓用可用空間清理。
- 中止拆解或可用空間清理作業 — 此功能可以讓您停止拆解或可用空間清理作業。如需詳細資訊，請參閱 63 頁的中止拆解或可用空間清理作業。
- 檢視記錄檔 — 此功能可以讓您檢視拆解和可用空間清理的記錄檔，包含上次拆解或可用空間清理作業的任何錯誤或失敗。如需詳細資訊，請參閱 63 頁的檢視記錄檔。

附註： 拆解或可用空間清理作業要耗費很長的時間。即使在背景中執行拆解和可用空間清理，您的電腦還是可能因爲處理器使用量增加而執行得慢一點。

使用按鍵順序啓動拆解

若要要指定按鍵順序，請依照下列步驟執行：

1. 開啓 File Sanitizer，按一下「**拆解**」。
2. 選取「**按鍵順序**」核取方塊。
3. 在可用的方塊中輸入字元。
4. 選取「**CTRL**」方塊或「**ALT**」方塊，然後選取「**SHIFT**」方塊。

   例如，若要使用 s 鍵和 ctrl+shift 鍵起始自動拆解，請在方塊中輸入 s，然後選取「**CTRL**」和「**SHIFT**」選項。

   附註： 請確定選取的按鍵順序不同於您已經設定的其他按鍵順序。

若要使用按鍵順序啓動拆解：

1. 按下您選擇的字元的同時，請按住 shift 鍵和 ctrl 或 alt 鍵（或任何您指定的組合）。
2. 如果開啓確認對話方塊，請按一下「**是**」。

使用 File Sanitizer 圖示

注意： 拆解過的資產無法復原。選取哪些項目要進行手動拆解之前請仔細考慮。

1. 瀏覽至您要拆解的文件或資料夾。
2. 將資產拖曳至桌面上的 File Sanitizer 圖示。
3. 當開啓確認對話方塊時，按一下「**是**」。

手動拆解一項資產

△ **注意：** 拆解過的資產無法復原。選取哪些項目要進行手動拆解前請仔細考慮。

1. 在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，再按一下「**File Sanitizer**」，然後按一下「**拆解一項**」。
2. 當開啓「瀏覽」對話方塊，請瀏覽至您要拆解的資產，然後按一下「**確定**」。

附註： 您選取的資產可以是單一檔案或資料夾。

3. 當開啓確認對話方塊時，按一下「**是**」。

－ 或 －

1. 在桌面的「**File Sanitizer**」圖示上按一下右鍵，然後按一下「**拆解一項**」。
2. 當開啓「瀏覽」對話方塊，請瀏覽至您要拆解的資產，然後按一下「**確定**」。
3. 當開啓確認對話方塊時，按一下「**是**」。

－ 或 －

1. 開啓 File Sanitizer，按一下「**拆解**」。
2. 按一下「**瀏覽**」按鈕。
3. 當開啓「瀏覽」對話方塊，請瀏覽至您想拆解的資產，然後按一下「**確定**」。
4. 當開啓確認對話方塊時，按一下「**是**」。

手動拆解所有選取的項目

1. 在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，按一下「**File Sanitizer**」，然後按一下「**立即拆解**」。
2. 當開啓確認對話方塊時，按一下「**是**」。

－ 或 －

1. 在桌面的「**File Sanitizer**」圖示上按一下滑鼠右鍵，然後按一下「**立即拆解**」。
2. 當開啓確認對話方塊時，按一下「**是**」。

－ 或 －

1. 開啓 File Sanitizer，按一下「**拆解**」。
2. 按一下「**立即拆解**」按鈕。
3. 當開啓確認對話方塊時，按一下「**是**」。

手動啓用可用空間清理

1. 在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，按一下「**File Sanitizer**」，然後按一下「**立即清理**」。
2. 當開啓確認對話方塊時，按一下「**是**」。

– 或 –

1. 開啓 File Sanitizer，按一下「**可用空間清理**」。
2. 按一下「**立即清理**」。
3. 當開啓確認對話方塊時，按一下「**是**」。

中止拆解或可用空間清理作業

當拆解或可用空間清理作業在進行時，HP ProtectTools Security Manager 圖示上方的通知區中會顯示一項訊息。此訊息提供有關拆解或可用空間清理過程（完成百分比）的詳細資料，並提供中止作業的選項。

若要中止作業：

▲ 按一下訊息，然後按一下「**停止**」以取消作業。

檢視記錄檔

每次執行拆解或可用空間清理作業時，就會產生記錄任何錯誤或失敗的記錄檔。記錄檔會根據最新的拆解或可用空間清理作業不斷地更新。

附註： 成功拆解或清理的檔案不會出現在記錄檔中。

拆解作業會建立一個記錄檔，而可用空間清理作業則會建立另一個記錄檔。這兩個記錄檔都存放在硬碟上：

- C:\Program Files\Hewlett-Packard\File Sanitizer**[Username]**_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer**[Username]**_DiskBleachLog.txt

10 HP ProtectTools Device Access Manager（僅限特定機型）

Windows® 作業系統管理員使用 HP ProtectTools Device Access Manager 來控制存取系統上的裝置，並防止未經授權存取：

- 它爲每位使用者建立裝置設定檔，以定義允許或拒絕使用者存取的裝置。
- 使用者還會被分組，例如預先定義的「裝置管理員」群組，或者可以使用「控制台」的「管理工具」區段中的「電腦管理」選項定義的群組。
- 可以依據群組成員資格來授與或拒絕裝置存取。
- 針對裝置類別（例如 CD-ROM 光碟機和 DVD 光碟機），可以分別允許或拒絕讀取和寫入存取。

另外，也可將讀取及修改裝置存取控制原則的權限授予有限的使用者。

設定程序

開啓 Device Access Manager

若要開啓 Device Access Manager，請依照下列步驟進行：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」以及「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Device Access Manager**」。

設定裝置存取

HP ProtectTools Device Access Manager 提供三種檢視：

- 「簡易組態」檢視可用來允許或拒絕「裝置管理員」群組成員存取的裝置類別。
- 「裝置類別組態」檢視可用來授與或拒絕存取裝置類型，或授與或拒絕特定使用者或群組存取特定裝置。
- 「使用者存取設定」檢視可用來指定哪些使用者可以檢視或修改「簡易組態」和「裝置類別組態」的資訊。

裝置管理員群組

安裝 Device Access Manager 時，會建立「裝置管理員」群組。

系統管理員可以透過拒絕存取一組裝置類別來實作簡易的裝置存取控制原則，除非使用者被歸類爲信任的（在裝置存取方面）。區別「裝置信任的」使用者和「非裝置信任的」使用者的建議方法是讓所有「裝置信任的」使用者成爲「裝置管理員」群組的成員。授與「裝置管理員」群組成員透過「簡易組態」或「裝置類別組態」檢視存取裝置的權限，如此可以確保「裝置信任的」使用者可以完整存取指定組的裝置類別。

附註： 新增使用者到「裝置管理員」群組並不會自動允許該使用者存取裝置。但是，「簡易組態」檢視可以用來授與「裝置信任的」使用者存取所需的裝置類別組的權限。

若要新增使用者到「裝置管理員」群組，請依照下列步驟進行：

- 針對 Windows 7、Vista 或 XP Professional 版本，請使用標準的「本機使用者和群組」 MMC 嵌入式管理單元。
- 針對 Windows 7、Vista® 或 XP Home 版本，請透過授權的帳戶在命令提示字元視窗中輸入下列命令：

  c:\> net localgroup “Device Administrators” username /ADD

簡易組態

管理員和授權的使用者可以使用「簡易組態」檢視來修改所有「非裝置管理員」對下列裝置類別的存取：

附註： 若要使用此檢視來讀取裝置存取資訊，使用者或群組必須在「**使用者存取設定**」檢視中被授與「讀取」存取。若要使用此檢視來修改裝置存取資訊，使用者或群組必須在「**使用者存取設定**」檢視中被授與「變更」存取。

- 所有抽取式媒體（磁碟、USB 快閃磁碟機等。）
- 所有 DVD/CD-ROM 光碟機

- 所有序列埠和並列埠
- 所有 Bluetooth® 裝置
- 所有紅外線裝置
- 所有數據機裝置
- 所有 PCMCIA 裝置
- 所有 1394 裝置

若要允許或拒絕所有「非裝置管理員」對某種裝置類別的存取，請依照以下步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**簡易組態**」。
2. 在右側窗格中，若要拒絕存取，選取裝置類別或特定裝置的核取方塊。清除核取方塊以允許存取該裝置類別或特定裝置。

   如果核取方塊變爲灰色，表示影響存取狀況的值已在「裝置類別組態」檢視中被變更。若要將值重設回簡易設定，請按一下核取方塊以清除或設定，然後按一下「**是**」確認。
3. 按一下「**儲存**」圖示。

   附註： 如果背景服務未執行，會開啓一個對話方塊詢問您是否要啓動它。按一下「**是**」。
4. 按一下「**確定**」。

啓動背景服務

裝置設定檔套用前，HP ProtectTools Security Manager 會開啓一個對話方塊，詢問您是否要啓動 HP ProtectTools 裝置鎖定/稽核背景服務。按一下「**是**」。背景服務會啓動，而且此後在系統開機時會自動啓動。

附註： 背景服務提示顯示前必須先定義裝置設定檔。

管理員也可以啓動或停止此服務：

1. 按一下「**開始**」，然後按一下「**控制台**」。
2. 按一下「**管理工具**」，然後按一下「**服務**」。
3. 搜尋「**HP ProtectTools 裝置鎖定/稽核**」服務。

停止裝置鎖定/稽核服務並不會停止裝置鎖定。有兩個元件執行裝置鎖定：

- 裝置鎖定/稽核服務
- DAMDrv.sys 驅動程式

啓動服務會啓動裝置驅動程式，但停止服務不會停止驅動程式。

若要判斷背景服務是否正在執行，請開啓一個命令提示字元視窗，然後輸入 sc query flcdlock。

若要判斷裝置驅動程式是否正在執行，請開啓一個命令提示字元視窗，然後輸入 sc query damdrv。

裝置類別組態

管理員和授權的使用者可以檢視並修改允許或拒絕裝置類別或特定裝置存取權限的使用者和群組清單。

附註： 若要使用此檢視來讀取裝置存取資訊，使用者或群組必須在「**使用者存取設定**」檢視中被授與「讀取」存取。若要使用此檢視來修改裝置存取資訊，使用者或群組必須在「**使用者存取設定**」檢視中被授與「變更」存取。

「裝置類別組態」檢視有下列區段：

- **裝置清單** — 顯示安裝在系統或先前可能安裝在系統中的所有裝置類別和裝置。
  - 保護通常套用於裝置類別。選取的使用者或群組將能夠存取此裝置類別中的任何裝置。
  - 保護也可以套用於特定裝置。
- **使用者清單** — 顯示所有允許或拒絕存取選取之裝置類別或特定裝置的使用者和群組。
  - 「使用者清單」項目可以針對特定使用者或該使用者所屬的群組建立。
  - 如果「使用者清單」中的使用者或群組項目無法使用，表示設定是由「裝置清單」中的裝置類別或從「類別」資料夾繼承的。
  - 某些裝置類別（例如 DVD 和 CD-ROM），可以藉由分別允許或拒絕讀取和寫入作業的存取而進一步加以控制。

    有關其他裝置和類別，可以繼承讀取和寫入存取權限。例如，「讀取」存取可以從較高的類別繼承，但「寫入」存取可以針對使用者或群組而特別拒絕。

    附註： 如果「讀取」核取方塊空白，那麼存取控制項目不影響裝置的讀取存取。它不會授與也不會拒絕裝置的讀取存取。

    範例 1 — 如果拒絕使用者或群組對裝置或裝置類別的寫入存取：

    可僅針對在裝置階層中此裝置下的一個裝置，授與該使用者、該群組或該群組某成員的寫入存取或讀取 + 寫入存取。

    範例 2 — 如果允許使用者或群組對裝置或裝置類別的寫入存取：

    可僅針對該裝置，或在裝置階層中此裝置下的一個裝置，拒絕該使用者、該群組或該群組某成員的寫入存取或讀取 + 寫入存取。

    範例 3 — 如果允許使用者或群組對裝置或裝置類別的讀取存取：

    可僅針對該裝置，或在裝置階層中此裝置下的一個裝置，拒絕該使用者、該群組或該群組某成員的讀取存取或讀取 + 寫入存取。

    範例 4 — 如果拒絕使用者或群組對裝置或裝置類別的讀取存取：

    可僅針對在裝置階層中此裝置下的一個裝置，授與該使用者、該群組或該群組某成員的讀取存取或讀取 + 寫入存取。

    範例 5 — 如果允許使用者或群組對裝置或裝置類別的讀取 + 寫入存取：

    可僅針對該裝置，或在裝置階層中此裝置下的一個裝置，拒絕該使用者、該群組或該群組某成員的寫入存取或讀取 + 寫入存取。

    範例 6 — 如果拒絕使用者或群組對裝置或裝置類別的讀取 + 寫入存取：

    可僅針對在裝置階層中此裝置下的一個裝置，授與該使用者、該群組或該群組某成員的讀取存取或讀取 + 寫入存取。

拒絕使用者或群組的存取

若要防止使用者或群組存取某個裝置或裝置類別，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 在裝置清單中，按一下您要設定的裝置類別。
   - 裝置類別
   - 所有裝置
   - 個別裝置
3. 在「**使用者/群組**」下，按一下要拒絕存取的使用者或群組。
4. 按一下使用者或群組旁邊的「**拒絕**」。
5. 按一下「**儲存**」圖示。

附註： 當針對使用者在相同的裝置層級中同時設定拒絕和允許設定時，拒絕存取會優先於允許存取。

允許使用者或群組的存取

若要授與使用者或群組存取某個裝置或裝置類別的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 在裝置清單中，按一下下列其中一項：
   - 裝置類別
   - 所有裝置
   - 個別裝置
3. 按一下「**新增**」。

   「**選取使用者或群組**」對話方塊隨即開啓。
4. 按一下「**進階**」，然後按一下「**立即尋找**」以搜尋要新增的使用者或群組。
5. 按一下要新增到可用使用者或群組清單中的使用者或群組，然後按一下「**確定**」。
6. 再按一下「**確定**」。
7. 按一下「**允許**」，授與此使用者或群組存取權。
8. 按一下「**儲存**」圖示。

移除使用者或群組的存取

若要移除使用者或群組存取某個裝置或裝置類別的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 在裝置清單中，按一下您要設定的裝置類別。
   - 裝置類別
   - 所有裝置
   - 個別裝置
3. 在「**使用者/群組**」下，按一下要移除的使用者或群組，然後按一下「**移除**」。
4. 按一下「**儲存**」圖示。

允許群組中的一位使用者存取裝置類別

若要允許一位使用者存取裝置類別，但拒絕該使用者群組的所有其他成員進行存取，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 在裝置清單中，按一下您要設定的裝置類別。
   - 裝置類別
   - 所有裝置
   - 個別裝置
3. 在「**使用者/群組**」下，選取要拒絕存取的群組，然後按一下「**拒絕**」。
4. 瀏覽到所需類別下方的資料夾，然後新增特定的使用者。
5. 按一下「**允許**」，將存取權授與此使用者。
6. 按一下「**儲存**」圖示。

允許群組中的一位使用者存取特定裝置

管理員可以授與一個使用者存取特定的裝置，但拒絕該使用者群組的所有其他成員存取該類別中的所有裝置：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 在裝置清單中，按一下您要設定的裝置類別，然後瀏覽到其下方的資料夾。
3. 按一下「**新增**」。「**選取使用者或群組**」對話方塊隨即開啓。
4. 按一下「**進階**」，然後按一下「**立即尋找**」以搜尋要拒絕存取該類別中所有裝置的使用者群組。
5. 按一下該群組，然後按一下「**確定**」。
6. 瀏覽到要允許使用者存取之裝置類別下的特定裝置。

7. 按一下「**新增**」。「**選取使用者或群組**」對話方塊隨即開啓。
8. 按一下「**進階**」，然後按一下「**立即尋找**」以搜尋要新增的使用者或群組。
9. 按一下要允許存取的使用者，然後按一下「**確定**」。
10. 按一下「**允許**」，將存取權授與此使用者。
11. 按一下「**儲存**」圖示。

重設組態

△ **注意：** 重設組態會捨棄所有已經進行的裝置組態變更，並將所有設定返回到出廠時的設定值。

若要將組態設定重設爲出廠預設值，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
2. 按一下「**重設**」按鈕。
3. 按一下「**是**」確認。
4. 按一下「**儲存**」圖示。

進階工作

控制組態設定的存取

在「**使用者存取設定**」檢視中，管理員指定允許使用「簡易組態」和「裝置類別組態」頁面的群組或使用者。

附註： 使用者或群組必須有「完整使用者管理員權限」才能修改「使用者存取設定」檢視中的設定。

- 使用者或群組必須在「使用者存取設定」檢視中被授與「檢視（唯讀）組態設定」存取，才能檢視「簡易組態」和「裝置類別組態」的資訊。
- 使用者或群組必須在「使用者存取設定」檢視中被授與「變更組態設定」存取，才能變更「簡易組態」和「裝置類別組態」的資訊。

附註： 即使是「管理員」群組的成員也必須被授與「讀取」存取，才能檢視「簡易組態」和「裝置類別組態」檢視，被授與「變更」存取才能使用「簡易組態」和「裝置類別組態」檢視變更資料。

附註： 評估完所有使用者和群組的存取層級後，如果在特定存取層級中沒有爲使用者選取「允許」或「拒絕」，則使用者在該層級的存取爲拒絕。

授與現有的群組或使用者存取權

若要授與現有的群組或使用者檢視或變更組態設定的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
2. 按一下要允許存取的使用者或群組。
3. 在「**權限**」下，針對每種要授與選取之群組或使用者的權限類型按一下「**允許**」：

   附註： 授與的權限是累計式的。例如，被授與「變更組態設定」的使用者會自動被授與「檢視（唯讀）組態設定」權限。被授與「完整使用者管理員權限」的使用者也會被授與「變更組態設定」和「檢視（唯讀）組態設定」權限。

   - 完整使用者管理員權限
   - 變更組態設定
   - 檢視（唯讀）組態設定
4. 按一下「**儲存**」圖示。

拒絕現有的群組或使用者存取權

若要拒絕現有的群組或使用者檢視或變更組態設定的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
2. 按一下要拒絕存取的使用者或群組。

3. 在「**權限**」下，針對每種要拒絕選取之群組或使用者的權限類型按一下「**拒絕**」：
   - 完整使用者管理員權限
   - 變更組態設定
   - 檢視（唯讀）組態設定
4. 按一下「**儲存**」圖示。

新增群組或使用者

若要授與新的群組或使用者檢視或變更組態設定的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
2. 按一下「**新增**」。「**選取使用者或群組**」對話方塊隨即開啓。
3. 按一下「**進階**」，然後按一下「**立即尋找**」以搜尋要新增的使用者或群組。
4. 按一下群組或使用者，按一下「**確定**」，然後再按一下「**確定**」。
5. 按一下「**允許**」，將存取權授與此使用者。
6. 按一下「**儲存**」圖示。

移除群組或使用者存取

若要移除群組或使用者檢視或變更組態設定的權限，請依照下列步驟進行：

1. 在「**HP ProtectTools 管理主控台**」的左側窗格中，按一下「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
2. 按一下群組或使用者，然後按一下「**移除**」。
3. 按一下「**儲存**」圖示。

相關說明文件

HP ProtectTools Device Access Manager 與企業版產品 HP ProtectTools Enterprise Device Access Manager 相容。搭配企業版產品運作時，HP ProtectTools Device Access Manager 允許以唯讀方式存取本身的功能。

更多有關 HP ProtectTools Device Access Manager 的資訊可在網站上取得，網址是 http://www.hp.com/hps/security/products。

11 HP ProtectTools LoJack Pro

Absolute Software 公司推出的 Computrace LoJack Pro（需另外購買），著重在解決愈來愈多電腦遺失或被盜的問題。

啓用此軟體能夠啓用 Computrace 代理程式，它會在您的電腦中保持作用，即使硬碟被重新格式化或被替換亦然。

LoJack Pro 允許遠端監控、管理和追蹤電腦。如果電腦遺失或被盜，Absolute 公司的「復原團隊」會協助您復原。*

附註： *此功能因地理位置而有所不同。如需其他詳細資訊，請參閱 Absolute Software 的訂購合約。

12 疑難排解

HP ProtectTools Security Manager

簡短說明	細節	解決方式
安裝 Security Manager 之後才安裝的智慧卡和 USB 權杖，無法在 Security Manager 中使用。	若要在 Secuirty Manager 中使用智慧卡和 USB 權杖，支援軟體（驅動程式、PKCS#11 提供者等）必須在安裝 Security Manager 之前安裝完成。 如果您已經安裝 Security Manager，請在安裝智慧卡或權杖支援軟體後進行下列步驟：	登入 Password Manager。 在 HP ProtectTools Security Manager 中，依序按一下「**Password Manager**」、「**認證**」以及「**智慧卡**」。 如果出現提示，請重新啓動電腦。
某些應用程式網頁會產生錯誤，導致使用者無法執行或完成工作。	某些網頁應用程式會因爲「單一登入」的停用功能模式而停止運作並報告錯誤。例如，如果 Internet Explorer 中出現含有 **!** 符號的黃色三角形，代表出現錯誤。	Security Manager 單一登入並不支援所有軟體 Web 介面。透過關閉「單一登入」支援來停用特定網頁的「單一登入」支援。請參閱「單一登入」的完整說明文件，它可在 Security Manager 的軟體說明檔中取得。 如果您無法針對指定應用程式停用特定的「單一登入」功能，請聯絡 HP 技術支援部門，並透過 HP 客服中心聯絡人要求提供第三級支援。
登入期間您無法看到「**瀏覽虛擬 Token (Browse for Virtual Token)**」選項。	使用者無法在 Password Manager 中移動註冊之虛擬權杖的位置，因爲瀏覽的選項已被移除以減少安全性的風險。	將瀏覽選項移除的原因爲：它能讓非使用者刪除並重新命名檔案，進而掌控整個 Windows 系統。
網域系統管理員即使擁有授權，仍無法變更 Windows 密碼。	這會發生在網域管理員使用在網域和本機電腦具「管理員」權限的帳戶登入網域並使用 Password Manager 註冊網域身份後。當網域管理員嘗試從 Password Manager 變更 Windows 密碼時，管理員會得到登入失敗的錯誤：**使用者帳戶限制**。	Password Manager 無法透過「**變更 Windows 密碼**」來變更網域使用者的帳戶密碼。Security Manager 只能變更本機電腦帳戶的密碼。網域使用者可以透過「**Windows 安全性**」的「**變更密碼**」選項來變更其密碼，但由於網域使用者在本機電腦沒有實體帳戶，因此 Password Manager 只能變更用來登入的密碼。
Password Manager 與 Corel WordPerfect 12 密碼 GINA 之間有不相容的問題。	如果使用者登入 Password Manager，以 WordPerfect 建立一個文件，然後以密碼保護儲存，則 Password Manager 無法手動或自動偵測或識別密碼 GINA。	HP 正在尋找做爲未來產品增強的方法。
Password Manager 無法識別螢幕上的「**連線**」按鈕。	如果遠端桌面連線 (RDP) 的「單一登入」認證設爲「**連線**」，在重新啓動單一登入時，則一律進入「**另存爲**」模式，而不是「**連線**」模式。	HP 正在尋找做爲未來產品增強的方法。
從睡眠模式轉換到休眠模式後，使用者無法登入 Password Manager（只會發生在 Windows XP Service Pack 1）。	在允許系統轉換至休眠和睡眠模式之後，「管理員」或使用者無法登入 Password Manager，且不管選取何種登入認證（密碼、指紋或 Java Card），都只會顯示 Windows 登入畫面。	透過 Windows Update 將 Windows 更新爲 Service Pack 2。如需造成原因的詳細資訊，請參閱 Microsoft 知識庫第 813301 號文章，網址爲：http://www.microsoft.com。

簡短說明	細節	解決方式
		登入時，使用者必須選取 Password Manager 並且登入。在登入 Password Manager 後，使用者會收到登入 Windows 的提示（使用者可能需要選取 Windows 登入選項）以完成登入程序。 如果使用者先登入 Windows，就必須手動登入 Password Manager。
安全性功能的「**還原身份識別 (Restore Identity)**」程序會失去與虛擬 Token 的關聯性。	當使用者還原身份時，Password Manager 可能會在登入畫面失去與虛擬權杖位置的關聯。即使 Password Manager 已經註冊虛擬權杖，使用者還是需要重新註冊權杖，以還原關聯。	目前這是依照設計而發生的結果。 如果解除安裝 Security Manager 時沒有保存身份，權杖的系統（伺服器）部分就會被損毀，因此無法繼續使用權杖進行登入，即使權杖的用戶端部分已經透過身份還原也不行。 HP 正在調查解決方法的長期選項。

HP ProtectTools Device Access Manager

已拒絕使用者存取 Device Access Manager 中的裝置，但是裝置仍可供存取。

- **說明** — Device Access Manager 的「簡易組態」及/或「裝置類別組態」都可用來拒絕使用者存取裝置。雖然已拒絕存取，使用者仍然能夠存取裝置。
- **解決方法：**
  - 確認「HP ProtectTools 裝置鎖定/稽核」服務已啓動。
  - 以管理使用者的身分按一下「**控制台**」，然後按一下「**系統及維護**」。在「系統管理工具」視窗中，按一下「**服務**」，然後找出「**HP ProtectTools 裝置鎖定/稽核**」服務。確認服務已啓動，而且啓動類型是「**自動**」

使用者取得非預期的裝置存取權，或者使用者未能取得預期的裝置存取權。

- **說明** — Device Access Manager 已用於拒絕使用者存取某些裝置或允許使用者存取其他裝置。使用者使用系統時，可存取他們認爲 Device Access Manager 已拒絕存取的裝置，並且無法存取他們認爲 Device Access Manager 應該允許存取的裝置。
- **解決方法：**
  - 使用 Device Access Manager 的「裝置類別組態」可深入瞭解使用者的裝置設定。
  - 按一下「**Security Manager**」，並且按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。展開裝置類別樹狀結構的層級，然後檢視此使用者相關的設定。針對使用者或針對使用者及管理員等可能屬於其中成員的任何 Windows 群組，檢查可能已經設定的任何「拒絕」權限。

允許或拒絕 — 哪一個優先？

- **說明** — 在「裝置類別組態」中，已設定下列組態：
  - 在裝置類別階層的同一個層級（例如 DVD/CD-ROM 光碟機），已將允許權限授予 Windows 群組（例如 BUILTIN\Administrators），並且已將拒絕權限授予另一個 Windows 群組（例如 BUILTIN\Users）。
  - 如果使用者是這兩個群組的成員（例如管理員），哪一個的優先順序最高？
- **解決方法：**
  - 使用者會無法存取裝置。拒絕的優先順序高於允許。
  - 這是由於 Windows 處理裝置有效權限的方式才導致拒絕存取的情形。如果拒絕某個群組且允許某個群組，而使用者是這兩個群組的成員，則會拒絕使用者，這是因爲拒絕存取的優先順序高於允許存取。
  - 其中一個暫時解決的方法是在 DVD/CD-ROM 光碟機層級拒絕使用者群組，而在 DVD/CD-ROM 光碟機之下的層級允許管理員群組。
  - 另一個暫時解決的方法是建立特定的 Windows 群組，一個用來允取存取 DVD/CD，而另一個則用來拒絕存取 DVD/CD，然後將特定的使用者新增至適當的群組中。

已經使用「簡易組態」檢視定義裝置存取控制原則，但是管理使用者無法存取裝置。

- **說明** —「簡易組態」會拒絕使用者及來賓的存取，但是允許裝置管理員。
- **解決方法：** 將管理使用者新增至「裝置管理員」群組。

其他事項

受影響的軟體 – 簡短說明	細節	解決方式
安全管理員 (Security Manager) — 收到警告：「**安全性應用程式必須等到 HP Protect Tools 的安全管理員已經安裝完畢，才能開始安裝 (The security application can not be installed until the HP Protect Tools Security Manager is installed)**」。	所有安全性應用程式（例如 Java Card Security 和生物測定）都是 Security Manager 介面的可延伸外掛程式。必須先安裝 Security Manager，才能載入 HP 核准的安全性外掛程式。	安全管理員 (Security Manager) 軟體必須先安裝完畢，才能安裝任何的安全性外掛程式。
HP ProtectTools Security Manager – 關閉 Security Manager 介面時會間歇傳回錯誤。	在所有插件應用程式完成載入前使用螢幕右上方的關閉按鈕，會產生間歇性（1/12 的機會）的錯誤。	這與在關閉並重新啓動 Security Manager 時的插件服務載入時間計時依存性相關。由於 PTHOST.exe 是儲藏其他應用程式（插件）的殼層，因此會依賴插件完成其載入時間（服務）的能力。在插件有足夠時間完成載入前關閉殼層是根本原因。 允許安全管理員 (Security Manager) 完成服務載入訊息（可在安全管理員 (Security Manager) 視窗上方看到），並在左側欄位中列示所有的外掛程式。爲了預防錯誤發生，請給予充足的時間，讓這些外掛程式全部載入。
HP ProtectTools — 未限制的存取或未控制的系統管理員權限造成安全上的風險。	許多風險都是因爲未限制用戶端電腦的存取行爲而導致，包括下列幾項： • 刪除 PSD • 惡意修改使用者設定 • 停用安全性政策與功能	建議管理員依照限制終端使用者權限和限制使用者存取的「最佳實務」進行。 未獲授權的使用者不應授與管理權限。

辭彙

ATM Automatic Technology Manager，允許網路管理員以 BIOS 層級遠端管理系統。

Drive Encryption 透過將硬碟加密，讓未經適當授權的人無法讀取資訊來保護資料。

Drive Encryption 登入畫面 在 Windows 啓動之前所顯示的登入畫面。使用者必須輸入其 Windows 使用者名稱和密碼或 Java 卡 PIN 碼。在大部分的情況下，在 Drive Encryption 登入畫面輸入正確資訊後即可直接存取 Windows，而不需要在 Windows 登入畫面再次登入。

DriveLock 爲安全性功能，會將硬碟連結到使用者，當電腦啓動時，會要求使用者正確輸入 DriveLock 密碼。

HP SpareKey Drive Encryption 金鑰備份。

Java 卡 插入電腦中的抽取式卡。它包含登入所需的識別資訊。使用 Java 卡在 Drive Encryption 登入畫面登入時，需要插入 Java 卡，並輸入您的使用者名稱和 Java 卡 PIN 碼。

Live Messenger 歷程記錄檢視器 Privacy Manager Chat 元件可讓您搜尋並檢視加密的聊天記錄工作階段。

PKI 一種公開金鑰基礎架構標準，可用來定義介面以建立、使用和管理憑證及密碼編譯金鑰。

Privacy Manager 憑證 您每次進行密碼編譯作業（例如簽署和加密電子郵件訊息和 Microsoft Office 文件）時都需要用來驗證的數位憑證。

PSD 個人安全磁碟機，提供受保護的儲存區以儲存敏感性資訊。

SATA 裝置模式 電腦和大量儲存裝置之間的資料傳輸模式，例如硬碟和光碟機。

TXT 信任式執行技術。

USB 權杖 (Token) 儲存使用者身份識別資訊的安全性裝置。如同 Java 卡或生物測定讀取器，可用來驗證電腦的擁有者。

Windows 使用者帳戶 有權登入網路或個人電腦的個人設定檔。

Windows 登入安全性 透過要求使用特定認證進行存取，來保護 Windows 帳戶。

Windows 管理員 擁有完整權限的使用者，可修改權限並管理其他使用者。

手動拆解 略過自動拆解排程，立刻拆解資產或選取的資產。

主控台 您可以存取並管理程式功能和設定的集中位置。

加密 密碼編譯所使用的程序（如使用演譯法），可將純文字轉換成加密文字，防止未授權的收件者讀取該資料。資料加密類型有許多種，它們是網路安全性的基礎。常見的類型包含資料加密標準 (Data Encryption Standard) 和公開金鑰加密。

加密檔案系統 (EFS) 用來加密選定資料夾中所有檔案和子資料夾的系統。

可用空間清理　在刪除的資產上安全地寫入任意資料，以覆蓋刪除資產的內容。

生物測定　使用實體功能的驗證認證類別（如指紋）來識別使用者身份。

安全登入法　用來登入電腦的方法。

自動拆解　使用者在 File Sanitizer 中設定之已排程的拆解。

身份識別　HP ProtectTools Security Manager 中的一個認證和設定群組，其處理方式類似於特殊使用者的帳戶或設定檔。

使用者　已註冊 Drive Encryption 的任何人。非管理員使用者在 Drive Encryption 中的權限有限，他們只能註冊（經管理員同意）及登入。

拆解　執行一個演算法以模糊資產中的資料。

拆解設定檔　指定的清除方法和資產清單。

拆解週期　各項資產執行拆解演算法的次數。選取的拆解週期次數越高，電腦就越安全。

信任的 IM 通訊　在通訊工作階段期間，由信任的寄件者傳送給「信任的連絡人 (Trusted Contact)」的可信任訊息。

信任的寄件者　傳送已簽署和/或加密的電子郵件和 Microsoft Office 文件的「信任的連絡人 (Trusted Contact)」。

信任的連絡人　接受「信任的連絡人 (Trusted Contact)」邀請的人。

信任的連絡人收件者　收到邀請成爲「信任的連絡人 (Trusted Contact)」的人。

信任的連絡人清單　列出信任的連絡人。

信任的連絡人邀請　傳送給個人邀請其成爲「信任的連絡人 (Trusted Contact)」的電子郵件。

信任的郵件　在通訊工作階段期間，由信任的寄件者傳送給「信任的連絡人 (Trusted Contact)」的可信任訊息。

建議的簽署者　由 Microsoft Word 或 Microsoft Excel 文件的所有人指定，可在文件中新增簽章線的使用者。

按鍵順序　特定鍵的組合，按下時會啓動自動拆解，例如 ctrl+alt+s。

指紋　指紋影像的數位化擷取。Security Manager 不會儲存您實際的指紋影像。

爲信任的連絡人密封　一種可以新增數位簽章，加密電子郵件，以及在使用您選擇的安全登入法進行驗證後傳送電子郵件的工作。

背景服務　必須執行 HP ProtectTools 裝置鎖定/稽核背景服務，才能套用裝置存取控制原則。它可以在「控制台」之「管理工具」選項下的「服務」應用程式內檢視。如果它未執行，HP ProtectTools Security Manager 會在套用裝置存取控制原則時嘗試啓動它。

重新開機　電腦的重新啓動程序。

密碼編譯　加密和解密資料的實務，目的是只允許特定的個人解碼該資料。

密碼編譯服務提供者 (CSP)　密碼編譯演算法的提供者或文件庫，可應用於定義完善的介面中，以執行特殊的密碼編譯功能。

授權的使用者　在「使用者存取設定」檢視中被授與權限，可以檢視或修改「簡易組態」和「裝置類別組態」檢視之組態設定的使用者。

啓用　必須先完成此工作才能存取任何一項 Drive Encryption 功能。可使用 HP ProtectTools 設定精靈啓用 Drive Encryption。只有管理員可以啓用 Drive Encryption。啓用程序包含啓用軟體、加密磁碟機、建立使用者帳戶，以及在抽取式儲存裝置上建立初始備份加密金鑰。

移轉　可管理、還原和轉送「Privacy Manager 憑證」和「信任的連絡人 (Trusted Contact)」的工作。

聊天歷程記錄工作階段　加密的檔案，包含聊天工作階段中雙方交談的記錄。

備份　使用備份功能將重要程式資訊的副本儲存在程式以外的位置。然後將來可以用來將資訊還原到同一部或另一部電腦中。

單一登入　爲一種功能，可儲存驗證資訊，並讓您使用 Security Manager 來存取需要密碼驗證的網際網路和 Windows 應用程式。

單純刪除　刪除資產的 Windows 參照。資產內容仍保留在硬碟上，直到透過可用空間清理寫入模糊資料以將其覆寫。

智慧卡　一小片硬體，大小和形狀類似信用卡，可儲存擁有者的身份識別資訊。它可用來驗證電腦的擁有者。

登入　Security Manager 中的一個物件，由使用者名稱和密碼（以及其他可能選取的資訊）所組成，可以用來登入網站或其他程式。

虛擬權杖 (Token)　運作方式很像 Java 卡和卡片讀取器的安全性功能。Token 是儲存在電腦硬碟或 Windows 註冊表中。當您以虛擬 Token 登入時，系統會要求您提供使用者 PIN 碼，來完成驗證。

開機驗證　當電腦開機時，需要進行某些驗證形式的安全性功能，如 Java 卡、安全晶片或密碼。

傳送安全性按鈕　一個在 Microsoft Outlook 電子郵件訊息工具列上顯示的軟體按鈕。按一下這個按鈕，您便可以簽署和/或加密 Microsoft Outlook 電子郵件訊息。

群組　有相同存取層級或被拒絕存取某個裝置類別或特定裝置的一群使用者。

裝置存取控制原則　允許或拒絕使用者存取的裝置清單。

裝置類別　特定類型的所有裝置，例如磁碟機。

解密　密碼編譯所使用的程序，可將加密的資料轉換成純文字。

資產　位於硬碟機中資料元件，由個人資訊或檔案、歷程和 Web 相關資料等所組成。

撤銷密碼　當使用者申請數位憑證時所建立的密碼。當使用者想要撤銷數位憑證時需要這個密碼。如此可以確保只有使用者可以撤銷憑證。

管理員　**請參閱**「Windows 管理員」。

緊急復原封存　受保護的儲存區，可將某個平台擁有者金鑰的基本使用者金鑰重新加密成另一個。

網域　屬於網路一部份的電腦群組，並且共用通用目錄資料庫。網域的名稱是唯一的，且每個網域都有一組通用的規則和程序。

網路帳戶　Windows 使用者或管理員帳戶，可位於本機電腦、工作群組或網域。

認證　使用者用來證明其具有驗證程序中的特定工作權限之方法。

儀表板　您可以存取並管理程式功能和設定的集中位置。

數位憑證　確認個人或公司的識別身份之電子認證，方法是將數位憑證所有人的識別身份繫結到一對用來簽署數位資訊的電子金鑰。

數位簽章　與檔案一起傳送的資料，可確認資料的傳送者，以及檔案在簽署後未經修改。

憑證授權單位　發出執行公開金鑰基礎架構所需之憑證的服務。

還原　從先前儲存的備份檔將程式資訊複製到此程式中的程序。

簽章線　預留給數位簽章的視覺顯示位置。文件簽署後，就會顯示簽署者的名稱和驗證法。簽署日期和簽署者的職稱也可以包含在內。

簽署與加密按鈕　一種顯示在 Microsoft Outlook 應用程式工具列上的軟體按鈕。按一下這個按鈕，您便可以在 Microsoft Outlook 文件中簽署、加密或移除加密。

識別卡　一個 Windows 資訊看板的小工具，用來以視覺的方式識別您的桌面，包含您的使用者名稱和選擇的圖片。按一下識別卡以開啓 HP ProtectTools 管理主控台。

權杖　請參閱「安全登入法」。

顯現　一種可以讓使用者解密一個或多個聊天記錄工作階段，以純文字顯示「連絡人螢幕名稱」，並且能夠檢視工作階段的工作。

驗證　驗證使用者是否有權執行工作的程序，例如存取電腦，修改特定程式的設定，或檢視保護的資料。

索引