HP ProtectTools

快速入門

第 1 版 2011 年 1 月

文件編號：638391-AB1

目錄

1 安全性簡介

HP ProtectTools Security Manager 軟體提供安全功能，有助於防範未經授權存取電腦、網路及重要資料。

應用程式	功能
HP ProtectTools 管理主控台（適用於管理員）	• 需要 Microsoft Windows 管理員權限才能存取。 • 提供一些模組的存取權限，這些模組可由管理員進行設定，但一般使用者無法使用。 • 可以進行初始安全性設定，並針對所有使用者設定選項或需求。
關於 HP ProtectTools Security Manager（適用於使用者）	• 允許使用者設定管理員提供的選項。 • 可讓管理員提供使用者對部分 HP ProtectTools 模組有限制的控制權。

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 管理主控台（適用於管理員）	• 使用「Security Manager 設定精靈」來安裝及設定安全層級和安全登入方法。 • 設定對使用者隱匿的選項。 • 設定 Device Access Manager（裝置存取管理員）的設定和使用者存取權。 • 使用管理員工具來新增及移除 HP ProtectTools 使用者及檢視使用者狀態。
關於 HP ProtectTools Security Manager（適用於使用者）	• 組合管理、設定和變更密碼。 • 設定和變更 Windows 密碼、指紋及智慧卡等使用者認證。 • 設定和變更 File Sanitizer 的拆解、清理及其他設定。 • 檢視 Device Access Manager 的設定。 • 設定 Computrace for HP ProtectTools。 • 設定偏好設定與「備份和還原」選項。
Credential Manager for HP ProtectTools (Password Manager)	• 儲存、組合管理和保護您的使用者名稱及密碼。 • 設定網站和程式的的登入畫面，以供快速及安全的存取。 • 您可在 Password Manager 中輸入要保存的網站使用者名稱和密碼。下次造訪此網站時，Password Manager 會自動填入並提交該資訊。 • 建立強式密碼以增強帳戶安全性。Password Manager 會自動填入和提交資訊。
HP ProtectTools 磁碟機解密（HP ProtectTools Drive Encryption，僅限特定機型）	• 提供徹底的完整磁碟區硬碟加密。 • 強制預先開機驗證以便解密和存取資料。
File Sanitizer for HP ProtectTools	• 拆解電腦上的數位資產（敏感資訊，包括應用程式檔案、過去的內容或 Web 相關內容或其他機密資料），並定期清理硬碟中已刪除的資產。
Device Access Manager for HP ProtectTools（僅限特定機型）	• 可讓 IT 管理員根據使用者設定檔控制對裝置的存取。 • 防範未經授權的使用者利用外接式儲存媒體取出資料，以及避免其由外接式媒體將病毒引入系統中。 • 可讓管理員停用特定個人或使用者群組對可寫入裝置的存取。
HP ProtectTools 隱私管理員（HP ProtectTools Privacy Manager，僅限特定機型）	• 用來取得授權單位的憑證，當您使用 Microsoft 電子郵件和 Microsoft Office 文件時，即可由此憑證驗證通訊的來源、完整性及安全性。

模組	重要功能
Computrace for HP ProtectTools（另外購買）	• 提供安全資產追蹤。 • 監控使用者活動，以及硬體和軟體變更。 • 即使重新格式化或更換硬碟，仍然保持作用。 • 必須另外購買追蹤與追查訂閱才能啓用。
Embedded Security for HP ProtectTools（僅限特定機型）	• 使用信任平台模組 (TPM) 嵌入式安全晶片，以防範未經授權存取儲存在電腦上的使用者資料和認證。 • 允許建立個人安全磁碟機 (PSD)，有助於保護使用者檔案及資料夾資訊。 • 支援協力廠商應用程式（例如，Microsoft Outlook 和 Internet Explorer）以保護數位憑證作業。

HP ProtectTools 安全性產品說明及常用範例

大部分 HP ProtectTools 安全性產品都同時具有使用者驗證（通常爲密碼）與系統管理備份，如果遺失、無法使用或忘記密碼，或是在任何時候基於公司安全性需要存取權的情況下，便可利用他們進行存取。

附註： 有些 HP ProtectTools 安全性產品是專爲限制資料存取而設計。當資料重要到使用者寧可遺失資訊，也不願其洩露時，就應該對資料進行加密。建議您在安全的位置中備份所有資料。

Credential Manager for HP ProtectTools

Credential Manager（Security Manager 的一部分）會儲存使用者名稱及密碼，並且可用來：

- 儲存網際網路存取或電子郵件的登入名稱及密碼。
- 自動將使用者登入至網站或電子郵件。
- 管理和組織驗證。
- 選取 Web 或網路資產，以及直接存取連結。
- 必要時，檢視名稱及密碼。

範例 1： 她是一位大型製造商的採購人員，透過網際網路爲公司進行大部分的交易。她也經常造訪許多需要登入資訊的知名網站。由於對安全性有敏銳的警覺，因此在所有的帳戶上並不使用相同密碼。此採購人員已決定使用 Credential Manager，將 Web 連結與不同的使用者名稱及密碼相配。當她前往網站登入時，Credential Manager 就會自動出示認證。如果她想要檢視使用者名稱及密碼，則可以設定 Credential Manager 顯現。

Credential Manager 也可用來管理和組織驗證。此工具允許使用者選取 Web 或網路資產以及直接存取連結。必要時，使用者也可以檢視使用者名稱及密碼。

範例 2： 一位勤奮工作的會計師 (CPA) 獲得升遷，即將管理整個會計部門。這個團隊必須登入大量客戶的 Web 帳戶，而每個帳戶會使用不同的登入資訊。其他工作人員也需要共用這些登入資訊，因此機密性將構成問題。會計師決定在 Credential Manager for HP ProtectTools 內組織所有 Web 連結、公司使用者名稱及密碼。組織完成後，會計師就可以爲員工部署 Credential Manager，讓他們在 Web 帳戶上工作，但永遠都不知道目前所用的登入認證。

Drive Encryption for HP ProtectTools

Drive Encryption 可用來限制對整個電腦硬碟或次要磁碟機的資料存取。Drive Encryption 也可以管理自我加密磁碟機。

範例 1： 一位醫生想要確保只有他才可以存取其電腦硬碟上的任何資料。 這位醫生啓用 Drive Encryption，此程式會在 Windows 登入前要求預先開機驗證。 一旦設定該驗證後，若未在作業系統啓動之前提供密碼，就無法存取硬碟。 醫生還能選擇使用 SED（自我加密磁碟機）選項將資料加密，以進一步提升磁碟機安全性。

由於 Embedded Security for HP ProtectTools 及 Drive Encryption for HP ProtectTools 都已繫結至原始主機板，因此即使在磁碟機已移除時，也不允許存取加密資料。

範例 2： 醫院管理人想要確保只有醫生及獲得授權的人員，才可以在沒有共用個人密碼的情況下存取其本機電腦上的所有資料。IT 部門因此將管理員、醫生和所有獲得授權的人員新增爲 Drive Encryption 使用者。現在，只有獲得授權的人員才能使用其個人使用者名稱及密碼啓動電腦或網域。

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools 可用來永久刪除資料，包括網際網路瀏覽器活動、暫存檔案、先前刪除的資料或任何其他資訊。File Sanitizer 可以設定爲手動執行，或按照使用者定義排程自動執行。

範例 1： 一位律師經常處理敏感的客戶資訊，他想要確保已刪除檔案中的資料再也無法復原。這位律師現在使用 File Sanitizer 來「拆解」刪除的檔案，因此要復原幾乎是不可能的。

當 Windows 刪除資料時，通常並非實際從硬碟中清除資料。反而只是將硬碟磁區標記爲可供日後使用。在資料遭到覆寫以前，都能夠使用可在網際網路上取得的一般工具輕易復原。File Sanitizer 以隨機資料覆寫磁區（必要時覆寫多次），因此會使得刪除的資料無法判讀且無法復原。

範例 2： 一位研究人員希望在她登出時，系統自動拆解刪除的資料、暫存檔案、瀏覽器活動等項目。她使用 File Sanitizer 排定「拆解」時程，因此她可以選取要系統自動永久移除的一般檔案或任何自訂檔案。

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools 可用來阻止未經授權存取可複製資料的 USB 快閃磁碟機。它也可以在 CD/DVD 光碟機存取、USB 裝置控制、網路連線等方面加以限制。管理員還能排定何時能存取磁碟機以及存取的時間長短。例如，當外部廠商需要存取公司電腦，但不得將資料複製到 USB 磁碟機時，即是這種情況。Device Access Manager for HP ProtectTools 允許管理員限制和管理對硬體的存取。

範例 1： 藥品供應公司的經理經常處理個人用藥記錄以及其公司的資訊。員工需要存取此資料，但是絕對不得透過 USB 磁碟機或任何其他外接式儲存媒體，從電腦取出該資料。網路雖然受到安全保護，但是電腦仍有可利用以複製和竊取資料的 CD 燒錄器和 USB 連接埠。這位經理因此透過 Device Access Manager 停用 USB 連接埠和 CD 燒錄器，使其無用武之地。雖然封鎖了 USB 連接埠，但是滑鼠和鍵盤仍然可以使用。

範例 2： 保險公司不希望員工從家中安裝或載入個人軟體或資料。但還是有些員工必須存取所有電腦上的 USB 連接埠。IT 管理員因此使用 Device Access Manager 啓用這些員工的存取權，而封鎖其他員工的外部存取。

Privacy Manager for HP ProtectTools

當網際網路電子郵件通訊必須受到安全保護時，您可以使用 Privacy Manager for HP ProtectTools。使用者可以建立和傳送只能由通過驗證之收件者開啓的電子郵件。有了 Privacy Manager，冒名者就無法侵奪或攔截資訊。

範例 1： 股票經紀人想要確保他的電子郵件只會傳送至特定客戶，沒有人可以僞冒此電子郵件帳戶而進行攔截。股票經紀人爲此向 Privacy Manager 註冊他自己及其客戶。Privacy Manager 簽發給他們每個使用者一個驗證憑證 (CA)。當股票經紀人和他的客戶使用此工具時，都必須先進行驗證才能交換電子郵件。

Privacy Manager for HP ProtectTools 可讓您輕鬆地傳送和接收其收件者已確認且通過驗證的電子郵件。您也可以將郵件服務加密。此加密程序與在網際網路上以一般信用卡購物時所使用的加密程序相似。

範例 2： 總執行長想要確保只有董事會的成員才可以檢視他透過電子郵件傳送的資訊。總執行長因此使用選項加密自己與董事之間收發的電子郵件。Privacy Manager 憑證驗證允許總執行長和董事持有加密金鑰的副本，所以只有他們才能將機密電子郵件解密。

Computrace for HP ProtectTools（原來爲 LoJack Pro）

Computrace for HP ProtectTools（另外購買）是一項服務，可在使用者存取網際網路時追蹤失竊電腦的位置。

範例 1： 校長已指示 IT 部門記錄學校的所有電腦。清查電腦之後，IT 管理員隨即向 Computrace 註冊所有的電腦，一旦電腦失竊時便可進行追蹤。最近學校發現有幾台電腦不見了，IT 管理員因此向警方和 Computrace 專員報備。隨後就找到了電腦並發還給學校。

Computrace for HP ProtectTools 也可以在遠端協助管理和尋找電腦，以及監控電腦使用情況和應用程式。

範例 2： 不動產經紀公司需要管理和更新全球各地的電腦。他們使用 Computrace 來監控和更新電腦，而不必派遣 IT 人員到每部電腦前。

Embedded Security for HP ProtectTools（僅限特定機型）

Embedded Security for HP ProtectTools 提供建立個人安全磁碟機的功能。此功能可讓使用者在電腦上建立除非進行存取否則完全隱匿的虛擬磁碟機分割區。只要是資料需要秘密保護而資料其餘部分不予加密的地方，就可以使用 Embedded Security。

範例 1： 倉庫管理員有一部電腦，多位工作人員會在一天當中不定時進行存取。管理員想要加密和隱藏電腦上的機密倉庫資料。他希望資料保護得夠安全，即使有人盜取硬碟，也無法解密資料或加以讀取。倉庫管理員決定啓用 Embedded Security，並將機密資料移至個人安全磁碟機。倉庫管理員可以輸入密碼，並且存取機密資料，就像存取另一部硬碟一樣。當他登出或重新啓動個人安全磁碟機時，若沒有正確的密碼，就無法看見此部磁碟機或將其開啓。工作人員因此永遠無法在存取電腦時看見機密資料。

Embedded Security 會保護位於主機板上的硬體 TPM（信任平台模組）晶片內的加密金鑰。這是唯一符合抵抗密碼攻擊最低需求的加密工具。遭到這種攻擊時，攻擊者會試圖猜出解密的密碼。Embedded Security 也可以加密整個磁碟機和電子郵件。

範例 2： 股票經紀人想要將極爲敏感的資料傳輸至另一部使用可攜式磁碟機的電腦。她想要確保即使密碼洩露，也只有這兩部電腦才能開啓磁碟機。股票經紀人爲此使用 Embedded Security TPM 移轉作業，讓第二部電腦具有能解密資料的必要加密金鑰。在傳輸過程中，即使他人持有密碼，仍然只有這兩部實體電腦才能解密資料。

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

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：

- 啓用預先開機驗證功能時，有助於防止存取作業系統。請參閱下列章節：
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- 個人安全磁碟機功能（由 Embedded Security for HP ProtectTools 模組提供）會加密敏感資料，有助於杜絕未經驗證存取資料。請參閱下列章節：
  - Embedded Security for HP ProtectTools
- Computrace 可以在電腦失竊後追蹤其位置。請參閱下列章節：
  - Computrace for HP ProtectTools

限制存取敏感性資料

假設審計人員上門查帳而必須讓他存取電腦以檢閱敏感的財務資料時，您並不希望此審計人員有辦法列印檔案或將檔案儲存到像 CD 之類的可寫入裝置。下列功能可以協助限制資料存取：

- Device Access Manager for HP ProtectTools 允許 IT 管理員限制對可寫入裝置的存取，讓敏感資訊無法被列印或從硬碟複製到抽取式媒體。

防止未獲授權的使用者從內部或外部位置進行存取

未經授權存取沒有安全保護的商用電腦，對公司網路資源（例如，金融服務業、行政部門或研發小組的資訊）以及對私人資訊（例如，就醫記錄或個人財務記錄）而言，都毫無疑問會構成重大風險。下列功能可以協助防止未經授權的存取：

- 啓用預先開機驗證功能時，有助於防止存取作業系統。請參閱下列章節：
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- 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。

- Device Access Manager for HP ProtectTools 允許 IT 管理員限制對可寫入裝置的存取，讓敏感資訊無法從硬碟複製出來。
- File Sanitizer 可以藉由拆解重要檔案及資料夾或清理硬碟上的已刪除資產（覆寫已刪除而目前仍可復原的資料），保護資料刪除作業的安全。
- 當您使用 Microsoft 電子郵件或 Microsoft Office 文件時，可以使用 Privacy Manager 取得授權單位的憑證，讓傳送與儲存重要資訊的過程更安全、更有保障。

建立強式密碼原則

如果公司政策開始實施，要求數十項 Web 應用程式和資料庫都必須使用強式密碼原則，那麼 Security Manager 便可提供受保護的密碼存放庫以及單一登入的便利功能。

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層級，並決定要部署的安全性功能，例如 Drive Encryption 或 Embedded Security。

  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定義的安全性功能，也可以啓用和停用某些功能。例如，如果安全性主管決定要部署智慧卡，則 IT 管理員可以同時啓用密碼和智慧卡模式。
- 使用者 — 使用安全性功能。例如，如果安全性主管和 IT 管理員已爲系統啓用智慧卡，使用者便可設定智慧卡 PIN 碼，並使用此卡供驗證之用。

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 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	設定於下列模組中	功能
Windows 登入密碼	Windows® 控制台或 HP ProtectTools Security Manager	可以用作手動登入和驗證，以存取各種 Security Manager 功能。
Security Manager Backup and Recovery 密碼	Security Manager，依個別使用者	保護 Security Manager 備份與復原檔的存取。

HP ProtectTools 密碼	設定於下列模組中	功能
智慧卡 PIN 碼	Credential Manager	可以當做多因子驗證使用。 可以當做 Windows 驗證使用。 驗證 Drive Encryption 的使用者（如果選取的是智慧卡權杖）。
緊急復原權杖密碼	Embedded Security，依 IT 管理員	保護緊急復原權杖的存取，此權杖爲嵌入式安全晶片的備份檔案。
擁有者密碼	Embedded Security，依 IT 管理員	保護系統和 TPM 晶片以避免未經授權存取 Embedded Security 的所有擁有者功能。
BIOS 管理員密碼	Computer Setup，依 IT 管理員	保護對 Computer Setup 公用程式的存取。

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。
- 不要使用您的姓名或任何其他個人資訊（例如，您的生日、寵物名字或母親娘家姓氏）做爲密碼，即使您倒過來拼寫也不可以。
- 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 的「備份和還原」功能來選取及備份 HP ProtectTools 機密資料和設定。

2 使用設定精靈快速入門

Security Manager 設定精靈會引導您啓用套用於這部電腦所有使用者的可用安全功能。您也可以在管理主控台的「安全功能」頁面上管理這些功能。

若要透過 Security Manager 設定精靈設定安全功能：

1. 從 Windows 資訊看板中的「HP ProtectTools」桌面小工具圖示或位於工作列最右側通知區中的工作列圖示，開啓 HP ProtectTools Security Manager。

「HP ProtectTools」桌面小工具圖示的橫幅色彩表示下列其中一種狀況：

- 紅色 — HP ProtectTools 尚未設定，或有一個 ProtectTools 模組有錯誤狀況。
- 黃色 — 在 Security Manager 中的「應用程式狀態」頁面中，查看必須做的設定變更。
- 藍色 — HP ProtectTools 已設定並運作正常。

小工具圖示底部所顯示的訊息，表示下列其中一種狀況：

- **立即設定** — 管理員必須按一下小工具圖示執行 Security Manager 設定精靈，才能設定電腦的驗證認證。

  設定精靈是獨立的應用程式。

- **立即註冊** — 使用者必須按一下小工具圖示，才能執行 Security Manager 快速入門精靈以登錄驗證認證。

  快速入門精靈會顯示在 Security Manager Dashboard 中。

- **立即檢查** — 按一下小工具圖示，在「安全性應用程式狀態」頁面上顯示進一步的詳細資料。

附註： Windows XP 沒有提供「HP ProtectTools」桌面小工具圖示。

– 或 –

依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。在左側窗格中，按一下「**設定精靈**」。

2. 閱讀「歡迎」畫面，然後按「**下一步**」。

3. 輸入 Windows 密碼，驗證您的身分，然後按「**下一步**」。

   如果您尚未建立 Windows 密碼，系統會提示您建立密碼。Windows 密碼是用來保護您的 Windows 帳戶，避免未獲授權的使用者存取，以及使用 HP ProtectTools Security Manager 功能。

4. 在 SpareKey 頁面上，選取三個安全性問題，並輸入各個問題的答案，然後按「**下一步**」。

   在 Security Manager Dashboard 中，您可以在 **Credential Manager** 底下的 SpareKey 頁面上選取不同的問題或變更答案。

   附註： 這個 SpareKey 設定僅套用於管理使用者。

5. 選取安全功能的核取方塊以啟用安全功能，然後按「**下一步**」。

   選取的功能愈多，電腦的安全性就愈高。

   附註： 這些設定套用於所有的使用者。如果未選取任何核取方塊，設定精靈將不會提示使用者註冊這些認證。

   - **Windows 登入安全性** — 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，使未經授權人士無法讀取資訊的方式，保護您的資料。
   - **預先開機安全性** — 藉由禁止未經授權人士在啟動 Windows 之前存取電腦的方式來保護您的電腦。

     附註： 「預先開機安全性」若不受 BIOS 支援便無法使用。

6. 設定精靈會提示您註冊或「登錄」您的認證。

   如果沒有指紋讀取器、智慧卡或網路攝影機可供使用，系統會提示您輸入 Windows 密碼。註冊之後，任何時候需要驗證，都可使用任何註冊的認證驗證您的身分。

   附註： 這些認證的註冊僅套用於管理使用者。

7. 在精靈的最後一頁，請按一下「**完成**」。

   此時會顯示 Security Manager Dashboard 首頁。

3 HP ProtectTools Security Manager 管理主控台

HP ProtectTools Security Manager 軟體提供安全功能，有助於防範未經授權存取電腦、網路及重要資料。而 HP ProtectTools Security Manager 的管理則是由管理主控台功能所提供的。

Security Manager Dashboard 另提供其他應用程式（僅限特定機型），當電腦遺失或遭竊時可協助其進行復原。

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
- 指定所需的認證進行驗證
- 管理電腦的使用者
- 調整裝置特定的參數
- 設定已安裝的 Security Manager 應用程式
- 新增其他的 Security Manager 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**」，然後按一下「**HP ProtectTools 管理主控台**」。

  － 或 －

  在 Security Manager 的左側面板中，按一下「**管理**」，然後按一下「**管理主控台**」。

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。

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

－ 或 －

在 Security Manager 的左側面板中，按一下「**管理**」，然後按一下「**管理主控台**」。

主控台包含下列元件：

- **首頁** — 讓您設定下列安全性選項：
  - **增強系統安全性**
  - **需要強式驗證**
  - **管理 HP ProtectTools 使用者**
  - **瞭解如何集中管理 HP ProtectTools**
- **系統** — 讓您設定使用者和裝置的下列安全功能和驗證：
  - **安全性**
  - **使用者**
  - **認證**
- **應用程式** — 讓您配置 HP ProtectTools Security Manager 和 Security Manager 應用程式的設定。
- **資料** — 提供連結至可保護資料的 Security Manager 應用程式的展開式功能表。
- **集中管理** — 顯示存取額外解決方案、產品更新和訊息的標籤。
- **設定精靈** — 引導您逐步設定 HP ProtectTools Security Manager。
- **關於** — 顯示 HP ProtectTools Security Manager 相關資訊，例如版本號碼和著作權聲明。
- **主要區域** — 顯示特定應用程式的畫面。

  ? — 顯示管理主控台軟體「說明」。此圖示位於視窗畫面的右上角，就在最大化和最小化圖示的旁邊。

設定您的系統

從 HP ProtectTools 管理主控台左側的功能表面板可存取「**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。
- **認證** – 管理電腦內建或連接的安全性裝置設定值。

設定電腦適用的驗證

在驗證應用程式內，您可以設定支配電腦存取的原則。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時所需的認證。

若要在您電腦上設定驗證：

1. 在管理主控台的左側面板中，按一下「**安全性**」，然後按一下「**驗證**」。
2. 若要設定登入驗證，請按一下「**登入原則**」標籤並進行變更，然後按一下「**套用**」。
3. 若要設定工作階段驗證，請按一下「**工作階段原則**」標籤並進行變更，然後按一下「**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. 在管理主控台的左側面板中，按一下「**安全性**」，然後按一下「**驗證**」。
2. 在「**登入原則**」標籤上按向下箭頭，然後選取使用者類別：
   - **適用於此電腦的管理員**
   - **適用於非管理員的使用者**
3. 指定選定的使用者類別所需的驗證認證。
4. 選擇是否需要任一指定的認證，或者需要所有指定的認證，才能驗證使用者。
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. 在管理主控台的左側面板中，按一下「**安全性**」，然後按一下「**驗證**」。
2. 在「**工作階段原則**」標籤上按向下箭頭，然後選取使用者類別：
   - **適用於此電腦的管理員**
   - **適用於非管理員的使用者**

3. 按向下箭頭，然後選取所選使用者類別所需的驗證認證：

   - **需要其中一個指定的認證**

     附註： 清除所有認證的核取方塊與選取「**不需要驗證**」具有同樣的效果。

   - **需要所有指定的認證**
   - **不需要驗證** — 選取此選項會清除視窗中所有的認證。

4. 按一下「**套用**」。

設定

1. 選取核取方塊以啓用下列設定，或清除核取方塊以停用下列設定：

   允許 One Step logon — 如果在 BIOS 或加密磁碟層級執行驗證，允許此電腦的使用者略過 Windows 登入。

2. 按一下「**套用**」。

管理使用者

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

會列出所有 HP ProtectTools 使用者，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。

若要管理使用者，請選取下列設定：

- 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**」。
- 若要設定使用者的其他認證，請按一下該使用者，然後按一下「**註冊**」。
- 若要檢視特定使用者的原則，請選取該使用者，然後在下方的視窗檢視原則。

認證

在認證應用程式內，可指定由 HP ProtectTools Security Manager 認可之任何內建或連接之安全性裝置可使用的設定值。

SpareKey

您可以設定是否允許 Windows 登入的 SpareKey 驗證，並管理使用者會在 SpareKey 註冊期間看到的安全性問題。

1. 針對用於 Windows 登入的 HP SpareKey 驗證，選取核取方塊以啓用，或清除核取方塊以停用。
2. 選取使用者會在 SpareKey 註冊期間看到的安全性問題。 您最多可指定三個自訂問題，也可以允許使用者輸入自己的密碼。
3. 按一下「**套用**」。

指紋

如果電腦已安裝或連接指紋讀取器，「指紋」頁面會顯示以下標籤：

- **註冊** — 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。

  ⚠ 注意： 若清除指紋讀取器中的所有資料，則會將包括管理員在內的所有使用者指紋資料一併清除。 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** — 移動滑桿可調整指紋讀取器掃過指紋時所使用的敏感度。

  如果指紋識別度不夠穩定，您可能需要選取較低的敏感度。 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** — 選取下列其中一個選項，設定指紋讀取器以節省電力並強化視覺回應：

  - **最佳化** — 指紋讀取器可在必要時隨時啟動。 第一次使用讀取器時，您可能會發現回應略微延遲。
  - **節省電力** — 指紋讀取器回應較慢，但是設定需要的電力較少。
  - **全功率** — 指紋讀取器已就緒，隨時可供使用，但是此設定使用的電力最多。

智慧卡

如果電腦已安裝或連接智慧卡讀取器，「智慧卡」頁面會顯示兩個標籤：

- **設定** — 設定電腦在取出智慧卡時自動鎖定。

  附註： 只有在登入 Windows 並將智慧卡當成驗證認證使用時，電腦才會鎖定。 取出未用於登入 Windows 的智慧卡，則不會鎖定電腦。

- **管理** — 選取下列其中一個選項：

  - **初始化智慧卡** — 備妥智慧卡以搭配 HP Protect Tools 使用。 如果先前已在 HP ProtectTools 之外初始化智慧卡（包含非對稱式金鑰配對及相關憑證），除非需要特定憑證的初始化，否則不需要再次初始化。
  - **變更智慧卡 PIN** — 讓您能夠變更搭配智慧卡使用的 PIN 碼。
  - **僅清除 HP ProtectTools 資料** — 僅清除智慧卡初始化期間建立的 HP ProtectTools 憑證。不會清除智慧卡中其他任何資料。
  - **清除智慧卡中全部的資料** — 清除指定之智慧卡中全部的資料。 智慧卡無法再搭配 HP ProtectTools 或其他任何應用程式使用。

附註： 無法使用您的智慧卡不支援的功能。

▲ 按一下「**套用**」。

登入

如果電腦已安裝或連接網路攝影機，而且已安裝 Face Recognition 程式，您可以設定 Face Recognition 安全性等級，在電腦的使用方便性與違反安全性的困難度之間取得平衡。

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 按一下「**認證**」，然後按一下「**臉孔**」。
3. 如需要更多的方便性，可按一下滑桿將其向左移動，或者將其向右移動以提高正確性。
   - **方便性** — 若要讓註冊的使用者能在最低限度的情況下取得存取權限，請按一下滑桿將其移至「**方便性**」位置。
   - **平衡** — 若要在安全性與使用方便性之間取得平衡，或者如果您的資訊具有高度敏感性，或者您的電腦所在區域可能會發生未獲授權的登入時，請按一下滑桿將其移至「**平衡**」位置。
   - **正確性** — 當註冊的景像或目前的照明條件低於正常情況時，若要讓使用者更不容易取得存取權限，降低錯誤接受的可能性，請按一下滑桿將其移至「**正確性**」位置。
4. 按一下「**進階**」，然後設定其他的安全性。 如需詳細資訊，請參閱位於第 34 頁的進階使用者設定。
5. 按一下「**套用**」。

設定您的應用程式

您可以使用「設定」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. 在管理主控台的左側面板中，按一下「**應用程式**」底下的「**設定**」。
2. 選取特定設定旁邊的核取方塊以啓用設定，或清除核取方塊以停用設定。
3. 按一下「**套用**」。

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精靈在登入時自動開啓。
- **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：

- **應用程式狀態** — 顯示所有應用程式的狀態。
- **Password Manager** — 爲電腦的所有使用者啓用 Password Manager。
- **Privacy Manager** — 爲電腦的所有使用者啓用 Privacy Manager。
- **啓用集中管理連結** — 允許此電腦的所有使用者藉由按一下「**集中管理**」的方式，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。

集中管理

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在「設定」頁面停用此功能。「集中管理」頁面有兩個標籤：

- **企業解決方案** — 如果可使用網際網路連線，便能夠存取 DigitalPersona 網站 (http://www.digitalpersona.com/) 以確認新的應用程式。
- **更新與訊息**
  - 如需新應用程式和更新的相關資訊，請選取「**隨時通知我新應用程式和新更新的相關資訊**」核取方塊。
  - 若要設定自動更新的排程，請選取日數。
  - 若要檢查是否有更新，請按「**立即檢查**」。

4 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。
- 登錄一個或多個景像以進行驗證。
- 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。

開啓 Security Manager

您可以使用下列任何一種方式來開啓 Security Manager：

- 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**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「**HP ProtectTools**」桌面小工具圖示。
- 按下快速鍵組合 ctrl+Windows 標誌鍵+h，開啓「**Security Manager 快速連結**」功能表。

  如需變更快速鍵組合的相關資訊，請參閱位於第 30 頁的設定。

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。

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

Dashboard 會顯示下列元件：

- **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：
  - **主畫面** — 管理密碼、設定您的驗證認證或檢查安全性應用程式的狀態。
  - **狀態** — 檢查 HP ProtectTools 安全性應用程式的狀態。

附註： 電腦上未安裝的應用程式未顯示在下列清單中。

- **我的登入** — 使用 Password Manager、認證管理員、密碼、SpareKey、智慧卡、臉孔和指紋管理您的驗證認證。
- **我的資料** — 使用 Drive Encryption 和 File Sanitizer 管理您資料的安全性。
- **我的電腦** — 使用 Device Access Manager 管理您電腦的安全性。
- **我的通訊** — 使用 Privacy Manager 管理您通訊的安全性。
- **管理** — 允許管理員存取下列選項：
  - **管理主控台** — 允許管理員管理安全性和使用者。
  - **集中管理** — 允許管理員存取額外的解決方案、產品更新和訊息。
- **進階** — 顯示存取其他功能的指令，包含以下指令：
  - **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 HP ProtectTools Security Manager 相關資訊，例如版本號碼和著作權聲明。
- **主要區域** — 顯示特定應用程式的畫面。
- **?** — 顯示 Security Manager 軟體「說明」。此圖示位於視窗的右上角，就在最大化和最小化圖示的旁邊。

安全性應用程式狀態

您可以在兩個位置檢視安裝的安全性應用程式的狀態：

- **HP ProtectTools 桌面小工具**

  HP ProtectTools 小工具圖示頂端的橫福色彩會改變，以反映所安裝之安全性應用程式的整體安全性狀態。

  - **紅色** — 警告
  - **黃色** — 注意：未設定。
  - **藍色** — 正常

  小工具圖示底部所顯示的訊息，表示下列其中一種狀況：

  - **立即設定** — 管理員必須按一下小工具圖示執行 Security Manager 設定精靈，才能設定電腦的驗證認證。

    設定精靈是獨立的應用程式。

  - **立即註冊** — 使用者必須按一下小工具圖示，才能執行 Security Manager 快速入門精靈以登錄驗證認證。

    快速入門精靈會顯示在 Security Manager Dashboard 中。

  - **立即檢查** — 按一下小工具圖示，在「安全性應用程式狀態」頁面上顯示進一步的詳細資料。

- **安全性應用程式狀態頁面** — 按一下 Security Manager Dashboard 上的「**狀態**」，就會顯示安裝之安全性應用程式的整體狀態，以及每一個應用程式的特定狀態。

我的登入

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。

- **Password Manager** – 建立和管理快速連結，這可讓您使用 Windows 密碼、指紋或智慧卡進行驗證，以啓動和登入網站及程式。
- **Credential Manager** – 提供輕鬆的方式以變更 Windows 密碼、登錄指紋或設定智慧卡。

按一下「**管理**」，然後按一下 Dashboard 左下角的「**集中管理**」，管理員就可以新增更多應用程式。

Password Manager

使用 Password Manager 是更輕鬆安全登入 Windows、網站和應用程式的方式。您可以用它來建立強式密碼，完全不需要寫下或記憶，然後使用指紋、智慧卡或 Windows 密碼輕鬆快速登入。

Password Manager 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。
- 檢視您的任一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。

「**Password Manager**」圖示會顯示在網頁的左上角或應用程式登入畫面上。 在尚未建立網站或應用程式登入之前，圖示上會顯示加號。

▲ 按一下「**Password Manager**」圖示可顯示內容功能表，您可以從下列選項做選擇。

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 Password Manager。
- **圖示設定** – 允許您指定顯示「**Password Manager**」圖示的條件。
- **說明** — 顯示 Security Manager 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。
- **新增登入** – 允許您將帳戶新增至登入。
- **開啓密碼管理員** – 啓動 Password Manager。
- **說明** — 顯示 Security Manager 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，Password Manager 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 Password Manager 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「**Password Manager**」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「**Password Manager 管理**」標籤的「**新增登入**」。某些選項需視連接至電腦的安全性裝置而定，例如：使用 ctrl+Windows 標誌鍵+h 快速鍵、掃過指紋或插入智慧卡。
   a. 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。
   b. 若要檢視此登入的密碼，請按一下「**顯示密碼**」。
   c. 若要填入登入欄位但不提交，請清除「**自動提交登入資料**」核取方塊。
   d. 若要啓用 VeriSign VIP 安全性，請選取「**我需要這個網站的 VIP 安全性**」核取方塊。

      這個選項只會針對 VeriSign 身分保護 (VIP) 可以使用的網站顯示。當網站支援時，您還可以選擇自動填寫您的 VIP 安全碼以及您慣用的驗證方法。
   e. 按一下「**確定**」，再按一下您要使用的驗證方法（指紋、密碼或臉孔），然後使用選取的驗證方法登入。

      「**Password Manager**」圖示的加號會被移除，通知您已建立登入。
   f. 如果 Password Manager 無法偵測登入欄位，請按一下「**更多欄位**」。
      - 選取登入所需要的每個欄位，或取消選取登入不需要的任何欄位。
      - 如果 Password Manager 無法偵測所有登入欄位，則會出現訊息詢問您是否要繼續執行。按一下「**是**」。
      - 隨後開啓的對話方塊中會填妥您的登入欄位。按一下每個欄位的圖示，將其拖曳至適當的登入欄位，然後按一下按鈕登入網站。

        附註： 一旦使用手動模式輸入網站的登入資料，將來您就必須使用此方法來登入相同的網站。

        附註： 手動輸入登入資料的模式僅適用於 Internet Explorer 8。
      - 按一下「**關閉**」。

每次您存取該網站或開啓程式時，網站的左上角或應用程式登入畫面就顯示「**Password Manager**」圖示，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「**Password Manager**」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「**Password Manager 管理**」標籤的「**編輯所需的登入**」。
3. 編輯您的登入資訊。
   - 若要選取包含其中一個預先格式化的選項的「**使用者名稱**」登入欄位，請按一下欄位右側的向下箭頭。
   - 若要選取包含其中一個預先格式化的選項的「**密碼**」登入欄位，請按一下欄位右側的向下箭頭。
   - 若要啓用 VeriSign VIP 安全性，請選取「**我需要這個網站的 VIP 安全性**」核取方塊。

     這個選項只會針對可以使用 VeriSign VIP 安全性的網站顯示。當網站支援時，您還可以選擇自動填寫您的 VIP 安全碼以及您慣用的驗證方法。
   - 若要將其他欄位從畫面新增至您的登入，請按一下「**更多欄位**」。
   - 若要檢視此登入的密碼，請按「**顯示密碼**」。
   - 若要填寫登入欄位但不提交，請清除「**自動提交登入資料**」核取方塊。
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，Password Manager 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 Password Manager 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 Password Manager 的「**登入**」功能表。

若要顯示「**登入**」功能表：

1. 按下「**Password Manager**」快速鍵組合（原廠設定是 ctrl+Windows 標誌鍵+h）。若要變更快速鍵組合，請按一下 Security Manager Dashboard 的「**Password Manager**」，然後按一下「**設定**」。
2. 掃過您的指紋（在內建或連接指紋讀取器的電腦上執行），或輸入您的 Windows 密碼。

將登入分類

建立一項或多項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「**Password Manager**」。
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。當您將滑鼠指標指向分類時，分類就會反白顯示。
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

Password Manager 是方便於管理登入名稱、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**」標籤上。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「**Password Manager**」，然後按一下「**管理**」標籤。

- **新增登入** — 按一下「**新增登入**」，並依照畫面上的指示執行。
- **您的登入** — 按一下現有的登入，選取下列其中一個選項，並依照畫面上的指示執行。
  - **開啓** — 開啓您擁有其現存登入的網站或程式。
  - **新增** — 新增登入。如需詳細資訊，請參閱位於第 26 頁的新增登入。
  - **編輯** — 編輯登入。如需詳細資訊，請參閱位於第 27 頁的編輯登入。
  - **刪除** — 刪除您擁有其現存登入的網站或程式。
- **新增類別** — 按一下「**新增類別**」，然後依照畫面上的指示執行。如需詳細資訊，請參閱位於第 27 頁的將登入分類。

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「**Password Manager**」圖示，顯示其內容功能表。
3. 按一下「**新增登入**」，然後依照畫面上的指示執行。

評估您密碼的強度

使用強式密碼登入網站和程式，是防護您身分的重要層面。

Password Manager 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。

Password Manager 圖示設定

Password Manager 會嘗試識別網站和程式的登入畫面。當 Password Manager 偵測出您尚未建立登入的登入畫面時，會顯示含有加號的「**Password Manager**」圖示，提示您新增該畫面的登入。

1. 按一下圖示箭頭，然後按一下「**圖示設定**」以自訂 Password Manager 處理可能登入網站的方式。
   - **提示爲登入畫面新增登入** — 按一下此選項後，當登入畫面顯示尚未設定登入時，Password Manager 會提示您新增登入。
   - **排除此畫面** — 選取此核取方塊，Password Manager 便不再提示您爲此登入畫面新增登入。

     若要爲先前已經排除的畫面新增登入：

     - 當顯示先前排除的網站登入或程式頁面時，開啓 Security Manager dashboard，然後按一下「**Password Manager**」。
     - 按一下「**新增登入**」。

       接著會開啓包含網站登入畫面或列在「**目前畫面**」欄位中之程式的「新增登入」對話方塊。
     - 按一下「**繼續**」。

       隨即顯示「將登入新增至密碼管理員」畫面。
     - 然後，遵循畫面上的指示執行。如需詳細資訊，請參閱位於第 26 頁的新增登入。
     - 當此網站登入或程式畫面開啓時，就會顯示「**Password Manager**」圖示。
2. 若要停用顯示提示爲登入畫面新增登入的選項，請選取此核取方塊。
3. 若要存取其他 Password Manager 設定，請按一下「**Password Manager**」，然後按一下 Security Manager Dashboard 上的「**設定**」。

VeriSign 身分保護 (VIP)

您可以建立用於啓用 VeriSign VIP 功能之網站的 VeriSign VIP 存取 Token。Password Manager 會使用這些 Token，建立合併使用拖放至啓用 VeriSign VIP 之登入畫面或手動輸入於指定欄位的 Token 的自動登入。

您可以從 Security Manager Dashboard 或任何啓用 VeriSign VIP 的網站，啓用 VeriSign VIP 並建立 Token。爲了使用 Token，您必須在每一個要使用該 Token 的網站註冊該 Token。

在 Token 註冊及第一次使用後，它會（選用）被附加，並與您慣用的登入認證一併提交。針對不允許附加 Token 的網站，您可拖放或手動輸入 Token 資訊。

若要啓用 VeriSign VIP 以及從 Security Manager Dashboard 建立 VeriSign VIP Token：

1. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 按一下「**Password Manager**」，然後按一下「**VIP**」。
3. 按一下「**取得 VIP**」。

   VeriSign VIP 頁面上會建立並顯示 VeriSign VIP Token。現在，只要您存取此頁面，就會顯示此 Token。

若要啓用 VeriSign VIP 以及從網站建立 VeriSign VIP Token：

1. 任何時候只要造訪啓用 VeriSign VIP 的網站，Password Manager 就會對您提出警示。
2. 建立畫面的登入。如需詳細資訊，請參閱位於第 26 頁的新增登入。
3. 在「建立登入」對話方塊中，選取「**我需要具有 VIP 的額外帳戶保護**」。

若要註冊網站的 VeriSign VIP Token：

1. 手動登入啓用 VeriSign VIP 的網站，或使用 Password Manager 登入。
2. 按一下顯示的 VeriSign VIP 氣球以建立此網站的登入。
3. 在「將登入新增至密碼管理員」對話方塊中，選取「**我需要這個網站的 VIP 安全性**」。

   這個選項只會針對可以使用 VeriSign VIP 安全性的網站顯示。當網站支援時，您還可以選擇自動填寫您的 VIP 安全碼以及您慣用的驗證方法。

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「**Password Manager**」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+win+h 開啓 Password Manager** — 開啓「**Password Manager 快速連結**」功能表的預設快速鍵是 ctrl+Windows 標誌鍵+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。

Credential Manager

您可以使用 Security Manager 認證來驗證您的身分。此電腦的管理員可以設定哪些認證可在您登入 Windows 帳戶、網站或程式時用來證明您的身分。

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。當您按一下「**我的登入**」底下的「**Credential Manager**」，就會顯示支援的認證、需求和目前的狀態，並且可能包含以下項目：

- 密碼
- SpareKey
- 指紋
- 智慧卡
- 臉孔

若要註冊或變更認證，按一下連結並依照畫面上的指示執行。

變更您的 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. 在 Security Manager Dashboard 中按一下「**Credential Manager**」，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。

設定您的 SpareKey

藉由回答先前由管理員定義之清單上的三個安全性問題，SpareKey 可讓您取得電腦的存取權（在受支援的平台上）。

在快速入門精靈的初始設定期間，HP ProtectTools Security Manager 會提示您設定個人的 SpareKey。

若要設定您的 SpareKey：

1. 在精靈的 SpareKey 頁面上，選取三個安全性問題，然後輸入每一個問題的答案。
2. 按「**下一步**」。

您可以在「**Credential Manager**」底下之 SpareKey 頁面上選取不同的問題或變更答案。

在設定 SpareKey 後，您可以從預先開機登入畫面或 Windows 歡迎使用畫面存取電腦。

註冊指紋

如果電腦有內建或連接的指紋讀取器，HP ProtectTools Security Manager 會在快速入門精靈的初始設定期間，提示您設定或「登錄」您的指紋。您也可以在 Security Manager Dashboard 中「**Credential Manager**」底下的「指紋」頁面註冊您的指紋。

1. 此時會顯示兩支手的輪廓。已註冊的手指會顯示爲綠色。按一下手指輪廓。

附註： 若要刪除先前註冊的指紋，請按一下該手指。

2. 選取要註冊的手指後，系統會提示您掃過指紋，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。對於其他手指，重複進行步驟 1 和 2。
4. 按「**下一步**」，然後按照螢幕指示進行。

注意： 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程式，則不會儲存您的變更。

設定智慧卡

管理員必須在智慧卡可用於驗證之前先初始化及註冊智慧卡。

正在初始化智慧卡

HP ProtectTools Security Manager 可以支援各種不同的智慧卡。做爲 PIN 碼使用的字元數及類型可能有所不同。智慧卡的製造商應該提供工具，以便安裝安全性憑證及管理 PIN 碼，這些都將由 HP ProtectTools 在其安全性演算法中使用。

附註： 必須安裝 ActivIdentity 軟體。

1. 將卡片插入讀取器。
2. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**ActivClient PIN 初始化工具**」。
3. 輸入 PIN 碼並加以確認。
4. 按「**下一步**」。

   智慧卡軟體將提供解除鎖定金鑰。當 PIN 碼輸入錯誤 5 次時，大多數的智慧卡將自行鎖定。金鑰係用來解除鎖定卡片。
5. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
6. 按一下「**認證**」，然後按一下「**智慧卡**」。
7. 按一下「**管理**」標籤。
8. 請確定已選取「**設定智慧卡**」。
9. 輸入您的 PIN，按一下「**套用**」，然後依照畫面上的指示執行。
10. 在成功初始化智慧卡之後，您將必須註冊智慧卡。

正在註冊智慧卡

在初始化智慧卡之後，管理員可以將卡片註冊爲 HP ProtectTools 管理主控台中的驗證方法：

1. 按一下「**集中管理**」底下的「**設定精靈**」。
2. 在「歡迎！」頁面上按「**下一步**」，然後輸入您的 Windows 密碼。
3. 在「SpareKey」頁面上，按一下「**跳過 SpareKey 設定**」（除非您想要更新 SpareKey 資訊）。
4. 在「啓用安全功能」頁面上按「**下一步**」。
5. 在「選擇您的認證」頁面上，確定已選取「**設定智慧卡**，然後按「**下一步**」。
6. 在「智慧卡」頁面上，輸入您的 PIN 碼，然後按「**下一步**」。
7. 按一下「**完成**」。

使用者也可以在 Security Manager 中註冊智慧卡。如需詳細資訊，請參閱 Security Manager for HP ProtectTools 軟體「說明」。

正在設定智慧卡

如果電腦已安裝或連接智慧卡讀取器，「智慧卡」頁面會顯示兩個標籤：

- **設定** — 設定電腦在取出智慧卡時自動鎖定。

  附註： 只有在登入 Windows 並將智慧卡當成驗證認證使用時，電腦才會鎖定。 取出未用於登入 Windows 的智慧卡，則不會鎖定電腦。

- **管理** — 選取下列其中一個選項：

  - **初始化智慧卡** — 備妥智慧卡以搭配 HP Protect Tools 使用。 如果先前已在 HP ProtectTools 之外初始化智慧卡（包含非對稱式金鑰配對及相關憑證），除非需要特定憑證的初始化，否則不需要再次初始化。
  - **變更智慧卡 PIN** — 讓您能夠變更搭配智慧卡使用的 PIN 碼。
  - **僅清除 HP ProtectTools 資料** — 僅清除智慧卡初始化期間建立的 HP ProtectTools 憑證。 不會清除智慧卡中其他任何資料。
  - **清除智慧卡中全部的資料** — 清除指定之智慧卡中全部的資料。 智慧卡無法再搭配 HP ProtectTools 或其他任何應用程式使用。

附註： 無法使用您的智慧卡不支援的功能。

▲ 按一下「**套用**」。

註冊臉孔登入的景像

如果電腦有內建或連接的網路攝影機，HP ProtectTools Security Manager 會在快速入門精靈的初始設定期間，提示您設定或「註冊」您的景像。您也可以在 Security Manager Dashboard 中「**Credential Manager**」底下的「臉孔登入」頁面註冊景像。

您必須註冊一個或多個景像以使用臉孔登入。在成功註冊之後，如果您因爲下列其中一個或多個條件已改變而無法順利進行登入時，您也可以註冊新的景像：

- 您的臉孔與上次註冊時相比，出現顯著的變化。
- 光線與您之前註冊的任一景像都不一樣。
- 上次註冊時，您有戴眼鏡（或沒有戴眼鏡）。

附註： 如果您在註冊景像時遇到困難，請試著將景像往網路攝影機移近。

若要從快速入門精靈註冊景像：

1. 在精靈的「臉孔」頁面上，按一下「**進階**」，然後設定其他的安全性。如需詳細資訊，請參閱位於第 34 頁的進階使用者設定。
2. 按一下「**確定**」。
3. 按一下「**開始**」。如果您已事先註冊景像，就按一下「**註冊新的景像**」。
4. 如果您未選取任何其他安全性選項，系統就會提示您選取其他安全性選項。 依照畫面上的指示執行，然後按「**下一步**」。 如需詳細資訊，請參閱位於第 34 頁的進階使用者設定。
5. 按一下「**相機**」圖示，然後依照畫面上的指示註冊您的景像。

   依照畫面上的指示執行，在擷取景像的同時務必看著您的影像。

6. 按「**下一步**」。
7. 按一下「**完成**」。

您也可以從 Security Manager Dashboard 註冊景像：

1. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 在「**我的登入**」底下，按一下「**Credential Manager**」，然後按一下「**臉孔**」。
3. 按一下「**進階**」，然後設定其他的安全性。如需詳細資訊，請參閱位於第 34 頁的進階使用者設定。
4. 按一下「**確定**」。
5. 按一下「**開始**」。如果您已事先註冊景像，就按一下「**註冊新的景像**」。
6. 如果您未選取任何其他安全性選項，系統就會提示您選取其他安全性選項。 依照畫面上的指示執行，然後按「**下一步**」。 如需詳細資訊，請參閱位於第 34 頁的進階使用者設定。
7. 按一下「**相機**」圖示，然後依照畫面上的指示註冊您的景像。

   依照畫面上的指示執行，在擷取景像的同時務必看著您的影像。

如需詳細資訊，請按一下藍色的「**?**」符號以參閱 Face Recognition 軟體「說明」。臉孔登入頁面右上角的圖示。

進階使用者設定

如果未選取其他安全性，這些選項也會顯示在「附加安全性」頁面上。

1. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 在「**我的登入**」底下，按一下「**Credential Manager**」，然後按一下「**臉孔**」。
3. 按一下「**進階**」，設定下列安全性選項：
   a. 「**安全性**」標籤 — 選取下列其中一個選項：
      - **無其他安全性** — 若您不希望爲臉孔登入新增其他安全性，請選取這個選項。
      - **針對其他安全性使用 PIN** — 選取這個選項，以要求利用使用者特定的 PIN 進行臉孔登入。
        - 按一下「**建立 PIN**」。
        - 輸入您的 Windows 密碼。
        - 輸入新的 PIN，然後重新輸入並確認新的 PIN。

          在建立 PIN 之後，您可以選取下列選項：「**變更**」、「**重設**」或「**移除 PIN**」。
      - **針對其他安全性使用 Bluetooth** — 選取這個選項，將具有 Bluetooth 功能的電話與 Face Recognition 進行配對。在 Windows 登入期間，一旦驗證過您的臉孔，Face Recognition

也會確認配對的 Bluetooth 電話是否存在。如果該電話存在（同時已啓用 Bluetooth），則您就會獲准登入 Windows。

- 請務必同時開啓電腦和電話的 Bluetooth 功能。

  如果具有 Bluetooth 功能的電話不存在，則系統會提示您啓用配對的 Bluetooth 電話，並重新啓動登入程序。30 秒後，Face Recognition 登入視窗就會暫停。若要起始登入程序，請按一下「**相機**」圖示。如果具備 Bluetooth 功能的電話不存在（同時已啓用 Bluetooth），您還可以使用一般的 Windows 密碼登入。

- 按一下「**新增**」。

- 當您的 Bluetooth 裝置顯示時，請加以選取，然後按「**下一步**」。

按一下「**確定**」。

b. 「**其他設定**」標籤 — 選取核取方塊以啓用下列一個或多個選項，或者清除核取方塊以停用選項。這些設定只會套用於目前的使用者。

- **針對臉孔辨識事件播放音效** — 在臉孔登入成功或失敗時播放音效。
- **登入失敗時提示更新景像** — 如果臉孔登入失敗，但密碼輸入成功，系統會提示您儲存一連串的影像，以便提升未來臉孔登入成功的機率。
- **登入失敗時提示註冊新景像** — 如果臉孔登入失敗，但密碼輸入成功，系統會提示您註冊新景像，以便提升未來臉孔登入成功的機率。

按一下「**確定**」。

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。

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. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 按一下 Dashboard 左上角的「身分識別卡」。
3. 按一下顯示用於此帳戶的 Windows 使用者名稱，輸入新名稱，然後按一下「**儲存**」。

若要變更顯示的圖片：

1. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 按一下 Dashboard 左上角的「身分識別卡」。
3. 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。在 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**」。

一般標籤

外觀 — 在工作列通知區域中顯示圖示

- 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。

指紋標籤

附註： 只有當電腦具有指紋讀取器並已安裝正確的驅動程式時，才能使用「**指紋**」標籤。

- **快速動作** — 使用「快速動作」可選取掃過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，請按一下「**（按鍵）+指紋**」選項，然後從功能表中選取其中一個可用的工作。

- **掃描指紋回應** — 只有在提供指紋讀取器時才會顯示。使用此設定可調整掃過指紋時出現的回應。
  - **啓用音效回應** — 掃過指紋後，Security Manager 會發出音訊回應，對於特定的程式事件播放不同的音效。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，也可以清除此選項以停用聲音回應。
  - **顯示掃描品質回應**

    若要顯示所有掃描（無論品質如何），請選取該核取方塊。

若只要顯示品質較佳的掃描，請清除該核取方塊。

備份和還原您的資料

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. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 在 Dashboard 左側面板中，按一下「**進階**」，然後按一下「**備份和還原**」。
3. 按一下「**備份資料**」。
4. 選取您要包含在備份中的模組。多數情況會選取所有的模組。
5. 驗證您的身分。
6. 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。
7. 輸入密碼以保護檔案。
8. 按一下「**完成**」。

若要還原資料：

1. 開啓 Security Manager Dashboard。如需詳細資訊，請參閱位於第 22 頁的開啓 Security Manager。
2. 在 Dashboard 左側面板中，按一下「**進階**」，然後按一下「**備份和還原**」。
3. 按一下「**還原資料**」。
4. 選取之前建立的儲存檔。在提供的欄位中輸入路徑，或按一下「**瀏覽**」。
5. 輸入用來保護檔案的密碼。
6. 選取您要還原資料的模組。多數情況會選取所有列出的模組。
7. 驗證您的 Windows 密碼。
8. 按一下「**完成**」。

5 Drive Encryption for HP ProtectTools（僅限特定機型）

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

HP ProtectTools Security Manager 設定精靈允許 Windows 管理員啓用 Drive Encryption、備份加密金鑰，以及選取或取消選取磁碟機。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：

- 選取 Drive Encryption 設定：
  - 啓用 TPM 密碼保護
  - 加密或解密使用軟體加密的個別磁碟機或分割區
  - 加密或解密使用硬體加密的個別自我加密磁碟機
  - 藉由停用睡眠或待命，確保隨時要求 Drive Encryption 預先開機驗證的方式，進一步加強安全性

附註： 僅能加密內建 SATA 和外接式 eSATA 硬碟。

- 建立備份金鑰
- 復原 Drive Encryption 金鑰
- 使用密碼、註冊指紋或智慧卡 PIN 碼啓用 Drive Encryption 預先開機驗證

開啓 Drive Encryption

管理員可以從 HP ProtectTools 管理主控台中存取 Drive Encryption。

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

一般工作

爲標準硬碟啓用 Drive Encryption

標準硬碟使用軟體加密進行加密。請依照下列步驟啓用 Drive Encryption：

1. 使用 HP ProtectTools Security Manager 設定精靈啓用 Drive Encryption。
2. 依照畫面上的指示執行，直到顯示「**啓用安全功能**」頁面後，再繼續以下的步驟 4。

－ 或 －

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**功能**」。
4. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。

附註： 如果沒有選取要加密的硬碟，則會啓用 Drive Encryption 預先開機驗證，但是不會將磁碟機加密。

5. 在「**要加密的磁碟機**」下方，選取在您要加密的硬碟核取方塊，然後按「**下一步**」。
6. 若要備份加密金鑰，請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。磁片、USB 隨身碟、Secure Digital (SD) 記憶卡或 MMC 都可以用來進行備份。

7. 在「**備份 Drive Encryption 金鑰**」下方，選取將要儲存加密金鑰的儲存裝置核取方塊。
8. 按「**下一步**」。

附註： 電腦將會重新啓動。

此時即已啓用 Drive Encryption。視磁碟機大小而定，磁碟機加密可能需要數小時。

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

爲自我加密磁碟機啓用 Drive Encryption

符合自我加密磁碟機管理之信任運算群組 OPAL 規格的自我加密磁碟機，可以使用軟體加密或硬體加密進行加密。請依照下列步驟，啓用自我加密磁碟機的 Drive Encryption：

1. 使用 HP ProtectTools Security Manager 設定精靈啓用 Drive Encryption。
2. 依照畫面上的指示執行，直到顯示「**啓用安全功能**」頁面後，再繼續以下「軟體加密」或「硬體加密」底下的步驟 4。

附註： 如果您的電腦沒有符合可進行自我加密磁碟機管理之信任運算群組 OPAL 規格的自我加密磁碟機，則無法使用硬體加密選項，將會依照預設使用軟體加密。

如果有同時使用自我加密磁碟機與標準硬碟的情況，則無法使用硬體加密選項，將會依照預設使用軟體加密。

－ 或 －

軟體加密

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**功能**」。
4. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。
5. 在「**要加密的磁碟機**」下方，選取在您要加密的硬碟核取方塊，然後按「**下一步**」。
6. 若要備份加密金鑰，請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。磁片、USB 隨身碟、Secure Digital (SD) 記憶卡或 MMC 都可以用來進行備份。

7. 在「**備份 Drive Encryption 金鑰**」下方，選取將要儲存加密金鑰的儲存裝置核取方塊。
8. 按一下「**套用**」。

附註： 電腦將會重新啟動。

此時即已啓用 Drive Encryption。視磁碟機大小而定，磁碟機加密可能需要數小時。

硬體加密

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**功能**」。
4. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。

附註： 如果只有顯示一部磁碟機，就會自動選取磁碟機核取方塊並且呈現灰色。

如果顯示一部以上的磁碟機，則自動選取這些磁碟機核取方塊，但不會呈現灰色。

除非至少選取了一部磁碟機，否則「**下一步**」按鈕就無法使用。

5. 確定已選取畫面底部的「**使用硬碟加密**」核取方塊。
6. 在「**要加密的磁碟機**」下方，選取在您要加密的硬碟核取方塊，然後按「**下一步**」。
7. 若要備份加密金鑰，請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。磁片、USB 隨身碟、Secure Digital (SD) 記憶卡或 MMC 都可以用來進行備份。

8. 在「**備份 Drive Encryption 金鑰**」下方，選取將要儲存加密金鑰的儲存裝置核取方塊。
9. 按一下「**套用**」。

附註： 電腦需要重新啟動。

此時即已啓用 Drive Encryption。磁碟機加密可能需要數分鐘。

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

停用 Drive Encryption

管理員可以使用 HP ProtectTools Security Manager 設定精靈停用 Drive Encryption。如需詳細資訊，請參閱 HP ProtectTools Security Manager 軟體「說明」。

▲ 依照畫面上的指示執行，直到顯示「**啓用安全功能**」頁面後，再繼續以下的步驟 4。

– 或 –

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**安全性**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**功能**」。
4. 清除「**Drive Encryption**」核取方塊，然後按「**下一步**」。

   隨即開始停用 Drive Encryption。

   附註： 如果已使用軟體加密，便會開始進行解密。視磁碟機大小而定，此作業可能需要數小時。當解密完成時，就會停用 Drive Encryption。

   如果已使用硬體加密，則磁碟機立即解密，這可能需要幾分鐘，然後才會停用 Drive Encryption。

   一旦停用磁碟機，就必須重新啓動電腦。

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： 在硬體加密的案例中，請確定已關閉電腦。如果電腦沒有關閉就接著重新啓動，則不會顯示 Drive Encryption 預先開機驗證畫面。

附註： 除非停用軟體或硬體加密，否則從睡眠或待命中喚醒時，會因爲有這種加密而不顯示 Drive Encryption 預先開機驗證。

從休眠中喚醒時，會顯示 Drive Encryption 預先開機驗證。

附註： 如果 Windows 管理員已在 HP ProtectTools Security Manager 中啓用預先開機安全性，您就可以立即在電腦開啓後登入電腦，而不是在 Drive Encryption 登入畫面上進行登入。

1. 按一下您的使用者名稱，然後輸入 Windows 密碼或智慧卡 PIN 碼，或是用已註冊的手指掃過。

   附註： 下列是支援的智慧卡：

智慧卡

- ActivIdentity 64K V2C 智慧卡
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB 金鑰 V3.0 ZFG-48001-A

PCMCIA 讀取器

- Express Card 54 SCR3340 內建讀取器
- SCR 201

- SCR 243（亦爲 HP 品牌）
- ActivCard
- Omnikey 4040
- Cisco

USB 讀取器

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP 智慧卡終端機

2. 按一下「**確定**」。

附註： 如果在 Drive Encryption 登入畫面使用復原金鑰登入，系統會提示您以密碼、智慧卡 PIN 碼或已註冊的手指在 Windows 登入畫面進行驗證。

藉由加密硬碟保護您的資料

強烈建議您使用 HP ProtectTools Security Manager 設定精靈，藉由加密硬碟保護您的資料：

1. 在左側窗格中，按一下「**Drive Encryption**」左邊的「**+**」圖示以顯示可用的選項。
2. 按一下「**設定**」。
3. 對於軟體加密的磁碟機，請選取要加密的磁碟機分割區。

附註： 這也適用於混合磁碟機案例，也就是標準硬碟與自我加密磁碟機同時都有一部或多部存在。

－ 或 －

▲ 對於硬體加密的磁碟機，請選取要加密的磁碟機。至少必須選取一部磁碟機。

顯示加密狀態

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

附註： 管理員可以使用 HP ProtectTools 管理主控台變更 Drive Encryption 狀態。

1. 開啓 HP ProtectTools Security Manager。
2. 在「**我的資料**」底下，按一下「**Drive Encryption**」。

在軟體加密案例中，「**磁碟機狀態**」下方會顯示下列其中一個狀態碼：

- 已啓用
- 已停用
- 未加密
- 已加密
- 加密
- 解密

在硬體加密案例中，「**磁碟機狀態**」下方會顯示下列狀態碼：

- 已加密

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）

管理員可以使用「Drive Encryption」下的「設定」頁面，檢視和變更 Drive Encryption 的狀態（啓用、非使用中或已啓用硬體加密），以及檢視電腦上所有硬碟的加密狀態。

附註： 硬體加密無法在「設定」頁面上加以變更。

- 如果狀態爲「已停用」，表示 Drive Encryption 尚未由 Windows 管理員啓用，無法保護硬碟。使用 HP ProtectTools Security Manager 設定精靈啓用 Drive Encryption。
- 如果狀態爲「已啓用」，表示已經啓用和設定 Drive Encryption。磁碟機處於下列其中一個狀態：

軟體加密

- 未加密
- 已加密
- 加密
- 解密

硬體加密

- 已加密

加密或解密個別磁碟機（僅限軟體加密）

管理員可以使用「設定」頁面加密電腦上的一部或多部硬碟，或是將已經加密的磁碟機解密。

1. 開啓 HP ProtectTools 管理主控台。
2. 在左側窗格中，按一下「**Drive Encryption**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**設定**」。
4. 在「**磁碟機狀態**」下方，選取或清除要加密或解密的每個硬碟旁的核取方塊，然後按一下「**套用**」。

附註： 當正在加密或解密磁碟機時，進度列會顯示在目前工作階段中完成程序的剩餘時間。

如果電腦在加密處理期間關機或起始睡眠/待命或休眠，接著又重新啓動，則進度列上的剩餘時間會重設至開頭，但實際的加密作業是從上次停止之處繼續進行。進度列（顯示爲百分比）和剩餘時間會更快速地改變以反映先前的進度。

附註： 不支援動態分割區。如果分割區顯示爲可用，但選取時卻無法進行加密，則此分割區是動態的。動態分割區是因爲在「磁碟管理」中壓縮分割區以建立新分割區而產生。

如果分割區將要轉換爲動態分割區，就會顯示警告。

備份與復原（管理員工作）

當 Drive Encryption 啓用時，管理員可以使用「加密金鑰備份」頁面，將加密金鑰備份至抽取式媒體，以及執行復原。

備份加密金鑰

管理員可以在抽取式儲存裝置上備份加密磁碟機的加密金鑰。

⚠ **注意：** 請妥善保管包含備份金鑰的儲存裝置，因爲如果您忘記密碼、遺失智慧卡或是未註冊手指，此裝置就是您唯一能用來存取硬碟的途徑。

1. 開啓 HP ProtectTools 管理主控台。
2. 在左側窗格中，按一下「**Drive Encryption**」左邊的「**+**」圖示以顯示可用的選項。
3. 按一下「**加密金鑰備份**」。
4. 插入要用來備份加密金鑰的儲存裝置。
5. 在「**磁碟機**」下方，選取要備份加密金鑰所在之裝置的核取方塊。
6. 按一下「**備份金鑰**」。
7. 閱讀所顯示頁面上的資訊，然後按「**下一步**」。此時便會將加密金鑰儲存到您選取的儲存裝置。

復原加密金鑰

管理員可以從之前儲存加密金鑰的抽取式儲存裝置中復原該加密金鑰：

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「Drive Encryption for HP ProtectTools」登入對話方塊開啓時，按一下「**選項**」。
4. 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。

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

Privacy Manager for HP ProtectTools 可讓您使用進階安全性（驗證）方法，在使用電子郵件或 Microsoft® Office 文件時驗證通訊的來源、完整性及安全性。

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
- 智慧卡
- Face Recognition

您可以在 Privacy Manager 中使用上述的任何安全登入法。

開啓 Privacy Manager

若要開啓 Privacy Manager：

- 若要存取 Microsoft Outlook 中 Outlook 特定功能，請在「**訊息**」標籤的「**隱私權**」群組中按一下「**安全地傳送**」。
- 若要存取 Microsoft Office 文件中的大部分功能，請在「**首頁**」標籤的「**隱私權**」群組中按一下「**簽署與加密**」。
- 若要存取其他功能，請存取 HP ProtectTools Security Manager Dashboard。
  - 依序按一下「**開始**」、「**所有程式**」、「**HP**」、「**HP ProtectTools Security Manager**」，然後按一下「**Privacy Manager**」。

    － 或 －

  - 按一下「**HP ProtectTools**」桌面小工具圖示。

    － 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，並且按一下「**Privacy Manager**」，然後按一下「**組態**」。

設定程序

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。

「憑證管理員」可讓您執行下列工作：

- 位於第 49 頁的申請 Privacy Manager 憑證
- 位於第 49 頁的取得預先指派的公司 Privacy Manager 憑證
- 位於第 51 頁的設定預設 Privacy Manager 憑證
- 位於第 50 頁的匯入協力廠商憑證
- 位於第 51 頁的檢視 Privacy Manager 憑證詳細資料
- 位於第 51 頁的更新 Privacy Manager 憑證
- 位於第 51 頁的設定預設 Privacy Manager 憑證
- 位於第 51 頁的刪除 Privacy Manager 憑證
- 位於第 52 頁的還原 Privacy Manager 憑證
- 位於第 52 頁的撤銷 Privacy Manager 憑證

申請 Privacy Manager 憑證

您必須先使用有效的電子郵件地址，在 Privacy Manager 中要求和安裝 Privacy Manager 憑證，才能使用 Privacy Manager 功能。此電子郵件地址必須在您要求 Privacy Manager 憑證的同一台電腦上設定爲 Microsoft Outlook 中的帳戶。

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下「**申請 Privacy Manager 憑證**」。
3. 在「歡迎」頁面中閱讀文字內容，然後按「**下一步**」。
4. 在「授權合約」頁面中，閱讀授權合約。
5. 確定已選取「**核取此處以接受此授權合約的條款**」旁的核取方塊，然後按「**下一步**」。
6. 在「您的憑證詳細資料」頁面中，輸入必要資訊，然後按「**下一步**」。
7. 在「已接受憑證要求」頁面中，按一下「**完成**」。

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

取得預先指派的公司 Privacy Manager 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**」。

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

若要安裝憑證，請參閱位於第 50 頁的設定 Privacy Manager 憑證。

設定 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，然後在 Outlook 2007 或 Outlook 2010 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「信任的連絡人」邀請程序，請依照畫面上的指示開始執行位於第 54 頁的使用 Microsoft Outlook 通訊錄新增信任的連絡人主題的步驟 2。

   － 或 －

   若您按「**取消**」，請參閱 位於第 52 頁的管理信任的連絡人以取得有關稍後新增「信任的連絡人」的詳細資訊。

匯入協力廠商憑證

您可以透過「憑證匯入精靈」將協力廠商憑證匯入 Privacy Manager。

若要使用此功能，必須在「**Privacy Manager**」底下的「設定」頁面啓用 HP ProtectTools 管理主控台中的「**允許使用協力廠商憑證**」。

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 選取「**憑證管理員**」標籤，然後按一下「**匯入憑證**」。

   如果不允許匯入憑證，則不會顯示此按鈕。
3. 選擇是否匯入已在此電腦上安裝的憑證或儲存爲 PFX（個人資訊交換/PKCS#12）檔的憑證，然後按「**下一步**」。
   - 若要匯入已在此電腦上安裝的憑證，請選取所需的憑證，然後按「**下一步**」。
   - 若要選取 PFX 憑證，請按一下「**瀏覽**」，並瀏覽至 PFX 檔的位置，然後按「**下一步**」。輸入 PFX 檔密碼，然後按「**下一步**」。
4. 匯入程序完成時，按「**下一步**」。
5. 出現可讓您備份匯入之憑證的選項。

   建議您將憑證備份至電腦硬碟以外的位置。

檢視 Privacy Manager 憑證詳細資料

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下「Privacy Manager 憑證」。
3. 按一下「**憑證詳細資料**」。
4. 檢視詳細資料完畢後，按一下「**確定**」。

更新 Privacy Manager 憑證

Privacy Manager 憑證即將過期時，將會通知您更新憑證：

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下「**更新憑證**」。
3. 依照畫面上的指示取得新的 Privacy Manager 憑證。

附註： Privacy Manager 憑證更新程序不會取代您舊有的 Privacy Manager 憑證。您必須取得新的 Privacy Manager 憑證，並使用位於第 49 頁的申請 Privacy Manager 憑證中相同的程序安裝憑證。

對於您公司使用 Microsoft Certificate Authority 簽發的公司憑證，CA 管理員必須使用與原始憑證相同的私密金鑰更新您的憑證，或者使用相同的私密金鑰簽發新憑證。

設定預設 Privacy Manager 憑證

Privacy Manager 只會顯示 Privacy Manager 憑證，即使在電腦上安裝其他憑證授權單位簽發的其他憑證也是如此。

如果電腦上有多個從 Privacy Manager 安裝的 Privacy Manager 憑證，您可以指定其中一個成爲預設憑證：

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下要當作預設憑證使用的 Privacy Manager 憑證，然後按一下「**設定爲預設**」。
3. 按一下「**確定**」。

附註： 您不需要使用預設的 Privacy Manager 憑證。您可以從多個 Privacy Manager 功能中選取要使用的任何 Privacy Manager 憑證。

刪除 Privacy Manager 憑證

如果刪除 Privacy Manager 憑證，則無法開啓任何檔案，或檢視以該憑證加密的任何資料。如果不慎刪除 Privacy Manager 憑證，您可以使用安裝憑證時建立的備份檔還原該憑證。如需詳細資訊，請參閱位於第 52 頁的還原 Privacy Manager 憑證。

若要刪除 Privacy Manager 憑證：

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下要刪除的 Privacy Manager 憑證，然後按一下「**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**」，然後按一下「**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，然後按一下「**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**」。

如需詳細資訊，請參閱位於第 50 頁的設定 Privacy Manager 憑證或位於第 61 頁的備份 Privacy Manager 憑證和信任的連絡人。

撤銷 Privacy Manager 憑證

如果您認爲 Privacy Manager 憑證的安全性受到危害，您可撤銷您自己的憑證。

附註： 被撤銷的 Privacy Manager 憑證並未被刪除。該憑證仍可用來檢視已加密的檔案。

1. 開啓 Privacy Manager，然後按一下「**憑證**」。
2. 按一下「**進階**」。
3. 按一下要撤銷的 Privacy Manager 憑證，然後按一下「**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. 然後，遵循畫面上的指示執行。

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. 您會收到「信任的連絡人」收件者所發出的電子郵件回應，然後按一下「**接受**」。

您可以將「信任的連絡人」電子郵件邀請傳送給個別收件者，也可以將邀請傳送給 Microsoft Outlook 通訊錄中所有的連絡人。

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」收件者必須在電腦上安裝 Privacy Manager 或替代用戶端。如需安裝替代用戶端的相關資訊，請存取 DigitalPersona 網站，網址爲 http://digitalpersona.com/privacymanager/download。

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： 若未取得 Privacy Manager 憑證，您會收到一項訊息通知您必須有 Privacy Manager 憑證才能傳送「信任的連絡人」申請。按一下「**確定**」以啓動「憑證申請精靈」。如需詳細資訊，請參閱位於第 49 頁的申請 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，然後按一下「**邀請我的 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： 若未取得 Privacy Manager 憑證，您會收到一項訊息通知您必須有 Privacy Manager 憑證才能傳送「信任的連絡人」申請。按一下「**確定**」以啓動「憑證申請精靈」。如需詳細資訊，請參閱位於第 49 頁的申請 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，然後按一下「**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，然後按一下「**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，然後按一下「**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

在 Microsoft Outlook 中使用 Privacy Manager

安裝 Privacy Manager 時，Microsoft Outlook 工具列會顯示「隱私權」按鈕，而各個 Microsoft Outlook 電子郵件訊息的工具列會顯示「安全地傳送」按鈕。按一下「**隱私權**」或「**安全地傳送**」旁邊的向下箭頭時，您可以從下列選項選擇：

- **簽署與傳送郵件**（僅限於「安全地傳送」按鈕）— 這個選項會將數位簽章新增至電子郵件，然後在您使用選擇的安全性登入法驗證時傳送電子郵件。
- **爲信任的連絡人密封並傳送訊息**（僅限於「安全地傳送」按鈕）— 這個選項會新增數位簽章，並且將電子郵件加密，然後在您使用選擇的安全性登入法驗證時傳送電子郵件。
- **邀請連絡人** — 這個選項可讓您傳送「信任的連絡人」邀請。如需詳細資訊，請參閱位於第 53 頁的新增信任的連絡人。
- **邀請 Outlook 連絡人** — 這個選項可用來傳送「信任的連絡人」邀請給 Microsoft Outlook 通訊錄中的所有連絡人。如需詳細資訊，請參閱位於第 54 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」選項可用來開啓 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 位於第 49 頁的管理 Privacy Manager 憑證、位於第 52 頁的管理信任的連絡人或 位於第 56 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「**電子郵件**」標籤。

   － 或 －

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

   － 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「**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「**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**」（Outlook 2003 的「**隱私權**」）旁邊的向下箭頭，然後按「**簽署與傳送**」。
4. 使用您選擇的安全登入法進行驗證。

密封與傳送電子郵件訊息

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**」（Outlook 2003 的「**隱私權**」）旁邊的向下箭頭，然後按「**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頭中。這個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

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 文件的工具列右邊。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** — 這個選項會將您的數位簽章新增至文件。
- **在簽署前新增簽章線**（僅限於 Microsoft Word 及 Microsoft Excel）— 依預設，簽署或加密 Microsoft Word 或 Microsoft Excel 文件時，會新增簽章線。若要關閉此選項，按一下「**新增簽章線**」即可移除核取標記。
- **加密文件** — 這個選項會新增您的數位簽章，並爲文件加密。
- **移除加密** — 此選項會從文件移除加密。
- **開啓 Privacy Manager 軟體** —「憑證」、「信任的連絡人」和「設定」選項可用來開啓 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 位於第 49 頁的管理 Privacy Manager 憑證、位於第 52 頁的管理信任的連絡人或 位於第 57 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「**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「**設定**」。
2. 選取您要設定的動作，再按一下「**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「**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「**確定**」。

如果您稍後決定要編輯此文件，請遵循下列步驟進行：

1. 按一下畫面左上角的「**Office**」按鈕。
2. 按一下「**準備**」，再按一下「**標示爲最終版本**」。
3. 當確認對話方塊開啓時，請按一下「**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 文件前新增簽章線

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，建立和儲存文件。
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「**在簽署前新增簽章線**」。

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

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

將建議的簽署者新增至 Microsoft Word 或 Microsoft Excel 文件

您可以指派建議的簽署者，以便將多個簽章線新增至文件。建議的簽署者是經過 Microsoft Word 或 Microsoft Excel 文件的擁有者指派，以將簽章線新增至文件的使用者。建議的簽署者可以是您本人或想要簽署您文件的其他人。例如，如果您準備的文件需要部門所有成員的簽署，您可以在文件的最末頁加入這些使用者的簽章線，並註明必須完成簽署的特定日期。

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「**Privacy Manager 簽章提供者**」。

   「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： 文件的擁有者可將建議的簽署者指派至擁有者自己的文件中。若要讓建議的簽署者能夠在簽章線顯示日期和/或職稱，則必須勾選「**在簽章線顯示簽署日期**」和/或「**在簽章線顯示簽署者職稱**」核取方塊。

8. 按一下「**確定**」。

新增建議的簽署者簽章線

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

您可以爲您自己和您「信任的連絡人」將 Microsoft Office 文件加密。加密文件並關閉文件時，您以及您從清單中選取的「信任的連絡人」必須進行驗證，才能開啓文件。

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」名稱，請按住 ctrl 鍵，然後按一下個別名稱。

5. 按一下「**確定**」。

如果您後來決定編輯文件，請依照位於第 59 頁的從 Microsoft Office 文件移除加密中的步驟進行。移除加密時，即可編輯文件。依照本章節的步驟再次爲文件加密。

從 Microsoft Office 文件移除加密

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

您可以將加密的 Microsoft Office 文件附加於電子郵件訊息，完全不需要簽署或爲電子郵件加密。若要這麼做，請建立含有已簽署或已加密文件的電子郵件，如同含有附件的一般電子郵件一般。

然而，爲了最佳安全性起見，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 文件之密封電子郵件，請遵循下列步驟進行：

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，請參閱位於第 57 頁的密封與傳送電子郵件訊息。

檢視已簽署的 Microsoft Office 文件

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

當開啓已簽署的 Microsoft Office 文件時，文件視窗底端的狀態列中會顯示「數位簽章」圖示。

1. 按一下「**數位簽章**」圖示，可切換顯示簽署此文件的所有使用者姓名以及簽署日期的「簽章」對話方塊顯示畫面。
2. 若要檢視每一個簽章的詳細資料，可用滑鼠右鍵按一下「簽章」對話方塊中的某個姓名，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。您也必須還原用來加密該檔案的 Privacy Manager 憑證。

如果您的憑證已遺失，必須還原用來爲檔案加密的 Privacy Manager 憑證，才能檢視加密的 Microsoft Office 文件。

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」。

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，然後按一下「**轉移**」。
2. 按一下「**備份**」。
3. 在「選取資料」頁面中，選取要加入轉移檔案的資料類別，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「轉移檔案已儲存」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，然後按一下「**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（由您的管理員自訂）。可以啓用或停用下列一項或多項功能：

- **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 Microsoft Outlook 中個別啓用或停用。

7 HP ProtectTools File Sanitizer

File Sanitizer 可讓您安全地拆解電腦上的資產（例如：個人資訊或檔案、過去的資料或 Web 相關資料或其他資料元件），以及定期清理硬碟上的已刪除資產。

附註： 此版本的 File Sanitizer 僅支援電腦硬碟。

拆解

拆解和標準 Windows® 刪除不同（也就是 File Sanitizer 中的單純刪除）。當您使用 File Sanitizer 拆解資產時，檔案會以無意義資料進行覆寫，使其無法擷取原始資產。Windows 單純刪除可能會將檔案（或資產）完整地留在硬碟上，或是處於以科學鑑定方法就可能復原的狀態。

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。藉由指定拆解週期數、哪些資產需要拆解、哪些資產拆解前需要先確認，以及哪些資產排除在拆解外，您也可以自訂拆解設定檔。如需詳細資訊，請參閱位於第 67 頁的選取或建立拆解設定檔。

您可以設定自動拆解排程，或者使用工作列最右邊通知區域中的「**HP ProtectTools**」圖示，手動啓用拆解。如需詳細資訊，請參閱位於第 66 頁的設定拆解排程、位於第 70 頁的手動拆解一個資產或位於第 70 頁的手動拆解所有選取的項目。

附註： .dll 檔案只有在已經移至「資源回收筒」時才會進行拆解，並從系統中移除。

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： 針對藉由選取 File Sanitizer 中「**單純刪除設定**」、將資產移至 Windows 資源回收筒或手動刪除資產所刪除的資產，可不定時執行「可用空間清理」功能。可用空間清理並未針對已拆解的資產提供額外的安全性。

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域中的「**HP ProtectTools**」圖示，手動啓用可用空間清理功能。如需詳細資訊，請參閱位於第 66 頁的設定可用空間清理排程或位於第 70 頁的手動啓用可用空間清理。

開啓 File Sanitizer

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

－ 或 －

▲ 按兩下桌面上的「**File Sanitizer**」圖示。

－ 或 －

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

設定程序

設定拆解排程

您可以選取預先定義的拆解設定檔，或建立您專用的拆解設定檔。如需詳細資訊，請參閱位於第 67 頁的選取或建立拆解設定檔。您也可以隨時以手動方式拆解資產。如需詳細資訊，請參閱位於第 69 頁的使用按鍵順序以起始拆解。

附註： 在特定時間開始已排程的工作。如果系統在排定的時間處於關機或睡眠/待命狀態，則 File Sanitizer 將不會嘗試重新啓動該工作。

1. 開啓 File Sanitizer，然後按一下「**拆解**」。
2. 選取一個或多個拆解選項：
   - **Windows 關機** — 在 Windows 關閉時拆解所有選定的資產。

     附註： 關機時會開啓對話方塊，詢問您是否要繼續拆解選定的資產，或是要略過此程序。

     按一下「**是**」略過拆解程序，或按一下「**否**」繼續進行拆解。
   - **Web 瀏覽器開啓** — 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** — 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** — 可讓您指定按鍵順序以起始拆解。如需詳細資訊，請參閱位於第 69 頁的使用按鍵順序以起始拆解。

附註： .dll 檔案只有在已經移至「資源回收筒」時才會進行拆解，並從系統中移除。

3. 若要排定未來拆解選定資產的時程，請選取「**啓用排程器**」核取方塊，輸入您的 Windows 密碼，然後選取日期和時間。
4. 按一下「**套用**」。

設定可用空間清理排程

針對藉由選取 File Sanitizer 中「**單純刪除設定**」、將資產移至 Windows 資源回收筒或手動刪除資產所刪除的資產，可不定時執行「可用空間清理」功能。可用空間清理並未針對已拆解的資產提供額外的安全性。

附註： 在特定時間開始已排程的工作。如果系統在排定的時間處於關機或睡眠/待命狀態，則 File Sanitizer 將不會嘗試重新啓動該工作。

1. 開啓 File Sanitizer，然後按一下「**清理**」。
2. 若要排定未來清理硬碟上已刪除之資產的時程，請選取「**啓用排程器**」核取方塊，輸入您的 Windows 密碼，然後選取日期和時間。
3. 按一下「**套用**」。

附註： 可用空間清理作業會耗費大量的時間。雖然可用空間清理作業是在背景中執行，不過增加處理器的使用率可能會影響電腦效能。

選取或建立拆解設定檔

藉由選取預先定義的設定檔或建立專用的設定檔，您可以指定清除方法，並選取要拆解的資產。

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時，會自動選取預先定義的清除方法和資產清單。您也可以檢視選取用來進行拆解之預先定義的資產清單。

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：
   - **高安全性**
   - **中安全性**
   - **低安全性**
3. 若要檢視選取用來進行拆解的資產，請按一下「**檢視詳細資料**」。
   a. **將會拆解選取的項目，並且顯示確認訊息。將會拆解未選取的項目，但不顯示確認訊息。**— 選取核取方塊以在拆解項目前顯示確認訊息，或是清除核取方塊以在不顯示確認訊息的情況下拆解項目。

   附註： 縱使已針對資產清除核取方塊，仍會拆解資產。

   b. 按一下「**套用**」。
4. 按一下「**套用**」。

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，然後依序按一下「**設定**」、「**進階安全性設定**」、「**檢視詳細資料**」。
2. 選取拆解週期數目。

附註： 將會針對每一個資產執行選取的拆解週期數目。例如，如果選擇 3 個拆解週期，則隱匿資料的演算法將會分別執行 3 次。如果選擇較高的安全性拆解週期，則拆解可能會耗費大量的時間。然而，您指定的拆解週期數目越高，資料就越不容易被擷取。

3. 若要選取要拆解的資產：
   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或資料夾的路徑。
   c. 按一下「**開啓**」，然後按一下「**確定**」。
   d. 在「**可用的拆解選項**」底下，按一下自訂資產，然後按一下「**新增**」。

   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. **將會拆解選取的項目，並且顯示確認訊息。將會拆解未選取的項目，但不顯示確認訊息。**— 選取核取方塊以在拆解項目前顯示確認訊息，或是清除核取方塊以在不顯示確認訊息的情況下拆解項目。

附註： 縱使已針對資產清除核取方塊，仍會拆解資產。

若要從可用的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：

   a. 在「**請勿拆解下列項目**」底下，按一下「**新增**」，然後瀏覽或輸入檔案或資料夾的路徑。

   b. 按一下「**開啓**」，然後按一下「**確定**」。

   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. 按一下「**套用**」。

自訂單純刪除設定檔

單純刪除僅執行標準資產刪除而不進行拆解。藉由指定要包含哪些資產、哪些資產刪除前要先確認以及要排除哪些資產，您就可以自訂單純刪除設定檔。

附註： 如果選取「**單純刪除設定**」，可針對手動刪除的資產不定時執行「可用空間清理」功能，或可使用 Windows「資源回收筒」執行該功能。

1. 開啓 File Sanitizer，依序按一下「**設定**」、「**單純刪除設定**」、「**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**」，接著瀏覽或輸入檔案或資料夾的路徑，然後按一下「**確定**」。

   c. 按一下自訂資產，然後按一下「**新增**」。

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

3. **將會拆解選取的項目，並且顯示確認訊息。將會拆解未選取的項目，但不顯示確認訊息。** — 選取核取方塊以在拆解項目前顯示確認訊息，或是清除核取方塊以在不顯示確認訊息的情況下拆解項目。

附註： 縱使已針對資產清除核取方塊，仍會拆解資產。

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

4. 若要保護資產免於自動刪除：

   a. 在「**請勿刪除下列項目**」底下，按一下「**新增**」，然後瀏覽或輸入檔案或資料夾的路徑。

   b. 按一下「**開啓**」，然後按一下「**確定**」。

   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. 按一下「**套用**」。

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 位於第 69 頁的使用按鍵順序以起始拆解。
- 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 位於第 69 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 位於第 70 頁的手動拆解一個資產或位於第 70 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 位於第 70 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 位於第 71 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 位於第 71 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。

使用按鍵順序以起始拆解

1. 開啓 File Sanitizer，然後按一下「**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**」。

手動拆解一個資產

⚠ **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域中的「**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，然後按一下「**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域中的「**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，然後按一下「**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域中的「**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，然後按一下「**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正在進行時，工作列最右邊的通知區域中的 HP ProtectTools Security Manager 圖示上方就會顯示訊息。該訊息會提供有關拆解或可用空間清理程序的詳細資料（完成百分比），並提供中止該作業的選項。

▲ 若要取消作業，請按一下該訊息，然後按一下「**停止**」。

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。

已經爲拆解作業建立一個記錄檔，又爲可用空間清理作業建立另一個記錄檔。兩個記錄檔都儲存在硬碟上：

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

針對 64 位元系統，記錄檔會儲存在硬碟上：

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer**[Username]**_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer**[Username]**_DiskBleachLog.txt

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

HP ProtectTools Device Access Manager 會藉由停用資料傳輸裝置來控制資料的存取。

附註： 部分使用者介面/輸入裝置（如滑鼠、鍵盤、觸控板和指紋讀取器），並非由 Device Access Manager 所控制。如需詳細資訊，請參閱位於第 82 頁的未受管理的裝置類別。

Windows® 作業系統管理員可使用 HP ProtectTools Device Access Manager，控制對系統裝置的存取，並防範未經授權的存取：

- 裝置設定檔是針對各個使用者建立的檔案，用來定義允許或拒絕使用者存取的裝置。
- 及時驗證 (JITA) 可讓預先定義的使用者驗證本身，以便存取未經驗證而遭到拒絕存取的裝置。
- 藉由將管理員和受信任的使用者加入「裝置管理員」群組，就可以排除由 Device Access Manager 對他們所施加的裝置存取限制。藉由使用「進階設定」可管理此群組的成員資格。
- 可根據群組成員資格或針對個別使用者，授予或拒絕裝置存取權。
- 對於 CD-ROM 光碟機和 DVD 光碟機之類的裝置類別，可分別允許或拒絕讀取權限和寫入權限。

開啓 Device Access Manager

1. 以管理員身分登入。
2. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
3. 在左側窗格中，按一下「**Device Access Manager**」。

使用者可以使用 HP ProtectTools Security Manager 檢視 HP ProtectTools Device Access Manager 原則。此主控台提供唯讀檢視。

設定程序

設定裝置存取

HP ProtectTools Device Access Manager 提供四種檢視：

- **簡易組態** — 根據「裝置管理員」群組中的成員資格，允許或拒絕對裝置類別的存取。
- **裝置類別組態** — 允許或拒絕對各類裝置或對特定使用者或群組之特定裝置的存取。
- **JITA 組態** — 設定及時驗證 (JITA)，允許選取的使用者藉由驗證本身來存取 DVD/CD-ROM 光碟機或抽取式媒體。
- **進階設定** — 設定 Device Access Manager 不會禁止存取的磁碟機代號清單，例如 C 或系統磁碟機。「裝置管理員」群組中的成員資格也可以透過這個檢視進行管理。

簡易組態

管理員可使用「**簡易組態**」檢視，以允許或拒絕所有非裝置管理員存取下列裝置類別：

- 所有抽取式媒體（磁碟及 USB 快閃磁碟機等）
- 所有 DVD/CD-ROM 光碟機
- 所有序列埠及並列埠
- 所有 Bluetooth® 裝置
- 所有數據機裝置
- 所有 PCMCIA/ExpressCard 裝置
- 所有 1394 裝置

若要允許或拒絕所有非裝置管理員對某個裝置類別的存取，請依照下列步驟執行：

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. 若要拒絕存取，請在右側窗格中，選取裝置類別或特定裝置的核取方塊。清除核取方塊可允許存取該裝置類別或特定裝置。

   如果核取方塊呈現灰色，表示已從「**裝置類別組態**」檢視內變更影響存取狀況的值。若要重設爲原廠設定，請按一下「**裝置類別組態**」檢視中的「**重設**」。
3. 按一下「**套用**」。

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

啓動背景服務

第一次定義及套用新原則時，「HP ProtectTools 裝置鎖定/稽核」背景服務會自動啓動，而且該服務設定爲在系統啓動時自動啓動。

附註： 首先必須定義裝置設定檔，背景服務提示才會顯示。

管理員也可以啟動或停止此服務：

1. 在 Windows 7 中，依序按一下「**開始**」、「**控制台**」以及「**系統及安全性**」。

   - 或 -

   在 Windows Vista® 中，依序按一下「**開始**」、「**控制台**」以及「**系統及維護**」。

   - 或 -

   在 Windows XP 中，依序按一下「**開始**」、「**控制台**」以及「**效能及維護**」。

2. 按一下「**系統管理工具**」，然後按一下「**服務**」。
3. 選取「**HP ProtectTools 裝置鎖定/稽核**」服務。
4. 若要啟動服務，請按一下「**開始**」。

   - 或 -

   服務執行中若要停止，請按一下「**停止**」。

停止「裝置鎖定/稽核」服務不會停止裝置鎖定。有兩項元件可強制進行裝置鎖定：

- 「裝置鎖定/稽核」服務
- DAMDrv.sys 驅動程式

啟動服務會啓動裝置驅動程式，但是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，請開啓命令提示字元視窗，然後輸入 sc query damdrv。

裝置類別組態

管理員可以檢視和修改被允許或拒絕存取裝置或特定裝置之類別的使用者及群組清單。

「**裝置類別組態**」檢視具有下列部分：

- **裝置清單** — 顯示系統上目前或先前可能已安裝的所有裝置類別或裝置。
  - 裝置類別通常會受到防護。選取的使用者或群組就能夠存取裝置類別中任何的裝置。
  - 特定裝置也會受到防護。
- **使用者清單** — 顯示被允許或拒絕存取選取的裝置或特定裝置的所有使用者及群組。
  - 可針對特定使用者或使用者爲其中成員的群組建立「使用者清單」項目。
  - 如果無法使用「使用者清單」中的使用者或群組項目，則會從「使用者清單」的裝置類別或從「類別」資料夾繼承設定。
  - 分別允許或拒絕讀取及寫入的權限，可以進一步控制 CD-ROM 光碟機及 DVD 光碟機之類的某些裝置類別。

    對於其他裝置及類別，則可繼承讀取及寫入權限。例如，可從較高類別繼承讀取權限，但是可特別針對某個使用者或群組拒絕寫入權限。

    附註： 如果「**讀取**」核取方塊遭到清除，則存取控制項目不會影響裝置的讀取權限，但是不會拒絕讀取權限。

附註： 「管理員」群組無法加入至「使用者清單」。反而會使用「裝置管理員」群組。

範例 1 — 如果拒絕某個使用者或群組寫入裝置或裝置類別：

只針對裝置階層中此裝置下的裝置，將寫入權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

範例 2 — 如果允許某個使用者或群組寫入裝置或裝置類別：

只針對相同裝置或裝置階層中此裝置下的裝置，拒絕將寫入權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

範例 3 — 如果允許某個使用者或群組讀取裝置或裝置類別：

只針對相同裝置或裝置階層中此裝置下的裝置，拒絕將讀取權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

範例 4 — 如果拒絕某個使用者或群組讀取裝置或裝置類別：

只針對裝置階層中此裝置下的裝置，將讀取權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

範例 5 — 如果允許某個使用者或群組讀取及寫入裝置或裝置類別：

只針對相同裝置或裝置階層中此裝置下的裝置，拒絕將寫入權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

範例 6 — 如果拒絕某個使用者或群組讀取及寫入裝置或裝置類別：

只針對裝置階層中此裝置下的裝置，將讀取權限或讀取及寫入權限授予同一位使用者、同一個群組或同一個群組的成員。

拒絕使用者或群組的存取

若要避免使用者或群組存取裝置或裝置類別：

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**」下方，按一下要拒絕存取的使用者或群組，然後按一下「**拒絕**」。
4. 按一下「**套用**」。

附註： 在使用者的同一個裝置層級設定拒絕及允許設定時，拒絕存取的優先順序會高於允許存取。

允許使用者或群組的存取

若要授予使用者或群組存取裝置或裝置類別的權限：

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. 按一下要加入至可用使用者及群組清單的使用者或群組，然後按一下「**確定**」。
6. 再次按一下「**確定**」。
7. 按一下「**允許**」即可將存取權授予此使用者。
8. 按一下「**套用**」。

允許群組某個使用者存取裝置類別

若要在拒絕存取使用者群組所有其他成員時，允許其中某個使用者存取裝置類別：

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. 瀏覽至所需類別下的資料夾，然後新增特定的使用者。
5. 按一下「**允許**」即可將存取權授予此使用者。
6. 按一下「**套用**」。

允許群組某個使用者存取特定裝置

管理員可以在拒絕該使用者群組所有成員存取類別中所有裝置的同時，允許存取某個特定裝置：

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，按一下要設定的裝置類別，然後瀏覽至該類別下的資料夾。

3. 在「**使用者/群組**」下，按一下要授予存取權的群組旁邊的「**允許**」。
4. 按一下要拒絕存取的群組旁邊的「**拒絕**」。
5. 瀏覽至允許裝置清單中的使用者存取的特定裝置。
6. 按一下「**新增**」。

   「選取使用者或群組」對話方塊隨即開啓。
7. 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。
8. 按一下要允取存取的使用者，然後按一下「**確定**」。
9. 按一下「**允許**」即可將存取權授予此使用者。
10. 按一下「**套用**」。

移除使用者或群組的設定

若要移除使用者或群組存取裝置或裝置類別的權限，請依照下列步驟執行：

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「**套用**」。

重設組態

⚠ **注意：** 重設組態會捨棄已設定的所有裝置組態變更，並且將所有設定回復爲原廠設定值。

若要將組態設定重設爲原廠設定：

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**」。
3. 按一下「**是**」以確認要求。
4. 按一下「**套用**」。

JITA 組態

JITA 組態允許管理員檢視及修改已允許使用及時驗證 (JITA) 存取裝置的使用者及群組清單。

啓用 JITA 的使用者，將可存取「**裝置類別組態**」或「**簡易組態**」中所建立之原則已受到限制的某些裝置。

- **案例** — 設定爲拒絕所有非裝置管理員存取 DVD/CD-ROM 光碟機的「簡易組態」原則。
- **結果** — 在嘗試存取 DVD/CD-ROM 光碟機時，啓用 JITA 的使用者和未啓用 JITA 的使用者一樣，都收到相同的「拒絕存取」訊息。接者會顯示氣球訊息，詢問使用者是否要進行 JITA 存取。如果按一下氣球，就會開啓「驗證使用者」對話方塊。當使用者成功輸入認證時，就會授予存取 DVD/CD-ROM 光碟機的權限。

JITA 期間可授權爲數分鐘或 0 分鐘的時間。O 分鐘的 JITA 期間將不會過期。使用者可以在從驗證起到登出系統爲止的期間存取裝置。

若設定爲如此，JITA 期間也可以延長。在此案例中，在 JITA 即將過期前的 1 分鐘，使用者可以按一下提示以延長其存取權限，無需重新驗證。

無論給予使用者有限或無限的 JITA 期間，當使用者登出系統或另一位使用者登入系統，JITA 期間就會過期。下次使用者登入並嘗試存取啓用 JITA 的裝置時，就會顯示輸入認證的提示。

下列裝置類別可使用 JITA：

- DVD/CD-ROM 光碟機
- 抽取式媒體

爲使用者或群組建立 JITA

管理員可允許使用者或群組使用及時驗證存取裝置。

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「**JITA 組態**」。
2. 在裝置的下拉式功能表中，選取「**抽取式媒體**」或「**DVD/CD-ROM 光碟機**」。
3. 按一下「**+**」以新增使用者或群組至 JITA 組態。
4. 選取「**已啓用**」核取方塊。
5. 將 JITA 期間設定爲所需的時間。
6. 按一下「**套用**」。

使用者必須先登出系統然後再登入系統以套用新的 JITA 設定。

爲使用者或群組建立可延伸的 JITA

管理員可允許使用者或群組使用可讓使用者在過期前加以延伸之及時驗證存取裝置。

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「**JITA 組態**」。
2. 在裝置的下拉式功能表中，選取「**抽取式媒體**」或「**DVD/CD-ROM 光碟機**」。
3. 按一下「**+**」以新增使用者或群組至 JITA 組態。
4. 選取「**已啓用**」核取方塊。
5. 將 JITA 期間設定爲所需的時間。

6. 選取「**可延伸**」核取方塊。
7. 按一下「**套用**」。

使用者必須先登出系統然後再登入系統以套用新的 JITA 設定。

針對使用者或群組停用 JITA

管理員可讓使用者或群組無法使用及時驗證存取裝置。

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「**JITA 組態**」。
2. 在裝置的下拉式功能表中，選取「**抽取式媒體**」或「**DVD/CD-ROM 光碟機**」。
3. 選取您要停用其 JITA 的使用者或群組。
4. 清除「**已啓用**」核取方塊。
5. 按一下「**套用**」。

當使用者登入並嘗試存取裝置時，存取遭拒。

進階設定

「進階設定」提供下列功能：

- 「裝置管理員」群組的管理
- Device Access Manager 永遠不會拒絕存取之磁碟機代號的管理。

使用「裝置管理員」群組，從 Device Access Manager 原則所施加的限制中排除受信任的使用者（與裝置存取相關）。受信任的使用者通常包括系統管理員。如需詳細資訊，請參閱位於第 81 頁的裝置管理員群組。

「**進階設定**」檢視也可讓管理員設定 Device Access Manager 不會針對任何使用者限制存取的磁碟機代號清單。

附註： 設定磁碟機代號清單時，Device Access Manager 背景服務必須在執行中。

若要啟動這些服務：

1. 套用「簡易組態」原則，例如拒絕所有非裝置管理員存取抽取式媒體。

   - 或 -

   以管理員權限開啟命令提示字元視窗，然後輸入以下內容：

   sc start flcdlock

   按下 enter 鍵。

2. 當服務啟動時，磁碟機清單即可進行編輯。輸入您不想讓 Device Access Manager 控制之裝置的磁碟機代號。

   顯示實體硬碟或分割區的磁碟機代號。

附註： 無論系統磁碟機（通常是 C）是否在清單中，任何使用者存取系統磁碟機都不會遭到拒絕。

裝置管理員群組

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

使用「裝置管理員」群組，從 Device Access Manager 原則所施加的限制中排除受信任的使用者（與裝置存取相關）。受信任的使用者通常包括系統管理員。

附註： 將使用者加入至「裝置管理員」群組不會自動允許使用者存取裝置。在「**裝置類別組態**」檢視中，如果「使用者」群組存取裝置遭到拒絕，則「裝置管理員」群組就必須被授予權限以供群組成員取得裝置存取權。不過，「**簡易組態**」檢視可用於拒絕所有非「裝置管理員」群組之成員存取裝置類別。

若要新增使用者至「裝置管理員」群組：

1. 在「**進階設定**」檢視中，按一下「**+**」。
2. 輸入受信任使用者的使用者名稱。
3. 按一下「**確定**」。
4. 按一下「**套用**」。

管理此群組成員資格的其他方式包括：

- 對於 Window 7 Professional 或 Windows Vista，可使用標準的「本機使用者和群組」Microsoft Management Console (MMC) 嵌入式管理單元將使用者加入至此群組。
- 針對 Windows 7、Windows Vista 或 Windows XP 家用版，可從具有管理員權限的帳號在命令提示字元視窗中輸入下列內容：

  net localgroup “Device Administrators” username /add

  在這個命令中，“username” 是您要加入此群組之使用者的使用者名稱。

eSATA 支援

爲了讓 Device Access Manager 控制 eSATA 裝置，必須要設定下列項目：

1. 系統啓動時必須連接磁碟機。
2. 使用「**進階設定**」檢視，確認 eSATA 磁碟機代號並未包含在 Device Access Manager 不會拒絕存取的磁碟機清單中。若 eSATA 磁碟機代號列在清單中，請刪除該磁碟機代號，然後按一下「**套用**」。
3. 藉由使用「**簡易組態**」檢視或「**裝置類別組態**」檢視，即可使用抽取式媒體裝置類別控制裝置。

未受管理的裝置類別

HP ProtectTools Device Access Manager 未管理下列裝置類別：

- 輸出/輸入裝置
  - 生物測定裝置
  - 滑鼠
  - 鍵盤
  - 印表機
  - 隨插即用 (PnP) 印表機
  - 印表機升級
  - 紅外線使用者介面裝置
  - 智慧卡讀取器
  - 多重連接埠序列
  - 磁碟機
  - 軟碟控制器 (FDC)

- 硬碟控制器 (HDC)
- 使用者介面裝置 (HID) 類別

- 電源
  - 電池
  - 進階電源管理 (APM) 支援
- 其他
  - 電腦
  - 解碼器
  - 顯示器
  - 處理器
  - 系統
  - 未知
  - 磁碟區
  - 磁碟區快照
  - 安全裝置
  - 安全加速器
  - Intel® 統一顯示驅動程式
  - 媒體驅動程式
  - 媒體交換器
  - 多功能
  - Legacard
  - 網路用戶端
  - 網路服務
  - 網路傳輸
  - SCSI 介面卡

9 竊盜追失

Computrace for HP ProtectTools（另外購買）可讓您在遠端監控、管理和追蹤電腦。

一旦啓用 Computrace for HP ProtectTools 之後，就要從 Absolute Software 客戶中心進行設定。管理員可以從此客戶中心設定 Computrace for HP ProtectTools，以監控或管理電腦。如果系統錯置或遭竊，客戶中心可以協助地方當局尋找並追回電腦。Computrace 一經設定，即使硬碟已清除或更換，仍然可以繼續運作。

若要啓用 Computrace for HP ProtectTools：

1. 連線到網際網路。
2. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools Security Manager**」。
3. 在 Security Manager 的左側窗格中，按一下「**竊盜復原**」。
4. 若要啓動 Computrace 啓動精靈，請按一下「**立即啓用**」。
5. 輸入您的連絡資訊及信用卡付款資訊，或輸入預先購買的產品金鑰。

啓動精靈會安全處理交易並在 Absolute Software 客戶中心網站上設立您的使用者帳戶。完成後，您會收到包含您的客戶中心帳戶資訊的確認電子郵件。

如果您先前已經執行過 Computrace 啓動精靈，且擁有客戶中心使用者帳戶，則您可以連絡您的 HP 帳戶代表購買額外授權。

若要登入客戶中心：

1. 移至 https://cc.absolute.com/。
2. 在「**登入 ID**」和「**密碼**」欄位中，輸入您在確認電子郵件中收到的認證，然後按一下「**登入**」。

使用客戶中心能讓您：

- 監控您的電腦。
- 保護您的遠端資料。
- 回報任何受 Computrace 保護的失竊電腦。

▲ 如需 Computrace for HP ProtectTools 的詳細資訊，請按一下「**瞭解更多資訊**」。

10 Embedded Security for HP ProtectTools（僅限特定機型）

附註： 您必須在電腦中安裝整合的信任平台模組 (TPM) 嵌入式安全晶片，才能使用 Embedded Security for ProtectTools。

Embedded Security for HP ProtectTools 可防止他人未獲授權地存取使用者資料或認證。這個軟體模組提供下列安全性功能：

- 增強的 Microsoft® 加密檔案系統 (EFS) 檔案和資料夾加密
- 建立 Personal Secure Drive (PSD) 來保護使用者資料
- 資料管理功能，例如備份與還原重要的階層
- 使用 Embedded Security 軟體時，針對受保護的數位憑證作業，提供支援協力廠商應用程式（例如 Microsoft Outlook 與 Internet Explorer）的支援

TPM 嵌入式安全晶片可以增強和啓用其他 HP ProtectTools Security Manager 安全功能。例如，當使用者登入 Windows 時，Credential Manager for HP ProtectTools 可以使用嵌入式晶片做爲驗證因子。

設定程序

⚠ **注意：** 爲降低安全性風險，強烈建議 IT 管理員立即初始化嵌入式安全晶片。若未初始化嵌入式安全晶片，可能導致未經授權使用者、電腦蠕蟲或病毒取得電腦的擁有權並掌控擁有者的工作，例如：處理緊急復原封存與設定使用者存取設定。

請依照下列各節中的步驟，啓用和初始化嵌入式安全晶片。

在 Computer Setup 中啓用嵌入式安全晶片

嵌入式安全晶片必須是在快速初始化精靈或是在 Computer Setup 公用程式中所啓用。

若要在 Computer Setup 中啓用嵌入式安全晶片：

1. 啓動或重新啓動電腦以開啓 Computer Setup，然後在螢幕左下角顯示「F10 = ROM 的設定 (F10 = ROM Based Setup)」訊息時，按下 f10 鍵。
2. 若尚未設定管理員密碼，請使用方向鍵依序選取「**安全性 (Security)**」、「**設定密碼 (Setup password)**，然後按下 enter 鍵。
3. 在「**新密碼 (New Password)**」與「**確認新密碼 (Verify New Password)**」方塊中鍵入您的密碼，接著按下 f10 鍵。
4. 在「**安全性 (Security)**」功能表中，使用方向鍵來選擇「**TPM 嵌入式安全性 (TPM Embedded Security)**」，再按下 enter 鍵。
5. 在「**Embedded Security**」下，如果有隱藏的裝置，請選擇「**可用 (Available)**」。
6. 選取「**嵌入式安全裝置狀態 (Embedded security device state)**」，然後將設定變更爲「**啓用 (Enable)**」。
7. 按下 f10 鍵，即可接受對「Embedded Security」組態所做的變更。
8. 若要儲存您的偏好設定並結束 Computer Setup，請使用方向鍵依序選取「**檔案 (File)**」、「**儲存變更並結束 (Save Changes and Exit)**」，然後依照畫面上的指示執行。

初始化嵌入式安全晶片

在 Embedded Security 的初始化過程中，您將執行下列工作：

- 設定嵌入式安全晶片的擁有者密碼，以保護嵌入式安全晶片全部的擁有者功能之存取。
- 設定緊急復原封存，它是保護的儲存區域，允許重新加密所有使用者的基本使用者金鑰。

若要初始化嵌入式安全晶片：

1. 在工作列最右邊通知區中的「**HP ProtectTools Security Manager**」圖示上按一下滑鼠右鍵，然後選取「**Embedded Security 初始化**」。

   HP ProtectTools 嵌入式安全性初始化精靈 (HP ProtectTools Embedded Security Initialization Wizard) 將會開啓。

2. 請依照螢幕上的說明繼續執行。

設定基本使用者帳戶

設定 Embedded Security 的基本使用者帳戶，以完成下列工作：

- 產生基本使用者金鑰來保護加密的資料，以及設定基本使用者金鑰密碼來保護基本使用者金鑰。
- 設定 Personal Secure Drive (PSD) 來儲存加密的檔案和資料夾。

注意： 保護基本使用者金鑰密碼。必須使用這個密碼，才能存取或復原加密的資料。

若要設定基本使用者帳戶和啟用使用者安全性功能：

1. 如果 Embedded Security 使用者初始化精靈未開啟，請依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在左側窗格中，按一下「**Embedded Security**」，然後再按一下「**使用者設定**」。
3. 在右側窗格中，於「**Embedded Security 功能**」下，按一下「**設定**」。

   Embedded Security 初始化精靈將會開啟。
4. 請依照螢幕上的說明繼續執行。

附註： 若要使用安全電子郵件，您必須先設定電子郵件用戶端，使其使用「嵌入式安全性」所建立的數位憑證。若沒有數位憑證，您必須向憑證授權單位取得數位憑證。如需設定電子郵件和取得數位憑證的指示，請參閱電子郵件用戶端的軟體說明。

一般工作

設定基本使用者帳戶後，可執行下列工作：

- 加密檔案和資料夾
- 傳送與接收加密的電子郵件

使用個人安全磁碟機

設定 PSD 後，系統會提示您在下次登入時鍵入基本使用者金鑰密碼。若正確輸入基本使用者金鑰密碼，即可從「Windows 檔案總管」直接存取 PSD。

加密檔案和資料夾

使用加密的檔案時，請考慮下列規則：

- 只能加密 NTFS 磁碟分割上的檔案和資料夾。不能加密 FAT 磁碟分割上的檔案和資料夾。
- 無法加密系統檔案和壓縮檔，也無法壓縮加密的檔案。
- 必須加密暫存資料夾，因爲這些資料夾可能是駭客的攻擊目標。
- 當您首次加密檔案或資料夾時，會自動設定復原原則。當您遺失您的加密憑證和私密金鑰時，這個原則就能讓您使用復原代理程式以解密資料。

若要加密檔案和資料夾：

1. 在要加密的檔案或資料夾上按一下滑鼠右鍵。
2. 按一下「**加密**」。
3. 按一下下列其中一個選項：
   - **僅將變更套用到這個資料夾。**
   - **將變更套用到這個資料夾、子資料夾和檔案。**
4. 按一下「**確定**」。

傳送與接收加密的電子郵件

Embedded Security 可讓您傳送和接收加密的電子郵件，但程序可能隨著您用來存取電子郵件的程式而異。如需詳細資訊，請參閱 Embedded Security 的軟體說明，以及您電子郵件程式的軟體說明。

變更基本使用者金鑰密碼

若要變更基本使用者金鑰密碼：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在左側窗格中，按一下「**Embedded Security**」，然後再按一下「**使用者設定**」。
3. 在右側窗格中的「**基本使用者密碼**」下方，按一下「**變更**」。
4. 鍵入舊密碼，然後設定和確認新密碼。
5. 按一下「**確定**」。

進階工作

管理員可以在 Embedded Security 中執行下列工作：

- 備份並還原 Embedded Security 認證、Embedded Security 設定以及個人安全磁碟機
- 變更擁有者密碼
- 重設使用者密碼
- 將使用者安全憑證從來源平台安全地轉移至目的地平台

備份和還原

Embedded Security 備份功能可建立一個封存，其中包含可在緊急狀況下還原的憑證資訊。

建立備份檔

若要建立備份檔：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Embedded Security**」，然後再按一下「**備份**」。
3. 在右側窗格中，按一下「**設定**」。HP Embedded Security for ProtectTools 備份精靈隨即開啓。
4. 請依照螢幕上的說明繼續執行。

從備份檔還原憑證資料

若要從備份檔還原資料：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Embedded Security**」，然後再按一下「**備份**」。
3. 在右側窗格中，按一下「**全部還原 (Restore all)**」。 HP Embedded Security for ProtectTools 備份精靈隨即開啓。
4. 請依照螢幕上的說明繼續執行。

變更擁有者密碼

管理員可以變更擁有者密碼：

1. 依序按一下「**開始**」、「**所有程式**」、「**HP**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Embedded Security**」，然後再按一下「**進階**」。
3. 在右側窗格中，於「**擁有者密碼**」下，按一下「**變更**」。
4. 鍵入舊的擁有者密碼，然後設定和確認新的擁有者密碼。
5. 按一下「**確定**」。

重設使用者密碼

當使用者忘記密碼時，管理員可協助使用者重設密碼。如需詳細資訊，請參閱軟體說明。

以轉移精靈 (Migration Wizard) 轉移金鑰

轉移是一項進階的管理員工作，可管理、還原和轉移金鑰和憑證。

如需移轉的詳細資訊，請參閱 Embedded Security 的軟體說明。

11 本地化密碼例外狀況

在「預先開機安全性」層級與「HP Drive Encryption」層級上，密碼本地化支援會受到限制，如下列各節所述。

預先開機安全性層級或 HP Drive Encryption 層級不支援 Windows IME

在 Windows 中，使用者可藉由使用標準的西式鍵盤選擇 IME（輸入法編輯器）以輸入複雜的字元及符號，例如日文或中文字元。

「預先開機安全性」或「HP Drive Encryption」層級並不支援 IME。 在「預先開機安全性」或「HP Drive Encryption」登入畫面上無法使用 IME 輸入 Windows 密碼，而且這麼做可能造成鎖定情況。 在某些情況下，當使用者輸入密碼時，Microsoft® Windows 不會顯示 IME。

例如，在 Windows XP 的某些日文安裝中，預設的 IME 雖稱爲 Microsoft IME Standard 2002 for Japanese，但實際上會轉譯爲鍵盤配置 E0010411。 然而，這依然是 IME，而不是鍵盤配置（Microsoft 爲 IME 保留鍵盤配置的編碼配置，擴充了鍵盤配置的概念）。 由於這個鍵盤配置無法在 BIOS 預先開機安全性密碼提示或 HP Drive Encryption 密碼提示的輸入環境中提供，使用此 IME 輸入的任何密碼都會遭到 HP ProtectTools 拒絕。 Microsoft IME Standard 2002 for Japanese 與 Microsoft Windows Vista® 中的「一般名稱」也有所不同。 Windows 會將某些 IME 對應至鍵盤配置。 在這種情況下，由於使用基本鍵盤配置定義（十六進位碼），HP ProtectTools 支援 IME。

解決方法是切換到下列其中一個可轉譯成鍵盤配置 00000411 的受支援鍵盤配置：

- Microsoft IME for Japanese
- 日文鍵盤配置
- Office 2007 IME for Japanese — 如果 Microsoft 或協力廠商使用的詞彙是 IME 或輸入法編輯器，那麼該輸入法可能並不是真正所謂的 IME。 這可能造成混淆，但是軟體會讀取十六進位碼表示。因此，如果 IME 對應至支援的鍵盤配置，HP ProtectTools 就可以支援該配置。

⚠ **警告！** 部署 HP ProtectTools 時，使用 Windows IME 所輸入的密碼將會遭到拒絕。

使用鍵盤配置的密碼變更亦受支援

如果密碼最初透過某一種鍵盤配置（例如美國英文 (409)）設定，然後使用者又使用同樣受支援的不同鍵盤配置（例如拉丁美洲 (080A)）變更密碼，則密碼變更可以在 HP Drive Encryption 中發生作用，但是當使用者使用存在於後者而不存在於前者的字元（例如 ē）時，就會在 BIOS 中失敗。

附註： 管理員可以解決這個問題，方法是使用 HP ProtectTools 的「管理使用者」功能從 HP ProtectTools 移除使用者、在作業系統中選取所需的鍵盤配置，然後再對相同的使用者執行 Security Manager 設定精靈。 BIOS 會儲存所需的鍵盤配置，而且可透過此鍵盤配置輸入的密碼也會在 BIOS 中設定妥當。

另一個潛在問題是使用可產生相同字元的不同鍵盤配置。 例如，雖然需要使用不同的按鍵順序，美式國際鍵盤配置 (20409) 和拉丁美洲鍵盤配置 (080A) 都可以產生字元 é。 如果密碼最初是以拉丁美洲鍵盤配置進行設定，即使後來使用美式國際鍵盤配置變更密碼，BIOS 中的設定仍然會是拉丁美洲鍵盤配置。

特殊鍵處理

- 中文、斯洛伐克文、加拿大法文和捷克文

  當使用者選取前述其中一個鍵盤配置，並接著輸入密碼（例如 abcdef）時，必須在 BIOS 預先開機安全性和 HP Drive Encryption 中輸入相同密碼，輸入小寫時要同時按住 shift 鍵，輸入大寫時要同時按住 shift 鍵及 caps lock 鍵。 數字密碼則必須使用數字鍵台來輸入。

- 韓文

  當使用者選取支援的韓文鍵盤配置並接著輸入密碼時，必須在 BIOS 預先開機安全性和 HP Drive Encryption 中輸入相同密碼，輸入小寫時要同時按住右側 alt 鍵，輸入大寫時要同時按住右側 alt 鍵及 caps lock 鍵。

- 下表列出不支援的字元：

語言	Windows	BIOS	Drive Encryption
阿拉伯文	ﻻ、ﻷ 和 ﻹ 鍵會產生兩個字元。	ﻻ、ﻷ 和 ﻹ 鍵會產生一個字元。	ﻻ、ﻷ 和 ﻹ 鍵會產生一個字元。
加拿大法文	ç、è、à 和 é 搭配 caps lock 會在 Windows 中輸入 Ç、È、À 和 É。	ç、è、à 和 é 搭配 caps lock 會在 BIOS 預先開機安全性中輸入 ç、è、à 和 é。	ç、è、à 和 é 搭配 caps lock 會在 HP Drive Encryption 中輸入 ç、è、à 和 é。
西班牙文	不支援 40a。 儘管如此，因爲軟體會將它轉換爲 c0a，所以仍然有用。 不過，鍵盤配置之間仍有細微差異存在，建議西班牙語系使用者將其 Windows 鍵盤配置變更爲 1040a（西班牙文分支）或 080a（拉丁美洲）。	N/A	N/A
美式國際	◦ 拒絕最上列的 ¡、¤、‘、'、¥ 和 × 鍵。 ◦ 拒絕第二列的 å、® 和 Þ 鍵。 ◦ 拒絕第三列的 á、ð 和 ø 鍵。 ◦ 拒絕最下列的 æ 鍵。	N/A	N/A
捷克文	◦ 拒絕 ğ 鍵。 ◦ 拒絕 į 鍵。 ◦ 拒絕 ų 鍵。 ◦ 拒絕 ė、ı 和 ż 鍵。 ◦ 拒絕 ģ、ķ、ļ、ņ 和 ţ 鍵。	N/A	N/A
斯洛伐克文	拒絕 ż 鍵。	◦ š、ś 和 ş 鍵會在輸入時遭到拒絕，但是透過螢幕小鍵盤輸入時則被接受。 ◦ ţ 廢鍵會產生兩個字元。	N/A
匈牙利文	拒絕 ż 鍵。	ţ 鍵會產生兩個字元。	N/A

語言	Windows	BIOS	Drive Encryption
斯洛維尼亞文	žŽ 鍵會在 Windows 中遭到拒絕，而 alt 鍵會在 BIOS 中產生廢鍵。	ú ·Ú ·ů ·Ů ·ş ·Ş ·ś ·Ś ·š 和 Š 鍵會在 BIOS 中遭到拒絕。	N/A
日文	僅 Windows XP 完整支援標準日文鍵盤配置 411。 一般情況下，一種在 Windows XP 中通常表示爲 Microsoft Standard IME 2002 的 IME 並不受支援。 不過，實地測試顯示，當輸入簡單字元時，此 IME 幾乎是鍵盤配置 411 的翻版。 因此，當使用本地化日文密碼保護 BIOS 和 HP Drive Encryption 安全時，軟體就會將該 IME 切換爲鍵盤配置 411。 如果可用，則 Microsoft Office 2007 IME 會是較佳的選擇。 儘管 IME 名稱不同，這實際上是受支援的鍵盤配置 411。	N/A	N/A

當密碼遭到拒絕時要如何處理

密碼可能因爲下列原因遭到拒絕：

- 使用者使用不支援的 IME。 這是雙位元組語言（韓文、日文、中文）常見的問題。 若要解決此問題：

  1. 依序按一下「**開始**」、「**控制台**」和「**地區及語言選項**」。
  2. 按一下「**語言**」標籤。
  3. 按一下「**詳細資料**」按鈕。
  4. 在「**設定**」標籤上，按一下「**新增**」按鈕以新增支援的鍵盤（在「中文輸入語言」下方新增美式鍵盤）。
  5. 設定預設輸入的支援鍵盤。
  6. 重新啓動 HP ProtectTools，然後再次輸入密碼。

- 使用者使用不支援的字元。 若要解決此問題：

  1. 變更 Windows 密碼，使其僅使用支援的字元。 位於第 97 頁的特殊鍵處理中列出了不支援的字元。
  2. 重新執行 Security Manager 設定精靈，然後輸入新的 Windows 密碼。

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 啟動之前所顯示的登入畫面。使用者必須輸入其 Windows 使用者名稱及密碼或智慧卡 PIN 碼。多數情況下，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
一種安全性功能，可在電腦啟動時，連繫硬碟與使用者，並要求使用者正確輸入 DriveLock 密碼。

HP SpareKey
Drive Encryption 金鑰的備份副本。

JITA
及時驗證。

PIN
個人識別碼。

PKI
公開金鑰基礎架構標準，其定義用於建立、使用和管理憑證及密碼編譯金鑰的介面。

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
電腦與大量儲存裝置（例如，硬碟和光碟機）之間的資料傳輸模式。

TXT
信任式執行技術。

USB 權杖 (Token)
一種儲存使用者相關識別資訊的安全裝置。和智慧卡或生物測定讀取器一樣，都是用來向電腦驗證擁有者。

Windows 使用者帳戶
授權個人登入網路或個人電腦的設定檔。

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
一個中央位置，您可以在其中存取和管理「HP ProtectTools 管理主控台 (HP ProtectTools Administrative Console)」的功能和設定。

加密
將演算法之類的程序用於密碼使用法中，並將明文轉換爲密碼文字，以避免未經授權的收件者閱讀該資料。資料加密分爲許多類型，並且是網路安全性的基礎。一般常見的類型包括資料加密標準及公開金鑰加密。

加密檔案系統 (EFS)
可將所選資料夾內所有檔案及子資料夾加密的系統。

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
在 HP ProtectTools Security Manager 中，是一個認證及設定的群組，其處理方式類似特定使用者的帳戶或設定檔。

使用者
任何註冊 Drive Encryption 的人。非管理員使用者在 Drive Encryption 中擁有有限的權限。他們僅可以註冊（在管理員的核准下）以及登入。

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。

信任平台模組 (TPM) 嵌入式安全晶片
HP ProtectTools Embedded Security Chip 的通稱。TPM 儲存主機系統的特定資訊（例如，加密金鑰、數位憑證和密碼）以驗證電腦，而非使用者。TPM 可將電腦因實體失竊或外部駭客攻擊而洩露資訊的風險降至最低。

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」。

信任的連絡人
接受「信任的連絡人」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」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」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」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
「HP ProtectTools Device Locking/Auditing」背景服務。若要套用裝置存取控制原則，必須執行此背景服務。在「控制台」中，可從「系統管理工具」選項下的「服務」應用程式檢視此背景服務。如果沒有執行，HP ProtectTools Security Manager 就會在套用裝置存取控制原則時嘗試將它啓動。

重新開機
重新啓動電腦的程序。

密碼編譯
爲了讓資料只能由特定個人成功解碼而進行的一種加密與解密資料做法。

密碼編譯服務提供者 (CSP)
密碼編譯演算法的提供者或程式庫，可透過正確定義的介面使用此演算法以執行特定的密碼編譯功能。

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」的工作。

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
一項功能，此功能會儲存驗證資訊，讓您使用 Security Manager 來存取需要密碼驗證的網際網路及 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。

場景
用來進行驗證的註冊之使用者的相片。

智慧卡
形狀大小與信用卡相仿的一小片硬體，其中儲存擁有者的相關識別資訊。用來向電腦驗證擁有者。

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)
作用與智慧卡及讀卡機非常類似的安全性功能。權杖會儲存在電腦硬碟或 Windows 登錄中。當您使用虛擬權杖登入時，系統會要求您提供使用者 PIN 碼以完成驗證。

開機驗證
一種安全性功能，可在電腦開機時要求某個形式的驗證，例如：智慧卡、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
在密碼編譯中用來轉換加密資料爲純文字的程序。

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，允許將基本使用者金鑰由一個平台擁有者金鑰重新加密爲另一個。

網域
屬於網路一部分且分享共用目錄資料庫的電腦群組。網域具有唯一的名稱，而且個別擁有一組通用規則及程序。

網路帳戶
在本機電腦、工作群組或網域中的 Windows 使用者或管理員帳戶。

認證
使用者在驗證程序中藉以證明有資格執行特定工作的方法。

儀表板
一個中央位置，您可以在其中存取和管理「Security Manager for HP ProtectTools」的功能和設定。

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 (CA)
簽發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
Microsoft Office 應用程式工具列中顯示的軟體按鈕。按一下此按鈕即可簽署、加密或移除 Microsoft Office 文件中的加密。

識別卡
透過視覺方式，以您的使用者名稱和選定圖片識別您桌面的 Windows 桌面小工具。按一下 ID 識別卡，開啓 HP ProtectTools 管理主控台。

權杖
請參閱「**安全登入法**」。

驗證
確認使用者是否獲得授權執行工作（例如，存取電腦、修改特定程式的設定，或檢視受保護的資料）的程序。

索引

十二畫

十三畫

十四畫

十五畫

十六畫

十七畫

十八畫

十九畫

二十三畫