HP Client Security

快速入門

第一版：2013 年 8 月

文件編號：735339-AB1

目錄

1 HP Client Security Manager 使用介紹

HP Client Security 允許您保護資料、裝置和身分，藉此強化電腦的安全性。

可供您的電腦使用的軟體模組會因機型而有所不同。

您可以預先安裝、預先載入或從 HP 網站下載 HP Client Security 軟體模組。如需更多資訊，請參閱 http://www.hp.com。

附註： 本指南中的指示是假設您已經安裝適用的 HP Client Security 軟體模組。

HP Client Security 功能

下表詳細說明 HP Client Security 模組的主要功能。

模組	關鍵功能
HP Client Security Manager	管理員可以執行下列功能： • 在 Windows® 啟動前保護您的電腦 • 使用強式驗證保護您的 Windows 帳戶 • 管理網站及應用程式的登入和密碼 • 輕鬆變更 Windows® 作業系統密碼 • 使用指紋強化安全性並提升便利性 • 設定智慧卡、非接觸式卡片或鄰近感應式卡片以進行驗證 • 使用您的 Bluetooth 電話作為識別方法 • 設定 PIN 以展開驗證選項 • 設定登入和工作階段原則 • 備份和還原程式資料 • 新增更多應用程式，例如 HP Drive Encryption、HP File Sanitizer、HP Trust Circles、HP Device Access Manager 及 HP Computrace 一般使用者可以執行以下功能： • 檢視「加密狀態」和「裝置存取管理員」的設定。 • 啟動 Computrace。 • 設定「偏好設定」與「備份和還原」選項。

模組	關鍵功能
Password Manager	一般使用者可以執行下列功能： • 組合管理與設定使用者名稱和密碼。 • 為電子郵件與網站帳戶建立更強有力的密碼，以提升帳戶安全性。Password Manager 會自動填入和提交資訊。 • 透過可自動記住並套用使用者認證的單次登入功能，簡化登入程序。 • 將一個帳戶標記為已洩漏，若其他帳戶有類似的認證，您將受到警告。 • 從支援的瀏覽器匯入登入資料。
HP 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。 • 提供可啟用自我加密磁碟機的選項（僅限特定機型）。
HP Device Access Manager	• 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通訊裝置的存取。
HP Trust Circles	• 提供檔案和文件的安全性。 • 加密檔案置於特定使用者資料夾內，並將檔案保護於 trust circle 內。 • 僅允許 trust circle 內的成員使用與分享檔案。
竊盜追失（Computrace，需另外購買）	• 必須另外購買追蹤與追查訂閱才能啟用。 • 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。

HP Client Security 產品說明和常見使用範例

大多數的 HP Client Security 產品都同時擁有使用者驗證（通常是密碼）和管理備份，以便在密碼遺失、無法使用或忘記時，或者因公司安全需要存取 or 的任何時候，獲得存取權。

附註： 有些 HP Client Security 產品的設計是為了限制對資料的存取。當資料重要到使用者寧可失去資訊而不願意受到危害時，應該加密該資料。建議在安全的位置備份所有資料。

Password Manager

Password Manager 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。

- 將一個帳戶標記為已洩漏，若其他帳戶有類似的認證，您將受到警告。
- 從支援的瀏覽器匯入登入資料。

範例 1：她是一位大型製造商的採購人員，透過網際網路為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 Password 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，Password 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 Password Manager 顯示。

Password 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：勤奮的員工升職了，現在他管理整個會計部門。這個團隊必須大量登入客戶的 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。 該員工決定使用 Password Manager 管理所有網路連結、公司使用者名稱、和密碼。完成後，該員工部署 Password Manager 至其他員工的電腦，讓他們能夠處理網路帳戶，但絕不會得知所使用的登入認證。

HP Drive Encryption（僅限特定機型）

HP Drive Encryption 用來限制對整個電腦硬碟或次要磁碟機上資料的存取。Drive Encryption 也可以管理自動加密磁碟機。

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。這位醫生啟用 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，若未在作業系統啟動之前提供密碼，就無法存取硬碟。醫生還能選擇使用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。

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為 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啟動電腦或網域。

HP Device Access Manager（僅限特定機型）

HP Device Access Manager 可讓管理員限制與管理對硬體的存取。Device Access Manager 可以用來阻止未經授權者存取可以在其中複製資料的 USB 快閃磁碟機。它也可以限制對 CD/DVD 光碟機的存取、對 USB 裝置的控制以及網路連線等等。例如，當外部廠商需要存取公司電腦，但應該不能夠將資料複製到 USB 磁碟機時。

範例 1： 醫療器材公司的管理員通常要處理個人醫療記錄及其公司資訊。員工必須存取此資料，但重要的是，不得透過 USB 磁碟機或其他任何外接式儲存媒體，從電腦移除該資料。網路的安全無虞，但是電腦所擁有的 CD 燒錄器和 USB 連接埠，可能會讓該資料遭到複製或竊取。因此，管理員會使用 Device Access Manager 停用 USB 連接埠和 CD 燒錄器，讓員工無法使用這兩者。即使 USB 連接埠遭到封鎖，滑鼠和鍵盤還是可以繼續運作。

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 啟用這些員工的存取權，而封鎖其他員工的外部存取。

Computrace（需另外購買）

Computrace（需另外購買）是一種服務，可以在使用者每次存取網際網路時，追蹤遭竊電腦的位置。Computrace 也可以協助遠端管理及尋找電腦，以及監視電腦使用情況和應用程式。

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。

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。

達成關鍵安全性目標

HP Client Security 模組可以共同運作，為各種安全性問題提供解決方案，包括以下的主要安全性目標：

- 防範針對性的竊盜行為
- 限制對敏感資料的存取
- 防範來自內部或外部位置的未經授權存取
- 建立強式密碼原則

防範針對性的竊盜行為

針對性的竊盜行為，範例之一就是在機場安檢站，針對含有機密資料和客戶資訊的電腦行竊。下列功能可以協助防範針對性的竊盜行為：

- 啟用預先開機驗證功能時，有助於防止存取作業系統。
  - HP Client Security—請參閱位於第 11 頁的 HP Client Security。
  - HP Drive Encryption — 請參閱位於第 25 頁的 HP Drive Encryption（僅限特定機型）。
- 即使硬碟被取下並安裝到未受保護的系統，加密仍可協助確保其中的資料無法存取。
- Computrace 可以在電腦失竊後追蹤其位置。
  - Computrace — 請參閱位於第 44 頁的竊盜復原（僅限特定機型）。

限制對敏感資料的存取

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

- HP Device Access Manager 可以讓 IT 管理員限制存取通訊裝置，如此便無法從硬碟複製敏感性的資訊。請參閱位於第 36 頁的系統檢視。

防範來自內部或外部位置的未經授權存取

未經授權的情況下存取不安全的企業電腦可能對公司網路資源造成極大的風險，例如從金融服務、行政、或研發團隊獲取資訊，或是如病人記錄或個人財務記錄等私人資訊。下列功能可以協助防止未經授權的存取：

- 啟用預先開機驗證功能時，有助於防止存取作業系統。（請參閱位於第 25 頁的 HP Drive Encryption（僅限特定機型）。
- HP Client Security 協助確保未經授權的使用者無法取得密碼，或存取經密碼保護的應用程式。請參閱位於第 11 頁的 HP Client Security。
- HP Device Access Manager 可以讓 IT 管理員限制存取可寫入裝置，如此便無法從硬碟複製敏感性的資訊。請參閱位於第 35 頁的 HP Device Access Manager（僅限特定機型）。

建立強式密碼原則

如果因公司政策而需使用強大的密碼，以管理數十個以網路為基礎的應用程式與資料庫，Password Manager 提供受保護的密碼管理庫，以及單一登入便利性。請參閱位於第 16 頁的 Password Manager。

其他安全性要素

指派安全性角色

在管理電腦安全性時（尤其是在大型組織中），將責任和權限分配給各種類型的管理員和使用者，是很重要的實務做法。

附註： 在小型組織或個人使用方面，這些角色可能都由同一人掌握。

對於 HP Client Security，可以將安全性職責與權限分成下列角色：

- 保全人員 — 定義公司或網路的安全性等級，並決定要部署的安全性功能，例如 Drive Encryption。

  附註： 保全人員可以與 HP 合作，共同自訂 HP Client Security 中的多項功能。如需更多資訊，請參閱 http://www.hp.com。

- IT 管理員 — 套用及管理由保全人員定義的安全性功能。也可以啟用和停用部分功能。例如，當保全人員決定要佈署部署智慧卡時，IT 管理員可以同時啟用密碼和智慧卡模式。
- 使用者 — 使用安全性功能。例如，如果保全人員和 IT 管理員已經為系統啟用智慧卡，使用者就可以設定智慧卡 PIN 碼，並使用該智慧卡進行驗證。

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

未經授權的使用者不應該被授予管理權限。

管理 HP Client Security 密碼

大部分的 HP Client Security 功能都以密碼保護。下表列出常用密碼、設定密碼所在的軟體模組，以及密碼功能。

僅限由 IT 管理員設定與使用的密碼會在表格中特別指明。所有其他密碼則可由一般使用者或管理員設定。

HP Client Security 密碼	在下列模組中設定	功能
Windows 登入密碼	Windows 控制台或 HP Client Security	可以用作手動登入和驗證，以存取各種 HP Client Security 功能。
HP Client Security 備份與復原密碼	個別使用者操作 HP Client Security	保護 HP Client Security 備份與復原檔案的存取。
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（如果已選取智慧卡的話）。

建立安全密碼

建立密碼時，您必須先遵循程式設定的規格。然而一般而言，請考量下列準則，以利您建立強式密碼並減少密碼遭到洩露的可能性：

- 使用至少包含 6 個字元的密碼，最好是超過 8 個字元。
- 在密碼中混合使用字母大小寫。
- 如果可能的話，在密碼中混合使用英數字元，並加入特殊字元和標點符號。
- 使用特殊字元或數字來代替關鍵字中的字母。例如，您可以使用數字 1 來代替字母 I 或 L。

- 合併使用 2 種以上語言的單字。
- 在中間使用數字或特殊字元分隔字或詞，例如 "Mary2-2Cat45"。
- 不要使用可能會出現在字典中的密碼。
- 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）做為密碼，即使您倒過來拼寫也不可以。
- 經常變更密碼。您可以逐次變更密碼中的幾個字元。
- 如果您要將密碼寫下來，請不要將它放在非常靠近電腦的常見位置。
- 不要將密碼儲存在電腦的檔案中，例如電子郵件。
- 不要共用帳戶或是向任何人告知您的密碼。

備份認證與設定

使用 HP Client Security 中的「備份與復原」工具，您可於中心管理備份，並從某些已安裝之 HP Client Security 模組中還原安全性認證。

2 快速入門

若要設定 HP Client Security 搭配您的認證使用，請使用下列其中一種方式啟動 HP Client Security。當精靈完成後，便無法由其他使用者再次啟動。

1. 從「開始」或「應用程式」畫面，按一下或點選 **HP Client Security** 應用程式 (Windows 8)。

   － 或 －

   從 Windowds 桌面，按一下或點選 **HP Client Security Gadget** 應用程式 (Windows 7)。

   － 或 －

   從 Windows 桌面的工作列最右端的通知區域中，連按兩下或點選兩下 **HP Client Security** 圖示。

   － 或 －

   在 Windows 桌面上，按一下或點選通知區域中的 **HP Client Security** 圖示，然後選取**開啟 HP Client Security**。

2. 隨即會啟動 HP Client Security 設定精靈並顯示「歡迎」頁面。

3. 閱讀「歡迎」頁面，輸入您的 Windows 密碼來驗證您的身分，然後按一下或點選**下一步**。

   如果您尚未建立 Windows 密碼，系統會提示您建立一組密碼。需要 Windows 密碼，才能確保經過授權的人員存取 Windows 帳戶，並使用 HP Client Security 功能。

4. 在 HP SpareKey 頁面上，選取三個安全性問題。輸入每一個問題的答案，然後按**下一步**。您也可以建立自訂問題。如需詳細資訊，請參閱位於第 12 頁的 HP SpareKey — 密碼復原。

5. 在「指紋」頁面上，註冊必要的指紋數下限，然後按一下或點選**下一步**。如需詳細資訊，請參閱位於第 11 頁的指紋。

6. 在「Drive Encryption」頁面上，啟動加密並備份加密金鑰，然後按一下或點選**下一步**。如需詳細資訊，請參閱 HP Drive Encryption 軟體「說明」。

附註： 這適用於使用者為管理員，且管理員尚未設定 HP Client Security 設定精靈的情況。

7. 在精靈的最後一頁，按一下或點選**完成**。

   此頁面提供功能和認證的狀態。

8. HP Client Security 設定精靈可確保啟用即時驗證和 File Sanitizer 功能。如需詳細資訊，請參閱 HP Device Access Manager 軟體「說明」和 HP File Sanitizer 軟體「說明」。

附註： 這適用於使用者為管理員，且管理員尚未設定 HP Client Security 設定精靈的情況。

開啟 HP Client Security

您可以使用下列其中一種方式開啟 HP Client Security 應用程式：

附註： 必須先完成 HP Client Security 設定精靈，才能啟動 HP Client Security 應用程式。

- 從「開始」或「應用程式」畫面，按一下或點選 **HP Client Security** 應用程式。

  － 或 －

從 Windowds 桌面，按一下或點選 **HP Client Security** Gadget 應用程式 (Windows 7)。

－ 或 －

從 Windows 桌面的工作列最右端的通知區域中，連按兩下或點選兩下 **HP Client Security** 圖示。

－ 或 －

在 Windows 桌面上，按一下或輕觸通知區域中的 **HP Client Security** 圖示，然後選取 **開啟 HP Client Security**。

3 小型企業適用的簡易設定指南

本章是針對示範可啟用 HP Client Security for Small Business 中最常見及最實用選項的基本步驟而設計。此軟體中的許多工具和選項都可以讓您微調偏好設定，並設定存取控制。本《簡易設定指南》的重點在於，以最少量的設定時間和精力，使每個模組運作。如需額外資訊，請選取您感興趣的模組，然後按一下右上角的 **?** 或「說明」按鈕。此按鈕將會自動顯示資訊，以協助您處理目前顯示的視窗。

快速入門

1. 從 Windows 桌面按兩下工作列最右邊的通知區域中的 **HP Client Security** 圖示，開啟 HP Client Security。
2. 輸入您的 Windows 密碼，或建立 Windows 密碼。
3. 完成 HP Client Security 安裝程式。

若要讓 HP Client Security Manager 在 Windows 登入期間只需要驗證一次，請參閱位於第 22 頁的安全性功能。

Password Manager

每個人都有一堆密碼，特別是在您定期存取的網站或使用的應用程式會要求您登入時。一般使用者會針對每個應用程式和網站使用相同的密碼，或使用有創意的密碼，且很快地忘記哪個應用程式使用哪個密碼。

Password Manager 可以自動記住您的密碼，或讓您能夠分辨哪些網站要記住密碼，哪些網站要省略密碼。一旦您登入電腦之後，Password Manager 將會提供您用於參與應用程式或網站的密碼或認證。

當您存取任何需要認證的應用程式或網站時，Password Manager 會自動識別網站，然後詢問您是否要該軟體記住您的資訊。如果您想排除特定網站，就可以拒絕此要求。

若要開始儲存 Web 位置、使用者名稱和密碼：

1. 例如，瀏覽至參與的網站或應用程式，然後按一下網頁左上角的 Password Manager 圖示以新增網路驗證。
2. 為此連結命名（選用），然後將使用者名稱和密碼輸入 Password Manager。
3. 完成時，按一下**確定**按鈕
4. Password Manager 也可以為您儲存網路共用和對應的網路磁碟機的使用者名稱和密碼。

在 Password Manager 中檢視與管理已儲存的驗證

Password Manager 可以讓您從一個集中位置，檢視、管理、備份與啟動您的驗證。Password Manager 也支援從 Windows 啟動已儲存的網站。

請使用以下鍵盤組合開啟 Password Manager。Ctrl+Windows 鍵+h 以開啟 Password Manager，然後按一下**登入**以啟動並授權已儲存的捷徑。

「密碼管理員」的**編輯**選項可讓您檢視並修改名稱、登入名稱，甚至顯示密碼。

HP Client Security for Small Business 允許備份所有認證與設定，並/或複製到其他電腦。

HP Device Access Manager

Device Access Manager 可用來限制對各種內建及外接式儲存裝置的使用，因此您的資料在硬碟上將仍然受到保護，而不會洩漏到公司外部。例如，允許使用者存取您的資料，但無法將其複製到 CD、個人的音樂播放程式或 USB 記憶體裝置。

1. 開啟 **Device Access Manager**（請參閱位於第 35 頁的開啟 Device Access Manager）。

   顯示目前的使用者存取。

2. 變更使用者、群組、或裝置的存取，請按一下或點選**變更**。如需詳細資訊，請參閱位於第 36 頁的系統檢視。

HP Drive Encryption

HP Drive Encryption 透過為整個硬碟加密，用來保護您的資料。如果您的電腦曾經遭竊，且/或硬碟從原始電腦移除，並放置在不同的電腦中，則硬碟上的資料將仍然受到保護。

另一個安全上的優點是，Drive Encryption 會在作業系統啟動前，要求您使用您的使用者名稱和密碼正確進行驗證。此程序稱為預先開機驗證。

為了簡化此程序，多個軟體模組會自動同步密碼，包括 Windows 使用者帳戶、授權網域、HP Drive Encryption、Password Manager 以及 HP Client Security。

若要在初始化設定過程中使用 HP Client Security 設定精靈設定 HP Drive Encryption，請參閱位於第 7 頁的快速入門。

4 HP Client Security

HP Client Security 首頁是方便存取 HP Client Security 功能、應用程式和設定的集中位置。首頁分為三個區段：

- **資料** — 提供使用於管理資料安全性的應用程式存取權。
- **裝置** — 提供使用於管理裝置安全性的應用程式存取權。
- **身分** — 提供驗證認證的註冊與管理。

將游標移到應用程式標題上方以顯示應用程式的說明。

HP Client Security 會在頁面底部提供使用者和管理設定的連結。點選或按一下**齒輪**（設定）圖示，可由 HP Client Security 來存取「進階設定」和功能。

身分功能、應用程式及設定

HP Client Security 提供的身分功能、應用程式和設定可協助您管理數位身分的各種層面。在 HP Client Security 首頁按一下或點選下列其中一個標題，然後輸入您的 Windows 密碼：

- **指紋** — 註冊與管理您的指紋認證。
- **SpareKey** — 設定和管理您的 HP SpareKey 認證，能在其他認證遺失或錯置時，用來登入您的電腦。也能讓您重設忘記的密碼。
- **Windows 密碼** — 可讓您輕易存取來變更 Windows 密碼。
- **Bluetooth 裝置** — 可讓您註冊和管理 Bluetooth 裝置。
- **卡片** — 可讓您註冊及管理智慧卡、非接觸式感應卡和近距離感應卡。
- **PIN** — 可讓您註冊和管理 PIN 認證。
- **RSA SecurID**—可讓您註冊並管理 RSA SecurID 認證（若經妥善設定）。
- **Password Manager** — 可讓您管理線上帳戶和應用程式的密碼。

指紋

HP Client Security 設定精靈會引導您執行指紋的設定或「註冊」程序。

您也可以按一下或點選 HP Client Security 首頁的**指紋**圖示，在「指紋」頁面上註冊或刪除您的指紋。

1. 在「指紋」頁面，滑動手指直到成功註冊為止。

   頁面會指示註冊所需要的指紋數目。最好使用食指或中指。

2. 若要刪除先前註冊的指紋，請按一下或點選**刪除**。
3. 若要註冊其餘手指，請按一下或點選**註冊其餘手指**。
4. 先按一下或點選**儲存**再離開頁面。

⚠ **注意：** 透過精靈註冊手指時，必須按**下一步**，才會儲存指紋資訊。如果您將電腦閒置一段時間，或關閉程式，您所做的變更將**不會**儲存。

▲ 若要存取「指紋管理設定」，讓管理員指定註冊、準確性和其他設定，請按一下或點選**管理設定**（需要管理權限）。

▲ 若要存取「指紋使用者設定」，讓您可以指定設定來支配指紋辨識的外觀與行為，請按一下或點選**使用者設定**。

指紋管理設定

管理員可為指紋讀取器指定註冊、準確性和其他設定。需要管理權限。

▲ 若要存取指紋 認證的「管理設定」，請按一下或點選「指紋」頁面上的**管理設定**。

- **使用者註冊** — 選擇使用者可以註冊的指紋數上限和下限。
- **辨識** — 移動滑桿可調整指紋讀取器在手指掃過時所使用的敏感度。

  如果指紋識別度不夠穩定，您可能需要選取較低的辨識設定。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。

指紋使用者設定

在「指紋使用者設定」頁面，您可以指定設定來支配指紋辨識的外觀與行為。

▲ 若要存取指紋 認證的「使用者設定」，請按一下或點選「指紋」頁面上的**使用者設定**。

- **啟用音效回應** — 掃過指紋後，HP Client Security 預設會發出音訊回應，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」設定中的「音效」標籤，您可以將新的音效指派給這些事件，也可以清除此核取方塊以停用音效回應。
- **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。

HP SpareKey — 密碼復原

藉由回答三個安全性問題，HP SpareKey 可讓您取得電腦的存取權（在受支援的平台上）。

在 HP Client Security 設定精靈的初始設定期間，HP Client Security 會提示您設定個人的 SpareKey。

若要設定您的 HP SpareKey：

1. 在精靈的 HP 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。

   您可以從預先定義的清單中選取問題，或撰寫您自己的問題。

2. 按一下或點選**註冊**。

若要刪除您的 HP SpareKey：

▲ 按一下或點選**刪除您的 SpareKey**。

在設定 SpareKey 後，您可以從開機驗證登入畫面或 Windows 歡迎畫面，使用您的 SpareKey 存取電腦。

您可以從 HP Client Security 首頁的「密碼復原」標題存取 SpareKey 頁面，在該頁面上選取不同的問題或變更答案。

若要存取 HP SpareKey「設定」，供管理員指定 HP SpareKey 認證的相關設定，請按一下**設定**（需要管理權限）。

HP SpareKey Settings

在 HP SpareKey「設定」頁面上，您可以指定設定來支配 HP SpareKey 認證的行為和使用方式。

▲ 若要啟動 HP SpareKey「設定」頁面，請按一下或點選 HP SpareKey 頁面的**設定**（需要管理權限）。

管理員可選取下列 設定：

- 指定在 HP SpareKey 設定期間向每位使用者呈現的問題。
- 最多可新增三個自訂的安全性問題，以便新增至向使用者呈現的清單中。
- 選擇是否允許使用者撰寫他們自己的安全性問題。
- 指定哪些驗證環境（Windows 或開機驗證）允許使用 HP SpareKey 執行密碼復原。

Windows 密碼

相較於透過 Windows 控制台變更 Windows 密碼，HP Client Security 能夠更簡單且快速地進行變更。

若要變更您的 Windows 密碼：

1. 從 HP Client Security 首頁，按一下或點選 **Windows 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. 按一下或點選**變更**便會立即將目前的密碼變更為您輸入的新密碼。

Bluetooth 裝置

如果管理員已啟用 Bluetooth 做為驗證認證，您就可以設定 Bluetooth 電話搭配其他認證以提供更高的安全性。

附註： 僅支援 Bluetooth 電話裝置。

1. 請確定已在電腦上啟用 Bluetooth 功能，而且 Bluetooth 電話已設定為探索模式。若要連接電話，您可能必須在 Bluetooth 裝置上輸入一組自動產生的代碼。根據 Bluetooth 裝置組態設定而定，電腦和電話兩者的配對代碼可能必須進行比對。
2. 若要註冊電話，請加以選取，然後按一下或點選**註冊**。

若要存取位於第 13 頁的 Bluetooth 裝置設定頁面，供管理員指定 Bluetooth 裝置的設定，請按一下**設定**（需要管理權限）。

Bluetooth 裝置設定

管理員可指定下列設定來支配 Bluetooth 裝置認證的行為和使用方式：

無訊息驗證

- **在驗證您的身分時，自動使用已連線的註冊 Bluetooth 裝置** — 選取此核取方塊可讓使用者使用 Bluetooth 認證進行驗證，而不需要使用者採取行動；或清除核取方塊停用此選項。

Bluetooth 近距離感應

- **當註冊的 Bluetooth 裝置超出電腦範圍時鎖定電腦**—選取核取方塊，則登入時連結的 Bluetooth 裝置超出範圍時鎖定電腦，清除核取方塊以停用此選項。

附註： 電腦上的 Bluetooth 模組必須支援此能力，方能利用此功能。

卡片

HP Client Security 可支援眾多不同類型的識別卡，即內建電腦晶片的小塑膠卡。包含智慧卡、非接觸式感應卡和近距離感應卡。如果電腦已連接其中一張卡片及適合的卡片讀取器，而且管理員已安裝製造商提供的相關驅動程式，並已啟用卡片做為驗證認證的話，您就可以使用這張卡片做為驗證認證之用。

智慧卡的製造商應該會提供工具，以便安裝安全性憑證及 PIN 管理，這些都將由 HP Client Security 在其安全性演算法中使用。做為 PIN 使用的字元數及類型可能有所不同。管理員必須先初始化智慧卡，然後才可以使用。

HP Client Security 支援下列智慧卡格式：

- CSP
- PKCS11

HP Client Security 支援下列類型的非接觸式卡片：

- 非接觸式 HID iCLASS 記憶卡
- 非接觸式 MiFare Classic 1k、4k 和迷你記憶卡

HP Client Security 支援下列近距離感應卡：

- HID 近距離感應卡

若要註冊智慧卡：

1. 在連接的智慧卡讀取器中插入卡片。
2. 辨識卡片後，輸入卡片的 PIN，然後按一下或點選**註冊**。

若要變更智慧卡 PIN：

1. 在連接的智慧卡讀取器中插入卡片。
2. 辨識卡片後，輸入卡片的 PIN，然後按一下或點選**驗證**。
3. 按一下或點**變更 PIN**，然後輸入新 PIN。

若要註冊非接觸式感應卡或近距離感應卡：

1. 在適合的讀取器上方或極接近的位置放置卡片。
2. 辨識卡片後，按一下或點選**註冊**。

若要刪除註冊的卡片：

1. 向讀取器出示卡片。
2. 僅針對智慧卡，輸入卡片的指派 PIN，然後按一下或點選**驗證**。
3. 按一下或點選**刪除**。

註冊卡片後，會在**註冊的卡片**下方顯示卡片的詳細資料。刪除卡片後，會從清單移除該卡片。

若要存取近距離感應卡、非接觸式感應卡和智慧卡設定，供管理員指定卡片認證的相關設定，請按一下或點選**設定**（需要管理權限）。

近距離感應卡、非接觸式感應卡和智慧卡設定

若要存取卡片的設定，請按一下或點選清單中的卡片，然後按一下或點選顯示的箭號。

若要變更智慧卡 PIN：

1. 向讀取器出示卡片
2. 輸入卡片的指派 PIN，然後按一下或點選**繼續**。
3. 輸入並確認新 PIN，然後按一下或點選**繼續**。

若要初始化智慧卡 PIN：

1. 向讀取器出示卡片
2. 輸入卡片的指派 PIN，然後按一下或點選**繼續**。
3. 輸入並確認新 PIN，然後按一下或點選**繼續**。
4. 按一下或點選**是**確認初始化。

若要清除卡片資料：

1. 向讀取器出示卡片
2. 輸入卡片的指派 PIN（僅限智慧卡），然後按一下或點選**繼續**。
3. 按一下或點選**是**以確認刪除。

PIN

如果管理員已啟用 PIN 做為驗證認證，您就可以設定 PIN 搭配其他認證以提供更高的安全性。

若要設定新 PIN：

▲ 輸入 PIN，再次輸入 PIN 以確認，然後按一下或點選**套用**。

若要刪除 PIN：

▲ 按一下或點選**刪除**，然後按一下或點選**是**確認。

若要存取 PIN「設定」，供管理員指定 PIN 認證的相關設定，請按一下或點選**設定**（需要管理權限）。

PIN 設定

在 PIN「設定」頁面上，您可以指定 PIN 認證可接受的長度下限和上限。

RSA SecurID

如果管理員已啟用 RSA 作為驗證認證，且下列條件成立，則可註冊或刪除 RSA SecurID 認證。

附註： 需要適當的設定。

- 必須已在 RSA 伺服器上建立使用者。
- 指派給使用者和電腦的 RSA SecurID 權杖必須已加入 RSA 伺服器網域。
- SecurID 軟體已安裝在電腦上。
- 適當設定的 RSA 伺服器有可用的連線。

若要註冊 RSA SecurID 認證：

▲ 輸入您的 RSA SecurID 使用者名稱和密碼（RSA SecurID 權杖碼或 PIN + 權杖碼，視您的環境而定），然後按一下或點選**套用**。

成功註冊時，畫面會顯示「您的 RSA SecurID 認證已成功註冊」訊息，並且啟用「刪除」按鈕。

若要刪除 RSA SecurID 認證：

▲ 按一下**刪除**，然後選取**是**以快顯「您確定要刪除您的 RSA SecurID 認證嗎？」對話方塊。

Password Manager

使用 Password Manager 是更輕鬆與安全登入網站和應用程式的方式。您可以建立強式密碼，完全不需要寫下或記憶，然後使用指紋、智慧卡、近距離感應卡、非接觸式感應卡、Bluetooth 電話、PIN、RSA 認證或您的 Windows 密碼輕鬆快速地登入。

附註： 由於網站的登入畫面結構不斷變化，因此 Password Manager 無法一直支援所有網站。

Password Manager 提供下列選項：

Password Manager 頁面

- 按一下或點選帳戶，自動地啟動網頁或應用程式並登入。
- 使用分類來組織您的帳戶。

密碼的強度

- 檢視您的任一密碼是否有安全性風險。
- 新增登入資料時，請檢查使用於網站和應用程式的個別密碼強度。
- 密碼強度是以紅色、黃色或綠色的狀態指示器表示。

Password Manager 圖示會顯示在網頁的左上角或應用程式登入畫面上。如果還沒有為網站或應用程式建立登入，圖示上會顯示加號。

▲ 按一下或點選 **Password Manager** 圖示可顯示內容功能表，您可以從下列選項做選擇：

- 將 [somedomain.com] 新增到 Password Manager
- 開啟 Password Manager
- 圖示設定
- 說明

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 Password Manager** — 允許您新增目前登入畫面的登入。
- **開啟 Password Manager** — 啟動 Password Manager。
- **圖示設定** — 允許您指定顯示 **Password Manager** 圖示的條件。
- **說明** — 顯示 HP Client Security 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** — 顯示**驗證您的身分**頁面。如果通過驗證，就會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 Password Manager。

- **開啟 Password Manager** — 啟動 Password Manager。
- **說明** — 顯示 HP Client Security 說明。

附註： 此電腦的管理員可能已經設定 HP Client Security 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 就會自動為您輸入資訊。您可以在瀏覽至網站或程式後使用這些登入。

若要新增登入：

1. 開啟網站或程式的登入畫面。
2. 按一下或點選 **Password Manager** 圖示，然後根據出現的是網站或程式的登入畫面，按一下或點選下列其中一項：
   - 對於網站，按一下或點選 **將 [somedomain.com] 新增至 Password Manager**。
   - 對於程式，按一下或點選**此登入畫面新增至 Password Manager**。
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。
   a. 若要在登入欄位中填入其中一個預先格式化的選項，請按一下或點選欄位右側的箭號。
   b. 若要檢視此登入的密碼，請按一下或點選**顯示密碼**。
   c. 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。
   d. 按一下或點選**確定**，選取您要使用的驗證方法（指紋、智慧卡、近距離感應卡、非接觸式感應卡、Bluetooth 電話、PIN 或密碼），然後使用選取的驗證方法登入。

      密碼管理員圖示的加號會被移除，通知您已建立登入。
   e. 如果 Password Manager 無法偵測登入欄位，請按一下或點選**更多欄位**。
      - 選取登入時所需之每個欄位的核取方塊，或清除登入時不需要之任何欄位的核取方塊。
      - 按一下或點選**關閉**。

每次您存取該網站或開啟程式時，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：

1. 開啟網站或程式的登入畫面。
2. 若要顯示可供您編輯登入資訊的對話方塊，請按一下或點選 **Password Manager** 圖示，然後按一下或點選**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。

   您也可以從 Password Manager 頁面中編輯帳戶資訊，方法是按一下或點選「登入」以顯示編輯選項，然後選取**編輯**。
3. 編輯您的登入資訊。
   - 若要編輯**帳戶名稱**，請在欄位中輸入新名稱。
   - 若要新增或編輯**分類**名稱，請在**分類**欄位中輸入或修改名稱。

- 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，請按一下或點選欄位右側的向下箭號。

  只有在 Password Manager 圖示內容功能表的「編輯」命令中編輯登入時，才能使用預先格式化的選項。

- 若要選取包含其中一個預先格式化選項的**密碼**登入欄位，請按一下或點選欄位右側的向下箭號。

  只有在 Password Manager 圖示內容功能表的「編輯」命令中編輯登入時，才能使用預先格式化的選項。

- 若要將其他欄位從畫面新增至您的登入，請按一下或點選**更多欄位**。
- 若要檢視此登入的密碼，請按一下或點選**顯示密碼**圖示。
- 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。
- 若要將此登入標示為具有洩露的密碼，請選取**此密碼已洩露**核取方塊。

  儲存變更後，也會將共用相同密碼的其他所有登入標示為已洩露。您接著可以瀏覽每一個受影響的帳戶，並視需要變更密碼。

4. 按一下或點選**確定**。

使用 Password Manager 快速連結功能表

若要啟動您已經建立登入的網站和程式，Password Manager 是快速簡便的方式。在 **Password Manager 快速連結**功能表，或 HP Client Security 的 Password Manager 頁面中，連按兩下或點選兩下程式或網站登入以開啟登入畫面，然後填入您的登入資料。

建立登入時，該登入會自動新增至 Password Manager 的**快速連結**功能表。

若要顯示**快速連結** 能表：

▲ 按下 **Password Manager** 的快速鍵組合（原廠設定為 Ctrl+Windows 鍵+h）若要變更快速鍵組合，請按一下 HP Client Security 首頁的 **Password Manager**，然後按一下或點選**設定**。

將登入分類

建立一項或多項分類來整理您的登入。

若要將登入指派給分類：

1. 從 HP Client Security 首頁，按一下或點選 **Password Manager**。
2. 按一下或點選帳戶項目，然後按一下或點選**編輯**。
3. 在**分類**欄位中輸入分類名稱。
4. 按一下或點選**儲存**。

若要從分類移除帳戶：

1. 從 HP Client Security 首頁，按一下或點選 **Password Manager**。
2. 按一下或點選帳戶項目，然後按一下或點選**編輯**。
3. 在**分類**欄位中清除分類名稱。
4. 按一下或點選**儲存**。

若要重新命名分類：

1. 從 HP Client Security 首頁，按一下或點選 **Password Manager**。
2. 按一下或點選帳戶項目，然後按一下或點選**編輯**。
3. 在**分類**欄位中變更分類名稱。
4. 按一下或點選**儲存**。

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 Password Manager 頁面中。

若要管理您的登入：

1. 從 HP Client Security 首頁，按一下或點選 **Password Manager**。
2. 按一下或點選現有的登入，然後選取下列其中一個選項，再依照畫面上的指示繼續執行：
   - **編輯** — 編輯登入。如需詳細資訊，請參閱位於第 17 頁的編輯登入。
   - **登入** — 登入選取的帳戶。
   - **刪除** — 刪除所選帳戶的登入。

若要新增網站或程式的其他登入：

1. 開啟網站或程式的登入畫面。
2. 按一下或點選 **Password Manager** 圖示，顯示其內容功能表。
3. 按一下或點選**新增登入**，然後依照畫面上的指示繼續執行。

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。

當您在為帳戶建立 Password Manager 登入期間輸入密碼時，密碼下方會顯示一條彩色軸來指出密碼的強度。這些色彩代表下列值：

- **紅色** — 弱
- **黃色** — 適中
- **綠色** — 強

Password Manager 圖示設定

Password Manager 會試著辨別網站和程式的登入畫面。當密碼管理員偵測出您尚未建立登入的登入畫面時，會顯示含有加號的 **Password Manager** 圖示，提示您新增該畫面的登入。

1. 按一下或點選圖示，再按一下或點選**圖示設定**，自訂 Password Manager 對可能登入的網站之處理方式。
   - **提示為登入畫面新增登入** — 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 便不再提示您為此登入畫面新增登入。
   - **不提示為登入畫面新增登入** — 選取選項按鈕。
2. 若要為先前已經排除的畫面新增登入：
   a. 登入先前排除的網站。
   b. 若要讓 Password Manager 記得此本網站，在彈出型對話方快按一下或點選**記憶**，以儲存密碼並建立此畫面的登入資料。
3. 若要存取其他 Password Manager 設定，請按一下或點選 Password Manager 圖示，按一下或點選**開啟 Password Manager**，然後按一下或點選 Password Manager 頁面的**設定**。

匯入和匯出登入

在 HP Password Manager 的匯入和匯出頁面，您可以匯入電腦上網頁瀏覽器所儲存的登入。您也可以從 HP Client Security 備份檔案匯入資料，以及將資料匯出至 HP Client Security 備份檔案。

▲ 若要啟動匯入和匯出頁面，請按一下或點選 Password Manager 頁面的**匯入和匯出**。

若要從瀏覽器匯入密碼：

1. 按一下或點選要從中匯入密碼的瀏覽器（只會顯示已安裝的瀏覽器）。
2. 針對不想要匯入密碼的任何帳戶清除此核取方塊。
3. 按一下或點選**匯入**。

可透過匯入和匯出 頁面上的相關連結（**其他選項**）下方與 HP Client Security 備份檔案之間匯入或匯出資料。

附註： 這項功能只能匯入和匯出 Password Manager 資料。如需備份和還原其他 HP Client Security 資料的詳細資訊，請參閱位於第 24 頁的備份和還原您的資料。

若要從 HP Client Security 備份檔案匯入資料：

1. 從 HP Password Manager 的匯入和匯出頁面，按一下或點選**從 HP Client Security 備份檔案匯入資料**。
2. 驗證您的身分。
3. 選取先前建立的備份檔案，或在提供的欄位中輸入路徑，然後按一下或點選**瀏覽**。
4. 輸入用來保護檔案的密碼，然後按一下或點選**下一步**。
5. 按一下或點選**還原**。

若要將資料匯出至 HP Client Security 備份檔案：

1. 從 HP Password Manager 的匯入和匯出頁面，按一下或點選**從 HP Client Security 備份檔案匯出資料**。
2. 驗證您的身分，然後按一下或點選**下一步**。
3. 輸入備份檔案的名稱。根據預設，此檔案會儲存到您的「文件」資料夾。若要指定不同的位置，請按一下或點選**瀏覽**。
4. 輸入並確認用來保護檔案的密碼，然後按一下或點選**儲存**。

設定

您可以指定將 Password Manager 個人化的設定：

- **提示為登入畫面新增登入** —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**登入**功能表。

  若要停用此功能，請清除**提示為登入畫面新增登入**旁的核取方塊。

- **使用 ctrl+win+h 開啟 Password Manager**—開啟 **Password Manager 快速連結**功能表的預設快速鍵是 Ctrl+Windows 鍵+h。

  若要變更快速鍵，請按一下或點選此選項，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。

  無法使用為 Windows 或 Windows 應用程式保留的組合鍵。

- 若要將設定還原為原廠預設值，請按一下或點選**還原預設值**。

進階設定

管理員可選取 HP Client Security 首頁的**齒輪**（設定）圖示，藉此存取下列選項。

- **管理員原則** — 可讓您設定管理員的登入和工作階段原則。
- **標準使用者原則** — 可讓您設定標準使用者的登入和工作階段原則。
- **安全性功能** — 可讓您使用強式驗證和/或在 Windows 啟動前啟用驗證，藉此保護您的 Windows 帳戶，以便增強電腦的安全性。
- **使用者**—可讓您管理使用者和憑證。
- **我的原則** — 允許您檢閱驗證原則和註冊狀態。
- **備份和還原** — 允許您備份或還原 HP Client Security 資料。
- **關於 HP Client Security**—顯示有關 HP Client Security 的版本資訊。

管理員原則

您可以為這台電腦的管理員設定登入和工作階段原則。這裡設定的登入原則可支配本機管理員用來登入 Windows 時的必要認證。這裡設定的工作階段原則可支配本機管理員在 Windows 工作階段中，用來驗證身分時的必要認證。

依預設，在點選或按一下**套用**後，會立即強制使用所有全新或變更的原則。

若要新增原則：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**管理員原則**。

3. 按一下或點選**新增原則**。
4. 按一下向下箭號，為新原則選取主要和（選用）次要認證，然後按一下或點選**新增**。
5. 按一下**套用**。

若要延遲全新或變更之原則的強制使用：

1. 按一下或點選**立即強制使用此原則**。
2. 選取**在特定的日期強制使用此原則**。
3. 輸入日期或使用快顯行事曆，選取必須強制使用此原則的日期。
4. 如果需要，請選取何時向使用者提醒新原則的相關資訊。
5. 按一下**套用**。

標準使用者原則

您可以為這台電腦的標準使用者設定登入和工作階段原則。這裡設定的登入原則可支配標準使用者用來登入 Windows 時的必要認證。這裡設定的工作階段原則可支配標準使用者在 Windows 工作階段中，用來驗證身分時的必要認證。

依預設，在點選或按一下**套用**後，會立即強制使用所有全新或變更的原則。

若要新增原則：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**標準使用者原則**。
3. 按一下或點選**新增原則**。
4. 按一下向下箭號，為新原則選取主要和（選用）次要認證，然後按一下或點選**新增**。
5. 按一下**套用**。

若要延遲全新或變更之原則的強制使用：

1. 按一下或點選**立即強制使用此原則**。
2. 選取**在特定的日期強制使用此原則**。
3. 輸入日期或使用快顯行事曆，選取必須強制使用此原則的日期。
4. 如果需要，請選取何時向使用者提醒新原則的相關資訊。
5. 按一下**套用**。

安全性功能

您可以啟用 HP Client Security Features，以防範未經授權存取電腦。

若要設定安全性功能：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**安全性功能**。

3. 選取核取方塊，然後按一下或點選**套用**以啟用安全性功能。選取的功能愈多，電腦的安全性就愈高。

   這些設定套用於所有的使用者。

   - **Windows 登入安全性** — 藉由要求使用 HP Client Security 認證進行存取，以保護您的 Windows 帳戶。
   - **預先開機安全性（開機驗證）** — 在 Windows 啟動前，保護您的電腦。此選項若不受 BIOS 支援便無法使用。
   - **允許 One Step logon** — 如果已在開機驗證或 Drive Encryption 層級上執行驗證，則此設定可略過 Windows 登入。

4. 按一下或點選**使用者**，然後按一下或點選使用者方塊。

使用者

您可以監控和管理這台電腦的 HP Client Security 使用者。

若要將其他 Windows 使用者新增至 HP Client Security：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**使用者**。
3. 按一下或點選**將其他 Windows 使用者新增至 HP Client Security**。
4. 輸入要新增的使用者名稱，然後按一下或點選**確定**。
5. 輸入使用者的 Windows 密碼。

   「使用者」頁面隨即會顯示新增的使用者標題。

若要從 HP Client Security 刪除 Windows 使用者：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**使用者**。
3. 按一下或點選要刪除的使用者名稱。
4. 按一下或點選**刪除使用者**，然後按一下或點選**是**加以確認。

若要顯示針對使用者強制使用的登入和工作階段原則的摘要：

▲ 按一下或點選**使用者**，然後按一下或點選使用者方塊。

我的原則

您可以顯示您的驗證原則和註冊狀態。「我的原則」頁面另外提供「管理員原則」和「標準使用者原則」頁面的連結。

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**我的原則**。

   隨即會顯示為目前登入的使用者所強制使用的登入和工作階段原則。

「我的原則」頁面另外提供位於第 21 頁的管理員原則和位於第 22 頁的標準使用者原則的連結。

備份和還原您的資料

建議您定期備份 HP Client Security 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 Password Manager。Drive Encryption 有一個獨立的備份方法。不會備份 Device Access Manager 和指紋驗證資訊。

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

若要備份資料：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**管理員原則**。
3. 按一下或點選**備份和還原**。
4. 按一下或點選**備份**，然後驗證您的身分。
5. 選取備份中要包含的模組，然後按一下或點選**下一步**。
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。若要指定不同的位置，請按一下或點選**瀏覽**。
7. 輸入並確認密碼以保護檔案。
8. 按一下或點選**儲存**。

若要還原資料：

1. 從 HP Client Security 首頁，按一下或點選**齒輪**圖示。
2. 在「進階設定」頁面，按一下或點選**管理員原則**。
3. 按一下或點選**備份和還原**。
4. 選取**還原**然後驗證您的身分。
5. 選取之前建立的儲存檔。在提供的欄位中輸入路徑。若要指定不同的位置，請按一下或點選**瀏覽**。
6. 輸入用來保護檔案的密碼，然後按一下或點選**下一步**。
7. 選取您要還原資料的模組。
8. 按一下或點選**還原**。

5 HP Drive Encryption（僅限特定機型）

HP Drive Encryption 可透過加密電腦的資料，提供完整的資料保護。當 Drive Encryption 啟動時，您必須在 Windows® 作業系統啟動前所顯示的 Drive Encryption 登入畫面中登入。

HP Client Security 主頁畫面允許 Windows 管理員啟用 Drive Encryption、備份加密金鑰，以及選取或取消選取要加密的磁碟機或分割區。如需詳細資訊，請參閱 HP Client Security 軟體說明。

Drive Encryption 可執行下列工作：

- 選取 Drive Encryption 設定：
  - 使用軟體加密來加密或解密個別磁碟機或磁碟分割
  - 使用硬體加密來加密或解密個別自我加密磁碟機
  - 停用「睡眠」或「待機」來進一步增加安全性，以確保永遠要求 Drive Encryption 預先開機驗證

附註： 僅能加密內建 SATA 和外接式 eSATA 硬碟。

- 建立備份金鑰
- 使用備份金鑰和 HP SpareKey 復原對已加密電腦的存取
- 使用密碼、註冊指紋或特定智慧卡的 PIN 碼啟用 Drive Encryption 預先開機驗證

開啟 Drive Encryption

管理員可以開啟 HP Client Security 來存取 Drive Encryption：

1. 從「開始」畫面按一下或點選 **HP Client Security** 應用程式 (Windows 8)。

   － 或 －

   從 Windows 桌面的工作列最右端的通知區域中，連按兩下或點選兩下 **HP Client Security** 圖示。

2. 按一下或點選 **Drive Encryption** 圖示。

一般工作

啟動標準硬碟的 Drive Encryption

標準硬碟使用軟體加密進行加密。依照下列步驟加密磁碟機或磁碟分割區：

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。
2. 選取要加密的磁碟機或分割區的核取方塊，然後按一下或點選**備份金鑰**。

附註： 為了得到更佳的安全性，請選取**停用睡眠模式以強化安全性**核取方塊。停用睡眠模式時，絕對不會將用於解除鎖定磁碟機的認證儲存在記憶體中。

3. 選取一或多個備份選項，然後按一下或點選**備份**。如需詳細資訊，請參閱位於第 28 頁的備份加密金鑰。

4. 備份加密金鑰時可以繼續處理您的工作。 請勿將電腦重新開機。

附註： 系統會提示您重新啟動電腦。重新啟動後會顯示磁碟機加密預先開機畫面，完成驗證後才會啟動 Windows。

此時即已啟用 Drive Encryption。視分割區的數量和大小而定，為選取的磁碟機分割區加密可能需要數小時。

如需詳細資訊，請參閱 HP Client Security 軟體說明。

啟動自我加密磁碟機的 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。硬體加密的速度比軟體加密快。不過，您不能選擇要加密的磁碟分割區，必須加密整個磁碟機，包括任何磁碟分割區。

要加密特定分割區，您就必須使用軟體加密。請務必清除**僅允許自我加密磁碟機 (SED) 的硬體加密**核取方塊.

請依照下列步驟，啟用自我加密磁碟機的 Drive Encryption：

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。

2. 選取要加密之磁碟機的核取方塊，然後按一下或點選**備份金鑰**。

附註： 為了得到更佳的安全性，請選取**停用睡眠模式以強化安全性**核取方塊。停用睡眠模式時，絕對不會將用於解除鎖定磁碟機的認證儲存在記憶體中。

3. 選取一或多個備份選項，然後按一下或點選**備份**。如需詳細資訊，請參閱位於第 28 頁的備份加密金鑰。

4. 備份加密金鑰時可以繼續處理您的工作。 請勿將電腦重新開機。

附註： 若為自我加密磁碟機，系統會提示您關閉電腦。

如需詳細資訊，請參閱 HP Client Security 軟體說明。

停用 Drive Encryption

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。

2. 清除所有加密磁碟機的核取方塊，然後按一下或點選**套用**。

   Drive Encryption 隨即開始停用。

附註： 如果已使用軟體加密，便會開始進行解密。視已加密硬碟分割區的大小而定，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，經過幾分鐘之後，Drive Encryption 就會停用。

Drive Encryption 停用之後，電腦若是經過硬體加密，您會收到關閉電腦的提示；電腦若是經過軟體加密，您會收到重新啟動電腦的提示。

在啟用 Drive Encryption 之後登入

當您在啟用 Drive Encryption 並註冊使用者帳戶之後開啟電腦時，就必須在 Drive Encryption 登入畫面進行登入：

附註： 從「睡眠」或「待命」狀態喚醒時，不論是軟體加密或硬體加密，Drive Encryption 預先開機驗證都不會出現。硬體加密會提供**停用睡眠模式以強化安全性**選項，啟用此選項會防止「睡眠」或「待命」發生。

從「休眠」狀態喚醒時，不論是軟體加密或硬體加密，Drive Encryption 預先開機驗證都會出現。

附註： 如果 Windows 管理員已在 HP Client Security 中啟用 BIOS Pre-boot Security，而且 One-Step Logon 已啟用（預設值），那麼您就可以在 BIOS Pre-boot Security 驗證之後立即登入電腦，而不需要在 Drive Encryption 登入畫面重新驗證。

單一使用者登入：

▲ 在**登入**頁面上，輸入您的 Windows 密碼、智慧卡 PIN 碼、SpareKey，或是用已註冊的手指掃過。

多使用者登入：

1. 在**選取要登入的使用者**頁面上，從下拉式清單中選取要登入的使用者，然後按一下或點選**下一步**。
2. 在**登入**頁面上，輸入您的 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：

支援的智慧卡

- Gemalto Cyberflex Access 64k V2c

附註： 如果在 Drive Encryption 登入畫面使用復原金鑰登入，那麼在 Windows 登入階段還需要其他認證才能存取使用者帳戶。

加密其他硬碟

強烈建議您使用 HP Drive Encryption 加密硬碟來保護您的資料。啟用此功能之後，可以透過下列步驟加密任何新增的硬碟或建立的分割區：

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。
2. 若是使用軟體加密的磁碟機，請選取要加密的磁碟分割。

附註： 這也適用於同時具有一個或多個標準硬碟以及一個或多個自我加密磁碟機的混合磁碟機情況。

– 或 –

▲ 對於硬體加密的磁碟機，請選取要加密的其他磁碟機。

進階工作

管理 Drive Encryption（管理員工作）

管理員可使用 Drive Encryption 來檢視與變更電腦上所有硬碟的加密狀態（「未加密」或「已加密」）。

- 如果狀態為「已啟用」，表示已啟動及設定 Drive Encryption。磁碟機為下列其中一種狀態：

軟體加密

  - 未加密
  - 已加密

- 加密
- 解密

硬體加密

- 已加密
- 未加密（適用於其他磁碟機）

加密或解密個別磁碟機分割區（僅限軟體加密）

管理員可以使用 Drive Encryption 加密電腦上的一個或多個硬碟分割區，或是將已經加密的磁碟機分割區解密。

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。
2. 在**磁碟機狀態**下方，選取或清除要加密或解密的每個硬碟分割區旁的核取方塊，然後按一下或點選**套用**。

附註： 在分割區進行加密或解密時，進度列會顯示分割區加密的百分比。

附註： 不支援動態磁碟分割。如果磁碟分割顯示為可用，但是在選取後無法加密，表示該磁碟分割是動態的。動態磁碟分割是由於在「磁碟管理」中縮小磁碟分割，以建立新的磁碟分割所造成。

如果磁碟分割將要轉換為動態磁碟分割，便會顯示警告。

磁碟管理

- **暱稱** — 您可以提供您的磁碟機或分割區名稱，更輕鬆地識別您的身分。
- **中斷連接的磁碟機** — Drive Encryption 可追蹤從電腦移除的磁碟。系統會將從電腦移除的磁碟，自動移至「已中斷連接」清單。如果磁碟回到系統，它會重新出現在「已連接」清單中。
- 如果您不再需要追蹤或管理已中斷連接的磁碟機，可從「已中斷連接」清單中移除已中斷連接的磁碟機。
- 在清除所有已連接磁碟機的核取方塊，且「已中斷連接」清單變為空白之前，Drive Encryption 仍將維持啟動。

備份與復原（管理員工作）

當啟動 Drive Encryption 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，並且執行復原。

備份加密金鑰

管理員可以將已加密磁碟機的加密金鑰備份於抽取式儲存裝置。

注意： 請妥善保管包含備份金鑰的儲存裝置，因為如果您忘記密碼、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電腦的途徑。裝置的存放位置也應受到保護，因為透過該儲存裝置即可存取 Windows。

1. 啟動 **Drive Encryption**。如需詳細資訊，請參閱位於第 25 頁的開啟 Drive Encryption。
2. 選取磁碟機的核取方塊，然後按一下或點選**備份金鑰**。

3. 在**建立 HP Drive Encryption 復原金鑰**下，選取下列一或多個選項：

   - **抽取式儲存裝置** — 選取核取方塊，然後選取將儲存加密金鑰的儲存裝置。
   - **SkyDrive** — 選取核取方塊。您必須連線至網際網路。登入 Microsoft SkyDrive，然後按一下或點選**是**。

   附註： 若要使用 SkyDrive 上儲存的 HP Drive Encryption 備份金鑰，必須將金鑰從 SkyDrive 下載至抽取式儲存裝置，然後在這台電腦上插入儲存裝置。

   - **TPM**（僅限特定機型） — 可讓您使用 TPM 密碼復原資料。

   注意： 如果清除 TPM 或電腦受損，您將遺失備份的存取能力。如果選擇此方式，也應選擇另一種備份方式。

4. 按一下或點選**備份**。

   此時便會將加密金鑰儲存到您選取的儲存裝置。

使用備份金鑰復原對已啟用電腦的存取

管理員可以使用啟用階段備份至抽取式儲存裝置的 Drive Encryption 金鑰，或是選取 Drive Encryption 中的**備份金鑰**選項，以執行復原。

1. 插入包含您的備份金鑰的抽取式儲存裝置。
2. 開啟電腦。
3. 當出現 HP Drive Encryption 登入對話方塊時，按一下或點選**復原**。
4. 輸入含有您備份金鑰的檔案路徑或名稱，然後按一下或點選**復原**。
5. 當出現確認對話方塊時，按一下或點選**確定**。

   Windows 登入畫面便會顯示。

附註： 如果在 Drive Encryption 登入畫面使用復原金鑰登入，那麼在 Windows 登入階段還需要其他認證才能存取使用者帳戶。在執行復原之後，強烈建議您重設密碼。

執行 HP SpareKey 復原

Drive Encryption 預先開機內的 SpareKey 復原會要求您必須正確回答安全性問題才可存取電腦。如需有關設定 SpareKey 復原的詳細資訊，請參閱 HP Client Security 軟體「說明」。

若要在忘記密碼時執行 HP SpareKey 復原：

1. 開啟電腦。
2. 當「HP Drive Encryption」頁面顯示時，瀏覽至使用者登入頁面。
3. 按一下 **SpareKey**。

   附註： 如果您的 SpareKey 尚未在 HP Client Security 中初始化，**SpareKey** 按鈕便無法使用。

4. 針對顯示的問題輸入正確答案，然後按一下**登入**。

   Windows 登入畫面便會顯示。

附註： 如果在 Drive Encryption 登入畫面使用 SpareKey 登入，那麼在 Windows 登入階段還需要其他認證才能存取使用者帳戶。在執行復原之後，強烈建議您重設密碼。

6 HP File Sanitizer（僅限特定機型）

File Sanitizer 可讓您安全地拆解電腦內建硬碟中的資產（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），以及定期清理電腦的內建硬碟。

File Sanitizer 無法用於處理或清理下列類型的磁碟機：

- 固態硬碟 (SSD)，包括涉及 SSD 裝置的 RAID 磁碟區
- 經由 USB、Firewire 或 eSATA 介面連接的外接式磁碟機

如果嘗試在 SSD 上進行拆解或清理作業，將會出現警告訊息，該作業則不會執行。

拆解

拆解與標準的 Windows® 刪除動作不同。當您使用 File Sanitizer 拆解資產時，會以無意義的資料覆寫檔案，因此幾乎無法再擷取原始資產。Windows 單純刪除動作可能會將檔案（或資產）完整保留在硬碟上，或是讓檔案保持在以科學鑑定方法就可能復原的狀態。

您可以排程未來的拆解時間，或選取 HP Client Security 主畫面上的 **File Sanitizer** 圖示，或使用 Windows 桌面的 **File Sanitizer** 圖示以手動啟動拆解。如需詳細資訊，請參閱位於第 31 頁的設定拆解排程、位於第 33 頁的按一下滑鼠右鍵拆解或位於第 33 頁的手動啟動拆解作業。

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

在 Windows 中，刪除資產並不會從硬碟完全移除資產的內容。Windows 只是刪除資產的參照或是資產在硬碟中的位置。除非有另一項資產以新資訊覆寫硬碟上的相同區域，否則原資產的內容會一直保留在硬碟中。

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

附註： 可用空間清理並未針對已拆解的資產提供額外的安全性。

您可以設定未來的可用空間清理時間，或選取 HP Client Security 主畫面上的 **File Sanitizer** 圖示，或使用 Windows 桌面的 **File Sanitizer** 圖示，以手動方式啟動可用空間清理或先前拆解的資產。如需詳細資訊，請參閱位於第 32 頁的設定可用空間清理排程、位於第 34 頁的手動啟動可用空間清理或位於第 33 頁的使用 File Sanitizer 圖示。

開啟 File Sanitizer

1. 從「開始」畫面按一下或點選 **HP Client Security** 應用程式 (Windows 8)。

   － 或 －

   從 Windows 桌面的工作列最右端的通知區域中，連按兩下或點選兩下 **HP Client Security** 圖示。

2. 在**資料**下，按一下或點選 **File Sanitizer**。

– 或 –

▲ 連按兩下或點選兩下 Windows 桌面的 **File Sanitizer** 圖示。

– 或 –

▲ 按一下滑鼠右鍵，或點選並按住 Windows 桌面的 **File Sanitizer** 圖示，然後選取**開啟 File Sanitizer**。

設定程序

拆解 — File Sanitizer 可安全地刪除或拆解所選類型的資產。

1. 在**拆解**下，選取要拆解的每一類檔案的核取方塊，或清除不想拆解之檔案的核取方塊。
   - **資源回收筒** — 拆解資源回收筒中的所有項目。
   - **暫存系統檔案** — 拆解系統暫存資料夾中找到的全部檔案。以下環境變數會根據下列順序進行搜尋，而第一個找到的路徑為系統資料夾：
     - TMP
     - TEMP
   - **Temporary Internet Files** — 拆解 Web 瀏覽器為加快瀏覽而儲存之網頁、影像和媒體的複本。
   - **Cookies** — 拆解網站存放在電腦上用來儲存偏好設定（如登入資訊）的所有檔案。
2. 若要開始拆解，請按一下或點選**拆解**。

清理 — 寫入隨機資料以釋放空間，並防止復原已刪除的項目。

▲ 若要開始清理，請按一下或點選**清理**。

File Sanitizer 選項 — 選取核取方塊以啟用下列每一個選項，或者清除核取方塊以停用選項：

- **啟用桌面圖示** — 在 Windows 桌面上顯示「File Sanitizer」圖示。
- **啟用按一下滑鼠右鍵** — 可讓您按一下滑鼠右鍵，或點選並按住資產，然後選取 **HP File Sanitizer – 拆解**。
- **先詢問 Windows 密碼再手動拆解** — 需要先驗證 Windows 密碼再手動拆解項目。
- **瀏覽器關閉時拆解 Cookies 和 Temporary Internet Files** — 在您關閉網頁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。

設定拆解排程

您可以排程時間以自動執行拆解，也可以隨時手動拆解資產。如需詳細資訊，請參閱位於第 31 頁的設定程序。

1. 開啟 File Sanitizer，然後按一下或點選**設定**。
2. 若要排程未來的時間以拆解選取的資產，請在**拆解排程** 下選取**永不**、**一次**、**每天**、**每週** 或**每月**，然後選取日期與時間：
   a. 按一下或點選「小時」、「分鐘」或「AM/PM」欄位。
   b. 持續捲動，直到所要的值與其他欄位顯示在相同的層級為止。
   c. 按一下或點選時間設定欄位周圍的空格。
   d. 針對每個欄位重複執行，直到選取正確的排程為止。

3. 會列出下列四種類型的資產：

   - **資源回收筒** — 拆解資源回收筒中的所有項目。
   - **暫存系統檔案** — 拆解系統暫存資料夾中找到的全部檔案。以下環境變數會根據下列順序進行搜尋，而第一個找到的路徑為系統資料夾：
     - TMP
     - TEMP
   - **Temporary Internet Files** — 拆解 Web 瀏覽器為加快瀏覽而儲存之網頁、影像和媒體的複本。
   - **Cookies** — 拆解網站存放在電腦上用來儲存偏好設定（如登入資訊）的所有檔案。

   如果核取，將在排定的時間拆解這些資產。

4. 若要選取其他的自訂資產進行拆解：

   a. 在**排程的拆解清單**下，按一下或點選**新增資料夾**，然後瀏覽至檔案或資料夾。

   b. 按一下或點選**開啟**，然後按一下或點選**確定**。

   若要從「排程的拆解清單」中移除資產，請清除資產的核取方塊。

設定可用空間清理排程

可用空間清理並未針對已拆解的資產提供額外的安全性。

1. 開啟 File Sanitizer，然後按一下或點選**設定**。
2. 若要排定未來的某個時間清理您的硬碟,在 **清理排程**下，選擇 **永不**、**一次**、**每日**、**每週**、**每月**，然後選定日期和時間。

   a. 按一下或點選「小時」、「分鐘」或「AM/PM」欄位。

   b. 持續捲動，直到所要的時間與其他欄位顯示在相同的層級為止。

   c. 按一下或點選時間設定欄位周圍的空格。

   d. 重複執行，直到選取正確的排程為止。

附註： 可用空間清理作業會耗費大量的時間。確定您的電腦已連接 AC 電源。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。您可以在下班時間或不使用電腦時，執行可用空間清理。

保護檔案免於拆解

若要保護檔案或資料夾免於拆解：

1. 開啟 File Sanitizer，然後按一下或點選**設定**。
2. 在**永不拆解清單**下，按一下或點選**新增資料夾**，然後瀏覽至檔案或資料夾。
3. 按一下或點選**開啟**，然後按一下或點選**確定**。

附註： 此清單中的檔案，只要還在清單中就會一直受到保護。

若要從排除清單中移除資產，請清除資產的核取方塊。

一般工作

使用 File Sanitizer 執行下列工作：

- **使用 File Sanitizer 圖示啟動拆解**－將檔案拖曳至 Windows 桌面上的 **File Sanitizer** 圖示。如需詳細資訊，請參閱位於第 33 頁的使用 File Sanitizer 圖示。
- **手動拆解特定資產或所有選取的資產**－隨時都可以拆解項目，不需要等到排定的拆解時間。如需詳細資訊，請參閱位於第 33 頁的按一下滑鼠右鍵拆解或位於第 33 頁的手動啟動拆解作業。
- **手動啟動可用空間清理**－隨時都可以啟動可用空間清理。如需詳細資訊，請參閱位於第 34 頁的手動啟動可用空間清理。
- **檢視記錄檔**－檢視拆解及可用空間清理記錄檔，該記錄檔包含最近一次拆解或可用空間清理作業的任何錯誤或失敗記錄。如需詳細資訊，請參閱位於第 34 頁的檢視記錄檔。

附註： 拆解或可用空間清理作業可能需要很長的時間。雖然拆解和可用空間清理是在背景執行，但增加的處理器用量可能會影響您電腦的效能。

使用 File Sanitizer 圖示

注意： 拆解過的資產無法復原。請仔細考量要選取哪些項目進行手動拆解。

當您以手動方式啟動拆解作業時，會拆解「File Sanitizer」檢視上的標準拆解清單（請參閱位於第 31 頁的設定程序）。

您可以使用下列一種方式，以手動方式啟動拆解作業：

1. 開啟「File Sanitizer」（請參閱位於第 30 頁的開啟 File Sanitizer），然後按一下或點選**拆解**。
2. 開啟確認對話方塊時，請確定核取要拆解的資產，然後按一下或點選**確定**。

－ 或 －

1. 按一下滑鼠右鍵，或點選並按住 Windows 桌面的 **File Sanitizer** 圖示，然後按一下或點選**立即拆解**。
2. 開啟確認對話方塊時，請確定核取要拆解的資產，然後按一下或點選**拆解**。

按一下滑鼠右鍵拆解

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。

如果已在「File Sanitizer」檢視上選取**啟用按一下滑鼠右鍵拆解**，即可依照下列方式拆解資產：

1. 瀏覽至要拆解的文件或資料夾。
2. 按一下滑鼠右鍵，或點選並按住檔案或資料夾，然後 選取 **HP File Sanitizer** － **拆解**。

手動啟動拆解作業

注意： 拆解過的資產無法復原。請仔細考量要選取哪些項目進行手動拆解。

當您以手動方式啟動拆解作業時，會拆解「File Sanitizer」檢視上的標準拆解清單（請參閱位於第 31 頁的設定程序）。

您可以使用下列一種方式，以手動方式啟動拆解作業：

1. 開啟「File Sanitizer」（請參閱位於第 30 頁的開啟 File Sanitizer），然後按一下或點選**拆解**。
2. 開啟確認對話方塊時，請確定核取要拆解的資產，然後按一下或點選**確定**。

– 或 –

1. 按一下滑鼠右鍵，或點選並按住 Windows 桌面的 **File Sanitizer** 圖示，然後按一下或點選**立即拆解**。
2. 開啟確認對話方塊時，請確定核取要拆解的資產，然後按一下或點選**拆解** 。

手動啟動可用空間清理

當您以手動方式啟動清理作業時，會清理「File Sanitizer」檢視上的標準拆解清單（請參閱位於第 31 頁的設定程序）。

您可以使用下列一種方式，以手動方式啟動清理作業：

1. 開啟「File Sanitizer」（請參閱位於第 30 頁的開啟 File Sanitizer），然後按一下或點選**清理** 。
2. 當出現確認對話方塊時，按一下或點選**確定**。

– 或 –

1. 按一下滑鼠右鍵，或點選並按住 Windows 桌面的 **File Sanitizer** 圖示，然後按一下或點選**立即清理**。
2. 當出現確認對話方塊時，按一下或點選**清理**。

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： 已成功拆解或清理的檔案不會出現在記錄檔中。

已經為拆解作業建立一個記錄檔，又為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的下列資料夾中：

- C:\Program Files\Hewlett-Packard\File Sanitizer**[使用者名稱]**_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer**[使用者名稱]**_DiskBleachLog.txt

針對 64 位元系統，記錄檔會儲存在硬碟的下列資料夾中：

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

7 HP Device Access Manager（僅限特定機型）

HP Device Access Manager 可透過停用資料傳輸裝置的方式控制資料存取。

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 37 頁的未受管理的裝置類別。

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

- 它為每位使用者建立裝置設定檔，以定義允許或拒絕使用者存取的裝置。
- Just In Time Authentication (JITA) 可讓預先定義的使用者自行驗證，以存取遭到拒絕的裝置。
- 管理員和受信任的使用者在 Device Access Manager 利用的裝置存取上，可以被排除在限制之外，方法是，將管理員和受信任的使用者加入到「裝置管理員」群組。此群組的成員資格是使用「進階設定」管理。
- 您可以依據群組成員資格或個人使用者來授與或拒絕裝置存取。
- 針對裝置類別（例如 CD-ROM 光碟機和 DVD 光碟機），可以分別允許或拒絕讀取和寫入存取。

HP Device Access Manager 正在完成 HP Client Security 設定精靈的過程中，使用下列設定值自動進行設定：

- 即時驗證 (JITA) 抽取式媒體是針對管理員及使用者啟用。
- 裝置原則允許其他裝置的完整存取權。

開啟 Device Access Manager

1. 從「開始」畫面按一下或點選 **HP Client Security** 應用程式 (Windows 8)。

   － 或 －

   從 Windows 桌面的工作列最右端的通知區域中，連按兩下或點選兩下 **HP Client Security** 圖示。

2. 在**裝置**下，按一下或點選**裝置權限**。
   - 標準使用者可檢視其目前的裝置存取權（請參閱位於第 35 頁的使用者檢視）。
   - 管理員可檢視和變更目前針對電腦所設定的裝置存取權，方法是按一下或點選**變更**，然後輸入管理員密碼（請參閱位於第 36 頁的系統檢視）。

使用者檢視

選取**裝置權限**時，會顯示使用者檢視。根據此原則，標準使用者和管理員可檢視他們對這台電腦上的裝置類別或個別裝置所擁有的存取權。

- **目前使用者** — 顯示目前登入的使用者名稱。
- **裝置類別** — 顯示裝置的類型。
- **存取** — 顯示您目前針對裝置類型或特地的裝置所設定的存取權。

- **持續時間** — 顯示存取 CD/DVD-ROM 光碟機或抽取式磁碟機的時間限制。
- **設定** — 管理員可變更哪些磁碟機的存取權將受到 Device Access Manager 控制。

系統檢視

在「系統」檢視上，管理員可允許或拒絕使用者群組或管理員群組存取此電腦的裝置。

▲ 管理員可存取「系統」檢視，方法是按一下或點選**變更**，輸入管理員密碼，然後從下列選項中選取：

- **Device Access Manager** — 若要開啟或關閉使用即時驗證的 HP Device Access Manager，請按一下或點選**開啟**或**關閉**。
- **此電腦上的使用者和群組** — 顯示允許或拒絕存取所選裝置類別的「使用者」群組或「管理員」群組。
- **裝置類別** — 顯示系統上目前或先前可能已安裝的裝置類別和裝置。若要展開清單，請按一下 **+** 圖示。隨即顯示連線至電腦的所有裝置，並展開「管理員」和「使用者」群組來顯示其成員資格。若要重新整理裝置清單，請按一下圓形的箭號（重新整理）圖示。
  - 裝置類別通常會受到防護。若將存取設為**允許**，選取的使用者或群組就能存取裝置類別中的任何裝置。
  - 特定裝置也會受到防護。
  - 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 光碟機或抽取式磁碟機。如需詳細資訊，請參閱位於第 37 頁的 JITA 組態。
  - 允許或拒絕存取其他裝置類別，例如抽取式媒體（如 USB 快閃磁碟機）、序列埠及並列埠、Bluetooth® 裝置、數據機裝置、PCMCIA/ExpressCard 裝置、1394 裝置、指紋讀取器和智慧卡讀取器。如果指紋讀取器和智慧卡讀取器遭到拒絕，則可將它們作為驗證認證，但無法在「工作階段原則」層級上使用。

    附註： 如果有使用 Bluetooth 裝置做為驗證認證，Device Access Manager 原則中不應限制 Bluetooth 裝置存取。
  - 在「群組」或「裝置類別」層級上選取設定，且系統詢問您是否要將設定套用至子物件時：

    是 — 將散佈設定。

    否 — 不會散佈設定。
  - 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。

    附註： 「管理員」群組無法加入至「使用者清單」。
- **存取** — 按一下或點選向下箭號，然後從底下選取要允許或拒絕存取的一種存取類型：
  - **允許 – 完整存取權**
  - **允許 – 唯讀**
  - **允許 – 需要 JITA** — 如需詳細資訊，請參閱位於第 37 頁的 JITA 組態。

    如果選取此存取類型，請在**持續時間**下，按一下或點選向下箭號以選取時間限制。
  - **Deny**（拒絕）
- **持續時間** — 按一下或點選向下箭號，選取存取 CD/DVD-ROM 光碟機或抽取式磁碟機的時間限制（請參閱位於第 37 頁的 JITA 組態）。

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。

啟用 JITA 的使用者，將可存取**裝置類別組態**檢視中所建立之原則已受到限制的某些裝置。

JITA 期間可授權為數分鐘或「不受限制」。不受限制的使用者可以在從驗證起到登出系統為止的期間存取裝置。

如果將限制的 JITA 期提供給使用者，則在 JITA 期間過期前一分鐘，系統將詢問使用者是否要延長存取權。當使用者登出系統或其他使用者登入後，JITA 期間會立即過期。下次使用者登入並嘗試存取啟用 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
- 抽取式磁碟機

為使用者或群組建立 JITA 原則

管理員可允許使用者或群組使用及時驗證 (JITA) 存取裝置。

1. 啟動 **Device Access Manager**，然後按一下或點選**變更**。
2. 選取使用者或群組，然後在**抽取式磁碟機**或 **DVD/CD-ROM 光碟機**的**存取**下方，按一下或點選向下箭號，然後選取**允許 – 需要 JITA**。
3. 在**持續時間**下方，按一下或點選向下箭號以選取 JITA 存取的期間。

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。

為使用者或群組停用 JITA 原則

管理員可讓使用者或群組無法使用及時驗證存取裝置。

1. 啟動 **Device Access Manager**，然後按一下或點選**變更**。
2. 選取使用者或群組，然後在**抽取式磁碟機**或 **DVD/CD-ROM 光碟機**的**存取**下方，按一下或點選向下箭號，然後選取**拒絕**。

當使用者登入並嘗試存取裝置時，存取遭拒。

設定

設定檢視允許管理員檢視及變更受 Device Access Manager 磁碟機控制的存取。

附註： 設定磁碟機代號清單時，必須啟用 Device Access Manager（請參閱位於第 36 頁的系統檢視）。

未受管理的裝置類別

HP Device Access Manager 不會管理下列裝置類別：

- 輸出/輸入裝置
  - CD-ROM
  - 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
- 紅外線使用者介面裝置
- 滑鼠
- 多重連接埠序列
- 鍵盤
- 隨插即用 (PnP) 印表機
- 印表機
- 印表機升級

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

8 HP Trust Circles

HP Trust Circles 是一個檔案及文件安全性應用程式，其結合了資料夾檔案加密與便利的信任圈文件共享功能。此應用程式可加密使用者指定的資料夾所儲存的檔案，使用一個 Trust Circle 來保護它們。一旦受到保護，唯有 Trust Circle 的成員可使用和共用這些檔案。如果非成員接收保護的檔案，檔案將維持加密，且非成員將無法存取內容。

開啟 Trust Circles

1. 在「開始」畫面，按一下或點選 **HP Client Security** 應用程式。

   － 或 －

   從 Windows 桌面上，連按兩下工作列最右邊通知區域中的 **HP Client Security** 圖示。

2. 在**資料**下，按一下或點選 **Trust Circles** 。

快速入門

有兩種方法可傳送電子郵件邀請及回覆電子郵件：

- **使用 Microsoft® Outlook** － 搭配使用 Trust Circles 與 Microsoft Outlook 可自動處理任何 Trust Circle 邀請及其他 Trust Circle 使用者的回應。
- **使用 Gmail、Yahoo、Outlook.com 或其他電子郵件服務 (SMTP)** － 當您輸入您的名稱、電子郵件地址和密碼時，Trust Circles 會使用您的電子郵件服務，將電子郵件邀請傳送到選擇加入您 Trust Circle 的成員。

若要設定您的基本設定檔：

1. 輸入您的名稱和電子郵件地址，然後按一下或點選**下一步**。

   受邀加入您 Trust Circle 的任何成員都會看到名稱。電子郵件地址可用來傳送、接收或回覆邀請。

2. 輸入電子郵件帳戶的密碼，然後按一下或點選**下一步**。

   系統將傳送測試電子郵件，確定電子郵件設定是正確的。

   附註： 電腦必須連線至網路。

3. 在 **Trust Circle 名稱**欄位中，輸入名稱，然後按一下或點選**下一步**。
4. 新增成員和資料夾，然後按一下或點選**下一步**。Trust Circle 是使用選取的任何資料夾所建立，並將電子郵件邀請傳送給選取的任何成員。若無法傳送邀請（不論原因為何），則將顯示通知。您可以按一下**您的 Trust Circle** ，然後連按兩下或點選兩下信任圈，從 Trust Circle 檢視中隨時及重新邀請成員。如需詳細資訊，請參閱位於第 40 頁的 Trust Circles。

Trust Circles

您可以在輸入電子郵件地址後的初始設定期間建立 Trust Circle，或在 Trust Circle 檢視上建立：

▲ 從 Trust Circle 檢視，按一下或點選**建立 Trust Circle**，然後輸入名稱。

- 若要將成員新增至 Trust Circle，請按一下或點選**成員**旁的 **M+** 圖示，然後依照畫面上的指示繼續執行。
- 若要將資料夾新增至 Trust Circle，請按一下或點選**資料夾**旁的 **+** 圖示，然後依照畫面上的指示繼續執行。

將資料夾新增至 Trust Circle

將資料夾新增至新的 Trust Circle：

- 在信任圈的建立過程中，您可以按一下或點選**資料夾**旁的 **+** 圖示，然後依照畫面上的指示新增資料夾。

  – 或 –

- 在 Windows 檔案總管中，按一下滑鼠右鍵，或點選並按住目前不屬於 Trust Circle 的資料夾，選取 **Trust Circle**，然後選取**從資料夾建立 Trust Circle**。

提示： 您可以選取一或多個資料夾。

將資料夾新增至現有的 Trust Circle：

- 檢視 Trust Circle 時，按一下**您的 Trust Circle**，然後點選兩下或輕觸兩下現有的 trust circle 以顯示目前的資料夾，按一下或點選**資料夾**旁的 **+** 圖示，然後依照畫面上的指示繼續執行。

  – 或 –

- 在 Windows 檔案總管中，按一下滑鼠右鍵，或點選並按住目前不屬於 Trust Circle 的資料夾，選取 **Trust Circle**，然後選取**從資料夾加至現有的 Trust Circle** 。

提示： 您可以選取一或多個資料夾。

將資料夾新增至 Trust Circle 後，Trust Circle 會自動加密資料夾及其內容。加密所有檔案後，畫面會顯示通知。此外，會在資料夾中所有加密的資料夾圖示和檔案圖示上顯示綠色的鎖符號，指出它們已受到完整的保護。

將成員新增至 Trust Circle

若要將成員新增至 Trust Circle，需要執行三個步驟：

1. **邀請** – Trust Circle 的擁有者需要先邀請成員。可將邀請電子郵件傳送給多個使用者或通訊群組清單/群組。
2. **接受** – 受邀者收到邀請並選擇接受或拒絕。如果受邀者接受邀請，會將電子郵件回應傳送給邀請人。若已將邀請傳送給群組，則每個成員都會收到邀請並選擇接受或拒絕。
3. **註冊** – 邀請人最終可決定是否將成員新增至 Trust Circle。如果邀請人決定註冊成員，會將電子郵件傳送給認可回應的受邀者。邀請人和受邀者可選擇驗證邀請程序的安全性。畫面會顯示受邀者的驗證代碼，邀請人必須撥打電話索取該代碼。驗證代碼後，邀請人可傳送最終的註冊電子郵件。

將成員新增至新的 Trust Circle：

▲ 在 Trust Circle 的建立過程中，您可以按一下或點選**成員**旁的 **M+** 圖示，然後依照畫面上的指示新增成員。

- 若是使用 Outlook，請從 Outlook 通訊錄選取連絡人，然後按一下**確定**。
- 若是使用其他電子郵件服務，請將新電子郵件地址手動新增至 Trust Circle，或者從 Trust Circle 中註冊的電子郵件地址中擷取。

將成員新增至現有的 Trust Circle：

▲ 檢視 Trust Circle 時，按一下**您的 Trust Circle**，並點選兩下或輕觸兩下現有的 trust circle 以顯示目前的成員，按一下或點選**成員**旁的 **M+** 圖示，然後依照畫面上的指示繼續執行。

- 若是使用 Outlook，請從 Outlook 通訊錄選取連絡人，然後按一下**確定**。
- 若是使用其他電子郵件服務，請將新電子郵件地址手動新增至 Trust Circle，或者從 Trust Circle 中註冊的電子郵件地址中擷取。

將檔案新增至 Trust Circle

您可以使用下列一種方式，將檔案新增至 Trust Circle：

- 將檔案複製或移動到現有的 Trust Circle 資料夾。

  － 或 －

- 在 Windows 檔案總管中，用滑鼠右鍵按一下或點選並按住某個未加密的檔案，並選擇 **Trust Circle**，然後選取**加密**。系統將提示您選取必須新增檔案的 Trust Circle。

提示： 您可以選取一或多個檔案。

加密的資料夾

Trust Circle 的任何成員皆可檢視和編輯該 Trust Circle 的檔案。

附註： Trust Circle Manager/Reader 不會在成員之間同步檔案。

必須以現有方式共用檔案，例如電子郵件、ftp 或雲端儲存提供者。複製或移動到 Trust Circle 資料夾的檔案，或在該資料夾中建立的檔案，都會立即受到保護。

從 Trust Circle 移除資料夾

從 Trust Circle 移除資料夾會解密資料夾及其所有內容，並移除他們的保護。

- 從 Trust Circle 檢視中，按一下或點選**您的 Trust Circles**，連按兩下或點選兩下現有的 Trust Circle 以顯示目前的資料夾，然後按一下或點選該資料夾旁邊的**垃圾桶**圖示。

  － 或 －

- 在 Windows 檔案總管中，按一下滑鼠右鍵，或點選並按住目前不屬於 Trust Circle 的資料夾，選取 **Trust Circle**，然後選取**從 Trust Circle 移除資料夾**。

提示： 您可以選取一或多個資料夾。

從 Trust Circle 移除檔案

若要自信任圈移除檔案，在 Windows 檔案總管中，用滑鼠右鍵按一下或點選並按住某個未加密的檔案，並選擇**信任圈**，然後選擇 **解密檔案**。

從 Trust Circle 移除成員

無法從 Trust Circle 移除完全註冊的成員。替代的方法是建立一個內含其他所有成員的新 Trust Circle ，將所有檔案和資料夾移至新 Trust Circle，然後刪除舊 Trust Circle 。如此可確保無法存取成員所接收的任何新檔案，但舊 Trust Circle 的成員仍可存取先前已共用的任何內容。

如果成員未完全註冊（即成員已受邀加入 Trust Circle，或尚未接受 Trust Circle 的邀請），您可以利用下列一種方式，從 Trust Circle 移除該成員：

- 從 Trust Circle 檢視中，按一下或點選**您的 Trust Circles**，然後連按兩下或點選兩下 Trust Circle 以顯示目前的成員清單。按一下或點選要移除之成員名稱旁的**垃圾桶**圖示。
- 從 Trust Circle 檢視中，按一下或點選**成員**，然後連按兩下或點選兩下成員以顯示其所屬的 Trust Circle。按一下或點選 Trust Circle 旁邊的**垃圾桶**圖示，從該 Trust Circle 移除成員。

刪除 Trust Circle

若要刪除 Trust Circle，需要具備所有權。

▲ 從 Trust Circle 檢視，按一下或點選**您的 Trust Circles**，按一下或點選欲刪除之 Trust Circle 旁的**垃圾桶**圖示。

這將從頁面中移除 Trust Circle ，並將電子郵件傳送給 Trust Circle 的所有成員 ，將刪除 Trust Circle 的消息通知這些成員。並且將解密該 Trust Circle 所包含的任何檔案或資料夾。

設定偏好設定

從 Trust Circle 檢視中，按一下或點選**偏好設定**。隨即顯示三個標籤

- **電子郵件設定**

選項	說明
使用者名稱	顯示目前正在使用的使用者名稱。若要變更，請在文字方塊中輸入新使用者名稱。系統會自動儲存變更。
電子郵件地址	顯示目前使用的電子郵件究戶。若要變更，請按一下或點選**變更電子郵件設定**，然後依照畫面上的指示繼續執行。
新成員確認	從下列選項選取： 。 **自動確認** — 收到受邀者的接受訊息時，不需任何手動輸入即可在 Trust Circle 中確認受邀者，並將確認電子郵件傳送給受邀者。 。 **手動確認** — 收到受邀者的接受訊息時 ，需要手動輸入才能在 Trust Circle 中註冊新成員，然後將確認電子郵件傳送給受邀者。 。 **需要驗證** — 收到受邀者的接受訊息時，需要驗證代碼才能完整註冊受邀者。Trust Circle 的擁有者必須連絡受邀者 並向他們索取驗證代碼。輸入正確的代碼後會傳送確認電子郵件。
定期驗證	定期驗證需要使用者在指定的逾時（以分鐘為單位記錄）後，以及執行敏感的作業時，輸入 Windows 密碼。此設定允許使用者開啟或關閉驗證。
驗證逾時	選取需要驗證前必須經過的指定逾時期間（以分鐘為單位記錄）。
不顯示確認訊息	選取此核取方塊可停止顯示確認訊息，或清除核取方塊以顯示確認訊息。
我想透過匿名的使用情況追蹤來協助改善 HP Trust Circle	選取此核取方塊可參與計劃，或如果您不想要參與，請清除核取方塊。

- **備份/還原**

選項	說明
備份	將您的 Trust Circle Manager/Reader 應用程式資料（設定和 Trust Circle）複製到備份檔案。在發生損毀或系統故障的事件中，您可以使用此檔案，將新安裝的 Trust Circles 還原成檔案中儲存的狀態。 **附註：** 只會儲存您的 Trust Circle 應用程式資料（Trust Circle、設定和成員）。不會備份 Trust Circle 資料夾中的實際檔案。必須分開備份那些檔案。 若要備份 Trust Circle 設定和使用者資料： **1.** 按一下或點選**備份**。 **2.** 選擇備份檔案的檔案名稱和目錄，然後按一下或點選**儲存**。 **3.** 輸入密碼，確認密碼，然後按一下或點選**確定**。將需要此密碼才能還原此檔案。
還原	從備份檔案還原設定和 Trust Circle，通常是在系統損毀或移轉至其他電腦後執行。 若要還原 Trust Circle Manager 的設定和使用者資料： **1.** 按一下或點選**還原**。 **2.** 瀏覽至備份檔案的目錄和檔案名稱，然後按一下或點選**開啟**。 **3.** 輸入進行備份時所設定的密碼。

- **關於** — 顯示 Trust Circle Manager/Reader 軟體版本。畫面會顯示連結，可讓您將 Trust Circle Manager 升級至 Pro 版本，或顯示 HP 隱私權聲明。

9 竊盜復原（僅限特定機型）

Computrace（需另外購買）可讓您從遠端監視、管理以及追蹤您的電腦。

一旦啟用之後，就會從 Absolute Software Customer Center 設定 Computrace。管理員可以從 Customer Center 設定 Computrace 監視或管理電腦。如果系統錯置或遭竊，Customer Center 可以協助當地的授權單位尋找並復原電腦。如果有設定，即使清理或更換硬碟，Computrace 還是可以繼續運作。

若要啟用 Computrace：

1. 連線到網際網路。
2. 啟動 HP Client Security 如需詳細資訊，請參閱位於第 7 頁的開啟 HP Client Security。
3. 按一下**遭竊復原**。
4. 若要啟動「Computrace 啟用精靈」，請按一下**開始使用**。
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。

啟用精靈會安全地處理交易並在 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 啟動精靈，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。

▲ 如需關於 Computrace 的詳細資訊，請按一下**瞭解詳細資訊**。

10 本地化密碼例外狀況

在「開機驗證」層級與 HP Drive Encryption 層級上，密碼本地化支援會受到限制。如需詳細資訊，請參閱位於第 45 頁的開機驗證層級或「Drive Encryption」層級不支援 Windows IME。

當密碼遭到拒絕時要如何處理

密碼可能因為下列原因遭到拒絕：

- 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. 使用**控制台**新增支援的鍵盤配置（在「中文輸入語言」下方新增美式英文鍵盤）。
  2. 設定預設輸入的支援鍵盤。
  3. 啟動 HP Client Security，然後輸入 Windows 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。如需不支援的字元相關資訊，請參閱位於第 46 頁的特殊鍵處理。
  2. 啟動 HP Client Security，然後輸入 Windows 密碼。

開機驗證層級或「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。

開機驗證或「Drive Encryption」層級並不支援 IME。在開機驗證或「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。

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 Client Security 就可以支援該配置。

⚠ **警告！** 部署 HP Client Security 時，將拒絕使用 Windows IME 所輸入的密碼。

使用鍵盤配置的密碼變更亦受支援

如果最初是透過某種鍵盤配置（例如美國英文 (409)）設定鍵盤，然後使用者又使用另一種同樣受支援的鍵盤配置（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 Client Security 的「使用者」頁面（可從首頁的**齒輪**圖示存取），從 HP Client Security 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重新執行 HP Client Security 設定精靈。BIOS 會儲存所需的鍵盤配置，而且也會在 BIOS 中設定可透過此鍵盤配置輸入的密碼。

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，但美式國際鍵盤配置 (20409) 和拉丁美洲鍵盤配置 (080A) 都可以產生字元 é。如果最初是以拉丁美洲鍵盤配置設定密碼，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

  當使用者在開機授權和 HP Drive Encryption 中選擇先前的鍵盤配置輸入密碼時（例如 abcdef），必須按住 Shift 鍵以輸入小寫字母，並按住 Shift 鍵與 Caps Lock（大寫鎖定）以輸入大寫字母。數字密碼則必須使用數字鍵台來輸入。

- 韓文

  當使用者在開機授權和 HP Drive Encryption 中選擇支援的韓文鍵盤配置輸入密碼，必須按住右 alt 鍵以輸入小寫字母，並按住右 alt 鍵和 Caps Lock（大寫鎖定）以輸入大寫字母。

- 下表列出不支援的字元：

語言	Windows	BIOS	Drive Encryption
阿拉伯文	ﻹ、ﻷ 和 ﻵ 鍵會產生兩個字元。	ﻹ、ﻷ 和 ﻵ 鍵會產生一個字元。	ﻹ、ﻷ 和 ﻵ 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 及 É。	ç、è、à 和 é 搭配 Caps Lock 會在開機授權中輸入 ç、è、à 及 é。	ç、è、à 和 é 搭配 Caps Lock 會在 HP Drive Encryption 中輸入 ç、è、à 及 é。
西班牙文	不支援 40a。儘管如此，因為軟體會將它轉換為 c0a，因此仍然有用。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 鍵盤配置變更為 1040a（西班牙文分支）或 080a（拉丁美洲）。	N/A	N/A
美式國際	◦ 不接受最上列的 ¡、¤、‘、’、¥ 及 × 等鍵。 ◦ 不接受第二列的 å、® 及 Þ 等鍵。 ◦ 不接受第三列的 á、ð 及 ø 等鍵。 ◦ 不接受最下列的 æ 鍵。	N/A	N/A
捷克文	◦ 不接受 ğ 鍵。 ◦ 不接受 į 鍵。 ◦ 不接受 ų 鍵。 ◦ 不接受 ė、ı 及 ż 等鍵。 ◦ 不接受 ģ、ķ、ļ、ņ 及 ţ 等鍵。	N/A	N/A

語言	Windows	BIOS	Drive Encryption
斯洛伐克文	不接受 ż 鍵。	◦ 輸入 š、ś 及 ş 鍵時會被拒絕，但使用螢幕小鍵盤輸入時則可接受。 ◦ ţ 廢鍵會產生兩個字元。	N/A
匈牙利文	不接受 ż 鍵。	ţ 鍵會產生兩個字元。	N/A
斯洛維尼亞文	Windows 不接受 żŻ 鍵，且 alt 鍵會在 BIOS 中產生廢鍵。	BIOS 不接受 ú、Ú、ů、Ů、ş、Ş、ś、Ś、š 及 Š 等鍵。	N/A
日文	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

辭彙

Bluetooth
使用無線電傳輸以啟用具備 Bluetooth 功能的電腦、印表機、滑鼠、行動電話，以及在短距離內進行無線通訊之其他裝置的技術。

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
請參閱 Drive Encryption 預先開機驗證。

Drive Encryption 預先開機驗證
在 Windows 啟動之前所顯示的登入畫面。使用者必須輸入 Windows 使用者名稱及密碼或智慧卡 PIN 碼，或者掃過已註冊的手指。如果選取一步登入，則在 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 復原
藉由正確回答安全性問題即可存取電腦的能力。

PIN
註冊使用者進行驗證時使用的個人識別碼。

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。

Trust Circle
將資料繫結至定義的受信任使用者群組，藉此提供資料控制。這能防止資料在意外或蓄意的情況下傳送給錯誤的人員。利用 CryptoMill 的「零負擔金鑰管理 (Zero Overhead Key Management)」技術保護資料，以密碼編譯的方式將資料繫結至 Trust Circle。如此一來，可防止 trust circle 外的文件或機密資訊受到解密。

Trust Circle Manager/讀取器
Trust Circle Reader 只能接受 Trust Circle Manager 使用者所傳送的邀請。然而，Trust Circle Manager 可建立 Trust Circle。具備的功能包括透過電子郵件邀請某人加入 Trust Circle，及接受他人的 Trust Circle 邀請。在好友夥伴之間建立 Trust Circle 後，可安全地共用該 Trust Circle 所保護的檔案。

Trust Circle 資料夾
受 Trust Circle 保護的任何資料夾。

Windows 使用者帳戶
經授權登入網路或個人電腦的使用者。

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。

已連接裝置
連接到電腦連接埠的硬體裝置。

及時驗證
請參閱 HP Device Access Manager 軟體說明。

手動拆解
略過排定的拆解作業，立即拆解資產或選取的資產。

加密
將演算法之類的程序用於密碼使用法中，並將明文轉換為密碼文字，以避免未經授權的收件者閱讀該資料。資料加密分為許多類型，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
在已刪除的資產及未使用的空間上寫入隨機資料。此程序會降低已刪除資產的存在性，因此更難以復原原始資產。

安全登入法
用來登入電腦的方法。

自動拆解
您在 File Sanitizer 中排程的拆解。

身份識別
HP Client Security 中的認證和設定群組，其處理方式類似於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
演算法的執行會以無意義的資料覆寫資產中所包含的資料。

非接觸式卡片
含有電腦晶片可用於驗證的塑膠卡片。

信任平台模組 (TPM) 嵌入式安全晶片
TPM 會驗證電腦而非使用者，方法是，儲存主機系統專屬的資訊，例如加密金鑰、數位憑證以及密碼。TPM 會將實際竊賊所危害的電腦資訊以及外部駭客的攻擊之類的風險降至最低。

指紋
數位擷取的指紋影像。HP Client Security 不會儲存您實際的指紋影像。

重新開機
重新啟動電腦的程序。

首頁
可存取及管理 HP Client Security 功能和設定的集中位置。

啟用
必須先完成才能使用任何一項 Drive Encryption 功能的工作。管理員可以使用 HP Client Security 設定精靈或 HP Client Security 來啟動 Drive Encryption。啟動程序包含啟動軟體、加密磁碟機以及在抽取式儲存裝置上建立初始備份加密金鑰。

軟體加密
使用軟體一個磁區接著一個磁區的加密硬碟。此程序較硬體加密慢

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
儲存驗證資訊的功能，讓您使用 HP Client Security 以存取需要密碼驗證的網際網路與 Windows 應用程式。

智慧卡
可使用 PIN 進行驗證的硬體裝置。

登入
HP Client Security 中含有使用者名稱和密碼（與其他可能的特定資訊）的一項物件，可用於登入網站或其他程式。

硬體加密
使用符合「可信賴的運算群組」針對自我加密磁碟機管理 OPAL 規格的自我加密磁碟機，以完成即時加密。硬體加密是即時的，可能只需要花數分鐘的時間，但是軟體加密可能要花上數個小時。

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。

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為純文字的程序。

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。

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為另一個。

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
用來驗證個別使用者的特定資訊或硬體裝置。

鄰近感應式卡片
一張含有電腦晶片的塑膠卡片，可以與其他認證搭配用於驗證以獲得更多的安全性保障。

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。

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。

驗證
透過使用 Windows 密碼、指紋、智慧卡、非接觸式卡片或鄰近感應式卡片等認證方式驗證您的身分是否相符的程序。

索引

十二畫

十三畫

十四畫

十七畫

十九畫

二十三畫