



HP ProtectTools

快速入門

© Copyright 2012 Hewlett-Packard
Development Company, L.P.

Bluetooth 是其所有人所擁有的商標，由
Hewlett-Packard Company 取得授權使用
之。**Intel** 是 **Intel Corporation** 在美國和其他
國家/地區的商標，已取得授權使用之。
Microsoft 和 **Windows** 是 **Microsoft**
Corporation 在美國的註冊商標。

本文件包含的資訊可能有所變更，恕不另行
通知。**HP** 產品與服務的保固僅列於隨產品
及服務隨附的明確保固聲明中。本文件的任
何部份都不可構成任何額外的保固。**HP** 不
負責本文件在技術上或編輯上的錯誤或疏
失。

第 1 版：2012 年 8 月

文件編號：702113-AB1

目錄

1 安全性簡介	1
HP ProtectTools 功能	1
HP ProtectTools 安全性產品說明及常用範例	2
Password Manager	2
Drive Encryption for HP ProtectTools (僅限特定機型)	3
Device Access Manager for HP ProtectTools (僅限特定機型)	3
Computrace for HP ProtectTools (原來為 LoJack Pro) (另外購買)	3
達成關鍵安全性目標	4
防範針對性的竊盜行為	4
限制對敏感資料的存取	4
防範來自內部或外部位置的未經授權存取	4
建立強式密碼原則	5
其他安全性要素	5
指派安全性角色	5
管理 HP ProtectTools 密碼	5
建立安全密碼	6
備份認證和設定	6
2 快速入門	7
HP Client Security 設定精靈	7
HP ProtectTools Security Manager 設定精靈	8
HP Client Security 儀表板	8
3 小型企業適用的簡易設定指南	9
快速入門	9
Password Manager	9
在 Password Manager 中檢視與管理已儲存的驗證	10
Device Access Manager for HP ProtectTools	11
Drive Encryption for HP ProtectTools	11
4 HP ProtectTools Security Manager 管理主控台	13
快速入門	13
HP Client Security 設定精靈	13
HP ProtectTools Security Manager 設定精靈	14
HP Client Security 儀表板	14

開啟 HP ProtectTools 管理主控台	15
使用管理主控台	15
設定您的系統	15
設定電腦適用的驗證	16
登入原則	16
工作階段原則	16
設定	17
管理使用者	17
認證	17
SpareKey	17
指紋	18
臉孔	18
智慧卡	18
初始化智慧卡	18
註冊智慧卡	19
設定智慧卡	19
非接觸式卡片	20
鄰近感應式卡片	20
Bluetooth	20
PIN	20
應用程式	20
一般標籤	21
應用程式標籤	21
資料	21
電腦	21

5 HP ProtectTools Security Manager 22

開啟 Security Manager	22
使用 Security Manager 使用者主控台	22
您個人的識別卡	23
我的登入	23
Password Manager	23
對於尚未建立登入的網頁或程式	24
對於已經建立登入的網頁或程式	24
新增登入	24
編輯登入	25
使用 Password Manager 快速連結功能表	26
將登入分類	26
管理您的登入	26
評估您密碼的強度	27

Password Manager 圖示設定	27
設定	28
Credential Manager	28
變更您的 Windows 密碼	28
設定您的 SpareKey	28
註冊指紋	29
註冊臉孔登入的景像	29
驗證	30
昏暗模式	30
學習	31
刪除景像	31
進階使用者設定	31
設定智慧卡	31
初始化智慧卡	31
註冊智慧卡	32
變更智慧卡 PIN 碼	32
非接觸式卡片	32
鄰近感應式卡片	32
Bluetooth	32
PIN	33
管理	33
進階	33
設定您的偏好設定	33
備份和還原您的資料	33

6 Drive Encryption for HP ProtectTools (僅限特定機型) 35

開啟 Drive Encryption	35
一般工作	36
啟動標準硬碟的 Drive Encryption	36
啟動自我加密磁碟機的 Drive Encryption	36
停用 Drive Encryption	37
在啟用 Drive Encryption 之後登入	38
藉由加密硬碟保護您的資料	38
進階工作	39
管理 Drive Encryption (管理員工作)	39
使用「使用 TPM 提升安全性」(僅限特定機型)	39
加密或解密個別磁碟機分割區(僅限軟體加密)	39
備份與復原(管理員工作)	40
備份加密金鑰	40
使用備份金鑰復原對已啟用電腦的存取	40

執行 HP SpareKey 復原	41
顯示加密狀態	41
7 HP ProtectTools Device Access Manager (僅限特定機型)	43
開啟 Device Access Manager	43
設定程序	43
設定裝置存取	43
簡易組態	44
啟動背景服務	44
裝置類別組態	45
拒絕使用者或群組的存取	46
允許使用者或群組的存取	46
允許群組某個使用者存取裝置類別	46
允許群組某個使用者存取特定裝置	47
移除使用者或群組的設定	47
重設組態	47
JITA 組態	48
為使用者或群組建立 JITA	48
為使用者或群組建立可延伸的 JITA	48
針對使用者或群組停用 JITA	49
進階設定	49
裝置管理員群組	50
eSATA 裝置支援	50
未受管理的裝置類別	50
8 竊盜復原 (僅限特定機型)	52
9 本地化密碼例外狀況	53
當密碼遭到拒絕時要如何處理	53
預先開機安全性層級或 HP Drive Encryption 層級不支援 Windows IME	53
使用鍵盤配置的密碼變更亦受支援	53
特殊鍵處理	54
辭彙	56
索引	59


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 Security Manager 管理主控台（適用於管理員）	<ul style="list-style-type: none">● 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。
HP ProtectTools Security Manager 使用者主控台（適用於使用者）	<ul style="list-style-type: none">● 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 模組有限的控制權。

可供您的電腦使用的軟體模組會因機型而有所不同。

HP ProtectTools 軟體模組可能已預先安裝、預先載入，或是可從 HP 網站下載。如需詳細資訊，請前往 <http://www.hp.com>。

 **附註：** 本指南中的指示是根據以下假設撰寫而成：您已經安裝適用的 HP ProtectTools 軟體模組。

HP ProtectTools 功能


下表將詳細說明 HP ProtectTools 各模組的關鍵功能。

模組	關鍵功能
HP ProtectTools Security Manager 管理主控台	管理員可以執行下列功能： <ul style="list-style-type: none">● 使用 Security Manager 設定精靈設定安全性層級和安全登入法。● 設定對使用者隱匿的選項。● 啟用 Drive Encryption 與設定使用者存取。● 設定 Device Access Manager 原則和使用者存取。● 使用管理員工具來新增與移除 HP ProtectTools 使用者及檢視使用者狀態。
HP ProtectTools Security Manager 使用者主控台	一般使用者可以執行下列功能： <ul style="list-style-type: none">● 檢視加密狀態和 Device Access Manager 的設定。● 啟用 Computrace for HP ProtectTools。● 設定「偏好設定」與「備份和還原」選項。

模組	關鍵功能
Credential Manager	<p>一般使用者可以執行下列功能：</p> <ul style="list-style-type: none"> 變更使用者名稱和密碼。 設定和變更 Windows 密碼、指紋、臉孔影像、智慧卡、鄰近感應式卡片或非接觸式卡片等使用者認證。
Password Manager	<p>一般使用者可以執行下列功能：</p> <ul style="list-style-type: none"> 組合管理與設定使用者名稱和密碼。 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。 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。
Drive Encryption for HP ProtectTools(僅限特定機型)	<ul style="list-style-type: none"> 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）。
Device Access Manager for HP ProtectTools(僅限特定機型)	<ul style="list-style-type: none"> 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。
竊盜追失（CompuTrace for HP ProtectTools，另外購買）	<ul style="list-style-type: none"> 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 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（通常為密碼）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，便可利用它們進行存取。

 **附註：** 有些 HP ProtectTools 安全性產品是專為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。

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。

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 2：一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 **Password Manager** 內組織所有 **Web** 連結、公司使用者名稱及密碼。組織完成後，會計師就可以為員工部署 **Password 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 (僅限特定機型)

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。

Drive Encryption for HP ProtectTools 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路。

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

Device Access Manager for HP ProtectTools 允許管理員限制和管理對硬體的存取。**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。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。

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** 啟用這些員工的存取權，而封鎖其他員工的外部存取。

Computrace for HP ProtectTools (原來為 LoJack Pro) (另外購買)

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。**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 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 ProtectTools 模組可以通力合作，為各種安全性問題提供解決方案，包括下列關鍵安全性目標：

- 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。
 - Security Manager for HP ProtectTools—請參閱[位於第 22 頁的 HP ProtectTools Security Manager](#)。
 - Drive Encryption for HP ProtectTools—請參閱[位於第 35 頁的 Drive Encryption for HP ProtectTools \(僅限特定機型\)](#)。
- 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 for HP ProtectTools—請參閱[位於第 52 頁的竊盜復原 \(僅限特定機型\)](#)。

限制對敏感資料的存取

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 管理員限制對通訊裝置的存取，讓敏感資訊無法從硬碟複製出來。請參閱[位於第 45 頁的裝置類別組態](#)。

防範來自內部或外部位置的未經授權存取

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：

- 啟用預先開機驗證功能時，有助於防止存取作業系統。
 - Security Manager for HP ProtectTools—請參閱[位於第 22 頁的 HP ProtectTools Security Manager](#)。
 - Drive Encryption for HP ProtectTools—請參閱[位於第 35 頁的 Drive Encryption for HP ProtectTools \(僅限特定機型\)](#)。
- Security Manager 有助於確保未經授權的使用者無法取得受密碼保護之應用程式的密碼或存取權限。請參閱[位於第 22 頁的 HP ProtectTools Security Manager](#)。
- 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。請參閱[位於第 43 頁的 HP ProtectTools Device Access Manager \(僅限特定機型\)](#)。


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。請參閱[位於第 22 頁的 HP ProtectTools Security 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。

就 HP ProtectTools 而言，安全性責任和權限可以分配給下列角色：

- 安全性主管一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。

 **附註：** HP ProtectTools 中的許多功能都可以由安全性主管與 HP 合作進行自訂。如需詳細資訊，請前往 <http://www.hp.com>。

- IT 管理員一套用和管理安全性主管定義的安全性功能，也可以啟用和停用某些功能。例如，如果安全性主管決定要部署智慧卡，則 IT 管理員可以同時啟用密碼和智慧卡模式。
- 使用者一使用安全功能。例如，如果安全性主管和 IT 管理員已為系統啟用智慧卡，使用者便可設定智慧卡 PIN 碼，並使用此卡供驗證之用。

 **注意：** 建議使用者遵循「最佳做法」來限制使用者權限和使用者存取權。

未經授權的使用者不應該被授予管理權限。

管理 HP ProtectTools 密碼

大部分 HP ProtectTools Security Manager 功能都受到密碼保護。下表列出常用的密碼、設定密碼的所在軟體模組，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 ProtectTools 密碼	在下列模組中設定	功能
Windows 登入密碼	Windows 控制台或 HP ProtectTools Security Manager	可用於手動登入，以及當做存取各種 Security Manager 功能時的驗證。
Security Manager Backup and Recovery 密碼	Security Manager，由個別使用者設定	保護對 Security Manager Backup and Recovery 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 **l** 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符號來分隔單字或字詞，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。

備份認證和設定

您可以下列方式備份認證：


- 使用 **Drive Encryption for HP ProtectTools** 來選取並備份 **HP ProtectTools** 認證。
- 使用 **HP ProtectTools Security Manager** 中的 **Backup and Recovery** 工具當做集中位置，您可以在此處為部分已安裝的 **HP ProtectTools** 模組，備分與還原其中的安全憑證。

2 快速入門

若要設定 HP ProtectTools 的設定，請使用 HP Client Security 設定精靈或 HP ProtectTools Security Manager 設定精靈。

完成 HP Client Security 設定精靈之後，應用程式狀態會顯示在 HP Client Security 儀表板上。

HP Client Security 設定精靈

 **附註：** 管理 HP ProtectTools 需要管理權限。

HP Client Security 設定精靈可引導您逐步設定最常使用的 Security Manager 功能。如果您先前還未完成 HP Client Security 設定精靈，可以使用下列其中一種方式啟動 HP Client Security 設定精靈：


▲ 從「啟動」畫面，按一下或點選「**HP Client Security**」應用程式。

- 或 -

從 Windows 桌面，按一下或點選「**HP ProtectTools**」小工具。


頁面會以下列順序顯示：

1. **Windows 密碼**—輸入您的 Windows 密碼。
這將會使用強式驗證保護您的 Windows 帳戶。
2. **SpareKey**—若要註冊 SpareKey 選項，請選取三個安全性問題。
3. **登錄指紋**—如果有安裝指紋讀取器及相關的驅動程式，您可以登錄指紋。您必須至少選取並註冊 2 個指紋。
4. **Drive Encryption**—如果有安裝 Drive Encryption for HP ProtectTools，您可以在主要磁碟機上啟用加密：
 - 適用於傳統硬碟的軟體加密
 - 偵測到自我加密磁碟機時的硬體加密您必須在啟用加密之前，在下列一或多個裝置上儲存加密金鑰：

 **附註：** 如果您此時取消精靈，將無法啟用 Windows 和 Drive Encryption 驗證。

- **抽取式媒體**，例如 FAT 32 格式的 USB 快閃磁碟機。
 - 如果在顯示 Drive Encryption 頁面之前偵測到單一抽取式裝置，預設會選取這個選項。
 - 如果偵測到 2 或多個抽取式裝置，請選取其中一個顯示的磁碟機。
 - **SkyDrive**—如果偵測到網際網路連線，則可使用這個選項。
需要 Windows® Live ID。請輸入您的 ID 和密碼，或註冊一個新的 ID。
5. 「完成」頁面會顯示一個成功通知，而且您會收到重新開機的提示，以啟用 Drive Encryption。

HP ProtectTools Security Manager 設定精靈

 **附註：** 管理 HP ProtectTools 需要管理權限。

HP ProtectTools Security Manager 設定精靈會引導您逐步設定 Security Manager 的功能。除了精靈中找到的設定之外，管理員還可以透過「管理主控台」設定其他許多安全性功能。這些設定值會套用到電腦，以及共用該電腦的所有使用者。

若要啟動 HP ProtectTools Security Manager 設定精靈：

- ▲ 在「管理主控台」的左側面板中，按一下「**設定精靈**」，然後按照畫面上的指示進行，直到設定完成為止。

管理員可以從 HP ProtectTools Security Manager 使用者主控台啟動「管理主控台」。如需詳細資訊，請參閱[位於第 13 頁的 HP ProtectTools Security Manager 管理主控台](#)。

所有共用這部電腦的使用者都可以使用 Security Manager 及其應用程式。

HP Client Security 儀表板

若要先前已完成 HP Client Security 設定精靈的情況下開啟 HP Client Security：

- ▲ 從「啟動」畫面輸入 hp，然後選取「**HP Client Security**」。

儀表板會針對每個應用程式，顯示功能及相關狀態的快速總覽。

- ▲ 按一下或點選某個應用程式列可顯示所選應用程式的詳細資訊：
 - 「**立即設定**」按鈕表示應用程式尚未設定。按一下或點選該按鈕可開啟應用程式頁面來設定應用程式。
 - 「**設定**」按鈕表示應用程式狀態沒有問題。按一下或點選該按鈕可存取應用程式的設定。
 - 系統會針對使用者組態啟動「**使用者主控台**」。
 - 系統會針對需要管理員權限的組態啟動「**管理主控台**」。
 - 啟動「使用者主控台」或「管理主控台」之後，「**狀態儀表板**」會保持開啟狀態，而且一旦進行設定並關閉主控台之後，就會重新整理狀態。

3 小型企業適用的簡易設定指南

本章的目的在於為 **HP ProtectTools for Small Business** 中最常見的實用選項，示範基本的啟用步驟。這套軟體有許多工具和選項，可讓您微調您的偏好設定並設定存取控制。本簡易設定指南著重於協助您以最少的心力和時間完成設定，使每個模組開始運作。如需詳細資訊，只要選取您感興趣的模組，然後按一下右上角的「？」或「說明」按鈕。此按鈕就會自動提供資訊，以協助您使用目前顯示的視窗。

快速入門

1. 從 Windows 桌面的工作列最右端的通知區域中，連按兩下 **HP ProtectTools** 圖示，開啟 **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** 設定為「強式驗證原則」。

此設定的設計是為了防止登入 Windows 之後的未經授權存取；如果需要高度安全性，或如果使用者經常要在工作期間離開其系統的話，則建議使用此設定。如果您要變更此設定，請按一下「工作階段原則」標籤，然後進行選擇。

若要讓 **HP ProtectTools Security Manager** 在 Windows 登入期間只需要驗證一次，請依照下列程序進行。

1. 從 Windows 桌面的工作列最右端的通知區域中，連按兩下 **HP ProtectTools** 圖示，開啟 **HP ProtectTools Security Manager**。
2. 在左窗格中，按一下「管理」，然後按一下「管理主控台」。
3. 在左窗格的「系統」底下，選取「安全性」群組中的「驗證」。
4. 按一下「工作階段原則」標籤，然後選取工作階段的登入組合需求。若要反向選取這些選項，按一下「還原預設值」。
5. 完成時，按一下「套用」按鈕。

Password Manager

密碼！我們全都有數個密碼，尤其是如果您經常存取需要登入的網站或使用需要登入的應用程式。一般使用者會針對每個應用程式和網站使用相同的密碼，或使用非常有創意但立即忘掉哪個密碼搭配哪個應用程式的密碼。

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。



附註： 在目前和往後的造訪中，Password Manager 將用到的區域會反白顯示。

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。

若要開啟 Password Manager，請使用下列其中一項方法：

- 使用按鍵組合 **ctrl+Windows 標誌鍵+h** 以開啟 Password Manager，然後按一下「**開啟**」以啟動並驗證已儲存的捷徑。
 - 或 -
- 在 Password Manager 中選取「**管理**」標籤，以開啟 HP ProtectTools Security Manager 來編輯認證。

Password Manager 的「**編輯**」選項可讓您檢視與修改名稱、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/或複製到其他電腦。

Device Access Manager for HP ProtectTools

Device Access Manager 可以用來限制各種內建和外接式儲存裝置的使用，讓您的資料始終安全地存放在硬碟中，而不會洩露到公司外部。例如，您可以允許使用者存取您的資料，但是不准他們將資料複製到 CD、個人音樂播放器，或 USB 記憶體裝置。以下是輕鬆完成此設定的方式。

1. 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示，開啟 HP ProtectTools Security Manager 使用者主控台。
2. 在 HP ProtectTools Security Manager 的左窗格中，按一下「**管理**」，然後按一下「**管理主控台**」。
3. 按一下「**Device Access Manager**」，然後按一下「**裝置類別組態**」。
4. 下一步是選取誰將在所有人都遭封鎖後，繼續擁有存取權限。
5. 選取您要限制的硬體裝置，然後按一下「**套用**」按鈕完成此程序。
6. 選取「**新增**」，按一下「**進階**」，然後按一下「**立即尋找**」。
7. 選取所需的使用者，然後按一下「**確定**」>「**確定**」>「**套用**」。
您的選擇便會顯示在「**使用者/群組**」方塊。
8. 選取使用者將使用的「**裝置類別**」，選取「**允許**」或「**拒絕**」，然後按一下「**套用**」。

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools 是透過加密整個硬碟來保護您的資料。如果您的電腦遭竊而且（或是）其中的硬碟被取下並裝到另一部電腦上，您硬碟中的資料仍會受到保護。


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。

為了讓您更容易使用，有多個軟體模組會自動同步處理密碼，包括 Windows 使用者帳戶、網域、Drive Encryption for HP ProtectTools、Password Manager 以及 HP ProtectTools Security Manager。

請依照下列簡單的步驟，啟用 Drive Encryption for HP ProtectTools：

1. 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示，開啟 HP ProtectTools Security Manager。
2. 在左窗格中，按一下「**管理**」，然後按一下「**管理主控台**」。
3. 在左側窗格中，按一下「**設定精靈**」。
4. 在「歡迎」畫面中，選取「**下一步**」。
5. 輸入您的 Windows 密碼以啟動啟用精靈，然後按「**下一步**」。
6. 如果不需要使用 SpareKey，請略過。
7. 核取「**Drive Encryption**」方塊，然後按「**下一步**」。
8. 核取要加密的磁碟機，然後按「**下一步**」。
9. Drive Encryption 組態視窗需要一個 USB 快閃磁碟機或其他外接式裝置，才能儲存加密復原金鑰。使這個復原金鑰維持在安全狀態，如果預先開機密碼遺失或失敗，此金鑰將用來復原資料或存取磁碟機。

10. 按「**下一步**」，完成程序，然後按一下「**完成**」。移除 USB 快閃磁碟機，然後當您準備好了就可以將電腦重新開機。
11. 系統啟動時，Drive Encryption 會要求您的 Windows 密碼。輸入密碼，然後按一下「**確定**」。

 **附註：** 磁碟機正在加密時，電腦的運作看起來可能很緩慢。一旦完全加密之後，效能將會回復正常。存取磁碟機上的資料時，會依管理員的需要，進行加密或解密。

Drive Encryption 驗證將會透過 Windows 登入，直接「鏈結」到 Windows 桌面，如此便不需要輸入兩次密碼。

4 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 使用者主控台另提供其他應用程式，當電腦遺失或遭竊時可協助其進行復原（僅限特定機型）。

本機管理員可以使用管理主控台執行下列工作：


- 啟用或停用安全功能
- 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

快速入門

若要設定 HP ProtectTools 的設定，請使用 HP Client Security 設定精靈或 HP ProtectTools Security Manager 設定精靈。

完成 HP Client Security 設定精靈之後，應用程式狀態會顯示在 HP Client Security 儀表板上。

HP Client Security 設定精靈

 **附註：** 管理 HP ProtectTools 需要管理權限。

HP Client Security 設定精靈可引導您逐步設定最常使用的 Security Manager 功能。如果您先前還未完成 HP Client Security 設定精靈，可以使用下列其中一種方式啟動 HP Client Security 設定精靈：

▲ 從「啟動」畫面，按一下或點選「**HP Client Security**」應用程式。

- 或 -

從 Windows 桌面，按一下或點選「**HP ProtectTools**」小工具。


頁面會以下列順序顯示：

1. **Windows 密碼**—輸入您的 Windows 密碼。
這將會使用強式驗證保護您的 Windows 帳戶。
2. **SpareKey**—若要註冊 SpareKey 選項，請選取三個安全性問題。
3. **登錄指紋**—如果有安裝指紋讀取器及相關的驅動程式，您可以登錄指紋。您必須至少選取並註冊 2 個指紋。

4. **Drive Encryption**—如果有安裝 Drive Encryption for HP ProtectTools，您可以在主要磁碟機上啟用加密：

- 適用於傳統硬碟的軟體加密
- 偵測到自我加密磁碟機時的硬體加密


您必須在啟用加密之前，在下列一或多個裝置上儲存加密金鑰：

 **附註：** 如果您此時取消精靈，將無法啟用 Windows 和 Drive Encryption 驗證。

- **抽取式媒體**，例如 FAT 32 格式的 USB 快閃磁碟機。
 - 如果在顯示 Drive Encryption 頁面之前偵測到單一抽取式裝置，預設會選取這個選項。
 - 如果偵測到 2 或多個抽取式裝置，請選取其中一個顯示的磁碟機。
- **SkyDrive**—如果偵測到網際網路連線，則可使用這個選項。
需要 Windows® Live ID。請輸入您的 ID 和密碼，或註冊一個新的 ID。

5. 「完成」頁面會顯示一個成功通知，而且您會收到重新開機的提示，以啟用 Drive Encryption。

HP ProtectTools Security Manager 設定精靈

 **附註：** 管理 HP ProtectTools 需要管理權限。

HP ProtectTools Security Manager 設定精靈會引導您逐步設定 Security Manager 的功能。除了精靈中找到的設定之外，管理員還可以透過「管理主控台」設定其他許多安全性功能。這些設定值會套用到電腦，以及共用該電腦的所有使用者。

若要啟動 HP ProtectTools Security Manager 設定精靈：

- ▲ 在「管理主控台」的左側面板中，按一下「**設定精靈**」，然後按照畫面上的指示進行，直到設定完成為止。

管理員可以從 HP ProtectTools Security Manager 使用者主控台啟動「管理主控台」。如需詳細資訊，請參閱[位於第 13 頁的 HP ProtectTools Security Manager 管理主控台](#)。

所有共用這部電腦的使用者都可以使用 Security Manager 及其應用程式。

HP Client Security 儀表板

若要先前已完成 HP Client Security 設定精靈的情況下開啟 HP Client Security：

- ▲ 從「啟動」畫面輸入 hp，然後選取「**HP Client Security**」。

儀表板會針對每個應用程式，顯示功能及相關狀態的快速總覽。

- ▲ 按一下或點選某個應用程式列可顯示所選應用程式的詳細資訊：

- 「**立即設定**」按鈕表示應用程式尚未設定。按一下或點選該按鈕可開啟應用程式頁面來設定應用程式。
- 「**設定**」按鈕表示應用程式狀態沒有問題。按一下或點選該按鈕可存取應用程式的設定。
- 系統會針對使用者組態啟動「**使用者主控台**」。
- 系統會針對需要管理員權限的組態啟動「**管理主控台**」。
- 啟動「使用者主控台」或「管理主控台」之後，「**狀態儀表板**」會保持開啟狀態，而且一旦進行設定並關閉主控台之後，就會重新整理狀態。

開啟 HP ProtectTools 管理主控台

使用 HP ProtectTools 管理主控台進行管理工作，例如設定系統原則或設定軟體。開啟 HP ProtectTools Security Manager 來存取管理主控台：

1. 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示。
 - 或 -從「控制台」選取「系統及安全性」，然後選取「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 使用者主控台的左側面板中，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。

1. 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示。
 - 或 -從「控制台」選取「系統及安全性」，然後選取「**HP ProtectTools Security Manager**」。
2. 在 Security Manager 使用者主控台的左側面板中，按一下「**管理**」，然後按一下「**管理主控台**」。

管理主控台會在左側面板的「首頁」下方顯示下列選項：

- **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**—讓您設定 HP ProtectTools Security Manager 和 Security Manager 應用程式的設定。
- **資料**—讓您設定 Drive Encryption 的設定（僅限特定機型）。
- **電腦**—讓您設定 Device Access Manager 的設定。
- **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並進行設定。

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，選取使用者類別，例如管理員或標準使用者。
3. 按一下驗證認證以顯示編輯對話方塊。
4. 若要要求搭配使用兩個驗證認證，請按向下箭頭選取各個認證，然後按一下「**確定**」。
5. 若要移除認證，請按一下「**X**」，或是在認證上按一下滑鼠右鍵，然後按一下「**刪除**」。
6. 按一下組態對話方塊中的「**是**」。
7. 若要確認使用者是否能夠登入，請按一下「**Check that HP ProtectTools can log on**」（檢查 HP ProtectTools 是否可登入）。
8. 若要還原為原始設定，請按一下「**還原預設值**」。
9. 按一下「**套用**」。

工作階段原則

若要定義支配 Windows 工作階段期間執行驗證所需之認證的原則：

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，選取使用者類別，例如管理員或標準使用者。
3. 按一下驗證認證以顯示編輯對話方塊。
4. 若要要求搭配使用兩個驗證認證，請按向下箭頭選取各個認證，然後按一下「**確定**」。
5. 若要移除認證，請按一下「**X**」，或是在認證上按一下滑鼠右鍵，然後按一下「**刪除**」。
6. 按一下組態對話方塊中的「**是**」。
7. 若要確認使用者是否能夠登入，請按一下「**Check that HP ProtectTools can log on**」（檢查 HP ProtectTools 是否可登入）。
8. 若要還原為原始設定，請按一下「**還原預設值**」。
9. 按一下「**套用**」。

設定

若要在 BIOS 層級或 Drive Encryption 層級已執行驗證時，允許此電腦的使用者略過 Windows 登入：

1. 在管理主控台的左側面板中，按一下「**安全性**」，然後按一下「**設定**」。
2. 允許 **One Step Logon**—選取此核取方塊以啟用 One Step Logon，或清除核取方塊以停用。
3. 按一下「**套用**」。

管理使用者

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

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，可設定由 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. 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。
2. 若要允許使用 SpareKey 復原 Windows 登入，請選取此核取方塊。
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。

臉孔

如果電腦已安裝或連接網路攝影機，而且已安裝 **Face Recognition** 程式，管理員可以設定 **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. 按一下「**認證**」，然後按一下「**臉孔**」。
2. 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**—當註冊的影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。
3. 若要將設定還原為原始值，請按一下「**還原預設值**」。
4. 按一下「**套用**」。

智慧卡

管理員必須先初始化智慧卡，然後智慧卡才可以用於驗證。Windows 支援大部分的 CSP 和 PKCS11 標準智慧卡。

初始化智慧卡

HP ProtectTools Security Manager 可以支援各種不同的智慧卡。做為 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：** 必須安裝智慧卡中介軟體。

1. 取得並安裝使用中智慧卡的中介軟體（例如 ActivIdentity 智慧卡的 ActivClient 6.x）。
2. 將智慧卡插入讀取器。

3. 初始化（格式化）智慧卡。
 - a. 啟動智慧卡初始化工具，或者該工具可能會在智慧卡插入讀取器時顯示。
 - b. 依照畫面上的指示設定 PIN。
 - c. 記下解鎖碼以供日後參考。
4. 建立金鑰配對和憑證。
 - a. 啟用「**HP ProtectTools 管理主控台**」。
 - b. 依序按一下「**認證**」、「**智慧卡**」，然後按一下「**管理**」標籤。
 - c. 請確定已選取「**初始化智慧卡**」。
 - d. 輸入您的 PIN，按一下「**套用**」，然後依照畫面上的指示繼續執行。

在成功初始化智慧卡之後，您必須註冊智慧卡。

註冊智慧卡

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

1. 按一下「**設定精靈**」。
2. 在「**歡迎**」畫面中，按「**下一步**」。
3. 輸入您的 Windows 密碼，然後按「**下一步**」。
4. 在「**SpareKey**」頁面中，按一下「**跳過 SpareKey 設定**」（除非您想要更新 SpareKey 資訊），然後按「**下一步**」。
5. 在「**啟用安全功能**」頁面中，按一下「**下一步**」。
6. 在「**選擇您的認證**」頁面中，確定已選取「**智慧卡**」，然後按「**下一步**」。
7. 在「**智慧卡**」頁面中，輸入您的 PIN，然後按一下「**下一步**」。
8. 按一下「**完成**」。

使用者也可以在 Security Manager 使用者主控台中註冊智慧卡。如需詳細資訊，請按一下「智慧卡」頁面右上角的藍色「？」圖示以參閱 HP ProtectTools Security Manager 軟體「說明」。

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**—選取「**在智慧卡移除時鎖定電腦**」核取方塊，以設定電腦於智慧卡移除時自動鎖定，然後按一下「**套用**」。



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 ProtectTools 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或相關中介軟體不支援的功能。

- ▲ 按一下「**套用**」。

非接觸式卡片

非接觸式卡片是一小張含有電腦晶片的塑膠卡片。如果電腦已連接非接觸式卡片讀取器並安裝製造商提供的相關驅動程式，而且非接觸式卡片已被選取做為驗證認證的話，您就可以使用您的非接觸式卡片進行驗證。HP ProtectTools 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
- ▲ 若要設定您的非接觸卡片，請將它放在非常靠近讀取器的位置，接著依照畫面上的指示繼續執行，然後按一下「**套用**」。

鄰近感應式卡片

鄰近感應式卡片是一小張含有電腦晶片的塑膠卡片。如果電腦已連接鄰近感應式卡片讀取器並安裝製造商提供的相關驅動程式，而且鄰近感應式卡片已被選取做為驗證認證，您就可以用鄰近感應式卡片搭配其他認證以提供更高的安全性。

- ▲ 若要設定鄰近感應式卡片，請將卡放在非常靠近讀取器的位置，然後按一下「**套用**」。

Bluetooth

如果電腦具備 Bluetooth® 功能、Bluetooth 已被選取做為驗證認證，而且 Bluetooth 電話已經與電腦配對，您就可以使用您的 Bluetooth 電話搭配其他認證以提供更高的安全性。指定 Bluetooth 設定：

- ▲ 若要允許無訊息驗證，請選取此核取方塊，然後按一下「**套用**」。

PIN

如果 PIN 已被選取做為驗證認證，您就可以使用 PIN 搭配其他認證以提供更高的安全性。指定 PIN 設定：

1. 按一下向上或向下箭頭以選取 PIN 的最小長度。
允許的上限是 8 位數。
2. 按一下「**套用**」。

應用程式

管理主控台左側面板「應用程式」下方的「設定」頁面包含兩個標籤，可讓您自訂目前已安裝之 HP ProtectTools Security Manager 應用程式的行為。

- ▲ 在管理主控台的左側面板中，按一下「**應用程式**」底下的「**設定**」。

一般標籤

「一般」標籤上有下列設定可供使用：

- **不針對管理員自動啟動設定精靈**—選取此選項即可防止精靈在登入時自動開啟。
 - **不針對使用者自動啟動快速入門精靈**—選取此選項即可防止使用者設定在登入時自動開啟。
1. 選取特定設定旁邊的核取方塊以啟用設定，或清除核取方塊以停用設定。
 2. 按一下「套用」。

應用程式標籤

管理員可以啟用或停用下列應用程式：

- **狀態**—選取此核取方塊可啟用所有應用程式，清除此核取方塊可停用所有應用程式。
 - **Password Manager**—為電腦的所有使用者啟用 Password Manager。
1. 選取特定設定旁邊的核取方塊以啟用設定，或清除核取方塊以停用設定。
 2. 按一下「套用」。

若要使所有應用程式回復出廠設定，請按「**還原預設值**」按鈕。

資料

管理主控台左側面板的「資料」區段可讓您設定下列應用程式的設定：

- **Drive Encryption**—進行設定並顯示磁碟機狀態。如需詳細資訊，請按一下「Drive Encryption」頁面右上角的藍色「？」圖示以參閱 Drive Encryption 軟體「說明」。

電腦

管理主控台左側面板的「電腦」區段可讓您配置 Device Access Manager 應用程式的設定：

- 簡易組態
- 裝置類別組態
- 及時驗證 (JITA) 組態
- 進階設定

如需詳細資訊，請按一下「Device Access Manager」頁面右上角的藍色「？」圖示以參閱 Device Access Manager 軟體「說明」。

5 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。
- 登錄一個或多個影像以進行驗證。
- 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。

開啟 Security Manager

您可以使用下列其中一種方式開啟 Security Manager：

- ▲ 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示。


- 或 -

從「控制台」選取「系統及安全性」，然後選取「**HP ProtectTools Security Manager**」。


使用 Security Manager 使用者主控台

Security Manager 使用者主控台是方便存取 Security Manager 功能、應用程式和設定的集中位置。使用者主控台會顯示下列元件：

- **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示。
- **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。
 - **竊盜追失**—Computrace for HP ProtectTools（另外購買）
- **我的登入**—使用「密碼管理員」和 Credential Manager 管理您的驗證認證。
- **我的資料**—使用 Drive Encryption 管理您資料的安全性。

 **附註：** 如果未安裝此應用程式，則不會顯示這個項目。

- **我的電腦**—使用 Device Access Manager 管理您電腦的安全性。

 **附註：** 如果未安裝此應用程式，則不會顯示這個項目。

- **管理**—允許管理員存取「**管理主控台**」來管理安全性和使用者。

- **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 使用者主控台說明。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。

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. 開啟 Security Manager 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 按一下使用者主控台左上角的「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」。

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。

- **密碼管理員**—建立和管理快速連結，這可讓您使用 Windows 密碼、指紋、臉孔、智慧卡、鄰近感應式卡片、非接觸式卡片、Bluetooth 電話或 PIN 碼進行驗證，以啟動和登入網站及程式。
- **Credential Manager**—可用來變更 Windows 密碼、註冊指紋、註冊臉孔，或設定智慧卡、非接觸式卡片、鄰近感應式卡片、Bluetooth 電話或 PIN 碼。

管理員按一下「管理」，然後按一下 Dashboard 左下角的「集中管理」，就可以存取其他可用安全性應用程式的相關資訊。

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、臉孔、智慧卡、鄰近感應式卡片、非接觸式卡片、PIN 或 Windows 密碼輕鬆快速地登入。

Password Manager 提供下列選項：

「管理」標籤

- 新增、編輯或刪除登入。
- 使用已設定的快速連結來啟動您的預設瀏覽器，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。

「密碼強度」標籤

- 檢查用於網站和應用程式之個別密碼的強度，以及整體密碼強度。
- 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「**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] 新增至密碼管理員—允許您新增目前登入畫面的登入。
- 開啟密碼管理員—啟動密碼管理員。
- 圖示設定—允許您指定顯示「密碼管理員」圖示的條件。
- 說明—顯示 Security Manager 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自動輸入登入欄位，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「密碼管理員」。
- 開啟密碼管理員—啟動密碼管理員。
- 說明—顯示 Security Manager 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

您只要輸入一次登入資訊，即可輕鬆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。您可以在瀏覽到網站或程式後使用這些登入，也可以從「**Password Manager 快速連結**」功能表按一下登入，讓 Password Manager 開啟網站或程式，並且將您登入。

若要新增登入：

1. 開啟網站或程式的登入畫面。
2. 按一下「**Password Manager**」圖示上的箭頭，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 [domain name] 新增至 Password Manager**」。
 - 對於程式，按一下「**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。您也可以透過下列方式顯示此對話方塊：按一下「**Password Manager 管理**」標籤的「**新增登入**」，使用 **ctrl+Windows 標誌鍵+h** 快速鍵，或是掃過您的手指。
 - 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. 按一下「**確定**」，選取您要使用的驗證方法（指紋、臉孔、智慧卡、鄰近感應式卡片、非接觸式卡片、Bluetooth 電話、PIN 或密碼），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。
 - e. 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。
 - 按一下「**關閉**」。

每次您存取該網站或開啟程式時，網站或應用程式登入畫面的左上角就會顯示「**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「**Password Manager**」圖示上的箭頭，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 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**」功能表中或 Password Manager 的「**管理**」標籤中，連接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**」功能表：

1. 按下「**密碼管理員**」快速鍵組合（**ctrl+Windows 標誌鍵+h** 為原廠設定）。若要變更快速鍵組合，請按兩下 Security Manager 使用者主控台上的「**密碼管理員**」，然後按一下「**設定**」。
2. 掃描您的指紋（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 使用者主控台中，按一下「**密碼管理員**」。
2. 按一下「**管理**」標籤，然後按一下「**新增分類**」。
3. 輸入分類的名稱。
4. 按一下「**確定**」。

若要將登入新增至分類：

1. 將滑鼠指標指向所需的登入。
2. 按住滑鼠左鍵。
3. 將登入拖放到分類的清單中。當您將滑鼠指標指向分類時，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，則各個登入會列在登入清單的網站名稱之下並縮排。

若要管理您的登入：

- ▲ 從 Security Manager 使用者主控台中，按一下「**密碼管理員**」，然後按一下「**管理**」標籤。
 - **新增登入**—按一下「**新增登入**」，並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。
 - **開啟**—開啟您有現有登入的網站或程式。
 - **新增**—新增登入。如需詳細資訊，請參閱[位於第 24 頁的新增登入](#)。

- **編輯**—編輯登入。如需詳細資訊，請參閱[位於第 25 頁的編輯登入](#)。
- **刪除**—刪除您有現有登入的網站或程式。
- **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 26 頁的將登入分類](#)。

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「**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，讓您更加容易監控與提升安全性。

在「**密碼強度**」標籤上有紅色、黃色或綠色的狀態指示器，可呈現用於網站和應用程式之個別密碼的強度，以及整體密碼強度。

Password Manager 圖示設定

Password Manager 會嘗試識別網站和程式的登入畫面。當它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，然後按一下「**圖示設定**」以自訂密碼管理員處理可能登入網站的方式。
 - **提示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，密碼管理員會提示您新增登入。
 - **排除此畫面**—選取此核取方塊，密碼管理員便不再提示您為此登入畫面新增登入。

若要為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，開啟 **Security Manager** 使用者主控台，然後按一下「**密碼管理員**」。
 - 按一下「**新增登入**」。
- 接著會開啟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 **Password Manager**」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 24 頁的新增登入](#)。
 - 當此網站登入畫面或程式畫面開啟時，就會顯示「**Password Manager**」圖示。

不提示為登入畫面新增登入—選取選項按鈕。

2. 若要存取其他密碼管理員設定，請按兩下「**密碼管理員**」，然後按一下 **Security Manager** 使用者主控台上的「**設定**」。

設定

您可以指定將 Password Manager 個人化的設定：

1. **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「密碼管理員」圖示就會出現，指示您可以將此畫面的登入新增至「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。
2. **使用 ctrl+win+h 開啟密碼管理員**—開啟「密碼管理員快速連結」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。

可用的認證會因為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
- 臉孔
- 智慧卡
- 非接觸式卡片
- 鄰近感應式卡片
- Bluetooth
- PIN

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 使用者主控台中，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為您輸入的新密碼。

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 HP ProtectTools Security Manager 設定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. 按一下「建立」。


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 歡迎畫面，使用您的 SpareKey 存取電腦。


註冊指紋

如果管理員在「選擇您的認證」畫面中選取了「指紋」，而且您的電腦已內建或連接指紋讀取器，HP ProtectTools Security Manager 設定精靈會引導您進行設定或「註冊」指紋的程序：您也可以在 Security Manager 使用者主控台中「Credential Manager」底下的「指紋」頁面註冊您的指紋。

1. 在精靈的「指紋」頁面上，會顯示兩個手的輪廓。已註冊的手指會以反白顯示。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. 系統會提示您掃過指紋，直到指紋成功註冊為止。已註冊的手指會在輪廓中反白顯示。
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：** 透過精靈註冊手指時，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。

註冊臉孔登入的景像

如果您選擇臉孔登入，而且電腦已內建或連接網路攝影機的話，HP ProtectTools Security Manager 設定精靈會提示您註冊景像。您也可以在 Security Manager 使用者主控台中「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，如果您因為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 HP ProtectTools Security Manager 設定精靈註冊景像：

1. 在精靈的「臉孔登入」頁面上，按一下「進階」，然後設定其他選項。如需詳細資訊，請參閱 [位於第 31 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. 在景象註冊期間，您可以按一下「播放視訊」來觀看示範。

如果這是您第一次註冊，將會出現對話方塊詢問您是否要觀看示範視訊。按一下「是」或「否」。

5. 在低照明環境中，軟體可以自動增加畫面亮度；或者，若要變更背景光，請按一下「**電燈泡**」圖示。
6. 按一下「**相機**」圖示，然後依照畫面上的指示註冊您的景像。

 **附註：** 在擷取景像的同時，請務必看著您的影像，適時地轉動頭部。


7. 按「**下一步**」。

您也可以從 **Security Manager** 使用者主控台註冊景像：

1. 開啟 **Security Manager** 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 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**」來設定其他選項。如需詳細資訊，請參閱[位於第 31 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. 如果系統提示您輸入 **Windows** 密碼，請輸入密碼，然後按「**下一步**」。
7. 在景象註冊期間，您可以按一下「**播放視訊**」來觀看示範。

如果這是您第一次註冊，將會出現對話方塊詢問您是否要觀看示範視訊。按一下「**是**」或「**否**」。

8. 在低照明環境中，軟體可以自動增加畫面亮度；或者，若要變更背景光，請按一下「**電燈泡**」圖示。
9. 按一下「**相機**」圖示，然後依照畫面上的指示註冊您的景像。


 **附註：** 在擷取景像的同時，請務必看著您的影像，適時地轉動頭部。

如需詳細資訊，請按一下「**臉孔註冊**」頁面右上角的藍色「**?**」圖示以參閱 **Face Recognition** 軟體「**說明**」。

驗證

註冊一個或多個景像後，在登入電腦或啟動新的 **Windows** 工作階段時，可使用您的臉孔進行驗證。

1. 啟動驗證畫面，且相機偵測到您的臉孔後，您有 **5 秒鐘** 的時間開始進行登入程序。如果成功驗證您的臉孔，即可存取電腦。
2. 如果臉孔登入逾時，**Face Recognition** 會暫停。按一下「**相機**」圖示可恢復驗證程序。

 **附註：** 如果光線不足，而且您無法使用 **Face Recognition** 登入，您可以輸入 **Windows** 密碼登入電腦。

3. 登入電腦後，如果 **Face Recognition** 要求您新增其他景像，以便您未來更容易登入，請按一下「**是**」。

昏暗模式

如果進行臉孔登入時光線太暗，臉孔登入畫面背景顏色會自動切換至白色畫面，以便提供更好的臉孔光源。

若要手動切換臉孔登入畫面背景顏色，請按一下「**電燈泡**」圖示。

學習

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의影像，以便提升未來臉孔登入成功的機率。

刪除影像

若要刪除目前註冊的影像：

1. 開啟 Security Manager 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 在「我的登入」底下，按一下「**Credential Manager**」，然後按一下「臉孔」。
3. 按一下要刪除的影像，然後按一下「垃圾桶」圖示。
4. 按一下確認對話方塊中的「**確定**」。

進階使用者設定


1. 開啟 Security Manager 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 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**」，設定下列選項：

其他設定標籤—選取核取方塊以啟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影像**—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擷取的影像，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影像**—如果臉孔登入失敗，但密碼輸入成功，系統會提示您註冊新影像，以便提升未來臉孔登入成功的機率。
4. 若要將設定還原為原始值，請按一下「**還原預設值**」。
5. 按一下「**確定**」。

設定智慧卡

如果電腦已內建或連接智慧卡讀取器，而且管理員已啟用智慧卡做為驗證認證，並已執行 HP ProtectTools 管理主控台軟體「說明」中所述步驟，HP ProtectTools Security Manager 設定精靈會提示您插入並設定智慧卡。您也可以 Security Manager 使用者主控台中「**Credential Manager**」底下的「智慧卡」頁面上設定您的智慧卡。

 **附註：** 管理員必須先初始化智慧卡，然後才可以使用。

初始化智慧卡

HP ProtectTools Security Manager 可以支援各種不同的智慧卡。做為 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會提供工具，以便安裝安全性憑證及 PIN 碼管理，這些都將由 HP ProtectTools 在其安全性演算法中使用。

管理員也可使用製造商的軟體和 HP ProtectTools 管理主控台來初始化智慧卡。如需詳細資訊，請參閱 HP ProtectTools 管理主控台軟體「說明」。

註冊智慧卡

在初始化智慧卡後，使用者可以在 **Security Manager** 中加以註冊：

1. 開啟 **Security Manager** 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 按一下「**Credential Manager**」，然後按一下「**智慧卡**」。
3. 請確定已選取「**設定**」。
4. 輸入您的 Windows 密碼及 PIN 碼，然後按一下「**儲存**」。

管理員也可以在 **HP ProtectTools** 管理主控台中註冊智慧卡。如需詳細資訊，請參閱 **HP ProtectTools** 管理主控台軟體「說明」。

變更智慧卡 PIN 碼

若要變更智慧卡 PIN 碼：

1. 插入已事先經過格式化與初始化處理的智慧卡。
2. 選取「**變更智慧卡 PIN**」。
3. 輸入舊的 PIN 碼，然後輸入並確認新的 PIN。

非接觸式卡片

非接觸式卡片是一小張含有電腦晶片的塑膠卡片。如果電腦已連接非接觸式卡片讀取器，而且管理員已安裝製造商提供的相關驅動程式，並已啟用非接觸式卡片做為驗證認證的話，您就可以使用您的非接觸式卡片做為驗證認證。**HP ProtectTools** 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
- ▲ 若要設定您的非接觸卡片，請將它放在非常靠近讀取器的位置，接著依照畫面上的指示繼續執行，然後按一下「**套用**」。

鄰近感應式卡片

鄰近感應式卡片是一小張含有電腦晶片的塑膠卡片。如果電腦已連接鄰近感應式卡片讀取器，而且管理員已安裝製造商提供的相關驅動程式，並已啟用鄰近感應式卡片做為驗證認證的話，您就可以用鄰近感應式卡片搭配其他認證以提供更高的安全性。

- ▲ 若要設定您的鄰近感應式卡片，請將它放在非常靠近讀取器的位置，接著依照畫面上的指示繼續執行，然後按一下「**套用**」。

Bluetooth

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「**註冊**」。
3. 按一下確認對話方塊中的「**確定**」。

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。

- ▲ 若要設定新的 PIN，請輸入 PIN，然後再次輸入加以確認。

管理

按一下「**管理**」，然後選取 HP ProtectTools Security Manager 使用者主控台左下角面板中的「**管理主控台**」，管理員就可以存取「管理主控台」和「集中管理」。

如需詳細資訊，請參閱 HP ProtectTools 管理主控台軟體「說明」。

進階

按一下「使用者主控台」左下角面板中的「**進階**」，您就可以存取下列選項：

- **偏好設定**—允許您將 Security Manager 設定個人化。
- **備份和還原**—允許您備份和還原 Security Manager 資料。
- **關於**—顯示 Security Manager 的版本資訊

設定您的偏好設定


您可以將 HP ProtectTools Security Manager 設定個人化。在 Security Manager 使用者主控台中，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。
- **指紋掃描回應**—只有在有指紋讀取器時才會顯示。使用此設定可調整掃過指紋時出現的回應。
 - **啟用音效回應**—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「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，也可以清除此選項以停用音效回應。
 - **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。

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「密碼管理員」和 Face Recognition 資訊。Drive Encryption 有一個獨立的備份方法。Device Access Manager 和指紋驗證資訊則不會備份。

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. 開啟 Security Manager 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 在「使用者主控台」的左側面板上，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. 開啟 Security Manager 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 在「使用者主控台」的左側面板上，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**」。

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

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

HP ProtectTools Security Manager (HP Client Security 設定精靈、進階設定精靈或管理主控台) 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 ProtectTools Security Manager 軟體「說明」。

Drive Encryption 可執行下列工作：

- 選取 Drive Encryption 設定：
 - 啟動受 TPM 保護的密碼
 - 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 ProtectTools Security Manager 使用者主控台來存取 Drive Encryption。


1. 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示。
- 或 -
從「**控制台**」選取「**系統及安全性**」，然後選取「**HP ProtectTools Security Manager**」。
2. 在 HP ProtectTools Security Manager 使用者主控台的左側面板中，選取「**管理**」，然後選取「**管理主控台**」。
3. 在 HP ProtectTools 管理主控台的左側面板中，選取「**Drive Encryption**」。

一般工作

啟動標準硬碟的 Drive Encryption

標準硬碟是使用軟體加密來加密的。請依照下列步驟啟動 Drive Encryption：

1. 啟用「**HP ProtectTools 管理主控台**」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，按一下「**設定精靈**」。
3. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。
4. 若要備份加密金鑰，請連接外接式裝置來記錄這個金鑰。如果其他方法失敗，必須使用這個金鑰來存取資料。
5. 在「**備份 Drive Encryption 金鑰**」下方，選取即將儲存加密金鑰的儲存裝置核取方塊。
6. 按「**下一步**」。


 **附註：** 系統會提示您重新啟動電腦。重新啟動之後，Drive Encryption 預先開機畫面隨即顯示並要求驗證，然後 Windows 才會啟動。

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 ProtectTools Security Manager 軟體「說明」。

啟動自我加密磁碟機的 Drive Encryption

如果自我加密磁碟機符合「信賴運算群組」針對自我加密磁碟機管理的 OPAL 規格，則可以使用軟體加密或硬體加密來加密。請依照下列步驟啟動自我加密磁碟機的 Drive Encryption：

 **附註：** 您電腦中的「所有」磁碟機必須都是符合「信賴運算群組」之自我加密磁碟機管理 OPAL 規格的自我加密磁碟機，才可以使用硬體加密。在這種情況下，將會有「**使用硬體磁碟機加密**」選項，因此硬體或軟體加密都可供使用。

如果是同時有自我加密磁碟機和標準硬碟的情況，則不會有「**使用硬體磁碟機加密**」選項，因此只有軟體加密可供使用。如需詳細資訊，請參閱[位於第 36 頁的啟動標準硬碟的 Drive Encryption](#)。

▲ 使用 HP ProtectTools Security Manager 設定精靈停用 Drive Encryption。

- 或 -


軟體加密

1. 啟用「**HP ProtectTools 管理主控台**」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，按一下「**設定精靈**」。
3. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。

 **附註：** 如果畫面底部有「**使用硬體磁碟機加密**」選項，請清除該核取方塊。

4. 在「**要加密的磁碟機**」下方，選取您要加密之硬碟的核取方塊，然後按一下「**下一步**」。
5. 若要備份加密金鑰，請將儲存裝置插入適當的插槽。


6. 在「**備份 Drive Encryption 金鑰**」下方，選取即將儲存加密金鑰的儲存裝置核取方塊。
7. 按一下「**套用**」。

 **附註：** 電腦將會重新啟動。

Drive Encryption 已經啟動。磁碟機的加密可能會花上數個小時，視磁碟機大小而定。

硬體加密


1. 啟用「**HP ProtectTools 管理主控台**」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，按一下「**設定精靈**」。
3. 選取「**Drive Encryption**」核取方塊，然後按「**下一步**」。
4. 如果畫面底部有「**使用硬體磁碟機加密**」核取方塊，請確認已加以選取。
如果此核取方塊已清除或是無法使用，代表已套用軟體加密。如需詳細資訊，請參閱[位於第 36 頁的啟動標準硬碟的 Drive Encryption](#)。
5. 在「**要加密的磁碟機**」下方，選取您要加密之硬碟的核取方塊，然後按一下「**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，磁碟 0 將會自動選取並且呈現灰色，另外還會提供可選取其他磁碟機進行硬體加密的選項。

除非至少選取了一部磁碟機，否則「**下一步**」按鈕就無法使用。

6. 若要備份加密金鑰，請將儲存裝置插入適當的插槽。
7. 在「**備份 Drive Encryption 金鑰**」下方，選取即將儲存加密金鑰的儲存裝置核取方塊。
8. 按一下「**套用**」。

 **附註：** 系統會提示您重新啟動電腦。Drive Encryption 預先開機畫面將會顯示並要求驗證，然後 Windows 才會啟動。

Drive Encryption 已經啟動。磁碟機的加密可能要花上幾分鐘的時間。


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**」。

1. 啟用「**HP ProtectTools 管理主控台**」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，按一下「**設定精靈**」。
3. 清除「**Drive Encryption**」核取方塊，然後按「**下一步**」。

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 並註冊您的使用者帳戶之後開啟電腦時，必須在 Drive Encryption 登入畫面中登入：

 **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 ProtectTools Security Manager 中啟用「BIOS 預先開機安全性」，而且 One-Step Logon 已啟用（預設值），那麼您就可以在 BIOS 預先開機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、臉孔，或是用已註冊的手指掃過。


多使用者登入：

1. 在「Select user to log on」（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「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


- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (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。

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。啟用此功能之後，任何新增的硬碟或建立的分割區都可以透過下列步驟完成加密：

1. 在左側面板中，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. 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）

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

 **附註：** 在 Drive Encryption「設定」頁面上，只能選取或取消選取其他硬碟進行硬體加密。

- 如果狀態為「已停用」，表示 Drive Encryption 尚未由 Windows 管理員啟用，無法保護硬碟。使用 HP ProtectTools Security Manager 設定精靈停用 Drive Encryption。
- 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）

使用「使用 TPM 提升安全性」（僅限特定機型）

在啟用信任平台模組 (TPM) 並選取 Drive Encryption 的「使用 TPM 提升安全性」功能之後，Drive Encryption 密碼將會受到 TPM 安全晶片的保護。如果硬碟被取下並安裝在另一部電腦上，對這部硬碟的存取都會遭到拒絕。

 **注意：** TPM 所有權不得與 Windows TPM.msc 共用。

 **附註：** 由於密碼受 TPM 安全晶片保護，因此，如果硬碟移到另一部電腦上，除非已將 TPM 設定轉移到該電腦，否則將無法存取硬碟上的資料。


 **附註：** TPM 選項必須在 BIOS 設定中啟用。


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「設定」頁面加密電腦上的一個或多個硬碟分割，或是將已經加密的磁碟機分割區解密。

1. 啟用「**HP ProtectTools 管理主控台**」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，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，選取或清除您要加密或解密之各硬碟旁邊的核取方塊，然後按一下「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，以及完成程序的剩餘時間。

 **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。


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。

 **附註：** 若要儲存加密金鑰，您必須使用具有 FAT32 或 FAT16 格式的 USB 儲存裝置。USB 隨身碟、Secure Digital (SD) 記憶卡或 MultiMedia Card (MMC) 記憶卡都可以用來進行備份。

1. 啟用「HP ProtectTools 管理主控台」。如需詳細資訊，請參閱[位於第 15 頁的開啟 HP ProtectTools 管理主控台](#)。
2. 在左側面板中，按一下「Drive Encryption」左邊的「+」圖示以顯示可用的選項。
3. 按一下「備份加密金鑰」。
4. 插入用於備份加密金鑰的儲存裝置。

 **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。USB 隨身碟、Secure Digital (SD) 記憶卡或 MultiMedia Card (MMC) 記憶卡都可以用來進行備份。在某些情況下，可能會使用 SkyDrive。


5. 在「磁碟機」下方，選取您要備份加密金鑰的裝置核取方塊。
6. 按一下「備份金鑰」。
7. 閱讀所顯示頁面上的資訊，然後按一下「確定」。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，或是在 Security Manager 中選取「備份 Drive Encryption 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「Drive Encryption for HP ProtectTools 登入」對話方塊開啟時，按一下「選項」。
4. 按一下「復原」。

5. 輸入含有您備份金鑰的檔案路徑或名稱，然後按一下「**復原**」。
- 或 -
按一下「**瀏覽**」搜尋所需的備份檔案，按一下「**確定**」，然後按一下「**復原**」。
6. 當出現確認對話方塊時，按一下「**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 Security Manager 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「Drive Encryption for HP ProtectTools」頁面顯示時，請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 Security Manager 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。

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. 啟用「**HP ProtectTools 使用者主控台**」。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
2. 在「**我的資料**」底下，按一下「**Drive Encryption**」。

在軟體或硬體加密案例中，磁碟機加密狀態會顯示下列其中一項：

- 已啟用
- 已停用

在軟體加密案例中，每一個硬碟機或硬碟分割區的磁碟機加密狀態會顯示下列其中一項：

- 未加密
- 已加密
- 正在加密
- 正在解密


在硬體加密案例中，磁碟機加密狀態會顯示下列其中一項

- 未加密
- 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。

7 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 50 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。

開啟 Device Access Manager

1. 以管理員身分登入。
2. 從「**HP Client Security 儀表板**」啟動 **HP ProtectTools Security Manager**。
 - 或 -
 - 從 Windows 桌面的工作列最右端的通知區域中，連接兩下 **HP ProtectTools** 圖示。
 - 或 -
 - 從「**控制台**」選取「**系統及安全性**」，然後選取「**HP ProtectTools Security Manager**」。
3. 在 HP ProtectTools Security Manager 使用者主控台的左側面板中，按一下「**管理**」，然後選取「**管理主控台**」。
4. 在管理主控台的左側面板中，按一下「**Device Access Manager**」。

標準使用者可以使用 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

管理員可以使用「**簡易組態**」檢視來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

 **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。


- 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的裝置類別存取權，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。若要重設為原廠設定，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，則會開啟對話方塊詢問您是否要啟動該服務。按一下「**是**」。

4. 按一下「**確定**」。

啟動背景服務

第一次定義及套用新原則時，「**HP ProtectTools 裝置鎖定/稽核**」背景服務會自動啟動，而且該服務設定為在系統啟動時自動啟動。

 **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。

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

啟動服務會啟動裝置驅動程式，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，請開啟命令提示字元視窗，然後輸入 `sc query flcdlock`。

若要判斷裝置驅動程式是否正在執行，請開啟命令提示字元視窗，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為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**」對話方塊隨即開啟。
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**」對話方塊隨即開啟。
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為原廠設定值。

 **附註：** 「進階設定」頁面不會重設。

若要將組態設定重設為原廠設定：

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。

啟用 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**—設定為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，啟用 JITA 的使用者和未啟用 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。若點選氣球，就會顯示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 期間可授權為數分鐘或 0 分鐘的時間。0 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為止的期間存取裝置。

若設定為如此，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
- 抽取式媒體

為使用者或群組建立 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「**已啟用**」核取方塊。
5. 將 JITA 期間設定為所需的時間。
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。

為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「**已啟用**」核取方塊。

5. 將 JITA 期間設定為所需的時間。
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「**已啟用**」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含系統管理員。如需詳細資訊，請參閱[位於第 50 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含系統管理員。

 **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」。

eSATA 裝置支援

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

1. 系統啟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

8 竊盜復原（僅限特定機型）

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

一旦啟用 **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。

若要啟用 **Computrace for HP ProtectTools**：

1. 連線到網際網路。
2. 開啟 **Security Manager** 使用者主控台。如需詳細資訊，請參閱[位於第 22 頁的開啟 Security Manager](#)。
3. 在 **Security Manager** 的左側窗格中，按一下「竊盜復原」。
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 **Computrace for HP ProtectTools** 的詳細資訊，請按一下「**瞭解更多資訊**」。

9 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。

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. 重新啟動 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。如需不支援的字元的詳細資訊，請參閱 HP ProtectTools 管理主控台軟體說明。
 2. 重新執行 HP ProtectTools Security Manager 設定精靈，然後輸入新的 Windows 密碼。

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。

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	ʔ、ʕ 和 ʔ 鍵會產生兩個字元。	ʔ、ʕ 和 ʔ 鍵會產生一個字元。	ʔ、ʕ 和 ʔ 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，因為軟體會將它轉換為 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 鍵盤配置變更為 1040a（西班牙文分支）或 080a（拉丁美洲）。	N/A	N/A
美式國際	<ul style="list-style-type: none"> ◦ 拒絕最上列的 j、ı、‘、’、¥ 和 × 鍵。 ◦ 拒絕第二列的 å、® 和 Þ 鍵。 ◦ 拒絕第三列的 á、ó 和 ø 鍵。 ◦ 拒絕最下列的 æ 鍵。 	N/A	N/A
捷克文	<ul style="list-style-type: none"> ◦ 拒絕 ě 鍵。 ◦ 拒絕 ě 鍵。 ◦ 拒絕 ů 鍵。 ◦ 拒絕 é、ı 和 z 鍵。 ◦ 拒絕 ě、k、l、n 和 r 鍵。 	N/A	N/A

語言	Windows	BIOS	Drive Encryption
斯洛伐克文	拒絕 z 鍵。	<ul style="list-style-type: none"> š、ś 和 ŝ 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。 ť 廢鍵會產生兩個字元。 	N/A
匈牙利文	拒絕 z 鍵。	ť 鍵會產生兩個字元。	N/A
斯洛維尼亞文	zŽ 鍵會在 Windows 中遭到拒絕，而 alt 鍵會在 BIOS 中產生廢鍵。	ú ·Ú ·ù ·Û ·ş ·Ş ·š ·Š 和 Š 鍵會在 BIOS 中遭到拒絕。	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

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 復原

藉由正確回答安全性問題即可存取電腦的能力。

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。

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。

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。

加密

將演算法之類的程序用於密碼使用中，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。

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。

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。

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。

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。

背景服務

「HP ProtectTools 裝置鎖定/稽核」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。如果未執行，HP ProtectTools Security Manager 會嘗試將它啟動，才會套用裝置存取控制原則。

重新開機

重新啟動電腦的程序。

密碼編譯

為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。

啟用

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 設定精靈啟用 Drive Encryption。只有管理員可以啟用 Drive Encryption。啟用程序包含啟用軟體、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。

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。

場景

可用於驗證的已註冊使用者影像。

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

包含使用者名稱和密碼（可能另有其他選定資訊）的 Security Manager 物件，可用於登入網站或其他程式。

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。

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。

管理主控台

供管理員存取及管理 HP ProtectTools 功能和設定的集中位置。

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

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。

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。

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

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

B

Bluetooth 20, 32

C

Computrace 52
Credential Manager 28

D

Device Access Manager for
HP ProtectTools
easy setup 11
開啟 43
Drive Encryption for
HP ProtectTools 35
easy setup 11

E

eSATA 50

H

HP Client Security 儀表板 8, 14
HP ProtectTools Device Access
Manager 43
HP ProtectTools Drive
Encryption 39
加密個別磁碟機 39
在啟用 Drive Encryption 之後登
入 36
停用 36
啟用 36
備份與復原 40
解密個別磁碟機 39
管理 Drive Encryption 39
HP ProtectTools Security
Manager 22
Backup and Recovery 密碼 5
HP ProtectTools Security Manager
設定精靈 8, 14
HP ProtectTools 功能 1
HP ProtectTools 管理主控台 8,
13, 14
開啟 15
HP SpareKey 復原 41

J

JITA
為使用者或群組建立 48
為使用者或群組建立可延伸的
48
針對使用者或群組停用 49
組態 48

P

Password Manager 21, 23, 24
檢視與管理已儲存的驗證 10
簡易設定 9
PIN 33

S

Security Manager, 開啟 22
SpareKey
設定 17, 28

T

TPM 39

W

Windows 登入密碼 5

一畫

一般標籤, 設定 21

三畫

小型企業適用的簡易設定指南 9

四畫

允許存取 46
及時驗證組態 48

五畫

加密
軟體 36, 37, 39, 41
硬碟 38
硬碟分割區 39
硬體 36, 37, 41
磁碟機 35
加密狀態, 顯示 41
加密金鑰
備份 40

功能, HP ProtectTools 1
未受管理的裝置類別 50
未經授權的存取, 防範 4
正在設定
管理主控台 15
目標, 安全性 4

六畫

存取
防範未經授權的 4
控制 43
安全性 5
角色 5
關鍵目標 4

七畫

快速入門 9, 44
快速連結
功能表 26

八畫

使用者
允許存取 46
拒絕存取 46
移除 47
使用者主控台設定 22
拒絕 46
昏暗模式 30
非接觸式卡片 20, 32

九畫

指定安全設定值 17
指紋
設定 18
註冊 29
背景服務 44
重設 47
限制
存取敏感資料 4
裝置存取 43

十畫

特殊鍵處理 54

十一畫

- 停用 Drive Encryption 37
- 偏好設定, 設定 33
- 密碼
 - HP ProtectTools 5
 - 安全 6
 - 使用不同鍵盤配置的變更 53
 - 例外狀況 53
 - 原則 5
 - 強度 27
 - 準則 6
 - 管理 5
 - 遭到拒絕 53
 - 變更 28
- 控制裝置存取 43
- 啟動
 - 自我加密磁碟機的 Drive Encryption 36
 - 標準硬碟的 Drive Encryption 36
- 移除
 - 存取 47
- 組態
 - 重設 47
 - 裝置類別 45
 - 簡易 44
- 設定 17, 33
 - 一般標籤 21
 - 進階使用者 31
 - 新增 21, 22
 - 裝置存取 43
 - 圖示 27
 - 應用程式 21, 22
- 設定精靈 8, 14
- 軟體加密 36, 37, 39, 41

十二畫

- 備份
 - HP ProtectTools 認證 6
 - 加密金鑰 40
 - 資料 33
- 復原
 - 使用備份金鑰存取 40
- 景像
 - 刪除 31
 - 註冊 29
- 智慧卡 31
 - PIN 5
 - 初始化 18, 31
 - 設定 19

- 註冊 19, 32
- 變更 PIN 碼 32
- 登入
 - 分類 26
 - 新增 24
 - 管理 26
 - 編輯 25
- 登入電腦 38
- 硬體加密 36, 37, 41
- 註冊
 - 指紋 29
 - 景像 29
- 進階設定 49
- 開啟
 - Device Access Manager for HP ProtectTools 43
 - HP ProtectTools 管理主控台 15
 - Security Manager 22
 - 開啟 Drive Encryption 35

十三畫

- 群組
 - 允許存取 46
 - 拒絕存取 46
 - 移除 47
- 裝置, 允許使用者的存取 47
- 裝置設定值
 - SpareKey 17
 - 指紋 18
 - 智慧卡 19
 - 臉孔 18
- 裝置類別
 - 允許使用者的存取 46
 - 未受管理 50
- 裝置類別組態
 - 組態 45
- 解密
 - 硬碟分割區 39
 - 磁碟機 35
- 資料
 - 限制存取 4
 - 備份 33
 - 還原 33
- 電燈泡圖示 30

十四畫

- 管理
 - 加密或解密磁碟機分割區 39
 - 使用者 17

- 密碼 21, 23, 24
- 認證 28
- 管理主控台
 - 正在設定 15
 - 使用 15
- 精靈
 - HP ProtectTools Client Security 設定 7
 - HP ProtectTools Security Manager 設定 7
 - 精靈, HP ProtectTools Security Manager 設定 8, 14
 - 認證 23
 - 指定 17

十五畫

- 鄰近感應式卡片 20, 32

十六畫

- 學習 31
- 螢幕顏色 30

十七畫

- 應用程式 20
- 應用程式標籤, 設定 21
- 臉孔, 設定 18
- 還原
 - HP ProtectTools 認證 6
 - 資料 33

十八畫

- 簡易組態 44

十九畫

- 識別卡 23
- 關鍵安全性目標 4

二十三畫

- 竊盜, 防範 4
- 竊盜復原 52
- 驗證 16, 30

