HP ProtectTools for Small Business Security Software 5.10 版

使用指南

HP ProtectTools for Small Business Security Software 5.10 版使用指南

HP 商用個人電腦

第 2 版： 2010 年 5 月

文件編號：610663-AB2

有關本書

本指南提供 HP ProtectTools for Small Business Security Software 的資訊。

⚠ **警告!** 以此方式標示的文字代表若不依照指示方法操作，可能會導致人身傷害或喪失生命。

△ **注意：** 以此方式標示的文字代表若不依照指示方法操作，可能會導致設備損壞或資料遺失。

附註： 以此方式強調之文字提供重要的補充資訊。

目錄

1 安全性簡介

HP 深知您的時間極爲寶貴，必須投注在業務的營運與拓展上，沒有餘暇再爲尋找適合保護電腦、資料及企業的安全性軟體而操心。

您必須認真考慮容易使用而且能夠強力保護企業資產的安全性解決方案。安全性不是「聊勝於無」的措施，而是「必要」的考量！

HP 推出易於實作而且使用簡單的安全保護軟體，名叫 HP ProtectTools for Small Business。

HP ProtectTools for Small Business Security Software 提供的功能，可以協助防止未經授權存取電腦和重要資料的事件。HP ProtectTools 軟體的各種模組會提供增強的安全功能。

HP ProtectTools for Small Business 有兩種版本可供使用：HP ProtectTools Security Manager 管理主控台與 HP ProtectTools Security Manager（適用於一般使用者）。管理員和一般使用者版本都可以在「**開始**」>「**所有程式**」功能表上找到。

功能	特點
HP ProtectTools Security Manager 管理主控台	• 需要 Microsoft Windows 系統管理員權限才能存取 • 存取由管理員設定，而一般使用者無法使用的模組 • 可進行初始安全性設定，以及針對一般使用者的設定選項或需求
HP ProtectTools Security Manager（適用於一般使用者）	• 允許使用者設定由管理員提供的選項 • 可限制存取，使用者所能控制的 HP ProtectTools 模組數量也有所限制

HP ProtectTools 軟體模組可以預先安裝、預先載入，或以可設定選項或選購的方式取得。請造訪 http://www.hp.com 以取得更多資訊。

HP ProtectTools 功能

下表詳述 HP ProtectTools for Small Business 模組的主要功能：

模組	重要功能
HP ProtectTools Security Manager 管理主控台	• 管理員使用 Security Manager 設定精靈安裝及設定安全性及安全登入法的層級。 • 設定基本使用者無法看見的選項。 • 設定 Device Access Manager 組態和使用者存取權。 • 管理員工具可用來新增和移除 HP ProtectTools 使用者，以及檢視使用者狀態。
HP ProtectTools Security Manager（適用於一般使用者）	• 組織、設定及變更使用者名稱和密碼。 • 設定及變更使用者認證，例如 Windows 密碼和智慧卡。 • 設定及變更 File Sanitizer 拆解、整理和設定值。 • 檢視 Device Access Manager 的設定。 • 設定「偏好設定」和「備份與還原」選項。
Credential Manager for HP ProtectTools（密碼管理員）	• 專爲儲存、組織和保護您的使用者名稱及密碼而量身打造。 • 可讓您設定網站和程式的登入畫面，以便快速而安全地存取。 • 當您存取各種網站而想要儲存自己的使用者名稱及密碼時，請輸入到「密碼管理員」中，這樣您就不需要重新回憶它們。您下次再造訪這個網站時，「密碼管理員」將會自動填寫和提交資料。 • 可讓您建立強度更大的密碼，而不必抄下或記憶它，使您的帳戶更安全。
Drive Encryption for HP ProtectTools	• 提供完整的全磁碟區硬碟加密。 • 強制預先開機驗證，以解密及存取硬碟上的資料。 • 協助您符合法規或產業需求，以保護機密和敏感性資料。 • 透過加密整個硬碟機，保護您的資料免於遭到未經授權的存取。如果 PC 曾經遭竊，而磁碟機已從原始系統移除並放置在其他系統中，資料將不會受到威脅。

模組	重要功能
File Sanitizer for HP ProtectTools	• 刪除 Windows 中的資料並不會將內容從您的硬碟中完全移除。Windows 只會刪除資料的參考。資料仍然保留在硬碟中，直到其他檔案以新的資訊覆寫硬碟上的相同區域爲止。但是，您可以透過 File Sanitizer，完全且自動地清除文件、Web 瀏覽器歷程記錄、暫存檔案等等。 • 可讓您安全清除電腦上的重要檔案和資料夾（個人資訊或檔案、歷程或網路相關資料或其他資料元件），並且定期清理硬碟（覆寫先前已刪除的資料）。
Device Access Manager for HP ProtectTools	• 可用以根據使用者設定檔控制對媒體磁碟機、USB 和其他硬體裝置的存取。 • 可讓您限制使用者儲存重要資料的能力。 • 防止使用者使用外接式儲存裝置（例如，個人音樂播放器），從電腦或您的網路中複製資料。 • 防止使用者將病毒從外接式媒體引入系統中。 • 可讓您選擇依據使用者或使用者群組停用一組裝置，例如 USB Key、可寫入裝置、個人音樂播放器等。擁有管理員密碼的人員可以登入電腦並複製其中的資訊，但是其他使用者則無法這麼做。

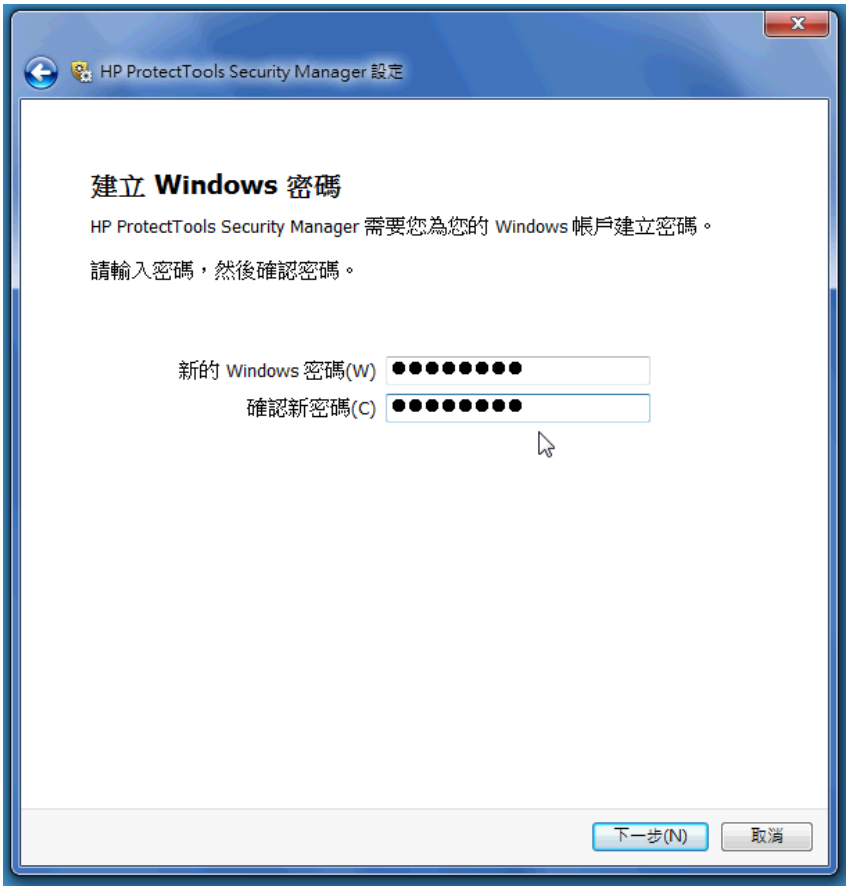
2 說明最有用選項的 Easy Setup 指南

本「Easy Setup 指南」專爲示範啓用 HP ProtectTools for Small Business 內最常見與最有用選項的基本步驟而量身設計。此軟體中有許多可供您用來微調偏好設定以及設定存取控制的工具和選項。「Easy Setup 指南」的內容著重在，使用最少量的設定工作和時間讓每個模組都能執行。如需其他資訊，只要選擇您感興趣的模組，然後按一下右上角的「?」或「說明」按鈕即可。此按鈕將會自動提供資訊，協助您處理目前顯示的視窗。

快速入門

1. 從小工具圖示、工作列圖示（金色盾牌），或按一下「**開始**」>「**所有程式**」>「**HP**」，開啓 HP ProtectTools Security Manager。

2. 輸入您的 Windows 密碼，或建立 Windows 密碼。

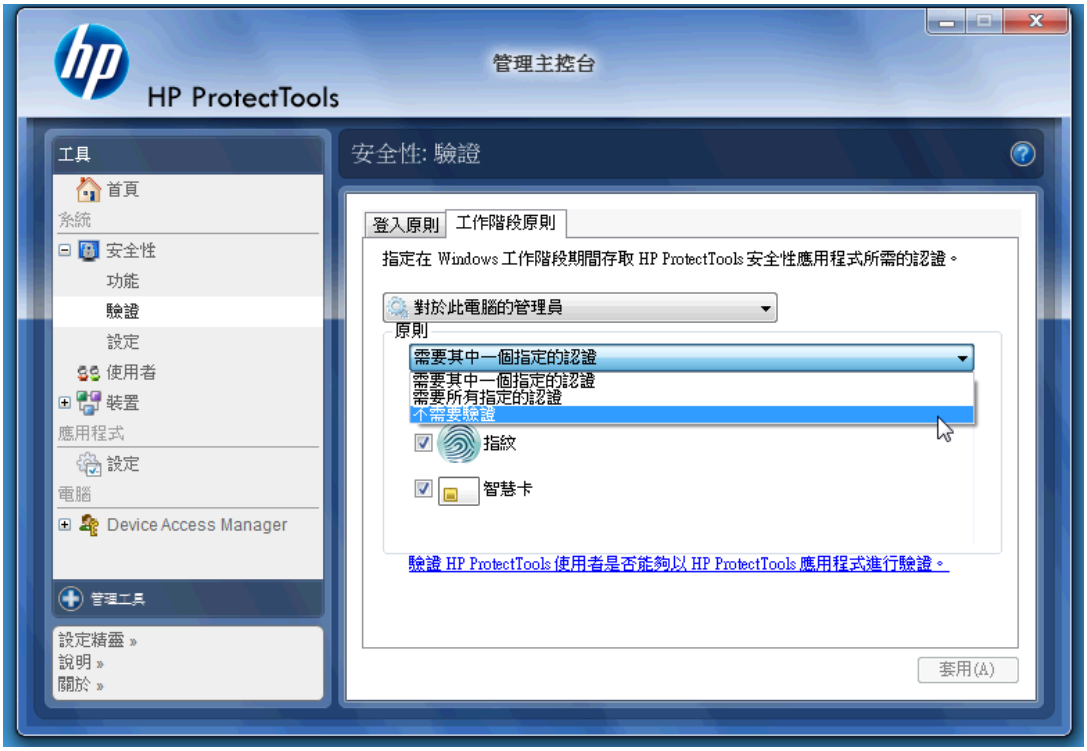


3. 完成設定精靈。

附註： 根據預設，HP ProtectTools Security Manager 會設定爲「增強式驗證原則」。

此設定的設計目的是在 Windows 接受登入時防止未獲授權的存取，如果您需要高安全性，或是使用者整天經常不在系統上，最好使用此設定。如果您想要變更此設定，請按一下「工作階段原則」標籤，然後進行選取。

若要將 HP ProtectTools Security Manager 設定爲整個工作階段都只使用初始 Windows 登入，請變更下列組態：



若要讓 HP ProtectTools Security Manager 在 Windows 登入期間僅進行一次驗證：

1. 按一下「**開始**」>「**所有程式**」>「**HP**」>「**HP ProtectTools 管理主控台**」。
2. 在左側「**工具**」窗格中，選擇「**安全性**」群組中的「**驗證**」。
3. 按一下「**工作階段原則**」標籤，然後從「**原則**」底下的下拉式功能表中選取「**不需要驗證**」。
4. 完成時，按一下「**套用**」按鈕。

Credential Manager for HP ProtectTools（密碼管理員）

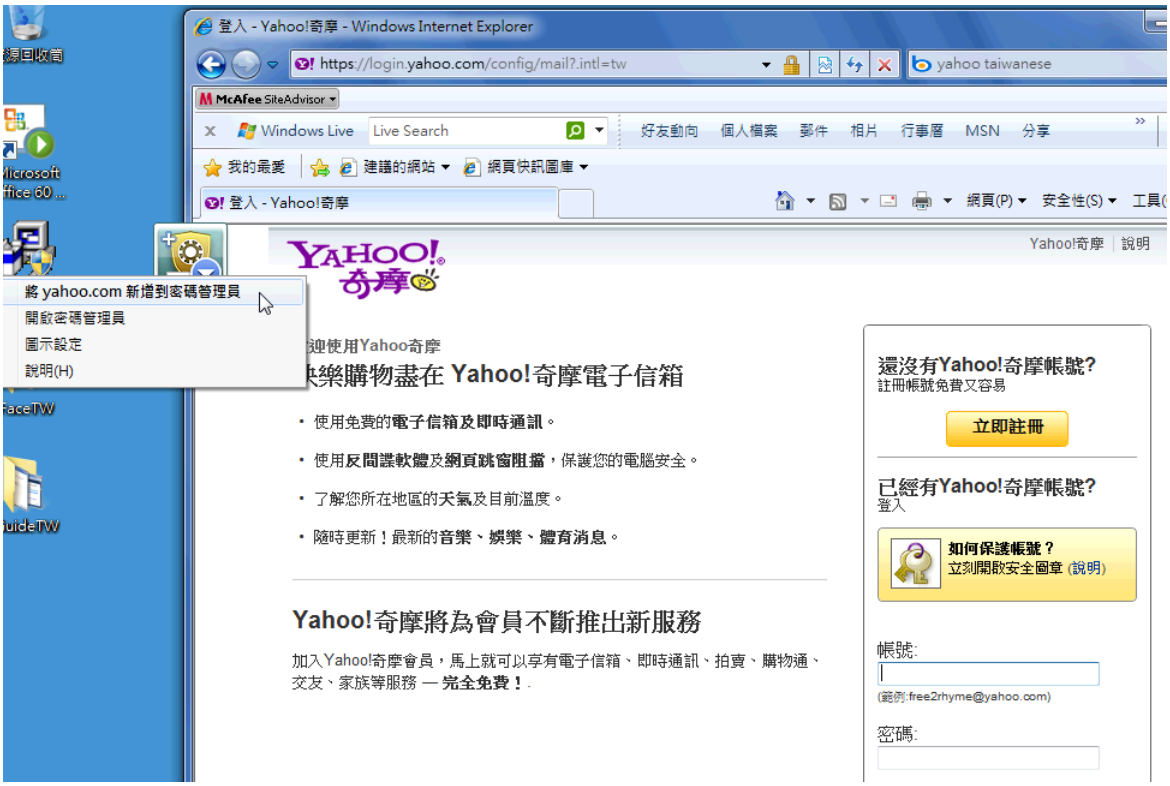
說到密碼！想必大家都有不少密碼，尤其是如果您經常存取網站或使用需要登入的應用程式，便會用到許多密碼。一般的使用者通常會在所有應用程式和網站上使用相同的密碼，不然很容易忘記或搞混哪個密碼要搭配哪個應用程式使用。

要是有軟體會自動爲您記住不重要網站的密碼，或是讓您能夠分辨要記住或要略過的網站，豈不更好？ Credential Manager for HP ProtectTools 可以滿足您這個要求。Credential Manager 就是提供這項功能的密碼管理員。一旦登入電腦後，Credential Manager 將會在需要時提供您的密碼或認證。

當您存取任何需要認證的應用程式或網站時，Credential Manager 就會自動識別站台，並詢問您是否要軟體記住您的資訊。如果您表示同意，就永遠不需要重新回憶該密碼。如果您想要將特定網站排除在外，可以拒絕記憶您資訊的要求。

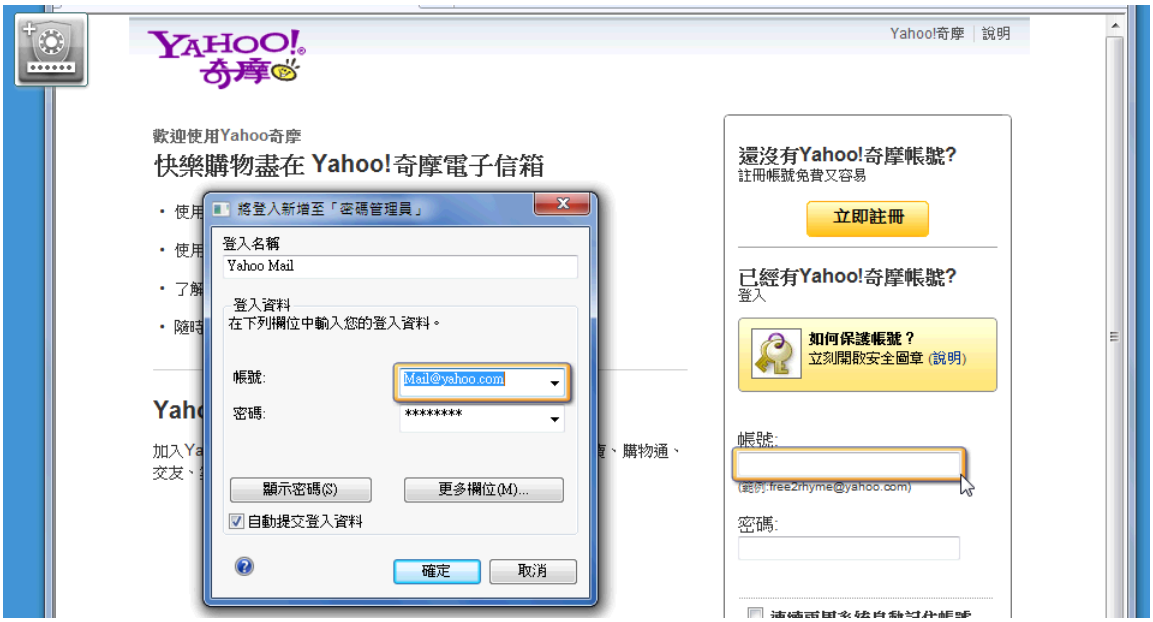
若要開始儲存網站位置、使用者名稱及密碼：

1. 舉例來說，請瀏覽至您的 Web 郵件帳戶，並告訴 Credential Manager（按一下圖示）要新增 Web 驗證。



2. 爲連結命名（也可以不命名），並在 Credential Manager 中輸入使用者名稱及密碼。

附註： 網頁會將 Credential Manager 現在要使用而之後會造訪的區域反白。



3. 完成時，按一下「**確定**」按鈕。

4. Credential Manager 也可以儲存您的網路共用或對應網路磁碟機的使用者名稱及密碼。

檢視和管理儲存在 Credential Manager 中的驗證

Credential Manager 的優點在於，您可以從單一個集中位置進行檢視、管理、備份和啓動驗證。Credential Manager 也支援從 Windows 啓動儲存的網站。

若要開啓「密碼管理員」，請使用下列兩個方法的其中一個：

- 使用 Ctrl+Windows+H 的鍵盤組合來開啓「密碼管理員」。選取「**開啓**」將會快速啓動和驗證儲存的捷徑。

或

- 選取 Password Manager 中的「**管理**」標籤來開啓 HP ProtectTools Security Manager，而您可以在這裡編輯認證。

Credential Manager 的「**編輯**」選項可讓您檢視和修改名稱、登入名稱，甚至顯示密碼。

HP ProtectTools for Small Business 允許將所有認證和設定備份和/或複製到另一部電腦。


HP ProtectTools
Security Manager
Ashley
安全性應用程式
首頁
Credential Manager
密碼管理員
認證
我的資料
File Sanitizer
我的電腦
Device Access Manager
進一步探索
管理 »
說明 »
進階 »
偏好設定 »
備份和還原 »
關於 »
備份和還原
HP ProtectTools 備份和還原精靈可協助您安全地備份 HP ProtectTools 應用程式所管理的資料。這份資料可在 HP ProtectTools 所保護的任何電腦上還原。
不會備份像指紋資料之類的認證。
選擇您想要做的事。
備份資料
還原資料
檢視備份和還原記錄

File Sanitizer for HP ProtectTools

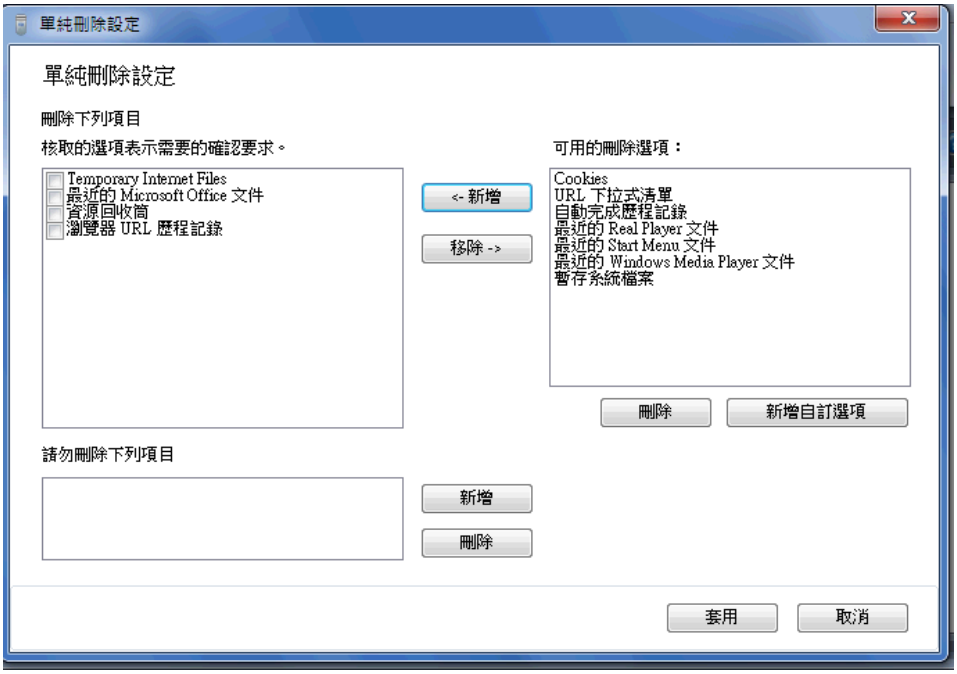
File Sanitizer 是爲了使未獲授權的人員不易復原您所刪除的資料而設計。有多個選項可供您用來進行手動清除或建立定期排程，以便清除選取的檔案及資料夾，包括瀏覽器歷程記錄。

以下是一些簡易的組態設定。

若要開始永久清除您刪除的資料，請選擇您不再需要的檔案或資料夾。

1. 瀏覽至「**Security Manager**」>「**File Sanitizer**」>「**設定**」。選取「**單純刪除設定**」，然後按一下「**檢視詳細資料**」按鈕。

2. 在「單純刪除設定」視窗右側選取您想要定期地永久刪除的項目，然後按一下「**<-新增**」按鈕，將選取的項目移至「刪除」側。



3. 從「資源回收筒」開始，新增您可能想要透過「拆解」清除的其他項目。

4. 當您選取了要永久清除的所有項目時，按一下「**套用**」按鈕。

5. 瀏覽至「**拆解**」選項，並設定何時要執行動作。「**立即拆解**」按鈕會立即清除您在剛才設定的「單純刪除設定」視窗中選取的項目。

6. 每次啟動「拆解」並完成動作時，小型的快顯泡泡圖就會在工作列中出現。

Device Access Manager for HP ProtectTools

Device Access Manager 可以用來限制各種內建式和外接式儲存裝置的使用，讓您的資料安全無虞地保留在硬碟中，而不會跨出您的企業大門半步。例如，允許使用者存取您的資料，但是不讓他們將資料複製到光碟、個人播放器或 USB 記憶體裝置。以下是進行這項設定的簡易方式。

1. 按一下「**開始**」>「**所有程式**」>「**HP**」>「**管理主控台**」>「**Device Access Manager**」>「**簡易組態**」。

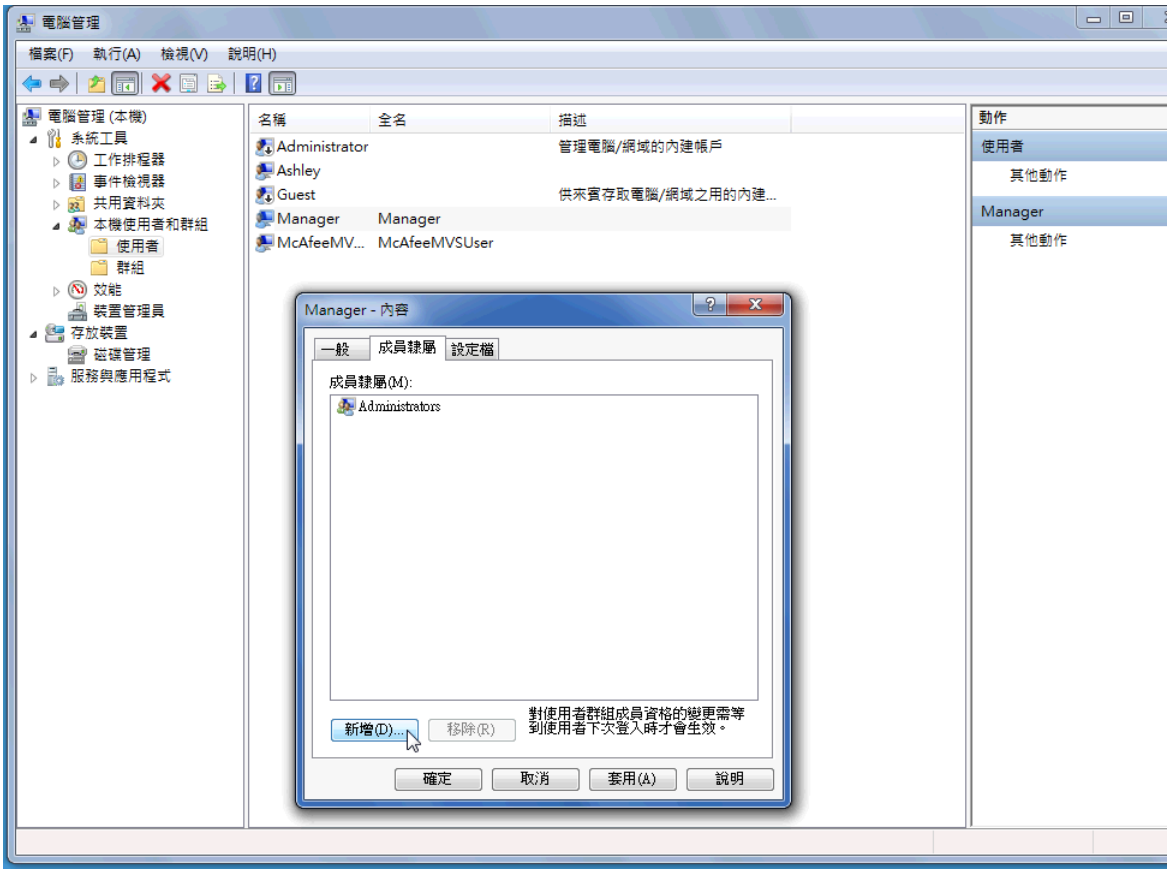
2. 選取您想要限制的硬體裝置，然後按一下「**套用**」按鈕以完成程序。

3. 接下來的步驟是要選取可以繼續進行存取的使用者，而不讓其他所有人員存取。

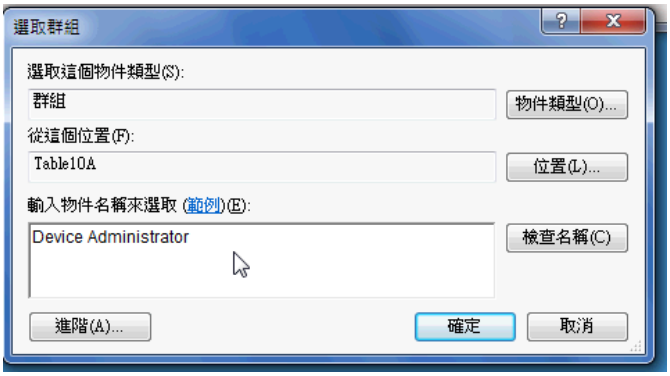
4. 瀏覽至「**我的電腦**」並加以選取，用滑鼠右鍵按一下，再依次選取「**管理**」>「**電腦管理**」>「**系統工具**」>「**本機使用者和群組**」>「**使用者**」。

5. 按兩下要允許其繼續存取所封鎖硬體的使用者（在本例中爲「Manager」）。

6. 在「**成員隸屬**」標籤中，按一下「**新增**」按鈕。



7. 在「**選取群組**」視窗中，您可以使用「**進階**」選項，或者只是輸入「Device Administrators」群組。按一下「**確定**」按鈕，再按幾次「確定」按鈕即可關閉視窗。您必須登出後再重新登入，才能取得權限。



現在除了對「Device Administrators」群組包含的人員以外，所有的內建式和外接式儲存磁碟機（包括光碟機、USB 磁碟機、個人音樂播放器等）都無法運作。

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools 軟體會透過加密整個硬碟機，保護您的資料。 如果 PC 曾經遭竊且/或磁碟機已從原始系統移除並放置在其他系統中，硬碟機上的資料將保持受保護的狀態。

進一步的安全性優點在於，Drive Encryption 將會要求您在系統開機前使用您的使用者名稱和密碼正確地進行驗證。 此程序稱爲 PreBoot 驗證。

爲了您的方便，Windows 使用者、網域、HP ProtectTool 專用 Credential Manager 和 HP ProtectTools Security Manager 全具有 Drive Encryption 的介面，以進行簡易密碼同步處理。

請使用下列簡單的步驟，啓動 Drive Encryption for HP ProtectTools。

1. 依序按下「**開始**」>「**所有程式**」>「**HP**」>「**HP ProtectTools 管理主控台**」>「**管理工具**」>「**設定精靈**」。 隨即顯示下列畫面。

2. 選取「歡迎使用」畫面中的「**下一步**」。
3. 需要 Windows 密碼才能開啓啓動精靈 >「**下一步**」。
4. 核取「**Drive Encryption**」方塊並選取「**下一步**」。

5. 下面的「Drive Encryption」設定視窗會顯示要加密的磁碟機，並且將要求 USB 快閃磁碟機儲存加密還原金鑰。 請妥善保存此還原金鑰，因爲萬一開機前密碼遺失或失效，將使用此金鑰來還原資料或存取磁碟機。

6. 選取「**下一步**」完成程序，並選取「**完成**」。 出現提示時，請取出 USB 快閃磁碟機，並在就緒時重新啓動系統。

7. 當系統開機至硬碟機時，Drive Encryption 會向您要求 Windows 密碼。 輸入密碼，然後按一下「**確定**」。

附註： 當磁碟機正在加密時，電腦的執行速度可能會變慢。 一旦完全加密之後，系統將會恢復正常。 當系統存取磁碟機上的資料時，將視需要加密或解密資料。

另請注意，Drive Encryption 驗證會透過 Credential Manager Windows 登入直接「鏈結」至桌面，而不需輸入密碼兩次。

3 HP ProtectTools for Small Business 的優點

存取 HP ProtectTools for Small Business Security Software

若要從 Windows「開始」功能表存取 HP ProtectTools Security Manager：

- 在 Windows 中，依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。

若要從 Windows「開始」功能表存取 HP ProtectTools Security Manager 管理主控台：

- 在 Windows 中，依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。

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：

- 限制存取機密資料
- 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

限制存取機密資料

假設契約審計師在現場工作，並已授予他檢視機密財務資料的權限；而您不希望審計師列印檔案或將檔案儲存在可寫入裝置，例如光碟。下列功能有助於限制存取資料：

Device Access Manager for HP ProtectTools 允許管理員限制可寫入裝置的存取，使機密資訊無法列印或從硬碟複製到可抽換式媒體上。請參閱「位於第 43 頁的裝置類別組態（進階）」。

防止未獲授權的使用者從內部或外部位置進行存取

未獲授權存取不安全的商用電腦，代表重要資料（例如財務服務、主管或研發團隊提供的資訊以及像是病歷或個人財務資料等私人資訊）面臨極大的風險。則下列功能有助於防止未獲授權的存取：

- 如果啓用預先開機驗證功能，則有助於防止他人存取作業系統。請參閱下列章節：
  - 位於第 32 頁的 Credential Manager for HP ProtectTools（密碼管理員）
  - 位於第 29 頁的 Drive Encryption for HP ProtectTools
- Credential Manager for HP ProtectTools 有助於確保讓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。請參閱下列章節：
  - 位於第 32 頁的 Credential Manager for HP ProtectTools（密碼管理員）
- Device Access Manager for HP ProtectTools 允許管理員限制對可寫入裝置的存取，使機密資訊無法從硬碟中被複製。請參閱下列章節：
  - 位於第 42 頁的 Device Access Manager for HP ProtectTools
- File Sanitizer 可讓您藉由拆解重要檔案與資料夾，或清理硬碟（覆寫先前已刪除但仍存在硬碟中的資料，使資料更不易復原）的方式，安全地刪除資料。請參閱下列章節：
  - 位於第 36 頁的 File Sanitizer for HP ProtectTools

建立不易破解的密碼政策

如果您需要對許多網路應用程式和資料庫採用強式密碼原則（難以破解的複雜密碼），Credential Manager for HP ProtectTools 就會提供受保護的密碼儲存庫和單一登入的便利。請參閱下列章節：

- 位於第 32 頁的 Credential Manager for HP ProtectTools（密碼管理員）

其他的安全性要素

指派安全性角色

爲了妥善保護資料，其中一項重要的作法就是將責任和權限劃分成各類型的管理員和使用者。

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。

在 HP ProtectTools for Small Business 中，安全性職責和權限可以劃分爲下列角色：

- 管理員 — 套用和管理安全功能。也可以啓用或停用某些功能。
- 使用者 — 使用安全功能。

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。

下表也會指出僅由管理員所設定和使用的密碼。所有其他密碼則可由一般使用者設定。

HP ProtectTools 密碼	在此 HP ProtectTools 模組中設定	功能
Password Manager 登入密碼	Password Manager	這個密碼可提供 2 個選項： • 在登入 Windows 後，它可用於個別的登入，以存取 Password Manager。 • 它可用來代替 Windows 登入程序，並允許同時存取 Windows 和 Password Manager。
電腦設定密碼 **附註：** 也稱爲 BIOS 管理員、F10 設定 或安全性設定密碼	BIOS，由管理員設定	保護對電腦設定公用程式的存取。
開機密碼	BIOS	當電腦啓動、重新啓動或從「休眠」狀態回復時，可保護對電腦內容的存取。
Windows 登入密碼	Windows 控制台	可用於手動登入。

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。

備份認證與設定

使用 HP ProtectTools Security Manager 中的「備份與復原」工具做爲集中位置，您可以在那裡從已安裝的 HP ProtectTools 模組備份和還原安全憑證。

4 HP ProtectTools Security Manager 管理主控台

關於 HP ProtectTools 管理主控台

HP ProtectTools Security Manager 的管理是透過管理主控台提供。

使用主控台，本機管理員可以：

- 啓用或停用安全功能
- 管理電腦使用者
- 調整裝置特定參數
- 設定 Security Manager 應用程式
- 新增其他 Security Manager 應用程式

使用管理主控台

Security Manager 管理主控台是管理 HP ProtectTools Security Manager 的集中位置。

若要開啓主控台：

- 選取「**開始**」>「**所有程式**」 >「**HP ProtectTools 管理主控台**」，或
- 按一下 Security Manager 主控台左下角的「**管理**」連結。

管理主控台由兩個側窗格組成：左側窗格和右側窗格。左側窗格包含管理工具。右側窗格包含用於設定工具的工作區域。

管理主控台的左側窗格由下列項目組成：

- **首頁** - 提供常用工作的快速存取途徑，包含啓用安全功能、指定安全憑證和管理使用者。
- **系統** - 管理全系統安全功能、使用者和驗證裝置的組態，例如智慧卡讀取器。
- **應用程式** - 包含設定 Security Manager 及其應用程式行爲的工具。
- **資料** - 提供備份與復原加密金鑰的工具。
- **電腦** - 提供進階安全性選項以選擇性地禁止可能危害電腦安全性的各類裝置，並爲不同的使用者和群組設定存取權限。

- **管理工具** - 會開啓預設瀏覽器並瀏覽至一個網頁，您可在該網頁可找到其他可擴充 Security Manager 功能的管理應用程式和工具，並在有新的應用程式和更新檔可用時通知您。
- **連結** - 提供下列項目：
  - **設定精靈** - 啓動「設定精靈」，該精靈會引導您逐步完成 Security Manager 的初始組態。
  - **說明** - 開啓說明檔，該說明檔提供有關 Security Manager 及其應用程式的資訊。
  - **關於** - 顯示有關 Security Manager 的資訊，包括版本編號和版權聲明。

設定精靈快速入門

HP ProtectTools Security Manager 的管理需要有管理權限。

HP ProtectTools Security Manager「設定精靈」會引導您逐步完成設定安全功能的程序。不過，您可以透過 HP ProtectTools Security Manager 主控台取得大量的其他功能。在精靈中找到的相同設定以及其他安全功能，都可以透過主控台設定，也可以從 Windows「開始」功能表或管理主控台內的連結存取。這些設定會套用至電腦和共用該電腦的所有使用者。

在第一次登入 Windows 時，系統會提示您設定 HP ProtectTools Security Manager。按一下「**確定**」以啓動 Security Manager「設定精靈」，精靈會引導您逐步完成設定程式的基本步驟。

附註： 您也可以按下管理主控台左側窗格底部區段的「**安全性精靈**」來啓動「安全性精靈」。

在「設定精靈」中，遵循畫面上的指示進行以完成設定。

若未完成精靈，則精靈將自動啓動直到您按一下「**不要再顯示此精靈**」爲止。

若要使用 HP ProtectTools Security Manager 應用程式，請由「**開始**」功能表或以滑鼠右鍵按一下工作列通知區域（系統匣）中的「**Security Manager**」圖示來啓動 HP ProtectTools Security Manager。共用此電腦的所有使用者都可使用 Security Manager 主控台及其應用程式。

設定系統

應用程式的「**系統**」群組，可由管理主控台左側的「**工具**」功能表存取。

藉由使用包含在此群組中的應用程式，您可以設定及管理此電腦及其使用者和裝置的原則和設定值。

下列應用程式包含在「系統」群組中。

- **安全性** - 管理安全功能、驗證原則和其他管理使用者在登入電腦或 HP ProtectTools 應用程式時的驗證方式的設定值。
- **使用者** - 設定、管理和註冊此電腦的使用者。
- **裝置** - 管理內建或連接至電腦的安全裝置的設定值。

啓用安全功能

這裡啓用的安全功能會套用至此電腦的所有使用者。

1. 在管理主控台的左側窗格中，展開「**安全性**」，並按一下「**功能**」。
2. 若要啓用安全功能，請按一下「**Windows 登入安全性**」和/或「**Drive Encryption**」旁邊對應的核取方塊。
   - **Windows 登入安全性** - 藉由要求使用特定認證才能存取的方式保護您的 Windows 帳戶。
   - **Drive Encryption** - 藉由加密硬碟使未獲正確授權的使用者無法讀取資訊的方式保護您的資料。
3. 按「**下一步**」按鈕。
4. 按一下「**套用**」按鈕。

定義 Security Manager 驗證原則

此電腦的 Security Manager 驗證原則被定義在兩個標籤（「登入」和「工作階段」）上，標籤會指定在使用者工作階段期間，存取電腦和 HP ProtectTools 應用程式時，驗證每一個類別的使用者所需的認證。

登入標籤

若要指定存取電腦所需的認證並登入 Windows：

1. 在管理主控台的左側窗格中，展開「**安全性**」，並按一下「**驗證**」。
2. 在「**登入**」標籤上，從下拉式清單中選取使用者類別。
3. 在「**原則**」區段中，按一下列出的認證旁邊的核取方塊，以指定選取的使用者類別所需的驗證認證。您必須至少指定一個認證。
4. 在「**原則**」區段的下拉式清單中，選擇需要「任何」（僅一個）指定的認證，或「所有」指定的認證，以驗證使用者。
5. 按一下「**套用**」按鈕。

工作階段標籤

若要定義在 Windows 工作階段期間登入 HP ProtectTools 應用程式時，用來管理驗證使用者所需認證的原則：

1. 在管理主控台的左側窗格中，展開「**安全性**」，並按一下「**驗證**」。
2. 在「**工作階段**」標籤上，選取使用者類別。
3. 在「**原則**」區段中，按下列出的認證旁邊的核取方塊，以指定選取的使用者類別所需的驗證認證。您必須至少指定一個認證。
4. 在「**原則**」區段的下拉式清單中，選擇需要「任何」（僅一個）指定的認證，或「所有」指定的認證，以驗證使用者。
5. 按一下「**套用**」按鈕。

定義設定值

您可以指定要允許的進階安全性設定。若要編輯設定值：

1. 在管理主控台的左側窗格中，展開「**安全性**」，並按一下「**設定**」。
2. 按一下適當的核取方塊以啓用或停用特定的設定。
3. 按一下「**套用**」按鈕以儲存變更。

附註： 如果已在 BIOS 層級執行驗證，則「**允許單一步驟登入**」設定會允許此電腦的使用者略過 Windows 登入。

管理使用者

在「使用者」應用程式中，Windows 管理員可管理此電腦的使用者和影響使用者的原則。若要存取管理主控台中的「使用者」應用程式，請按一下「**使用者**」。

HP ProtectTools 使用者都按照透過 Security Manager 所設定的驗證原則和符合該原則所需的認證列出和確認。

若要有效檢視適用於特定使用者的原則，請由清單選取該使用者，然後按一下「**檢視原則**」按鈕。

若要在使用者註冊認證時管理他們，請由清單中選取使用者，然後按一下「**註冊**」按鈕。

新增使用者

此程序會將使用者新增至登入清單。新增使用者之前，該使用者必須已在電腦中擁有 Windows 使用者帳戶，且必須在下列步驟進行時提供密碼。

若要新增使用者至使用者清單：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在管理主控台的左側窗格中，按一下「**使用者**」。
3. 按一下「**新增**」按鈕，「**選取使用者**」對話方塊隨即開啓。
4. 按一下「**進階**」按鈕，然後按一下「**立即尋找**」按鈕以搜尋要新增的使用者。
5. 按一下要新增至清單的使用者，然後按一下「**確定**」。
6. 在「**選取使用者**」對話方塊中按一下「**確定**」。
7. 輸入選取帳戶的 Windows 密碼，然後按一下「**完成**」。

附註： 您必須使用現有的 Windows 帳戶並確實輸入帳戶。您不能使用此對話方塊修改或新增 Windows 使用者帳戶。

移除使用者

附註： 此步驟不會刪除 Windows 使用者帳戶，而僅會將該帳戶從 Security Manager 移除。若要完全移除使用者，您必須將該帳戶從 Security Manager 及 Windows 移除。

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在管理主控台的左側窗格中，按一下「**使用者**」。

3. 按一下您想要移除的帳戶使用者名稱，然後按「**刪除**」。
4. 在確認對話方塊中，按一下「**是**」。

檢查使用者狀態

管理主控台的「使用者」區段會顯示每一個使用者目前的狀態：

- **綠色核取標記** - 表示使用者已設定所需的安全登入法。
- **紅色 X** - 表示使用者尚未設定所需的安全登入法且將於嘗試登入時被鎖定，而無法登入電腦。使用者必須執行設定精靈以設定所需的登入法。
- **空白** - 表示不需要安全登入法。

設定應用程式設定值

「設定」視窗包含設定 Security Manager 及其應用程式行爲的工具。若要修改設定值：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在管理主控台的左側窗格中，按一下「**設定**」。
3. 在「**一般**」標籤上，選擇 HP ProtectTools Security Manager 的一般設定，然後按一下「**套用**」按鈕。
4. 在「**應用程式**」標籤上，選取要啓用或停用的應用程式，然後按一下「**套用**」按鈕。

附註： 在電腦重新啓動前，啓用或停用應用程式可能不會生效。

加密磁碟機

Drive Encryption for HP ProtectTools 可讓您加密電腦硬碟，即使硬碟已經移出電腦或送去進行資料復原服務，任何未獲授權卻試圖存取硬碟資料的人都無法讀取和存取資料。

若要啓用或停用 Drive Encryption，請按一下管理主控台中的「設定精靈」。

△ 注意： 請務必將加密金鑰備份至 USB 快閃磁碟機，並將裝置存放在安全的地方。 如果忘記密碼，此裝置是供您存取硬碟機的唯一途徑。

如需有關使用 Drive Encryption for HP ProtectTools 的詳細資訊，請參閱 位於第 29 頁的 Drive Encryption for HP ProtectTools。

管理裝置存取

Device Access Manager for HP ProtectTools 提供進階安全性選項，以選擇性地禁止可能危害電腦安全性的各類裝置。如需有關使用 Device Access Manager for HP ProtectTools 的詳細資訊，請參閱 位於第 42 頁的 Device Access Manager for HP ProtectTools。

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager 可大幅提昇您電腦的安全性。藉由使用 Security Manager 應用程式，您可以：

- 管理登入和密碼
- 輕鬆變更 Windows 密碼
- 設定驗證認證，包含智慧卡
- 拆解或清理硬碟
- 檢視磁碟機加密狀態
- 檢視裝置存取設定
- 備份與還原 Security Manager 資料

管理密碼

Credential Manager for HP ProtectTools（密碼管理員）會建立和管理登入，您可以藉由驗證註冊的認證來啓動和登入網站與程式。

如需有關管理密碼的詳細資訊，請參閱 位於第 32 頁的 Credential Manager for HP ProtectTools（密碼管理員）。

設定認證

您可以使用 Security Manager 認證來確認您就是本人。此電腦的管理員可以設定要在登入 Windows 帳戶、網站或程式時用來證明您身分的認證。

可用的認證可能因內建或連接至電腦的安全裝置而有所不同。每一個支援的認證在「認證」群組中都有一個項目。

變更 Windows 密碼

Security Manager 讓變更 Windows 密碼比透過 Windows 「控制台」變更還更簡單快速。

若要變更 Windows 密碼：

1. 在 HP ProtectTools Security Manager 中，按一下左側窗格中的「**認證**」。
2. 按一下「**Windows 密碼**」。
3. 在「**目前的 Windows 密碼**」方塊中輸入您目前的密碼。

4. 在「**新的 Windows 密碼**」和「**確認新密碼**」方塊中輸入新密碼。
5. 按一下「**變更**」。

拆解或清理檔案

File Sanitizer for HP ProtectTools 藉由覆寫無意義的資料至檔案的方式刪除檔案。這個稱爲「拆解」的程序，藉由使刪除的檔案非常難以復原的方式，大幅提昇資訊的安全性。File Sanitizer 使用所謂的「清理」程序，覆寫先前使用過的空間，進一步提升資訊安全性。使用 File Sanitizer 刪除的檔案無法使用作業系統或其他常用的檔案復原軟體加以復原。

如需有關使用 File Sanitizer for HP ProtectTools 的詳細資訊，請參閱 位於第 36 頁的 File Sanitizer for HP ProtectTools。

檢視磁碟機加密狀態

Drive Encryption 是由 Windows 管理員在管理主控台中設定的。使用者可以在 Security Manager 中檢視其加密狀態。

若要檢視磁碟機加密狀態：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**加密狀態**」。「加密狀態」頁面會顯示磁碟機加密是作用中或者沒有作用，以及哪一個磁碟機已經加密或未加密。

檢視裝置存取

「裝置存取」是由 Windows 管理員在管理主控台中設定的。使用者可以在 Security Manager 中檢視其裝置存取設定值。

若要檢視裝置存取設定值：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，展開「**Device Access Manager**」。
3. 若要檢視哪些裝置遭到拒絕存取，按一下「**簡易組態**」。裝置旁邊有核取標記的就是遭到拒絕存取。
4. 若要檢視哪些使用者或群組遭到拒絕存取，按一下「**裝置類別組態**」。
5. 按一下裝置以檢視哪些使用者或群組遭到拒絕或被允許存取裝置。

新增應用程式

其他應用程式可能可以爲此程式新增新的功能。

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**搜尋其他**」。

附註： 如果沒有「**搜尋其他**」連結，表示您電腦的管理員已經停用該連結。

3. 在「**新增應用程式**」標籤上，瀏覽並搜尋其他應用程式。
4. 在「**更新與訊息**」標籤上，您可以藉由選取「**通知我有關新的應用程式和更新的消息**」核取方塊並設定檢查更新的日數，以獲得有關新的應用程式與更新的消息，或者您也可以按一下「**立即檢查**」按鈕，立即檢查更新。

設定偏好設定

「偏好設定」頁面可讓您選取「**在工作列上顯示圖示**」核取方塊，以在工作列通知區域（系統匣）中顯示 Security Manager 圖示。

若要存取「偏好設定」頁面：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**進階**」，然後按一下「**偏好設定**」。
3. 核取或取消核取「**在工作列上顯示圖示**」核取方塊，然後按一下「**套用**」。

備份與還原

定期備份您的 Security Manager 資料是良好的作法。備份資料的頻率視資料變更的頻率而定。例如，如果每天新增新的登入，您可能應該每天備份資料。

備份也可以用來由一部電腦轉移到另一部電腦，這有時也稱爲匯入和匯出。請記住，僅限由本功能所備份的資料。

若要將備份檔案還原至其他電腦，或者是重新安裝作業系統的相同電腦，那麼在由備份檔案還原資料之前，系統必須先安裝 HP ProtectTools Security Manager。

備份資料

在備份資料時，您是把登入和認證資訊儲存在加密的檔案中，並且受到您輸入的密碼保護。

若要備份資料：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**進階**」，然後按一下「**備份與還原**」。
3. 按一下「**備份資料**」。
4. 選取要包含在備份中的模組。在大多數情況下，您會選取所有的模組。按「**下一步**」。
5. 輸入您的密碼以確認身份，然後按一下箭頭按鈕。
6. 輸入路徑和儲存檔案的名稱。根據預設，檔案將儲存至您的「文件」資料夾。按一下「**瀏覽**」以指定不同的位置。按「**下一步**」。
7. 輸入並確認保護檔案的密碼。
8. 按一下「**完成**」。

還原資料

您可以由先前透過 Security Manager 的「備份與還原」功能建立的檔案（該檔案受到密碼保護且經過加密），還原您的資料。

若要還原資料：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**進階**」，然後按一下「**備份與還原**」。
3. 按一下「**還原資料**」。
4. 輸入路徑和儲存檔案的名稱，或按一下「**瀏覽**」並選取檔案。
5. 輸入用於保護檔案的密碼，並按「**下一步**」。
6. 選取要還原資料的模組。在大多數情況下，就是所有列出的模組。按「**下一步**」。
7. 按一下「**完成**」。

變更 Windows 使用者名稱和圖片

Windows 使用者名稱和圖片會顯示在 Security Manager 的左上角。

若要變更使用者名稱和/或圖片：

1. 按一下 Security Manager 中具有使用者名稱和圖片的左上角區段。
2. 若要變更使用者名稱，請在「**Windows 使用者名稱**」方塊中輸入名稱。
3. 若要變更圖片，按一下「**選擇圖片**」按鈕，並瀏覽以選取圖片。
4. 按一下「**儲存**」按鈕以儲存變更。

6 Drive Encryption for HP ProtectTools

附註： Drive Encryption for HP ProtectTools 僅提供給某些機型。

當今，不論是您的電腦或是公司員工的電腦都有可能遭竊，使公司的重要資料受到嚴重破壞。一旦將電腦硬碟上的每項資料都加密，那麼即使硬碟已經移出電腦或送去進行資料復原服務，任何未獲授權卻試圖存取硬碟資料的人都無法讀取和存取資料。

Drive Encryption for HP ProtectTools 軟體透過加密您的硬碟機，提供完整的資料保護。 當 Drive Encryption 啓用時，您必須在 Windows 啓動前顯示的 Drive Encryption 登入畫面中進行登入。

Drive Encryption 無法在相同的 Windows 工作階段期間防範未經授權的存取。 當 PC 開機並且您輸入使用者名稱和密碼之後，硬碟機上的資料仍是加密的，但是可供系統上的任何使用者使用。 當您離開電腦時，請務必使用密碼保護您的 Windows 工作階段。

附註： Drive Encryption for HP ProtectTools 僅可在 HP ProtectTools 管理主控台中透過「設定精靈」啓用。

附註： 當配置在使用 AMD 處理器又具有 RAID 的系統上時，Drive Encryption 不受 64 位元作業系統的支援。

附註： Drive Encryption 不支援字典攻擊防範。

Drive Encryption：

- 可將內部硬碟中的所有資料都加密
- 提供簡易的密碼存取與預先開機驗證
- 支援 Microsoft Windows XP、Windows Vista 和 Windows 7

在 Drive Encryption for HP ProtectTools 中可執行各種工作：

- 管理 Drive Encryption
  - 加密或解密個別磁碟機
- 備份與復原
  - 建立備份金鑰
  - 執行復原

注意： 請務必將加密金鑰備份至 USB 快閃磁碟機，並將裝置存放在安全的地方。 如果忘記密碼，此裝置是供您存取硬碟機的唯一途徑。

注意： 如果您決定解除安裝 Drive Encryption 模組或者您目前使用備份與還原解決方案，則必須先解密所有的加密磁碟機。 沒有這麼做的話，您將無法存取加密磁碟機上的資料。 重新安裝 Drive Encryption 模組也無法讓您存取加密磁碟機。

設定程序

開啓 Drive Encryption

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

一般工作

啓用 Drive Encryption

使用 HP ProtectTools 管理主控台「設定精靈」啓用 Drive Encryption。

停用 Drive Encryption

使用 HP ProtectTools 管理主控台「設定精靈」停用 Drive Encryption。

在啓用 Drive Encryption 之後登入

啓用 Drive Encryption 並註冊使用者帳戶後，當您開啓電腦時，必須在 Drive Encryption 登入畫面進行登入：

附註： 如果 Windows 管理員已啓用 HP ProtectTools 管理主控台中的「預先開機安全性」，您將在電腦啓動後立即登入電腦，而不必再經過 Drive Encryption 登入畫面。

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。

進階工作

管理 Drive Encryption（管理員工作）

Drive Encryption 視窗可讓 Windows 管理員檢視和變更 Drive Encryption 的狀態（作用中/非作用中），以及檢視電腦上所有硬碟的加密狀態。

加密或解密個別磁碟機

1. 在管理主控台的左側窗格中，展開「**Drive Encryption**」，並按一下「**加密管理**」。
2. 按一下「**變更加密**」按鈕。
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）

Drive Encryption：「備份與復原」視窗可讓 Windows 管理員備份與復原加密金鑰。

建立備份金鑰

△ **注意：** 請務必將含有備份金鑰的儲存裝置存放在安全的地方，因爲萬一您忘記密碼，此裝置是供您存取硬碟機的唯一途徑。

1. 在管理主控台的左側窗格中，展開「**Drive Encryption**」，並按一下「**備份與復原**」。
2. 按一下「**備份金鑰**」按鈕。
3. 在「選取備份磁碟」頁面中，按一下要備份加密金鑰的裝置名稱，然後按「**下一步**」。
4. 閱讀下一頁所顯示的資訊，然後按「**下一步**」。

   加密金鑰會儲存在您所選擇的存放裝置。
5. 當確認對話方塊開啓時，按一下「**確定**」。

附註： 請參閱 Drive Encryption for HP ProtectTools「說明」檔案，以取得有關管理與執行復原的資訊。

7 Credential Manager for HP ProtectTools（密碼管理員）

當您使用 Password Manager 時，登入 Windows、網站和程式會更簡便也更安全。

您可以使用 Password Manager 設定網站和程式的登入畫面，以便快速而安全地存取。首先，Password Manager 會記憶您的登入和您在每一個登入畫面的輸入方塊中所輸入的特定資料。然後，一旦您造訪登入畫面，在確認身分後，Password Manager 就會自動填寫及提交資料。

爲了能更快速地存取，只要使用可設定的快速鍵組合（預設的是 Ctrl+Windows+H），就可以顯示您的登入的功能表。在功能表上，只要選取登入，Password Manager 就會啓動該網站或程式，瀏覽至登入畫面，並自動將您登入。

爲了驗證身分，您要使用自己的 HP ProtectTools for Small Business 認證，例如您的 Windows 密碼。這表示您將會使用相同的認證，登入所有您設定的登入畫面。因此，您可以建立強度更大的密碼，而不必抄下或記憶它，使您的帳戶更安全。

Password Manager 可讓您檢視任何您的密碼是否有安全性風險，並自動產生一個強式、複雜的密碼，以便用於新網站。

有了 Password Manager，您就可以檢視自己的登入及密碼，並隨時編輯它們。許多 Password Manager 功能也可以由 Password Manager 圖示取得，只要已設定的程式的登入畫面或者任何網站的登入畫面顯示時，就會顯示該圖示，按一下該圖示就會顯示快顯功能表，供您從中選擇下列選項。

適用於尚未建立登入的網頁或程式：

下列選項會顯示在快顯功能表上。

- 新增 [某網域.com] 至 Password Manager – 用來新增目前登入畫面的登入。
- 開啓 Password Manager – 在 Password Manager 頁面上啓動 Security Manager。
- Password Manager 圖示設定 – 可讓您指定 Password Manager 顯示的條件。
- 說明 – 顯示 Password Manager 應用程式的線上說明。

適用於已經建立登入的網頁或程式：

下列選項會顯示在快顯功能表上。

- 填寫登入資料 – 將您的登入資料填入登入欄位中然後提交該頁面（如果登入建立或最後編輯時曾經指定提交）。
- 編輯登入 – 可讓您編輯此網站的登入資料。
- 新增登入 – 用來新增相同網站或程式的其他登入。

- 開啓 Password Manager – 在 Password Manager 頁面上啓動 Security Manager 儀表板。
- 說明 – 顯示 Password Manager 應用程式的線上說明。

新增登入

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 圖示上的箭頭，然後選取下列其中一項（視登入畫面屬於網站或程式而定）。
   - 適用於網站 – 選取「**新增 [網域名稱] 至 Password Manager**」。
   - 適用於程式 – 選取「**新增此登入畫面至 Password Manager**」。
3. 輸入您的登入資料。畫面上的登入欄位及其在對話方塊上的對應欄位，都以粗的橘色線條標示。也有其他顯示此對話方塊的選項可用，例如從 Password Manager 的「**管理**」標籤選取「新增登入」。某些選項會視連接至電腦的安全裝置而定；例如使用 Ctrl-H 快速鍵或插入智慧卡。
   - 按一下登入欄位右邊的箭頭，以使用多個預先格式化的選擇其中之一填入欄位。
   - 或者，也可按一下「**選擇其他欄位**」從畫面新增其他欄位至您的登入。
   - 如果想要將資料填入登入欄位但不要提交，請取消選取「**提交登入資料**」。
   - 如果想要檢視此登入的密碼，按一下「**顯示密碼**」。
4. 按一下「**確定**」。加號會從 Password Manager 圖示移除，讓您知道登入已經建立

現在，每次您登入該網站或啓動該程式時，Password Manager 圖示就會顯示，並表示可以使用您註冊的認證登入。

編輯登入

若要編輯登入：

1. 開啓網站或程式的登入畫面。
2. 按一下 Password Manager 圖示上的箭頭，然後選取「**編輯登入**」以顯示可供您編輯登入資訊的對話方塊。畫面上的登入欄位及其在對話方塊上的對應欄位，都以粗的橘色線條標示。
3. 編輯您的登入資訊。
   - 按一下登入欄位右邊的箭頭，以使用多個預先格式化的選擇其中之一填入欄位。
   - 或者，也可按一下「**選擇其他欄位**」從畫面新增其他欄位至您的登入。
   - 如果想要將資料填入登入欄位但不要提交，請取消選取「**提交帳戶資料**」。
   - 如果想要檢視此登入的密碼，按一下「顯示密碼」。
4. 按一下「**確定**」。

使用登入功能表

Password Manager 提供快速而便捷的方式以啓動已經建立登入的網站和程式。只要在「登入」功能表，或者在 Password Manager 中的「**管理**」標籤上連按兩下程式或網站圖示，就會啓動其登入畫面並填入您的登入資料。根據預設，資訊也會立即提交給網站，雖然您可以在初始設定或編輯登入時，取消選取「**提交帳戶資料**」。

當您建立登入時，它就會自動新增至您的 Password Manager「登入」功能表。

若要顯示「登入」功能表，請按下 Password Manager 快速鍵組合。Ctrl-H 是預設的組合，不過您也可以從「**Password Manager**」>「**設定**」中變更快速鍵組合。

按類別組織登入

使用類別使您的登入井然有序。建立一個以上的類別非常容易，只要將您的登入拖放至想要的類別中即可。

若要新增類別：

1. 在 Security Manager 左側窗格中，選取「**Password Manager**」。
2. 選取「**管理**」標籤，然後按一下「**新增類別**」。
3. 輸入類別的名稱。
4. 按一下「**確定**」。

若要新增登入至類別：

1. 將滑鼠指標放在想要的登入上。
2. 按下並按住滑鼠左鍵。
3. 將登入拖曳至類別清單中。當您將滑鼠移至類別上時，類別將反白顯示。
4. 當想要的類別反白顯示時，請釋放滑鼠按鈕。

您的登入並未移至該類別，只是複製到選取的類別。那表示您可將相同的登入新增至一個以上的類別。而且，只要按一下「**全部**」，就可以看見您所有的登入。

管理登入

Password Manager 讓您從集中位置無痛而直覺地管理登入資訊（使用者名稱、密碼和多個登入帳戶）。

您的登入列示在「**管理**」標籤上。當您爲相同網站建立多個登入時，每一個登入都會縮排列示在該網站名稱的登入清單中。

若要管理登入：

在 Security Manager 左側窗格中，選取「**Password Manager**」並按一下「**管理**」標籤。

- 新增登入 – 按一下「**新增登入**」並遵循畫面指示進行。
- 編輯登入 – 選取登入並按一下「**編輯**」。然後根據需要變更登入資料。
- 刪除登入 – 選取登入並按一下「**刪除**」。

若要爲網站或程式新增其他登入：

1. 啓動網站或程式的登入畫面。
2. 按一下 Password Manager 圖示以顯示其捷徑功能表。
3. 選取「**新增其他登入**」並遵循畫面指示進行。

評估密碼強度

使用強式密碼登入您的網站和程式，是保護您的身份的重要措施。

Password Manager 藉由立即自動分析您用於登入網站和程式的每一個密碼的強度，使監控和提升安全性更加容易。您可以在 Password Manager 的「**密碼強度**」標籤上，檢查用於登入的密碼強度。

Password Manager 圖示設定值

Password Manager 會嘗試識別網站和程式的登入畫面。當 Password Manager 找到您尚未爲其建立登入的登入畫面時，它會藉由顯示具有「+」號的 Password Manager 圖示提示您爲該畫面新增登入。

下列設定值皆可設定：

- 永遠提示 – 選取此選項讓 Password Manager 在顯示的登入畫面尚未設定登入時，提示您爲它新增登入。
- 不要爲此畫面提示 – 選取此選項則 Password Manager 將不會再次提示您爲此特定登入畫面新增登入。
- 永不提示 – 選取此選項以確保 Password Manager 永遠不會提示您尚未設定的登入畫面。

8 File Sanitizer for HP ProtectTools

File Sanitizer 這項工具可讓您安全清除電腦上的重要檔案和資料夾（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： File Sanitizer 目前只能在硬碟上作業。

關於拆解

刪除 Windows 中的檔案和/或資料夾並不會將內容從您的硬碟中完全移除。Windows 只會刪除參考，內容仍然保留在硬碟中，直到其他檔案以新的資訊覆寫硬碟上的相同區域爲止。

拆解不同於標準的 Windows 刪除（在 File Sanitizer 中又稱爲簡易刪除），因爲當您拆解資料時，就幾乎不可能擷取該資料。

當您選擇一個拆解設定檔（「高安全性」、「中安全性」或「低安全性」）時，系統會自動選取拆解所需的預先定義檔案和/或資料夾清單以及清除方法。您也可以自訂拆解設定檔，以便用來指定拆解的週期數、要包括在拆解之列的檔案、要在拆解前先確認的檔案以及要排除在拆解之外的檔案。

您可以設定自動拆解排程，也可以在需要時手動拆解檔案和/或資料夾。

關於可用空間清理

可用空間清理可讓您在刪除的檔案上安全地寫入隨機資料，預防使用者檢視已刪除檔案的原始內容。

附註： 可用空間清理適用於使用「Windows 資源回收筒」所刪除的檔案，也適用於手動刪除檔案之時。可用空間清理沒有對拆解的檔案提供其他安全性。

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。

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**」，然後按一下「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 左側窗格中，按一下「**File Sanitizer**」。

   － 或 －

- 在「**File Sanitizer**」圖示上連按兩下。

  － 或 －

- 在工作列最右邊之通知區域內的 HP ProtectTools 圖示上按一下滑鼠右鍵，反白顯示「**File Sanitizer**」，然後按一下「**開啓 File Sanitizer**」。

設定可用空間清理排程

若要設定可用空間清理排程：

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**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「**儲存**」圖示。

附註： 可用空間清理作業可能需要很長的時間。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速度變慢。

設定拆解排程

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**拆解**」。
2. 選取拆解選項：

   - **Windows 關閉** — 選擇此選項以便在 Windows 關機時拆解所有選取的檔案。

     附註： 當您選取此選項時，系統會在關機時顯示對話方塊，詢問您要繼續拆解選取的檔案，還是要略過該程序。按一下「是」以略過拆解程序，或按一下「否」繼續拆解。您必須迅速選取「是」或「否」選項，因爲 Windows 將會關閉該軟體以準備關機，因而產生錯誤。如果選取「否」以繼續拆解，Windows 可能會產生錯誤訊息指出 File Sanitizer 沒有回應。請等候 File Sanitizer 完成拆解，然後起再次啓動關機程序。

   - **Web 瀏覽器開啓** — 選擇此選項以便在開啓 Web 瀏覽器時拆解所有選取的網路相關檔案，例如瀏覽器 URL 歷程記錄。
   - **Web 瀏覽器結束** — 選擇此選項以便在關閉 Web 瀏覽器時拆解所有選取的網路相關檔案，例如瀏覽器 URL 歷程記錄。

- **按鍵順序** — 選擇此選項以使用按鍵順序啓動拆解。
- **排程器** — 請選取「啓用排程器」核取方塊，並輸入您的 Windows 密碼，然後輸入要拆解所選取檔案的日期和時間。

3. 按一下「**儲存**」圖示。

選取或建立拆解設定檔

您可以選取預先定義的拆解設定檔或建立您自己的設定檔，以指定清除的方法並選取要拆解的檔案和/或資料夾。

選取預先定義的拆解設定檔

當您選擇一個拆解設定檔（「高安全性」、「中安全性」或「低安全性」）時，系統會自動選取預先定義的清除方法和檔案清單。您可以按一下「檢視詳細資料」按鈕，檢視所選取要拆解之檔案的預先定義清單。

若要選取預先定義的拆解設定檔：

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**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之檔案的清單。
4. 在「**拆解下列項目**」底下，選取要在拆解前先確認之每個檔案旁邊的核取方塊。
5. 按一下「**套用**」。

自訂進階安全性拆解設定檔

當您建立拆解設定檔時，您可以指定拆解的週期數、要包括在拆解之列的檔案、要在拆解前先確認的檔案，以及要排除在拆解之外的檔案：

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」，按一下「**設定**」，選取「**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： 選取的拆解週期數將會針對每個檔案來執行。例如，如果您選擇 3 個拆解週期數，就會分別執行 3 次清除資料的演算法。如果您選擇高安全性拆解週期，則拆解可能會花費相當長的時間，但是您指定的拆解週期數越高，電腦就越安全。

3. 選取您要拆解的資產：
   a. 在「**可用的拆解選項**」底下，按一下檔案，然後按一下「**新增**」。
   b. 若要新增自訂檔案，請按一下「**新增自訂選項**」，輸入或瀏覽檔案名稱或資料夾名稱，然後按一下「**確定**」。按一下自訂檔案，然後按一下「**新增**」。

   附註： 若要從可用的拆解選項刪除檔案，請按一下檔案，然後按一下「**刪除**」。

4. 在「**拆解下列項目**」底下，選取要在拆解前先確認之每個檔案旁邊的核取方塊。

附註： 若要從拆解清單移除檔案，請按一下檔案，然後按一下「**移除**」。

5. 在「**請勿拆解下列項目**」底下，按一下「**新增**」以選取要排除在拆解外的特定檔案。

6. 當您完成設定拆解設定檔時，按一下「**套用**」。

自訂單純刪除設定檔

單純刪除設定檔會執行標準的檔案刪除，但不進行拆解。當您自訂單純刪除設定檔時，您可以指定要包括在單純刪除之列的檔案、要在執行單純刪除前先確認的檔案，以及要排除在單純刪除之外的檔案：

附註： 如果使用單純刪除，強烈建議您定期執行可用空間清理。

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」，按一下「**設定**」，選取「**單純刪除設定**」，然後按一下「**檢視詳細資料**」。

2. 選取您想要刪除的檔案：

   a. 在「**可用的刪除選項**」底下，按一下某個檔案，然後按一下「**新增**」。

   b. 若要新增自訂檔案，請按一下「**新增自訂選項**」，輸入或瀏覽檔案名稱或資料夾名稱，然後按一下「**確定**」。按一下自訂檔案，然後按一下「**新增**」。

   附註： 若要從可用的刪除選項刪除檔案，請按一下檔案，然後按一下「**刪除**」。

3. 在「**刪除下列項目**」底下，選取要在刪除前先確認之每個檔案旁邊的核取方塊。

附註： 若要從刪除清單移除檔案，請按一下檔案，然後按一下「**移除**」。

4. 在「**請勿刪除下列項目**」底下，按一下「**新增**」，以選取要排除在拆解外的特定檔案。

5. 當完成設定單純刪除設定檔時，按一下「**套用**」。

一般工作

使用按鍵順序啓動拆解

若要要指定按鍵順序，依照下列步驟執行：

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**拆解**」。

2. 選取「**按鍵順序**」核取方塊。

3. 在可用方塊中輸入字元，然後選取「**CTRL**」、「**ALT**」或「**SHIFT**」方塊，或者三個都選。

   例如，若要使用 S 鍵和 Ctrl+Shift 鍵，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與您已經設定的其他按鍵順序不同。

若要使用按鍵順序啓動拆解：

1. 按下選擇的字元時，按住 Ctrl、Alt 或 Shift 鍵（或任何您指定的組合鍵）。

2. 如果確認對話方塊開啓，請按一下「**是**」。

使用 File Sanitizer 圖示

△ **注意：** 拆解過的檔案無法復原。請仔細考慮要選取哪些項目進行手動拆解。

1. 瀏覽至您要拆解的文件或資料夾。
2. 將檔案拖曳至桌面上的 File Sanitizer 圖示。
3. 當確認對話方塊開啓時，按一下「**是**」。

手動拆解一項資產

△ **注意：** 拆解過的檔案無法復原。請仔細考慮要選取哪些項目進行手動拆解。

1. 在工作列最右邊之通知區域內的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，反白顯示「**File Sanitizer**」，然後按一下「**拆解一項**」。
2. 開啓「瀏覽」對話方塊時，請瀏覽至您要拆解的檔案，然後按一下「**開啓**」。

附註： 您選取的檔案可以是單一檔案或資料夾。

3. 當確認對話方塊開啓時，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「**拆解一項**」。
2. 開啓「瀏覽」對話方塊時，請瀏覽至您要拆解的檔案，然後按一下「**確定**」。
3. 當確認對話方塊開啓時，按一下「**是**」。

－ 或 －

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**拆解**」。
2. 按一下「**瀏覽**」按鈕。
3. 開啓「瀏覽」對話方塊時，請瀏覽至您要拆解的檔案，然後按一下「**開啓**」。
4. 當確認對話方塊開啓時，按一下「**是**」。

手動拆解所有選取的項目

1. 在工作列最右邊之通知區域內的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，反白顯示「**File Sanitizer**」，然後按一下「**立即拆解**」。
2. 當確認對話方塊開啓時，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. 當確認對話方塊開啓時，按一下「**是**」。

手動啓動可用空間清理

1. 在工作列最右邊之通知區域內的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，反白顯示「**File Sanitizer**」，然後按一下「**立即清理**」。
2. 接著會出現一個通知氣泡，確認清理作業已經開始。

－ 或 －

1. 在 Security Manager 左側窗格中，展開「**File Sanitizer**」並按一下「**清理**」。
2. 按一下「**立即清理**」。
3. 接著會出現一個通知氣泡，確認清理作業已經開始。

中止拆解或可用空間清理作業

當拆解或可用空間的清理作業正在進行時，會在通知區域的 HP ProtectTools Security Manager 圖示上方顯示一則訊息。訊息會提供拆解或可用空間清理程序的詳細資訊（完成百分比），並讓您有中止作業的選擇。

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。

一個記錄檔是爲拆解作業建立的，而另一個記錄檔則是爲可用空間清理作業而建立。兩個記錄檔案都放在硬碟的下列位置：

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

9 Device Access Manager for HP ProtectTools

這個安全性工具僅適用於管理員。Device Access Manager for HP ProtectTools 具有下列安全功能，可防止未獲授權者存取電腦系統附加的裝置：

- 裝置設定檔是針對每個使用者所建立，以定義裝置存取權
- 裝置存取權可以依據群組成員資格來授與或拒絕

附註： Device Access Manager 使用 Windows「本機使用者和群組」管理存取。Windows Home 版本不支援「本機使用者和群組」，所以無法正常執行 Device Access Manager。不過，如果使用 DOS 指令進行使用者設定，Device Access Manager 將可在 Microsoft Windows Vista Home 版中運作。請參閱 Device Access Manager 「說明」檔以取得說明。

啓動背景服務

爲了套用裝置設定檔，HP ProtectTools 裝置鎖定/稽核背景服務必須正在執行。在您首次嘗試套用裝置設定檔時，HP ProtectTools 管理主控台會開啓一個對話方塊，詢問您是否要開始背景服務。按一下「**是**」以開始背景服務，並將其設定爲每次系統開機時都自動執行。

簡易組態

Device Access Manager 會在初始化階段建立新的「使用者群組」，稱爲「裝置管理員」，以管理員身份存取或瀏覽裝置。經由 Device Access Manager 簡易設定，針對您所控制的裝置，將您要授予管理員存取權限的使用者放入此一群組中。

這項功能可以讓您拒絕下列裝置類別的存取：

- 所有非裝置管理員適用的 USB 裝置
- 所有非裝置管理員適用的所有抽取式磁碟（磁片、個人音樂播放器、隨身碟等等）
- 所有非裝置管理員適用的所有 DVD/CD-ROM 光碟機
- 所有非裝置管理員適用的所有序列埠和並列埠

若要拒絕所有非裝置管理員存取一種等級的裝置：

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，按一下「**Device Access Manager**」，然後再按一下「**簡易組態**」。
3. 在右側窗格中，選擇要拒絕存取之裝置的核取方塊。

4. 按一下「**儲存**」圖示。

附註： 如果背景服務並未執行，便會在此時嘗試啓動。按一下「**是**」允許啓動背景服務。

5. 按一下「**確定**」。

裝置類別組態（進階）

您還可以使用其他選項，准許或拒絕特定使用者或使用者群組存取裝置類型。

新增使用者或群組

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 按一下「**新增**」。「**選擇使用者或群組**」對話方塊便會開啓。
5. 按一下「**進階**」，然後按一下「**立刻尋找**」以搜尋要新增的使用者或群組。
6. 按一下使用者或群組以便新增至可用的使用者與群組清單中，然後按一下「**確定**」。
7. 按一下「**確定**」。

移除使用者或群組

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 按一下您要移除的使用者或群組，再按一下「**移除**」。

拒絕或允許存取使用者或群組

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 在「**使用者/群組**」之下，按一下要拒絕存取的使用者或群組。
5. 按一下要拒絕存取之使用者或群組旁邊的「**拒絕**」。
6. 按一下「**儲存**」，然後按「**確定**」。

使用者存取設定（進階）

「使用者存取設定」可讓管理員指定哪些使用者和群組可以使用「簡易組態」與「裝置類別組態」檢視。

使用者或群組必須獲准存取「**檢視組態設定（唯讀）**」，以檢視「簡易組態」和「裝置類別組態」資訊。

使用者或群組必須獲准存取「**變更組態設定**」，以變更「簡易組態」和「裝置類別組態」資訊。

使用者或群組必須獲准存取「**完整使用者管理員權限**」，以修改「簡易組態」和「裝置類別組態」檢視中的設定。

新增使用者或群組

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
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「**立即尋找**」以搜尋要新增的使用者或群組。
5. 按一下要新增至可用使用者和群組清單的使用者或群組，然後按一下「**確定**」。
6. 按一下「**確定**」。
7. 按一下「**儲存**」圖示。

移除使用者或群組

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
3. 按一下您想要移除的使用者或群組，然後按「**移除**」。
4. 按一下「**儲存**」圖示。

允許或拒絕權限

1. 依序按一下「**開始**」、「**所有程式**」，然後按一下「**HP ProtectTools 管理主控台**」。
2. 在左側窗格中，展開「**Device Access Manager**」，然後按一下「**使用者存取設定**」。
3. 在「**群組或使用者名稱**」方塊中，選取使用者或群組名稱。
4. 在「**權限**」方塊中，選取「**允許**」或「**拒絕**」核取方塊授予適當的權限。
5. 按一下「**儲存**」圖示。

辭彙

Automatic Technology Manager (ATM)。
允許網路管理員以 BIOS 等級遠端管理系統。

Windows 使用者帳戶。
有權登入網路或個人電腦的個人設定檔。

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。

可用空間清理。
爲模糊已刪除檔案之內容而在硬碟上以隨機資料對已刪除檔案所進行的安全寫入，這會讓資料更不易復原。

安全登入法。
用來登入電腦的方法。

自動拆解。
使用者在 File Sanitizer for HP ProtectTool 中已設定的拆解排程。

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。

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。

重新開機。
電腦的重新啓動程序。

清理。
請參閱「**釋放空間整理**」。

單純刪除。
安全地刪除機密資訊，包括檔案、歷程或網路相關內容或其他機密資料。

開機驗證。
開啓電腦時會要求某種形式之驗證（例如密碼）的安全功能。

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。

管理員。
請參閱「Windows 管理員」。

網域。
屬於網路一部分的電腦群組，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。
使用者在驗證程序中據以證明具備特定工作資格的方法，例如使用者名稱及密碼。

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