HP ProtectTools
使用指南

HP ProtectTools 使用指南

HP Compaq 商用個人電腦

第 1 版：2008 年 7 月

文件編號：491163-AB1

有關本書

本指南提供升級此電腦機型的基本資訊。

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

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

附註： 以此方式強調之文字提供重要的補充資訊。

目錄

1 安全性簡介

HP ProtectTools Security Manager for Administrators 軟體提供安全性功能，以協助防止未經授權存取至電腦、網路和重要資料。增強的安全性功能是由下列軟體模組提供：

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools

附註： Credential Manager、Java Card Security 及 Drive Encryption 皆使用 Security Manager 安裝精靈進行設定。

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

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

HP ProtectTools 功能

下表將詳細說明 HP ProtectTools 模組的重要功能：

模組	重要功能
HP ProtectTools Security Manager for Administrators	• 管理員使用 Security Manager 安裝精靈安裝及設定安全性及安全登入法的層級。 • 使用者也可以使用安裝精靈設定登入法。 • 管理員工具是用於新增及移除 ProtectTools 使用者及檢視使用者狀態。 • 從已安裝 HP ProtectTools 模組備份與復原安全性模組。
Credential Manager for HP ProtectTools	• Credential Manager 是個人密碼的儲藏箱，以「單一登入 (Single Sign On)」功能簡化登入程序，會自動記憶和套用使用者的認證。 • 「單一登入 (Single Sign On)」同時還藉由要求不同安全性技術的組合（例如 Java™ 卡和生物測定），爲使用者驗證提供額外的保護。 • 密碼儲存是透過軟體加密的方式保護，同時可以透過使用 TPM 嵌入式安全晶片及/或安全性裝置驗證（例如 Java 卡和生物測定）來強化功能。
Drive Encryption for HP ProtectTools	• Drive Encryption 提供完整、全磁碟區的硬碟加密。 • Drive Encryption 會強制預先開機驗證，以進行解密並存取硬碟上的資料。
Privacy Manager for HP ProtectTools	• Privacy Manager 是用於獲得授權憑證的工具，此憑證可在使用 Microsoft Mail、Microsoft Office 文件及 Live Messenger 時驗證來源、完整性及通訊的安全性。
File Sanitizer for HP ProtectTools	• File Sanitizer 可讓您安全銷毀電腦上的數位資源（即安全刪除敏感的資訊，包括應用程式檔案、歷史或網路相關的內容或其他機密資料），並定期整理硬碟（覆寫先前已刪除但目前仍存在硬碟中的資料，使資料更不易復原）。
Java Card Security for HP ProtectTools	• Java Card Security 是 Java Card 的管理軟體介面。Java Card 是保護驗證資料的個人安全性裝置，需要同時具有介面卡及 PIN 碼才能獲准存取。Java Card 可以用於存取 Credential Manager、Drive Encryption、HP BIOS 或任何數量的協力廠商存取點。 • Java Card Security 在硬碟開機前爲使用者驗證設定 HP ProtectTools Java Card。Java Card Security 能夠以 Embedded Security、Java Card 及密碼存取。 • Java Card Security 爲管理員及使用者設定不同的 Java Card。
BIOS Configuration for HP ProtectTools	• BIOS Configuration 提供開機使用者及管理員密碼管理的存取。 • BIOS Configuration 提供另一個開機前 BIOS 組態 (BIOS CONFIGURATION) 公用程式，稱爲「電腦設定 (Computer Setup)」。 • BIOS Configuration 啓用自動磁碟機鎖支援，它以嵌入式安全晶片來強化功能，幫助保護硬碟，即使硬碟從系統中移除，仍可以避免未經授權的存取，使用者除了嵌入式安全晶片的使用者密碼外，無需記住任何其他密碼。

模組	重要功能
Embedded Security for HP ProtectTools	• 嵌入式安全性 (Embedded Security) 是透過信任平台模組 (TPM) 的嵌入式安全晶片來保護儲存在本機電腦的敏感性使用者資料或機密，使其不受到未獲授權的使用者存取。 • Embedded Security 允許您建立個人安全磁碟機 (PSD)，在保護使用者檔案及資料夾資訊時很有用。 • 嵌入式安全性支援協力廠商應用程式（例如 Microsoft Outlook 與 Internet Explorer），進行受保護的數位憑證。
Device Access Manager for HP ProtectTools	• Device Access Manager 讓 IT 管理員可以依照使用者的設定檔控制裝置的存取（例如 USB 連接埠、選購裝置等）。 • 裝置存取管理員 (Device Access Manager) 能夠預防未獲授權的使用者，經由外部儲存媒體來移除資料或將病毒帶入系統中。 • 管理員可以爲特定的個人或使用者群組，停用可寫入裝置的存取權限。

存取 HP ProtectTools 安全性

若要從 Windows® 控制台存取 HP ProtectTools Security Manager for Administrators：

▲ 在 Windows Vista® 中，請按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。

－或－

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

附註： 如果您不是 HP ProtectTools 的管理員，您可以在非管理員模式下執行 HP ProtectTools 以檢視資訊，但您不能進行變更。

附註： 完成 Credential Manager 模組設定之後，便可同時從 Windows 登入畫面直接登入 Credential Manager 開啓 HP ProtectTools。如需詳細資訊，請參閱「23 頁的使用認證管理員 (Credential Manager) 登入 Windows」。

達成重要的安全性目標

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

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

防止發生針對性偷竊事件

這類意外的其中一例即是鎖定電腦或其機密資料及客戶資訊的竊盜行爲。這在開放辦公室的環境或不安全的區域內很容易發生。下列功能在電腦不幸被偷時可以協助保護資料：

- 預先開機驗證功能一旦啓用，就可以協助預防存取作業系統。請參閱下列程序：
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- 磁碟機鎖可以幫助確保即使硬碟被移除並安裝到不安全的系統中，資料也不會被存取。
- 由 Embedded Security for HP ProtectTools 模組所提供的 Personal Secure Drive 功能，可將敏感性資料先行加密，以協助確保資料必須通過驗證才能存取。請參閱下列程序：
  - 嵌入式安全性 (Embedded Security)「72 頁的設定程序」
  - 「74 頁的使用 Personal Secure Drive」

限制存取敏感性資料

假定有一位合約制的稽核人員被派到客戶的公司上班，並獲得審視電腦中敏感性財務資料的權限，但是您不想讓這位稽核人員將檔案列印出來，或是儲存到可寫入裝置 (例如 CD 上)。下列功能可協助您限制資料的存取：

- Device Access Manager for HP ProtectTools 讓 IT 管理員能限制可寫入裝置的存取，使敏感的資訊無法列印或從硬碟複製到卸除式的媒體上。請參閱「80 頁的裝置類別組態（進階）」。
- 磁碟機鎖可以幫助確保即使硬碟被移除並安裝到不安全的系統中，資料也不會被存取。

防止未獲授權的使用者從內部或外部位置進行存取

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

- 預先開機驗證功能一旦啓用，就可以協助預防存取作業系統。請參閱下列程序：
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- Embedded Security for HP ProtectTools 可經由下列程序，協助保護儲存在本機電腦上的敏感性使用者資料或認證：
  - 嵌入式安全性 (Embedded Security)「72 頁的設定程序」
  - 「74 頁的使用 Personal Secure Drive」
- Credential Manager for HP ProtectTools 是依據下列程序來確保未獲授權的使用者無法獲取密碼，或是存取受密碼保護的應用程式：
  - 認證管理員 (Credential Manager)「19 頁的設定程序」
  - 「24 頁的使用單一登入 (Single Sign On)」
- Device Access Manager for HP ProtectTools 讓 IT 管理員能限制可寫入裝置的存取，使敏感的資訊無法從硬碟上被複製。請參閱「79 頁的簡易組態」。
- Personal Secure Drive 功能，可將敏感性資料先行加密，以協助確保資料必須透過下列程序並通過驗證才能存取：
  - 嵌入式安全性 (Embedded Security)「72 頁的設定程序」
  - 「74 頁的使用 Personal Secure Drive」
- File Sanitizer 可讓您透過銷毀資源安全刪除資料，或整理硬碟（覆寫先前已刪除但目前仍存在硬碟中的資料，使資料更不易復原）。
- Privacy Manager 可讓您在使用 Microsoft Mail，Office 文件及 Live Messenger 時獲得授權憑證，讓傳送及接收重要資訊的過程更安全。

建立不易破解的密碼政策

如果公司要求針對數十種的網頁應用程式與資料庫採行不易破解的密碼政策時，Credential Manager for HP ProtectTools 將能透過下列程序爲密碼提供一個防護資料庫並提供單一登入 (Single Sign On) 的便利機制：

- 認證管理員 (Credential Manager)「19 頁的設定程序」
- 「24 頁的使用單一登入 (Single Sign On)」

如需更強的安全性，Embedded Security for HP ProtectTools 即可保護使用者名稱及密碼的儲存區。這讓使用者可以維持多個強式密碼，而無需另外寫下或嘗試以記憶的方式記下。請參閱「嵌入式安全72 頁的設定程序」。

其他的安全性要素

指派安全性角色

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

附註： 在小型的組織或個人用戶中，同一個人可能會兼具不同角色。

對於 HP ProtectTools，可將安全性責任和權限分割成下列角色：

- 安全性主管 — 定義公司或網路的安全性等級，並決定要部署的安全性功能，例如 Java™ 卡、生物測定讀取器或 USB Token 等裝置。
- IT 管理員 — 套用和管理安全性主管所定義的安全性功能。也能啓用和停用部份功能。例如，若安全主管已決定部署 Java 卡，IT 管理員就能啓用 Java 卡 BIOS 安全性模式。
- 使用者 — 使用安全性功能。例如，若安全性主管和 IT 管理員已啓用系統的 Java 卡，則使用者可設定 Java 卡 PIN 碼並使用該卡進行驗證。

管理 HP ProtectTools 密碼

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

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

HP ProtectTools 密碼	在此 HP ProtectTools 模組中設定	功能
認證管理員 (Credential Manager) 登入密碼	認證管理員 (Credential Manager)	這個密碼可提供 2 個選項： • 登入 Windows 後，您可以在不同的登入程序使用該選項來存取認證管理員 (Credential Manager)。 • 您可以使用它來取代 Windows 登入程序，以便同時存取 Windows 和認證管理員 (Credential Manager)。
認證管理員 (Credential Manager) 復原檔密碼	認證管理員 (Credential Manager)，由 IT 管理員設定	保護認證管理員 (Credential Manager) 復原檔的存取。
基本使用者金鑰密碼 **附註：** 也稱爲：嵌入式安全性 (Embedded Security) 密碼	嵌入式安全性 (Embedded Security)	用來存取嵌入式安全性 (Embedded Security) 功能，例如安全的電子郵件檔案，以及資料夾加密。在用於開機驗證時，當電腦啓動、重新啓動或從休眠狀態還原時，也可以保護對電腦內容的存取。
緊急復原記號 (Token) 密碼 **附註：** 也稱爲：緊急復原記號 (Token) 密碼	嵌入式安全性 (Embedded Security)，由 IT 管理員設定	保護緊急復原記號 (Token) — 嵌入式安全晶片的備份檔案之存取。
擁有者密碼	嵌入式安全性 (Embedded Security)，由 IT 管理員設定	保護系統和 TPM 晶片，防止他人在未獲授權的情況下，存取嵌入式安全性 (Embedded Security) 的全部擁有者功能。
Java™ 卡 PIN 碼	Java 卡安全性 (Java Card Security)	保護對 Java 卡內容的存取，並驗證 Java 卡使用者。當用於開機驗證時，Java 卡 PIN 碼

HP ProtectTools 密碼	在此 HP ProtectTools 模組中設定	功能
		也可以保護對電腦設定 (Computer Setup) 公用程式和電腦內容的存取。 如果選擇使用 Java 卡 Token 的話，就會驗證 Drive Encryption 機制的使用者。
電腦設定 (Computer Setup) 密碼 **附註：** 也稱爲 BIOS 管理員 (administrator)、F10 設定 (Setup) 或安全性設定 (Security Setup) 密碼	BIOS 組態 (BIOS Configuration)，由 IT 管理員設定	保護對電腦設定 (Computer Setup) 公用程式的存取。
開機密碼 (Power-On Password)	BIOS 組態 (BIOS Configuration)	當電腦啓動、重新啓動或從休眠狀態回復時，可保護對電腦內容的存取。
Windows 登入密碼	Windows 控制台	可使用於手動登入或儲存在 Java 卡上。

建立安全密碼

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

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

備份和還原 HP ProtectTools 認證

若要備份和還原所有支援的 HP ProtectTools 模組的認證，請參考以下資訊：

備份認證與設定

您可以利用下列任何一種方式來備份認證：

- 使用 Drive Encryption for HP ProtectTools 選取和備份 HP ProtectTools 認證。

  您也可以註冊「線上 Drive Encryption 金鑰復原服務」，以儲存加密金鑰的備份副本，以便您在忘記密碼且無法存取本機備份時仍然可以存取電腦。

  附註： 您必須與網際網路連線，並提供有效的電子郵件地址，才能註冊並透過此服務來復原您的密碼。

- 使用 Embedded Security for HP ProtectTools 備份 HP ProtectTools 認證。
- 使用 HP ProtectTools Security Manager for Administrators 中的 Backup and Recovery 工具作爲中央位置，可讓您從已安裝的 HP ProtectTools 模組備份與復原安全性認證。

2 HP ProtectTools Security Manager for Administrators

關於 HP ProtectTools Security Manager for Administrators

HP ProtectTools Security Manager for Administrators 提供安全性功能，以協助防止未經授權存取至電腦、網路和關鍵資料。Security Manager 具有可延伸性，所以可以擴大處理日新月異的威脅並在新支術上市時適時提供。

在初始安全性安裝時使用 HP ProtectTools Security Manager for Administrators 模組。Security Manager 集中式使用者介面有下列功能：

- **快速入門** - 安裝精靈會指引 Windows 作業系統管理員逐步完成安全性等級，及用於預先開機環境、Credential Manager 及 Drive Encryption 之安全登入法的設定。使用者也可以使用安裝精靈設定其安全登入法。請參閱「11 頁的快速入門 - 設定 HP ProtectTools Security Manager for Administrators」及「12 頁的快速入門 - 設定使用者安全登入法」，以取得詳細資訊。
- **管理員工具** - 讓 Windows 管理員可以新增及移除 ProtectTools 使用者及檢視使用者狀態。請參閱「14 頁的管理員工具 - 管理使用者（管理員工作）」，以取得詳細資訊。
- **Backup and Recovery** - 從已安裝 HP ProtectTools 模組備份與復原安全性認證。請參閱「15 頁的備份與復原」，以取得詳細資訊。
- **設定** - 可讓您自訂多個項目的行爲。請參閱「18 頁的設定」，以取得詳細資訊。

Security Manager 集中式使用者介面也包括一份專爲維護電腦最高安全性而設計的外加軟體模組清單。您可以選擇並設定任何數量的可用模組。

快速入門 - 設定 HP ProtectTools Security Manager for Administrators

「快速入門」安裝精靈可讓 Windows 管理員建立和/或更新安全性及安全登入法的層級。

使用者也可以使用設定精靈設定其安全登入法。

附註： Windows 管理員隨時想要變更安全性及安全登入法的層級時，都可以執行安裝精靈。

安裝精靈會逐步指引 Windows 管理員完成 Security Manager 設定：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**快速入門**」，然後按一下「**Security Manager 安裝**」按鈕。說明 Security Manager 功能的演示即會開始。
2. 如果您想在下次執行安裝精靈時略過 Security Manager 功能的演示，請在「歡迎 (Welcome)」畫面（如果有）中，取消「**精靈開始時自動播放視訊**」核取方塊。
3. 請詳讀本頁，然後按「**下一步**」。
4. 在「設定安全性等級」頁面上選擇安全性的層級。您可以選擇一個或多個下列層級：
   - HP Credential Manager – 保護您的 Windows 帳戶。
   - 預先開機安全性（某些機型）- 在 Windows 啓動前保護您的電腦。
   - HP Drive Encryption – 藉由硬碟加密保護您的電腦資料。選取這個選項會要求您將唯一的加密金鑰備份到卸除式的儲存裝置上。

   附註： 「安全性」參數會隨著您的選擇而變更。選擇愈多層級，電腦就愈安全。

   選擇安全性等級之後，請按「**下一步**」。
5. 依據您在步驟 4 所選的安全性等級，即會顯示以下頁面的其中一頁或多頁。
   - 保護您的 Windows 帳戶 – 將需要 Windows 密碼，因爲 Security Manager 必須同步化每個安全性等級的密碼。

     輸入並確認 Windows 密碼，或輸入您建立的密碼，然後按「**下一步**」。
   - 在 Windows 啓動之前保護您的系統（選擇性） – 如果您或使用者知道 BIOS 管理員密碼，也可輸該密碼。如果輸入 BIOS 管理員密碼，則 Windows 管理員或使用者即爲 BIOS 管理員。

     附註： 如果 BIOS 管理員密碼不存在，則您必須在繼續之前建立一組密碼。如果輸入 BIOS 管理員密碼，則您即爲 BIOS 管理員。

     輸入並確認 BIOS 管理員密碼，或輸入已建立的密碼。然後按「**下一步**」。
   - 藉由硬碟加密保護您的資料 – 您必須使用 USB 儲存裝置以儲存加密金鑰。選擇要加密的磁碟機（至少必須選擇一部），將儲存裝置插入適當的插槽，選擇要儲存加密金鑰的儲存裝置，然後按「**下一步**」。

6. 在「設定安全登入法」頁面上選擇一個或多個安全登入法。

   a. 在步驟 1 中，選擇一個或多個安全登入法。

   附註： 選擇的項目會套用於管理員及使用者。

   b. 在步驟 2 中，如果您想要提高安全性，請選擇核取方塊，讓登入電腦時需要您在步驟 1 中選取的**所有**安全登入法。

   如果您要**任何一個**選取的安全登入法在登入電腦時都有權限，請勿選擇此核取方塊。

   △ 注意： 如果您選擇此核取方塊且使用者尚未設定其登入法（Windows 密碼、指紋驗證和/或 HP ProtectTools Java™ Card），則使用者將無法登入電腦。建議所有使用者在選擇此選項前先設定登入法。

   c. 按「**下一步**」。摘要頁面會開啓，可讓您檢視您的選擇。

7. 按一下「檢視及啓用安全性設定」頁面上的「**啓用**」。

   當您按一下「**啓用**」，電腦即會設定您的安全性選擇。在安全性設定完成之前，您無法返回任何先前的精靈頁面。在您完成精靈之後，您仍可再次執行精靈以變更您的設定。

8. 依據您在步驟 6 所選的安全登入法，即會顯示以下頁面的其中一頁或多頁。依照螢幕上的指示繼續操作，然後按「**下一步**」。

   - 「註冊您的指紋」- 以手指在螢幕上按一下，此手指的指紋必須與您想要註冊的相同（您必須至少註冊兩枚指紋），在指紋感應器上緩慢掃過您選定的手指，然後繼續在指紋感應器上掃過相同的手指，直到完成所需的掃描次數爲止。重複此程序以註冊第二根手指，然後按一下「**完成**」。
   - 「註冊 HP ProtectTools Java Card」- 插入 HP ProtectTools Java Card，輸入 Java Card PIN，然後按一下「**完成**」。

9. 在「恭喜」頁面上，檢視您的選擇，然後按一下「**完成**」。

快速入門 - 設定使用者安全登入法

Windows 管理員完成安全性等級及安全登入法的設定之後，使用者執行安裝精靈以在電腦上新增爲 HP ProtectTools 使用者：

附註： 執行安裝精靈的使用者將會看到最多的精靈頁面。然而，「設定安全性等級」及「設定安全登入法」頁面無法提供設定，因爲這些是管理員專屬的工作。

1. 登入電腦。
2. 在 Security Manager 中，按一下「**快速入門**」，然後按一下「**Security Manager 安裝**」按鈕。
3. 如果您想在下次執行安裝精靈時略過 Security Manager 功能的演示，請在「歡迎 (Welcome)」畫面中，取消「**精靈開始時自動播放視訊**」核取方塊。
4. 請詳讀本頁，然後按「**下一步**」。
5. 在「設定安全性等級」頁面上，按「**下一步**」。

6. 依據管理員所設定的安全性等級，即會顯示以下兩頁的其中一頁或兩頁。

   - 保護您的 Windows 帳戶 – 需要 Windows 密碼，因爲 Security Manager 必須同步化每個安全性等級的密碼。

     附註： 如果僅選擇 HP Credential Manager 作爲安全層級，您將不會收到 Windows 密碼的提示，因爲 Credential Manager 已經知道您的 Windows 密碼。

     輸入並確認 Windows 密碼，或輸入您建立的密碼，然後按「**下一步**」。

   - 在 Windows 啓動之前保護您的系統（選擇性） – 如果您知道 BIOS 管理員密碼，也可輸入該密碼。如果輸入 BIOS 管理員密碼，則 Windows 管理員或使用者即爲 BIOS 管理員。

     附註： 如果 BIOS 管理員密碼不存在，則您必須在繼續之前建立一組密碼。如果輸入 BIOS 管理員密碼，則您即爲 BIOS 管理員。

     輸入並確認 BIOS 管理員密碼，或輸入已建立的密碼。然後按「**下一步**」。

7. 在「設定安全登入法」頁面上，按「**下一步**」。
8. 在「檢視及啓用安全性設定」頁面上，按一下「**啓用**」。
9. 依據管理員所設定的安全登入法，即會顯示以下兩頁的其中一頁或兩頁。依照螢幕上的指示繼續操作，然後按「**下一步**」。

   - 「註冊您的指紋」- 以手指在螢幕上按一下，此手指的指紋必須與您想要註冊的相同（您必須至少註冊兩枚指紋），在指紋感應器上緩慢掃過您選定的手指，然後繼續在指紋感應器上掃過相同的手指，直到完成所需的掃描次數爲止。重複此程序以註冊第二根手指，然後按一下「**完成**」。
   - 「註冊 HP ProtectTools Java Card」- 插入 HP ProtectTools Java Card，輸入 Java Card PIN，然後按一下「**完成**」。

10. 在「恭喜」頁面上，檢視您的選擇，然後按一下「**完成**」。

完成 Security Manager 設定之後登入

依 Windows 管理員於設定時所選的安全性等級及安全登入法而定，登入情況會有所不同。幾種可能的情況如下：

- 如果已設定全部 3 個的安全性等級且需要**所有**安全登入法，則使用者必須於首次登入時使用所有已設定的方式登入。此動作會將使用者登入 Windows。
- 如果已設定全部 3 個的安全性等級且**任何**安全登入法皆有權限，則使用者可以於首次登入時使用任何已設定的安全登入法登入。此動作會將使用者登入 Windows。
- 如果已設定 HP Drive Encryption 及 HP Credential Manager 的安全性等級且需要**所有**安全登入法，則使用者必須於 HP Drive Encryption 登入畫面開啓時使用所有已設定的方式登入。此動作會將使用者登入 Windows。
- 如果已設定 HP Drive Encryption 及 HP Credential Manager 的安全性等級且**任何**安全登入法皆有權限，則使用者可以於 HP Drive Encryption 登入畫面開啓時使用任何已設定的安全登入法登入。此動作會將使用者登入 Windows。

- 如果已設定 HP Credential Manager 的安全性等級且需要**所有**安全登入法，則使用者必須於 HP Credential Manager 登入畫面開啓時使用所有已設定的方式登入。此動作會將使用者登入 Windows。
- 如果已設定 HP Credential Manager 的安全性選項層級且**任何**已設定的安全登入法皆有權限，則使用者可以於 HP Credential Manager 登入畫面開啓時使用任何一種安全登入法登入。此動作會將使用者登入 Windows。

附註： 如果未設定 HP Credential Manager 的安全性等級，則使用者仍必須於 Windows 登入畫面中輸入其 Windows 密碼，無論其他安全性等級所要求的安全登入法爲何都是如此。

管理員工具 - 管理使用者（管理員工作）

Windows 管理員可以使用「管理員工具」功能新增及移除 HP ProtectTools 使用者及檢視使用者狀態。

在「管理員工具」中，「管理員」及「使用者」標籤顯示所選的安全登入法及使用者可以選擇使用其中任何選項或必須全部使用。如果想要變更安全性等級及安全登入法，您必須執行安裝精靈以進行變更。

新增使用者

Windows 管理員可以新增其他的管理員，或將一般使用者新增到使用者清單。這兩個的新增程序都相同。

附註： 新增使用者之前，該使用者必須已在電腦中擁有 Windows 使用者帳戶，且必須在下列步驟進行時提供密碼。

若要新增使用者至使用者清單：

1. 按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**管理員工具**」。
3. 按一下「**管理使用者**」按鈕。
4. 選取「**管理員**」或「**使用者**」標籤。
5. 按一下「**新增**」。
6. 按一下您想要新增的帳戶使用者名稱，或在「**使用者名稱**」對話方塊中輸入帳戶名稱，然後按「**下一步**」。

   附註： 您必須使用現存的 Windows 帳戶、按一下帳戶或輸入相同的帳戶。您不能使用此對話方塊修改或新增 Windows 使用者帳戶。
7. 爲所選的帳戶輸入 Windows 密碼，然後按一下「**確定**」。

   附註： 如果使用者將以指紋和/或 HP ProtectTools Java™ Card 等安全登入法登入，則必須現在登入到電腦並執行安裝精靈以設定上述安全登入法。

移除使用者

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

若要將使用者從使用者清單中移除：

1. 按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**管理員工具**」。
3. 按一下「**管理使用者**」按鈕。
4. 選取「**管理員**」或「**使用者**」標籤。
5. 按一下您想要移除的帳戶使用者名稱，然後按「**移除**」。

附註： 如果「管理員」清單中僅有一名「管理員」，則無法移除管理員。

6. 在確認對話方塊中，按一下「**是**」。

檢查使用者狀態

在「管理員工具」中，「管理員」及「使用者」標籤顯示目前各使用者的狀態：

- **綠色核取標記** - 指明使用者已設定所需的安全登入法。
- **黃色驚嘆號** - 指明使用者尚未設定一個或多個所需的或有權限的安全登入法。舉例而言，如果 Windows 管理員設定至少 2 個所需的安全登入法，且指明其中一種方式可用於登入電腦，則已設定其中一種方式的使用者即可使用該方式登入。黃色驚嘆號向 Windows 管理員指明使用者尚未設定其他安全登入法。
- **紅色 X** - 指明使用者尚未設定所需的安全登入法且將於嘗試登入時被鎖定，而無法登入電腦。使用者必須執行安裝精靈以設定所需的登入法。
- **空白** - 指明不需要安全登入法。

備份與復原

HP ProtectTools Backup and Restore 提供一個集中位置，可讓您從已安裝的 HP ProtectTools 模組備份與復原安全性認證。

在 Security Manager 中，按一下「**Backup and Restore**」，再按下列其中一個按鈕：

- 「**備份選項**」按鈕 – 讓您設定備份設定。如需詳細資訊，請參閱 16 頁的使用備份精靈。
- 「**備份**」按鈕 – 可讓您執行立即備份所有安全性認證。

附註： 您必須在執行備份之前使用「**備份選項**」按鈕設定備份設定。

- 「**排程備份**」按鈕 – 讓您設定排程備份。如果您需要排程的協助，請在「Windows 說明」中搜尋主題爲「工作排程」的文章。

附註： 排程備份之前，您必須使用「**備份選項**」按鈕設定備份設定。

- 「**還原**」按鈕 – 可讓您還原先前備份的安全性認證。如需詳細資訊，請參閱 17 頁的使用還原精靈。

△ **注意：** 非 HP ProtectTools Backup and Restore 建立的備份檔案（例如，先前以指定安全性模組建立的檔案）與 HP ProtectTools Backup and Restore 不相容，所以無法以 HP ProtectTools Backup and Restore 或其新版安全性模組還原。HP 建議您以 HP ProtectTools Backup and Restore 建立新的備份檔。

使用備份精靈

1. 在 Security Manager 中，按一下「**Backup and Restore**」，然後按一下「**備份選項**」以啓動「備份」精靈。
2. 如果您想在下次「備份」精靈執行時略過「歡迎」畫面，請取消「**顯示歡迎畫面**」核取方塊。
3. 按「**下一步**」。「安全性模組」頁面即開啓。
4. 請參閱下列的小節繼續。

安全性模組

若要選取模組備份，請依照這些步驟：

1. 勾選一列前端的核取方塊，將相關的模組新增到備份清單中。按一下「**全部選取**」或「**全部清除**」按鈕，快速將所有的模組從備份清單中新增或移除。請注意，模組的「狀態」欄位必須顯示爲「就緒」或「需要驗證」，才能加以選取。

   附註： 如果模組未就緒，則核取方塊無法使用。更新模組的狀態之後，請按一下該列右側的「**重新整理**」按鈕，以更新「狀態」欄位。按一下「**重新整理全部**」按鈕以更新全部模組的狀態。

2. 如有必要，請在「驗證」欄位爲每個選定的模組輸入所需的值。安全性裝置可能需要輸入驗證值，以利於裝置上存取認證資料。這些值可能包含密碼、PIN 等。
3. 按「**下一步**」。「檔案位置」頁面即會開啓。

檔案位置

「檔案位置」頁面可讓您選擇備份儲存檔及安全性權仗檔的位置。

安全性權仗檔會安全儲存用於加密備份儲存檔的金鑰。加密安全性權仗檔內容的密碼。將安全性權仗檔儲存於離線位置（USB 快閃磁碟機、光碟或其他媒體）提供雙層的安全性等級，因爲要存取儲存檔中的備份資料，您必須**擁有**安全性權仗檔並**知道**密碼。因此，HP 建議您將儲存檔及權仗檔儲存於兩個位於不同位置的不同卸除式媒體上。

若要設定檔案位置：

1. 確認或變更檔案名稱及您想要儲存儲存檔及安全性權仗檔的位置。若要變更位置，請按一下「**編輯**」按鈕，然後輸入新的檔案名稱，或按一下「**瀏覽**」，以選取新的位置。附檔名 .ptb 會自動附加到檔案名稱之後。

   附註： 一個即定儲存檔中的每一個模組僅允許一個備份資料實例。如果您指定一個現存的儲存檔，則可選擇在儲存檔中覆寫所選的模組資料或指定不同的儲存檔。如果您指定一個現存的儲存檔，則不會覆寫全部的檔案，而僅會覆寫所選模組的備份資料。

2. 若要以安全性權仗及密碼加密及保護儲存檔，請按一下「**以密碼保護儲存檔**」。然後輸入並確認用於安全性權仗檔加密的密碼。

3. 按一下「**記憶所有密碼及驗證值**」，以設定系統並安全快取（儲存）密碼，此密碼可啓用無人監控的備份。啓用此功能同時快取任何「安全性模組」中的驗證值。
4. 按一下「**立即備份**」以開始備份，或按「**下一步**」以儲存備份設定，而不要在此次執行備份。

   如果您選擇開始備份，則作業完成時會出現「備份完成」的頁面。

備份完成

「備份完成」頁面顯示備份作業的狀態。

1. 按一下「**檢視記錄**」以檢視關於備份作業的更多詳細資訊，包括錯誤。
2. 按一下「**完成**」離開精靈。

使用還原精靈

1. 在 Security Manager 中，按一下「**Backup and Restore**」，然後按一下「**還原**」以啓動「還原」精靈。
2. 如果您想在下次「還原」精靈執行時略過「歡迎」畫面，請取消「**顯示歡迎畫面**」核取方塊。
3. 按「**下一步**」。「檔案位置」頁面即會開啓。
4. 請參閱下列的小節繼續。

檔案位置

「檔案位置」頁面允許您選擇備份儲存檔及包含所需還原安全性認證的安全性權仗檔（如果有）。

若要選取備份檔案的位置，請依照這些步驟：

1. 如果頁面上沒有顯示儲存檔，請按一下「**編輯**」按鈕，然後按一下「**瀏覽**」以瀏覽至該檔案。
2. 如果頁面上沒有顯示安全性權仗檔，請按一下「**編輯**」按鈕，然後按一下「**瀏覽**」以瀏覽至該安全性權仗檔位置。
3. 如有必要，請輸入該檔案的密碼。
4. 按「**下一步**」。「安全性模組」頁面即開啓。

安全性模組

此頁面顯示在「檔案位置」頁面所選之檔案中具有備份資料的所有已安裝模組。

若要選取模組還原：

1. 勾選一列前端的核取方塊，將相關的模組新增到還原清單中。按一下「**全部選取**」或「**全部清除**」按鈕，快速將模組從還原清單中新增或移除。請注意，模組的「狀態」欄位必須顯示爲「就緒」或「需要驗證」，才能加以選取。

   附註： 如果模組未就緒，則核取方塊無法使用。更新模組的狀態之後，請按一下該列右側的「**重新整理**」按鈕，以更新「狀態」欄位。按一下「**重新整理全部**」按鈕以更新全部模組的狀態。

2. 如有必要，請在「驗證」欄位爲每個選定的模組輸入所需的值。可能需要驗證值，才能存取安全性裝置進行還原。這些值可能包含密碼、PIN 等。這些欄位中輸入的值會立即生效。
3. 按「**下一步**」。「確認」頁面即會開啓。

確認

1. 如果您想要變更還原設定，請按一下「**上一頁**」以返回還原設定畫面。
2. 確認您想要還原表列模組的認證，然後按一下「**立即還原**」開始還原。
3. 選擇您想要還原的檔案並按一下「**完成**」。
4. 在確認對話方塊中，按一下「**是**」

△ **注意：** 還原認證將會覆寫目前的認證，這可能導致資料遺失或系統鎖定。

還原完成

「還原完成」頁面顯示還原作業的狀態。

- 按一下「**檢視記錄**」以檢視關於還原作業的更多詳細資訊，包括錯誤。
- 按一下「**完成**」離開精靈。

設定

在 HP ProtectTools Security Manager for Administrators 中，按一下「**設定**」，以變更設定選項。

下列 Security Manager 設定可供使用：

- 選擇「**在工作列上顯示圖示**」核取方塊，以顯示能讓您啟動主機、開啓指定頁面和/或啓動指定應用程式的工作列圖示。
- 選擇「**顯示安全性桌面通知**」核取方塊，以顯示已安裝模組所產生的通知。
- 檢視或略過「備份」精靈「歡迎 (Welcome)」頁面。
- 檢視或略過「還原」精靈「歡迎 (Welcome)」頁面。

3 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools 可透過下列安全性功能，防止未獲授權的使用者存取您的電腦：

- 使用密碼登入至 Windows 以外的其他選擇，例如使用 Java Card 或生物測量讀取器登入 Windows。請參閱「20 頁的註冊認證」，以取得詳細資訊。
- 單一登入功能 (Single Sign On) 可自動記憶網站、應用程式及受保護的網路資源之認證。
- 支援選購的安全性裝置，如 Java 卡和生物測定讀取器。
- 支援其他安全性設定，如要求使用選購的安全性裝置進行驗證以解除電腦的鎖定。

設定程序

登入 Credential Manager

視組態而定，您可以使用下列任一方式登入認證管理員 (Credential Manager)：

- 通知區域中的 HP ProtectTools Security Manager for Administrators 圖示
- 在 Windows Vista® 中，請按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
- 在 Windows XP 中，請按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager**」。

附註： 在 Windows Vista 中，您必須啟動「HP ProtectTools Security Manager for Administrators」才能進行變更。

登入 Credential Manager 後，您便可以登錄額外的認證，例如指紋或 Java Card。請參閱「20 頁的註冊認證」，以取得詳細資訊。

在下一次登入時，即可選擇登入原則，並使用任何已註冊的認證組合。

使用認證管理員登入精靈 (Credential Manager LogonWizard)

若要使用認證管理員登入精靈 (Credential Manager Logon Wizard) 登入認證管理員 (Credential Manager)，請執行下列步驟：

1. 以下列任何方式開啓認證管理員登入精靈 (Credential Manager Logon Wizard)：
   - 從 Windows 登入畫面
   - 從通知區域中，透過連按兩下「**HP ProtectTools Security Manager for Administrators**」圖示
   - 從 HP ProtectTools Security Manager for Administrators 的「Credential Manager」中，透過按一下視窗右上角的「**登入**」連結
2. 請依照螢幕上的指示，登入認證管理員 (Credential Manager)。

註冊認證

您可以使用「我的身份 (My Identity)」頁面，來註冊各種驗證方法或認證。註冊之後，即可使用這些方法，來登入認證管理員 (Credential Manager)。

註冊指紋

指紋讀取器可讓您使用自己的指紋進行驗證以登入 Windows，而不使用 Windows 密碼。

設定指紋讀取器

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**註冊指紋 (Register Fingerprints)**」。
3. 依照螢幕上的指示，完成指紋註冊和設定指紋讀取器。
4. 若要爲其他 Windows 使用者設定指紋讀取器，請以該使用者的身份登入 Windows，然後重複執行上述步驟。

使用您的註冊指紋登入 Windows

1. 在註冊指紋後，立即重新啓動 Windows。
2. 在 Windows 歡迎畫面中，將任一隻已註冊的手指掃過指紋感應器，以登入 Windows。

註冊智慧卡或 Token

智慧卡是一張差不多信用卡大小的塑料卡片，含有可以載入資訊的內嵌微晶片。智慧卡爲個別使用者提供資訊及驗證的保護。使用密碼編譯爲基礎的身份識別時，智慧卡登入網路可以提供較強的驗證；驗證使用者網域時，以智慧卡登入網路可以證明使用者所屬的網域。

USB Token 就是智慧卡，只是形式不同。它不是將智慧晶片部署在塑料信用卡平面上，而是將智慧晶片插入塑料 Token 中，也就是 USB 金鑰。智慧卡與 Token 的主要不同之處在於存取的介面。智慧卡需要讀取器而 Token 是直接插入任何 USB 連接埠。其儲存及提供認證的核心功能相同。

USB Token 可用來提供較強的驗證。它提供增強的安全性並確保安全存取資訊。

附註： 您必須要有讀卡機才能設定此步驟。如果您沒有安裝讀卡機，也可以按照 22 頁的建立虛擬 Token 所述註冊一個虛擬權仗。

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**註冊智慧卡或 Token (Register Smart Card or Token)**」。
3. 在「**裝置類型 (Device Type)**」對話方塊中，按一下想要的裝置類型，然後按「**下一步 (Next)**」。
4. 如果選取智慧卡或 USB Token 作爲裝置類型，請確定已插入智慧卡或 Token 已連接至 USB 連接埠。

   附註： 如果未插入智慧卡或 Token 未連接至 USB 連接埠，「選擇 Token (Select Token)」對話方塊中的「下一步 (Next)」按鈕將不可用。
5. 在「裝置類型(Device Type)」對話方塊中，選擇「**下一步 (Next)**」。

   將顯示「Token 內容 (Token Properties)」對話方塊。
6. 輸入使用者 PIN 碼，選擇「**註冊智慧卡或 Token 以進行驗證 (Register smart card or token for authentication)**」，然後按一下「**完成 (Finish)**」。

註冊其他認證

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**註冊認證 (Register Credentials)**」。

   「Credential Manager 註冊精靈 (Credential Manager Registration Wizard)」便會開啓。
3. 請依照螢幕上的說明繼續執行。

一般工作

所有使用者都可以存取認證管理員 (Credential Manager) 的「我的身份 (My Identity)」頁面。從「我的身份 (My Identity)」頁面，您可以

- 變更 Windows 登入密碼
- 變更 Token PIN 碼
- 鎖定工作站

附註： 只有在 Credential Manager 傳統登入提示已啓用的情況下，才可使用此選項。請參閱「29 頁的範例 1 — 使用「進階設定 (Advanced Settings)」頁面，允許從認證管理員 (Credential Manager) 登入 Windows」。

建立虛擬 Token

虛擬 Token 的運作方式與 Java 卡或 USB Token 很類似。Token 是儲存在電腦硬碟或 Windows 註冊表中。當您以虛擬 Token 登入時，系統會要求您提供使用者 PIN 碼，來完成驗證。

若要建立新的虛擬 Token：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**註冊智慧卡或 Token (Register Smart Card or Token)**」。
3. 在「**裝置類型 (Device Type)**」對話方塊中，按一下「**虛擬 Token (Virtual Token)**」，然後按「**下一步 (Next)**」。
4. 指定 Token 的名稱及位置，然後按「**下一步 (Next)**」。

   新的虛擬 Token 可以儲存在檔案或 Windows 註冊表資料庫中。
5. 在「Token 內容」對話方塊中，爲新建立的虛擬 Token 指定主要 PIN 碼及使用者 PIN 碼，選擇「**註冊智慧卡或 Token 以進行驗證 (Register smart card or token for authentication)**」，然後按一下「**完成 (Finish)**」。

   將顯示「Token 內容 (Token Properties)」對話方塊。
6. 輸入使用者 PIN 碼，選擇「**註冊智慧卡或 Token 以進行驗證 (Register smart card or token for authentication)**」，然後按一下「**完成 (Finish)**」。

變更 Windows 登入密碼

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**變更 Windows 密碼 (Change Windows Password)**」。
3. 在「**舊密碼 (Old password)**」方塊中，鍵入您的舊密碼。
4. 在「**新密碼 (New Password)**」和「**確認密碼 (Confirm Password)**」方塊中鍵入新密碼。
5. 按一下「**完成 (Finish)**」。

變更 Token PIN 碼

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」，然後按一下「**變更 Token PIN 碼 (Change Token PIN)**」。
3. 在「裝置類型(Device Type)」對話方塊中，按一下想要的裝置類型，然後按「**下一步 (Next)**」。
4. 選擇要變更 PIN 碼的 Token，然後按「**下一步 (Next)**」。
5. 請依照螢幕上的指示完成 PIN 碼變更。

附註： 如果您連續多次輸入不正確的 Token PIN 碼，Token 會被鎖住。在解除鎖定之前，您將無法使用此 Token。

鎖定電腦（工作站）

如果您使用認證管理員 (Credential Manager) 登入 Windows，便會提供這項功能。當您離開桌面時，若要保護您的電腦，請使用「鎖定工作站 (Lock Workstation)」功能。這能防止未授權的使用者存取您的電腦。只有您和您電腦上的管理員群組成員可解除它的鎖定。

附註： 只有在 Credential Manager 傳統登入提示已啓用的情況下，才可使用此選項。請參閱「29 頁的範例 1 — 使用「進階設定 (Advanced Settings)」頁面，允許從認證管理員 (Credential Manager) 登入 Windows」。

爲強化安全性，您可以設定「鎖定工作站」功能，以便在解除鎖定電腦時需要 Java Card、生物測量讀取裝置或權仗。請參閱「29 頁的設定認證管理員 (Credential Manager) 設定」以取得詳細資訊。

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**我的身份 (My Identity)**」。
3. 按一下「**鎖定工作站 (Lock Workstation)**」立刻鎖定您的電腦。

   您必須使用 Windows 密碼或 Credential Manager 登入精靈，才能解除電腦的鎖定。

使用 Windows 登入

您可以在本機電腦或網路網域上，使用認證管理員 (Credential Manager) 來登入 Windows。當您第一次登入認證管理員 (Credential Manager) 時，系統會自動將您的本機 Windows 使用者帳戶新增爲 Windows 登入服務的帳戶。

使用認證管理員 (Credential Manager) 登入 Windows

您可以使用認證管理員 (Credential Manager)，來登入 Windows 網路或本機帳戶。

1. 如果您已註冊指紋以登入 Windows，請將手指掃過指紋感應器來登入。
2. 在 Windows XP 中，如果您尚未註冊指紋以登入 Windows，請按一下畫面左上角指紋圖示旁的鍵盤圖示。「Credential Manager 登入精靈 (Credential Manager Logon Wizard)」便會開啓。

   在 Windows Vista 中，如果您尚未註冊指紋以登入 Windows，按一下登入畫面中的「**Credential Manager**」圖示。「Credential Manager 登入精靈 (Credential Manager Logon Wizard)」便會開啓。

3. 按一下「**使用者名稱 (User name)**」方向鍵，再按一下您的名稱。
4. 在「**密碼 (Password)**」方塊中，鍵入您的密碼，然後按「**下一步 (Next)**」。
5. 選擇「**更多 (More)**」，然後按一下「**精靈選項 (Wizard Options)**」。
   a. 若要將它當做下次登入電腦時的預設使用者名稱，請選擇「**在下次登入時使用最後一個使用者名稱 (Use last user name on next logon)**」核取方塊。
   b. 若要將此登入原則當做預設的方法，請選擇「**下次登入時使用最後一個原則 (Use last policy on next logon)**」核取方塊。
6. 請依照螢幕上的說明繼續執行。若驗證資訊正確，您將會登入 Windows 帳戶和認證管理員 (Credential Manager)。

使用單一登入 (Single Sign On)

認證管理員 (Credential Manager) 有一個「單一登入 (Single Sign On)」功能，可儲存多個網際網路和 Windows 程式的使用者名稱和密碼，並在您存取已註冊的程式時，自動輸入登入認證。

附註： 安全性和隱私性是「單一登入 (Single Sign On)」的重要功能。所有認證都會加密，並只有在順利登入認證管理員 (Credential Manager) 後才能使用。

附註： 您也可以設定「單一登入 (Single Sign On)」，在登入到安全性的網站或程式時，使用 Java Card、指紋讀取裝置或權仗驗證您的驗證認證。這對於登入包含個人資訊的程式或網站時特別有用，例如銀行帳戶號碼。如需詳細資訊，請參閱「29 頁的設定認證管理員 (Credential Manager) 設定」。

註冊新應用程式

當您登入認證管理員 (Credential Manager) 時，認證管理員 (Credential Manager) 會提示您註冊您啓動的所有應用程式。您也可以手動註冊應用程式。

使用自動註冊

1. 開啓需要您登入的應用程式。
2. 按一下程式或網站密碼對話方塊中的「認證管理員 SSO (Credential Manager SSO)」圖示。
3. 鍵入您的程式或網站密碼，再按一下「**確定 (OK)**」。「**認證管理員單一登入 (Credential Manager Single Sign On)**」對話方塊便會開啓。
4. 按一下「**更多 (More)**」，並選擇下列選項：
   - 不要使用這個網站或應用程式的 SSO (Do not use SSO for this site or application)。
   - 提示選擇這個應用程式的帳戶 (Prompt to select account for this application)。
   - 填寫認證但不提交 (Fill in credentials but do not submit)。
   - 先驗證使用者再提交認證 (Authenticate user before submitting credentials)。
   - 顯示這個應用程式的 SSO 捷徑 (Show SSO shortcut for this application)。
5. 按一下「**是 (Yes)**」，完成註冊。

使用手動（拖放）註冊

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下左窗格中的「**服務及應用程式**」。
2. 按一下「**管理應用程式及認證**」。

   Credential Manager「單一登入(Single Sign On)」對話方塊便會顯示。
3. 若要修改或移除先前註冊的網站或應用程式，請從清單中選擇想要的記錄。
4. 依照螢幕上的說明繼續執行。

管理應用程式和認證

修改應用程式內容

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後從左窗格按一下「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**管理應用程式及認證 (Manage Applications and Credentials)**」。

   Credential Manager「單一登入 (Single Sign On)」對話方塊便會顯示。
3. 按一下要修改的應用程式項目，再按一下「**內容 (Properties)**」。
4. 按一下「**一般 (General)**」標籤，來修改應用程式名稱和說明。選擇或清除適當設定旁的核取方塊來變更設定。
5. 按一下「**指令檔 (Script)**」標籤來檢視和編輯 SSO 應用程式指令檔。
6. 按一下「**確定 (OK)**」。

從單一登入 (Single Sign On) 移除應用程式

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下左窗格中的「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**管理應用程式及認證 (Manage Applications and Credentials)**」。

   Credential Manager「單一登入 (Single Sign On)」對話方塊便會顯示。
3. 按一下要移除的應用程式項目，然後按一下「**移除 (Remove)**」。
4. 在確認對話方塊中，按一下「**是 (Yes)**」。
5. 按一下「**確定 (OK)**」。

匯出應用程式

您可以匯出應用程式來建立「單一登入 (Single Sign On)」應用程式指令檔的備份。接下來可使用此檔案以復原「單一登入 (Single Sign On)」資料。這個動作可彌補身份識別備份檔的不足，因其僅包含認證資訊。

若要匯出應用程式：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下左窗格中的「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**管理應用程式及認證 (Manage Applications and Credentials)**」。

   Credential Manager「單一登入 (Single Sign On)」對話方塊便會顯示。
3. 按一下要匯出的應用程式項目，然後按一下「**更多 (More)**」。
4. 依照螢幕上的指示完成匯出。
5. 按一下「**確定 (OK)**」。

匯入應用程式

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下左窗格中的「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**管理應用程式及認證 (Manage Applications and Credentials)**」。

   Credential Manager「單一登入 (Single Sign On)」對話方塊便會顯示。
3. 按一下要匯入的應用程式項目，然後按一下「**更多 (More)**」。
4. 依照螢幕上的指示完成匯入。
5. 按一下「**確定 (OK)**」。

修改認證

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**管理應用程式及認證 (Manage Applications and Credentials)**」。

   「Credential Manager 單一登入」對話方塊便會顯示。
3. 按一下要修改的應用程式項目，再按一下「**更多 (More)**」。
4. 一些可供選擇的選項包括：
   - 應用程式 (Applications)
     - 新增 (Add New)
     - 移除 (Remove)
     - 內容 (Properties)
     - 匯入指令檔 (Import Script)
     - 匯出指令檔 (Export Script)
   - 認證 (Credentials)
     - 新建 (Create New)
   - 檢視密碼 (View Password)

附註： 在檢視密碼之前，必須先驗證您的身份識別。

5. 請依照螢幕上的說明繼續執行。
6. 按一下「**確定 (OK)**」。

使用應用程式保護

這項功能可以讓您設定對應用程式的存取。您可以依據下列準則來限制存取：

- 使用者類別
- 使用時間
- 使用者無活動

限制存取應用程式

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」，然後按一下「**服務及應用程式 (Services and Applications)**」。
2. 按一下「**應用程式防護 (Application Protection)**」，然後按一下「**管理受保護的應用程式 (Manage Protected Applications)**」。
3. 選擇要管理存取的使用者類別。

附註： 如果這個類別不是「所有人 (Everyone)」，您可能必須選擇「**覆寫預設值 (Override default settings)**」，以覆寫「所有人 (Everyone)」類別的設定。

4. 按一下「**新增 (Add)**」。

「新增程式精靈 (Add a Program Wizard)」便會開啓。

5. 請依照螢幕上的說明繼續執行。

從應用程式移除保護

若要從應用程式移除保護：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**服務及應用程式 (Services and Applications)**」。
3. 按一下「**應用程式防護 (Application Protection)**」，然後按一下「**管理受保護的應用程式 (Manage Protected Applications)**」。
4. 選擇要管理存取的使用者類別。

附註： 如果這個類別不是「所有人 (Everyone)」，您可能必須按一下「**覆寫預設值 (Override default settings)**」，以覆寫「所有人 (Everyone)」類別的設定。

5. 按一下要移除的應用程式項目，再按一下「**移除 (Remove)**」。
6. 按一下「**確定 (OK)**」。

變更受保護應用程式的限制設定

1. 按一下「**應用程式防護 (Application Protection)**」，然後按一下「**管理受保護的應用程式 (Manage Protected Applications)**」。
2. 選擇要管理存取的使用者類別。

   附註： 如果這個類別不是「所有人 (Everyone)」，您可能必須按一下「**覆寫預設值 (Override default settings)**」，以覆寫「所有人 (Everyone)」類別的設定。

3. 按一下要變更的應用程式，再按一下「**內容 (Properties)**」。該應用程式的「**內容 (Properties)**」對話方塊便會開啓。
4. 按一下「**一般 (General)**」標籤。選擇下列其中一項設定：
   - 已停用 (無法使用) (Disabled (Cannot be used))
   - 已啓用 (可以不受限制地使用) (Enabled (Can be used without restrictions))
   - 受限 (使用依設定而異) (Restricted (Usage depends on settings))
5. 選擇「受限 (Restricted)」時，可以指定下列設定：
   a. 如果要依據時間、星期或日期來限制使用，請按一下「**排程 (Schedule)**」標籤，並設定組態。
   b. 如果要依據無活動的狀態來限制使用，請按一下「**進階 (Advanced)**」標籤，並選擇無活動的期間。
6. 按一下「**確定 (OK)**」，關閉應用程式的「**內容 (Properties)**」對話方塊。
7. 按一下「**確定 (OK)**」。

進階工作（僅適用於管理員）

僅有在具有管理員權限的使用者登入時，才會顯示 Credential Manager 的「多重驗證」頁面及「設定」頁面。在這些頁面中，您可以執行下列工作：

- 設定認證內容
- 設定認證管理員 (Credential Manager) 設定

設定認證內容

在「多重驗證」頁面的「認證」標籤上，您可以檢視可用的驗證方式清單並修改設定。

若要設定認證：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**多種要素驗證 (Multifactor Authentication)**」。
3. 按一下「**認證 (Credentials)**」標籤。

4. 按一下要修改的認證類型。您可以使用下列任何一種方式來修改認證：
   - 若要註冊認證，請按一下「**註冊 (Register)**」，然後依照螢幕上的指示進行。
   - 若要刪除認證，請按一下「**清除 (Clear)**」，再按一下確認對話方塊中的「**是 (Yes)**」。
   - 若要修改認證內容，按一下「**內容 (Properties)**」，然後依照螢幕上的指示進行。
5. 請按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

設定認證管理員 (Credential Manager) 設定

在「設定」頁面中，您可以使用下列標籤存取和修改多種設定：

- 一般 (General) — 可讓您修改基本組態的設定。
- 單一登入 (Single Sign On) — 可讓您修改目前使用者如何使用「單一登入 (Single Sign On)」的設定，例如，如何處理登入畫面的偵測、自動登入註冊的對話方塊，以及密碼顯示。
- 服務及應用程式 (Services and Applications) — 可讓您檢視可用的服務，並修改那些服務的設定。
- 安全性 (Security) — 可讓您選擇指紋讀取器軟體，並調整指紋讀取器的安全性等級。
- 智慧卡及 Token (Smart Cards and Tokens) — 可讓您檢視和修改所有可用 Java 卡和 Token 的內容。

若要修改認證管理員 (Credential Manager) 設定：

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**設定 (Settings)**」。
3. 針對您要修改的設定，按一下適當的標籤。
4. 依照螢幕上的指示來修改設定。
5. 請按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

範例 1 — 使用「進階設定 (Advanced Settings)」頁面，允許從認證管理員 (Credential Manager) 登入 Windows

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下左窗格中的「**Credential Manager**」。
2. 按一下「**設定 (Settings)**」。
3. 按一下「**一般 (General)**」標籤。
4. 在「**選取使用者登入 Windows 的方式 (Select the way users log on to Windows)**」下，選取「**使用 Credential Manager 登入 Windows (Use Credential Manager to log on to Windows)**」核取方塊。
5. 按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。
6. 重新啓動電腦。

附註： 選取「**使用 Credential Manager 登入 Windows**」核取方塊，可讓您鎖定電腦。請參閱「23 頁的鎖定電腦（工作站）」。

附註： 上述步驟在 Windows XP 作業系統中可能略有不同。

範例 2 — 使用「進階設定 (Advanced Settings)」頁面，在單一登入 (Single Sign On) 之前驗證使用者

1. 在 HP ProtectTools Security Manager for Administrators 中，按一下「**Credential Manager**」，然後按一下「**設定**」。
2. 按一下「**單一登入 (Single Sign On)**」標籤。
3. 在「**造訪註冊的登入對話方塊或網頁時 (When Registered Logon Dialog or Web Page is Visited)**」下，選擇「**先驗證使用者再提交認證 (Authenticate user before submitting credentials)**」核取方塊。
4. 按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。
5. 重新啓動電腦。

4 Drive Encryption for HP ProtectTools

△ **注意：** 如果您決定解除安裝 Drive Encryption 模組或您正使用備份與還原解決方案，則您必須先解密所有的加密磁碟機。如果您不這麼做，除非您已使用 Drive Encryption 復原服務註冊，否則將無法存取加密磁碟機上的資料。重新安裝 Drive Encryption 模組也無法讓您存取加密磁碟機。

設定程序

開啓 Drive Encryption

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**Drive Encryption**」。

一般工作

啓用 Drive Encryption

使用 HP ProtectTools Security Manager for Administrators 安裝精靈啓用 Drive Encryption。

停用 Drive Encryption

使用 HP ProtectTools Security Manager for Administrators 安裝精靈停用 Drive Encryption。

在啓用 Drive Encryption 之後登入

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

附註： 如果 Windows 管理員已啓用 HP ProtectTools Security Manager for Administrators 中的「預先開機安全性」，您將在電腦開啓後立即登入電腦，而不必再經過 Drive Encryption 登入畫面。

1. 選取您的使用者名稱，然後輸入 Windows 密碼或 Java™ 卡 PIN 碼，或者按下已註冊的手指指紋。
2. 按一下「**確定 (OK)**」。

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

進階工作

管理 Drive Encryption（管理員工作）

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

啓用 TPM 密碼保護

使用 Embedded Security for HP ProtectTools 啓用 TPM。啓用之後，登入於 Drive Encryption 登入畫面時會需要 Windows 使用者名稱和密碼。

附註： 由於密碼受 TPM 安全晶片保護，因此如果將硬碟移到另一台電腦上，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。

1. 使用 Embedded Security for HP ProtectTools 啓用 TPM。
2. 開啓 Drive Encryption，然後按一下「**加密管理 (Encryption Management)**」。
3. 選取「**TPM 密碼保護 (TPM-protected password)**」核取方塊。

加密或解密個別磁碟機

1. 開啓 Drive Encryption，然後按一下「**加密管理 (Encryption Management)**」。
2. 按一下「**變更加密 (Change Encryption)**」。
3. 在「變更加密 (Change Encryption)」對話方塊中，選取或清除要加密或解密之個別硬碟旁邊的核取方塊，然後按一下「**確定 (OK)**」。

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

備份與復原（管理員工作）

「復原」頁面可讓 Windows 管理員備份與復原加密金鑰。

建立備份金鑰

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

1. 開啓 Drive Encryption，然後按一下「**復原 (Recovery)**」。
2. 按一下「**備份金鑰 (Backup Keys)**」。
3. 在「選取備份磁碟 (Select Backup Disk)」頁面中，按一下要備份加密金鑰的裝置名稱，然後按「**下一步 (Next)**」。
4. 閱讀下一頁所顯示的資訊，然後按「**下一步 (Next)**」。

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

註冊線上復原

「線上 Drive Encryption 金鑰復原服務」會儲存加密金鑰的備份副本，以便您在忘記密碼且無法存取本機備份時，仍然可以存取電腦。

附註： 您必須與網際網路連線，並提供有效的電子郵件地址，才能註冊並透過此服務來復原您的密碼。

1. 開啓 Drive Encryption，然後按一下「**復原 (Recovery)**」。
2. 按一下「**註冊 (Register)**」。
3. 按一下下列選項之一：
   - 我想要建立這部 PC 的新復原帳戶。如果選擇這個選項，請輸入您的電子郵件地址和其他資訊，然後按「**下一步 (Next)**」。
   - 我想將這部 PC 新增到現有的 Web 復原帳戶。
4. 建立並確認密碼，選取安全性問題並輸入答案，然後按「**下一步 (Next)**」。

   附註： 帳戶啓用碼將會傳送到您提供的電子郵件地址。
5. 輸入啓用碼，然後按「**下一步 (Next)**」。
6. 輸入電腦序號，然後按「**下一步 (Next)**」。

   附註： 如果要找出電腦序號，按一下「**開始**」，然後按一下「**說明及支援**」。
7. 如果您沒有訂閱優待券，按一下「**按一下此處以購買優待券 (Click here to purchase coupons)**」連結。

   按一下連結隨即會將您導向 SafeBoot Recovery 服務網站。請不要結束精靈。
8. 按一下「**購買優待券代碼 (Purchase Coupon Codes)**」。
9. 選取您的國家/地區、電腦類型，然後按一下「**啓動 (Start)**」。
10. 按一下 1 年期訂閱選項或 3 年期訂閱選項旁邊的「**購買 (Buy)**」。
11. 按一下「**結帳 (Checkout)**」。
12. 閱讀條款和條件，然後按一下「**接受 (Accept)**」。
13. 輸入您的帳單資訊，然後按一下「**繼續 (Continue)**」。
14. 輸入您的信用卡資訊，然後按一下「**付款 (Make Payment)**」。
15. 寫下您的優待券代碼，然後回到精靈中的「帳戶啓用 (Account Activation)」頁面。
16. 輸入您的帳戶啓用碼，然後按「**下一步 (Next)**」。
17. 當確認對話方塊開啓時，按一下「**確定 (OK)**」。

管理現有的線上復原帳戶

如果您遺失密碼，修改個人設定，重設線上復原帳戶所用的密碼，以及檢視或更新您的帳戶，那麼在建立線上復原帳戶之後，就可以存取 SafeBoot Recovery 服務網站來復原對電腦的存取權。

1. 開啟 Drive Encryption，然後按一下「**復原 (Recovery)**」。
2. 按一下「**管理 (Manage)**」。
3. 當「SafeBoot Recovery 服務 (SafeBoot Recovery Service)」網頁開啟時，按一下「**復原服務帳戶 (Recovery Service Account)**」或「**復原程序 (Recovery Process)**」。
4. 在復原服務登入頁面上，輸入您的電子郵件地址、密碼，以及在方塊中看到的數字和字母。
5. 按一下「**登入 (Logon)**」。
6. 按一下「**設定檔 (Profile)**」更新您的個人資訊，例如電話號碼或帳單地址。

   － 或 －

   按一下「**重設密碼 (Reset Password)**」重設或變更您的密碼。

   － 或 －

   按一下「**我的訂閱 (My Subscriptions)**」檢視您目前的訂閱資訊。

附註： 您也可以在「我的訂閱」頁面中更新您的訂閱。按一下「**更新訂閱 (Renew Subscription)**」執行這個動作。

執行復原

執行本機復原

1. 開啟電腦。
2. 插入存有您備份金鑰的抽取式存放裝置。
3. 當「Drive Encryption for HP ProtectTools」登入對話方塊開啟時，按一下「**取消 (Cancel)**」。
4. 按一下畫面左下角的「**選項 (Options)**」，然後按一下「**復原 (Recovery)**」。
5. 按一下「**本機復原 (Local recovery)**」，然後按「**下一步 (Next)**」。
6. 選取含有您備份金鑰的檔案，或按一下「**瀏覽 (Browse)**」搜尋該檔案，然後按「**下一步 (Next)**」。
7. 當確認對話方塊開啟時，按一下「**確定 (OK)**」。

   復原程序完成，同時您的電腦會啟動。

附註： 執行復原之後，強烈建議您重設密碼。

執行線上復原

附註： 本節說明當您可以存取有網際網路連線的其他電腦時，如何執行線上復原。如果您無法存取電腦，請與 HP 技術支援聯絡。

1. 開啟電腦。
2. 當「Drive Encryption for HP ProtectTools」登入對話方塊開啟時，按一下「**取消**」。

3. 按一下畫面左下角的「**選項 (Options)**」，然後按一下「**復原 (Recovery)**」。
4. 按一下「**Web 復原 (Web recovery)**」，然後按「**下一步 (Next)**」。
5. 記下用戶端程式碼，然後按「**下一步 (Next)**」。
6. 在有網際網路連線的其他電腦上，存取 SafeBoot Recovery 服務網站，網址爲：http://www.safeboot-hp.com。
7. 按一下「**復原程序 (Recovery Process)**」。
8. 在復原服務登入頁面上，輸入您的電子郵件地址、密碼，以及在方塊中看到的數字和字母。
9. 按一下「**登入 (Logon)**」。
10. 按一下「**復原程序 (Recovery Process)**」。
11. 輸入您從所要復原的電腦記下的用戶端程式碼，並且在方塊中輸入看到的數字和字母。
12. 按一下「**提交 (Submit)**」。
13. 記下回應金鑰的每一行。
14. 在所要復原的電腦上，輸入您從 SafeBoot Recovery 服務網站記下的第一行回應金鑰，然後按一下 **Enter**。
15. 輸入第二行回應金鑰，然後按一下 **Enter**。
16. 輸入第三行回應金鑰，然後按一下 **Enter**。
17. 輸入第四行回應金鑰，然後按一下 **Enter**。

    附註： 第四行回應金鑰會比前面三行金鑰來得短。
18. 按一下「**完成 (Finish)**」。

附註： 執行復原之後，強烈建議您重設密碼。

5 Privacy Manager for HP ProtectTools

Privacy Manager 是用於獲得授權憑證的工具，此憑證可在使用 Microsoft mail、Microsoft Office 文件及 Live Messenger 時驗證來源、完整性及通訊的安全性。

Privacy Manager 使用 HP ProtectTools Security Manager for Administrators 提供，包含下列安全登入法的安全性基礎架構：

- 指紋驗證
- Windows® 密碼
- HP ProtectTools Java™ 卡
- 虛擬權仗
- Embedded Security for HP ProtectTools 基本使用者金鑰

您可以在 Privacy Manager 中使用上述的任何安全登入法。

開啓 Privacy Manager

若要開啓 Privacy Manager：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**Privacy Manager：登入與聊天 (Sign and Chat)**」。

－ 或 －

在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，按一下「**Privacy Manager: 登入與聊天 (Sign and Chat)**」，然後按一下「**組態 (Configuration)**」。

－ 或 －

在 Microsoft Outlook 電子郵件訊息的工具列上，按一下「**安全地傳送 (Send Securely)**」旁邊的向下箭頭，然後按一下「**憑證管理員 (Certificate Manager)**」或「**受信任連絡人管理員 (Trusted Contact Manager)**」。

－ 或 －

在 Microsoft Office 文件的工具列上，按一下「**登入與加密 (Sign and Encrypt)**」旁邊的向下箭頭，然後按一下「**憑證管理員 (Certificate Manager)**」或「**受信任連絡人管理員 (Trusted Contact Manager)**」。

設定程序

管理 Privacy Manager 憑證

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

申請並安裝 Privacy Manager 憑證

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

申請 Privacy Manager 憑證

1. 開啓 Privacy Manager，並按一下「**憑證管理員 (Certificate Manager)**」。
2. 按一下「**申請 Privacy Manager 憑證 (Privacy Manager Certificate)**」。
3. 閱讀「歡迎 (Welcome)」頁面中的文字，然後按「**下一步 (Next)**」。
4. 閱讀「授權合約 (License Agreement)」頁面中的授權合約。
5. 務必選取「**勾選此處以接受此授權合約的條款 (Check here to accept the terms of this license agreement)**」旁邊的核取方塊，然後按「**下一步 (Next)**」。
6. 在「您的憑證詳細資料」頁面中輸入必要的資訊，然後按「**下一步 (Next)**」。
7. 在「已接受憑證要求 (Certificate Request Accepted)」頁面中按一下「**完成 (Finish)**」。

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

安裝 Privacy Manager 憑證

1. 當您收到附加 Privacy Manager 憑證的電子郵件後，開啓此電子郵件，並按一下郵件右下角的「**設定 (Setup)**」按鈕。
2. 使用您選擇的安全登入法進行驗證。
3. 在「已安裝憑證 (Certificate Installed)」頁面中按「**下一步 (Next)**」。
4. 在「憑證備份 (Certificate Backup)」頁面中輸入備份檔案的位置及名稱，或者按一下「**瀏覽 (Browse)**」以搜尋位置。

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

5. 輸入並確認密碼，然後按「**下一步 (Next)**」。
6. 使用您選擇的安全登入法進行驗證。
7. 如果您選擇開始進行「信任的連絡人 (Trusted Contact)」邀請程序，請依照螢幕上的指示進行。

   － 或 －

如果您按「取消 (Cancel)」，稍後請參閱「管理信任的連絡人 (anaging Trusted Contacts)」以取得新增「信任的連絡人 (Trusted Contact)」的相關資訊。

檢視 Privacy Manager 憑證詳細資料

1. 開啓 Privacy Manager，並按一下「**憑證管理員 (Certificate Manager)**」。
2. 按一下「**Privacy Manager 憑證 (Privacy Manager Certificate)**」。
3. 按一下「**憑證詳細資料 (Certificate details)**」。
4. 當您檢視完詳細資料後，按一下「**確定 (OK)**」。

更新 Privacy Manager 憑證

當 Privacy Manager 憑證即將到期時，您會收到更新通知：

1. 開啓 Privacy Manager，並按一下「**憑證管理員 (Certificate Manager)**」。
2. 按一下「**Privacy Manager 憑證 (Privacy Manager Certificate)**」。
3. 按一下「**更新憑證 (Renew certificate)**」。
4. 請依照螢幕上的指示，購買新的 Privacy Manager 憑證。

附註： Privacy Manager 憑證更新程序不會取代舊的 Privacy Manager 憑證。您需要購買新的 Privacy Manager 憑證，並使用如「申請並安裝 Privacy Manager 憑證」一節所述之程序來安裝。

設定預設的 Privacy Manager 憑證

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

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

1. 開啓 Privacy Manager，並按一下「**憑證管理員 (Certificate Manager)**」。
2. 按一下要當作預設值使用的 Privacy Manager 憑證，然後按一下「**設定預設值 (Set default)**」。
3. 按一下「**確定 (OK)**」。

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

刪除 Privacy Manager 憑證

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

若要刪除 Privacy Manager 憑證：

1. 開啓 Privacy Manager，並按一下「**憑證管理員 (Certificate Manager)**」。
2. 按一下您要刪除的 Privacy Manager 憑證，然後按一下「**進階 (Advanced)**」。
3. 按一下「**刪除 (Delete)**」。

4. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。
5. 按一下「**關閉 (Close)**」，然後按一下「**套用 (Apply)**」。

還原 Privacy Manager 憑證

如果不小心刪除了 Privacy Manager 憑證，您可以使用安裝或匯出憑證時所建立的備份檔案加以還原：

1. 開啓 Privacy Manager，並按一下「**移轉 (Migration)**」。
2. 按一下「**匯入移轉檔案 (Import migration file)**」。
3. 按一下「移轉檔案 (Migration File)」頁面中，按一下「**瀏覽 (Browse)**」以搜尋您安裝或匯出 Privacy Manager 憑證時所建立的 .dppsm 檔，然後按「**下一步 (Next)**」。
4. 在「移轉檔案匯入」頁面中按一下「**完成 (Finish)**」。
5. 按一下「**關閉 (Close)**」，然後按一下「**套用 (Apply)**」。

附註： 請參閱「安裝 Privacy Manager 憑證」或「匯出 Privacy Manager 憑證 (Exporting Privacy Manager Certificates)」和「信任的連絡人(Trusted Contacts)」以取得更多資訊。

撤銷 Privacy Manager 憑證

如果您對 Privacy Manager 憑證的安全性已經產生疑慮，您可以撤銷自己的憑證：

附註： 撤銷的 Privacy Manager 憑證並不會被刪除。該憑證仍可用來檢視加密的檔案。

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

管理信任的連絡人

「信任的連絡人 (Trusted Contacts)」是與您交換 Privacy Manager 憑證的使用者，您可以與他們安全地相互通訊。

新增信任的連絡人

1. 首先，傳送一封電子郵件邀請函給「信任的連絡人 (Trusted Contact)」收件者。
2. 「信任的連絡人 (Trusted Contact)」收件者回應此電子郵件。
3. 您收到「信任的連絡人 (Trusted Contact)」收件者的電子郵件回應，然後按一下「接受 (Accept)」。

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

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

新增信任的連絡人

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

   － 或 －

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

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

3. 當出現「信任的連絡人邀請 (Trusted Contact Invitation)」對話方塊時，請閱讀文字，然後按一下「**確定 (OK)**」。

   接著將自動產生一封電子郵件。

4. 輸入一個或多個您要新增爲「信任的連絡人 (Trusted Contacts)」的收件者電子郵件地址。

5. 編輯文字，並簽署您的名字（選用）。

6. 按一下「**傳送 (Send)**」。

   附註： 如果您尚未取得 Privacy Manager 憑證，將有郵件通知您必須具有 Privacy Manager 憑證才能傳送「信任的連絡人 (Trusted Contact)」要求。按一下「確定 (OK)」以啓動「憑證要求精靈」。

7. 使用您選擇的安全登入法進行驗證。

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

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

9. 按一下「**確定 (OK)**」。

使用 Microsoft Outlook 通訊錄新增信任的連絡人

1. 啓動 Privacy Manager，按一下「**信任的聯絡人管理員 (Trusted Contacts Manager)**」，然後按一下「**邀請聯絡人 (Invite Contacts)**」。

   － 或 －

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

2. 當「信任的連絡人邀請 (Trusted Contact Invitation)」頁面開啓時，選擇您要新增爲「信任的連絡人 (Trusted Contacts)」的收件者電子郵件地址，然後按「**下一步 (Next)**」。

3. 當「傳送邀請 (Sending Invitation)」頁面開啓時，按一下「**完成 (Finish)**」。

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

4. 編輯文字，並簽署您的名字（選用）。
5. 按一下「**傳送 (Send)**」。

附註： 如果您尚未取得 Privacy Manager 憑證，將有郵件通知您必須具有 Privacy Manager 憑證才能傳送「信任的連絡人 (Trusted Contact)」要求。按一下「**確定 (OK)**」以啓動「憑證要求精靈 (Certificate Request Wizard)」。

6. 使用您選擇的安全登入法進行驗證。

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

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

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

8. 按一下「**確定 (OK)**」。

檢視信任的連絡人詳細資料

1. 開啓 Privacy Manager，並按一下「**受信任連絡人管理員 (Trusted Contacts Manager)**」。
2. 按一下「信任的連絡人 (Trusted Contact)」。
3. 按一下「**連絡人詳細資料 (Contact details)**」。
4. 當您檢視完詳細資料後，按一下「**確定 (OK)**」。

刪除信任的連絡人

1. 開啓 Privacy Manager，並按一下「**受信任連絡人管理員 (Trusted Contacts Manager)**」。
2. 按一下要刪除的「信任的連絡人 (Trusted Contact)」。
3. 按一下「**刪除連絡人 (Delete contact)**」。
4. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

檢查信任的連絡人的撤銷狀態

1. 開啓 Privacy Manager，並按一下「**受信任連絡人管理員 (Trusted Contacts Manager)**」。
2. 按一下「信任的連絡人 (Trusted Contact)」。
3. 按一下「**進階 (Advanced)**」按鈕。

   「進階的受信任連絡人管理 (Advanced Trusted Contact Management)」對話方塊便會開啓。

4. 按一下「**檢查撤銷 (Check Revocation)**」。
5. 按一下「**關閉 (Close)**」。

一般工作

在 Microsoft Office 中使用 Privacy Manager

安裝 Privacy Manager 憑證後，「簽署與加密」按鈕會顯示在所有 Microsoft Word、Microsoft Excel 和 Microsoft PowerPoint 文件的工具列右邊。

在 Microsoft Office 文件中設定 Privacy Manager

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

－ 或 －

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

   － 或 －

   在 Microsoft Office 文件的工具列上，按一下「**簽署與加密 (Sign and Encrypt)**」旁邊的向下箭頭，然後按一下「**設定 (Settings)**」。
2. 選取您要設定的動作，然後按一下「**確定 (OK)**」。

簽署 Microsoft Office 文件

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

如果您稍後決定要編輯此文件，請依照下列步驟進行：

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

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

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

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

附註： 選取這個選項後，「在簽署前新增簽章線 (Add Signature Line Before Signing)」旁邊會顯示核取標記。預設情況下，這個選項爲啓用。

4. 按一下「**簽署與加密 (Sign and Encrypt)**」旁邊的向下箭頭，然後按一下「**簽署文件 (Sign Document)**」。

5. 使用您選擇的安全登入法進行驗證。

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

您可以藉由指定建議的簽署者新增一個以上的簽章線至文件中。建議的簽署者是由 Microsoft Word 或 Microsoft Excel 文件的所有人指定，新增簽章線至文件中的使用者。建議的簽署者可以是您或是另一位您要其簽署文件的人。例如，如果您準備的文件需要由部門的所有成員簽署，您可以爲那些使用者將簽章線加在文件的最後一頁底部，並附上在指定日期簽署的說明。

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

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

2. 按一下「**插入 (Insert)**」功能表。

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

   「簽章設定 (Signature Setup)」對話方塊便會開啓。

4. 在「**建議的簽署者 (Suggested signer)**」底下的方塊中，輸入建議的簽署者姓名。

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

附註： 此訊息將出現在職稱處，當文件一經簽署，此訊息會被刪除或被使用者的職稱取代。

6. 選取「**在簽章線顯示簽署日期 (Show sign date in signature line)**」核取方塊以顯示日期。

7. 選取「**在簽章線顯示簽署者職稱 (Show signers title in signature line)**」核取方塊以顯示職稱。

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

8. 按一下「**確定 (OK)**」。

新增建議的簽署者的簽章線

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

若要簽署文件：

1. 在適當的簽章線上連按兩下。

2. 使用您選擇的安全登入法進行驗證。

   簽章線將根據文件所有人所指定的設定顯示。

加密 Microsoft Office 文件

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

若要加密 Microsoft Office 文件：

1. 在 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 中，建立並儲存文件。
2. 按一下「**首頁 (Home)**」功能表。
3. 按一下「**簽署與加密 (Sign and Encrypt)**」旁邊的向下箭頭，然後按一下「**加密文件**」。

   「選取信任的連絡人 (Select Trusted Contacts)」對話方塊便會開啓。
4. 按一下能夠開啓文件並檢視其內容之「信任的連絡人 (Trusted Contact)」姓名。

   附註： 若要選取多個「信任的連絡人 (Trusted Contact)」姓名，請按住 Ctrl 鍵並按一下個別名稱。
5. 按一下「**確定 (OK)**」。
6. 使用您選擇的安全登入法進行驗證。

如果您稍後決定要編輯此文件，請依照「**簽署 Microsoft Office 文件 (Signing a Microsoft Office Document)**」所示的步驟進行。移除加密後，您就可以編輯文件了。請依照本章節所述之步驟，再次加密文件。

從 Microsoft Office 文件中移除加密

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

若要從 Microsoft Office 文件中移除加密：

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

傳送加密的 Microsoft Office 文件

您可以將已加密的 Microsoft Office 文件附加於電子郵件訊息中，無需簽署或加密電子郵件本身。若要這麼做，只要依照通常傳送一般帶有附件的電子郵件的方式，建立並傳送帶有簽署或加密文件的電子郵件即可。

然而，爲了最佳安全性起見，建議您在附加簽署或加密的 Microsoft Office 文件時，也加密該電子郵件。

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

1. 在 Microsoft Outlook 中，按一下「**新增 (New)**」或「**回覆 (Reply)**」。
2. 輸入您的電子郵件訊息。
3. 附加 Microsoft Office 文件。
4. 請參閱「密封並傳送電子郵件訊息」以取得進一步指示。

檢視簽署的 Microsoft Office 文件

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

在開啓已簽署的 Microsoft Office 文件後，「簽章」對話方塊便會在文件旁邊開啓，顯示簽署此文件的使用者姓名和簽署日期。您可以在姓名上按一下滑鼠右鍵以檢視其他詳細資料。

檢視加密的 Microsoft Office 文件

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

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

在 Microsoft Outlook 中使用 Privacy Manager

安裝 Privacy Manager 後，「隱私權 (Privacy)」按鈕會顯示在 Microsoft Outlook 工具列上，同時「安全地傳送 (Send Securely)」按鈕也會顯示在每一封 Microsoft Outlook 電子郵件訊息的工具列上。

爲 Microsoft Outlook 設定 Privacy Manager

1. 開啓 **Privacy Manager**，按一下「**設定 (Settings)**」，然後按一下「**電子郵件 (E-mail)**」標籤。

   － 或 －

   在 Microsoft Outlook 的主工具列上，按一下「**隱私權 (Privacy)**」旁邊的向下箭頭，然後按一下「**設定 (Settings)**」。

   － 或 －

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

2. 選取您在傳送安全的電子郵件時執行的動作，然後按一下「**確定 (OK)**」。

簽署與傳送電子郵件訊息

- 在 Microsoft Outlook 中，按一下「**新增 (New)**」或「**回覆 (Reply)**」。
- 輸入您的電子郵件訊息。
- 按一下「**安全地傳送 (Send Securely)**」旁邊的向下箭頭，然後按一下「**簽署與傳送 (Sign and Send)**」。
- 使用您選擇的安全登入法進行驗證。

密封並傳送電子郵件訊息

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

若要密封並傳送電子郵件訊息給「信任的連絡人 (Trusted Contact)」：

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

3. 按一下「**安全地傳送 (Send Securely)**」旁邊的向下箭頭，然後按一下「**爲信任的連絡人密封並傳送 (Seal for Trusted Contacts and Send)**」。

4. 使用您選擇的安全登入法進行驗證。

檢視密封的電子郵件訊息

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

- 使用哪一種認證來驗證簽署這封電子郵件者的身份
- 用來驗證簽署這封電子郵件者之認證的產品

在 Windows Live Messenger 中使用 Privacy Manager

新增 Privacy Manager Chat 活動

若要將 Privacy Manager 聊天功能新增至 Windows Live Messenger，請依照下列步驟進行：

1. 登入 Windows Live 首頁。
2. 按一下「**Windows Live**」圖示，然後按一下「**Windows Live 服務 (Windows Live Services)**」。
3. 按一下「**藝廊 (Gallery)**」，然後按一下「**Messenger**」。
4. 按一下「**活動 (Activities)**」，然後按一下「**安全與安全性 (Safety and Security)**」。
5. 依照螢幕上的指示，按一下「**Privacy Manager Chat**」。

啓動 Privacy Manager Chat

附註： 爲了使用 Privacy Manager Chat，雙方均須安裝 Privacy Manager 和 Privacy Manager 憑證。如需安裝 Privacy Manager 憑證的詳細資訊，請參閱第 5 頁的「申請並安裝 Privacy Manager 憑證」。

1. 若要在 Windows Live Messenger 中啓動 Privacy Manager Chat，請執行下列任何一個程序：

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

   b. 按一下「**啓動 Privacy Manager Chat (Start Privacy Manager Chat)**」。

   － 或 －

   a. 連按兩下 Live Messenger 中的線上連絡人，然後按一下「**交談 (Conversation)**」功能表。

   b. 按一下「**動作**」然後按一下「**啓動 Privacy Manager Chat (Start Privacy Manager Chat)**」。

   Privacy Manager 會傳送邀請給連絡人，以啓動 Privacy Manager Chat。當受邀的連絡人接受後，Privacy Manager Chat 視窗就會開啓。如果受邀的連絡人沒有 Privacy Manager，就會出現提示要求其下載。

2. 按一下「**啓動 (Start)**」以開始安全聊天。

爲 Windows Live Messenger 設定 Privacy Manager Chat

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

   － 或 －

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

   － 或 －

   在 Privacy Manager 記錄檢視器中，按一下「**設定 (Settings)**」按鈕。

2. 若要指定 Privacy Manager Chat 在鎖定您的工作階段前等候的時間，請由「**處於不活動狀態 _ 分鐘後 (after _ minutes of inactivity)**」鎖定工作階段的方塊中選取一個數字。

3. 若要爲您的聊天工作階段指定記錄資料夾，按一下「**瀏覽 (Browse)**」以搜尋資料夾，然後按一下「**確定 (OK)**」。

4. 若要在關閉前先自動加密並儲存您的工作階段，請選取「**自動儲存安全聊天記錄 (Automatically save secure chat history)**」核取方塊。

5. 按一下「**確定 (OK)**」。

在 Privacy Manager Chat 視窗中聊天

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

- **儲存 (Save)** – 按一下此按鈕可以將您的聊天工作階段儲存到組態設定中所指定的資料夾。您還可以設定 Privacy Manager Chat 在關閉時自動儲存各個工作階段。
- **隱藏全部 (Hide all)**及**顯示全部 (Show all)** – 按一下適當的按鈕可以展開或摺疊顯示在「安全通訊 (Secure Communications)」視窗中的訊息。您也可以按一下訊息標頭來隱藏或顯示個別訊息。
- **您在嗎？(Are you there?)** – 按一下此按鈕可以要求聯絡人的驗證。
- **鎖定 (Lock)** – 按一下此按鈕可以關閉 Privacy Manager Chat 視窗並回到「聊天項目 (Privacy Manager Chat)」視窗。若要再次顯示「安全通訊 (Secure Communications)」視窗，按一下「**繼續工作階段 (Resume the session)**，然後使用您選擇的安全登入法進行驗證。
- **傳送 (Send)** – 按一下此按鈕可以傳送加密的訊息給您的聯絡人。
- **傳送簽署 (Send signed)** – 選擇此核取方塊可以電子簽署並加密您的訊息。如果此郵件被竄改，則當收件者收到時，郵件將標示爲無效。每次傳送簽署的郵件時都必須驗證。
- **傳送隱藏 (Send hidden)** – 選擇此核取方塊可以加密並傳送只顯示訊息標題的訊息。您的連絡人必須驗證才能閱讀訊息內容。

檢視聊天記錄

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

啓動聊天記錄檢視器

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**Privacy Manager：登入與聊天 (Sign and Chat)**」，然後按一下「**聊天記錄檢視器 (Chat History Viewer)**」。

   － 或 －

   ▲ 在「聊天 (Chat)」工作階段，按一下「**記錄檢視器 (History Viewer)**」或「**記錄 (History)**」。

   － 或 －

   ▲ 在「聊天設定 (Chat Configuration)」頁面中，按一下「**啓動 Live Messenger 記錄檢視器 (Start Live Messenger History Viewer)**」。

顯現所有工作階段

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

1. 在「聊天記錄檢視器 (Chat History Viewer)」中，在任何工作階段上按一下滑鼠右鍵，然後選取「**顯現所有工作階段 (Reveal All Sessions)**」。
2. 使用您選擇的安全登入法進行驗證。

   「連絡人螢幕名稱 (Contact Screen Name)」已經過解密。
3. 在任何工作階段上連按兩下，即可檢視其內容。

爲指定帳戶顯現工作階段

顯現工作階段會顯示目前所選取工作階段之已解密「連絡人螢幕名稱 (Contact Screen Name)」。

1. 在「聊天記錄檢視器」中，在任何工作階段上按一下滑鼠右鍵，然後選取「**顯現工作階段 (Reveal Session)**」。
2. 使用您選擇的安全登入法進行驗證。

   「連絡人螢幕名稱 (Contact Screen Names)」已經過解密。
3. 在顯現的工作階段上連按兩下，即可檢視其內容。

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

檢視工作階段 ID

▲ 在「聊天記錄檢視 (Chat History View)」中，在任何已顯現的工作階段上按一下滑鼠右鍵，然後選取「**檢視工作階段 ID (View session ID)**」。

檢視工作階段

檢視工作階段會開啓供檢視的檔案。如果工作階段先前尚未顯現（顯示解密的連絡人螢幕名稱），則會同時顯現工作階段。

1. 在「聊天記錄檢視器」中，在任何顯現的工作階段上按一下滑鼠右鍵，然後選取「**檢視 (View)**」。
2. 如果出現提示，請使用您選擇的安全登入法進行驗證。

   工作階段內容已經過解密。

搜尋工作階段的特定文字

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

1. 在「聊天記錄檢視器 (Chat History Viewer)」中，按一下「**搜尋 (Search)**」按鈕。
2. 輸入搜尋文字，設定任何需要的搜尋參數，然後按一下「**確定 (OK)**」。

   包含文字的工作階段會在檢視器視窗中反白顯示。

刪除工作階段

1. 選取聊天記錄工作階段。
2. 按一下「**刪除 (Delete)**」。

新增或移除欄位

預設情況下，最常使用的 3 個欄位會顯示在「聊天記錄檢視器 (Chat History Viewer)」中。您可以新增其他欄位到顯示畫面，也可以由顯示畫面移除欄位。

若要新增欄位到顯示畫面：

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

若要從顯示畫面移除欄位：

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

篩選顯示的工作階段

在「聊天記錄檢視器」中顯示一份所有帳戶的工作階段清單。

顯示特定帳戶的工作階段

▲ 在「聊天記錄檢視器」中，從「**顯示下列所屬的記錄 (Display history for)**」功能表選取帳戶。

顯示某日期範圍的工作階段

1. 在「聊天記錄檢視 (Chat History View)」中，按一下「**進階篩選 (Advanced Filter)**」圖示。

   「進階篩選 (Advanced Filter)」對話方塊便會開啓。
2. 選取「**僅顯示指定日期範圍內的工作階段 (Display only sessions within specified date range)**」核取方塊。

3. 在「**開始日期 (From date)**」和「**結束日期 (To date)**」方塊中，輸入日、月和/或年，或者按一下行事曆旁邊的向下箭頭以選取日期。

4. 按一下「**確定 (OK)**」。

顯示儲存在預設資料夾以外之資料夾中的工作階段

1. 在「聊天記錄檢視 (Chat History View)」中，按一下「**進階篩選 (Advanced Filter)**」圖示。

2. 選取「**使用替代記錄檔案資料夾 (Use an alternate history files folder)**」核取方塊。

3. 輸入資料夾位置，或者按一下「**瀏覽 (Browse)**」以搜尋資料夾。

4. 按一下「**確定 (OK)**」。

進階工作

移轉 Privacy Manager 憑證和信任的連絡人至不同電腦

您可以安全地移轉 Privacy Manager 憑證和信任的連絡人至不同電腦。若要這麼做，請將它們當成有密碼保護的檔案，匯出至網路位置或任何抽取式存放裝置，然後將檔案匯入新電腦。

匯出 Privacy Manager 憑證和信任的連絡人

您可以依照下列步驟，匯出 Privacy Manager 憑證和信任的連絡人至密碼保護的檔案：

1. 開啓 Privacy Manager，並按一下「**移轉 (Migration)**」。
2. 按一下「**匯出移轉檔案 (Export migration file)**」。
3. 在「選取資料」頁面中，選擇要包括在移轉檔案中的資料類別，然後按「**下一步 (Next)**」。
4. 在「移轉檔案」頁面中，輸入檔名或按一下「**瀏覽 (Browse)**」以搜尋位置，然後按「**下一步 (Next)**」。
5. 輸入並確認密碼，然後按「**下一步 (Next)**」。

附註： 將此密碼儲存在安全處所，因爲當您匯入移轉檔案時將需要此檔案。

6. 使用您選擇的安全登入法進行驗證。
7. 在「移轉檔案儲存 (Migration File Saved)」頁面中按一下「**完成 (Finish)**」。

匯入 Privacy Manager 憑證和信任的連絡人

您可以依照下列步驟，匯入 Privacy Manager 憑證和信任的連絡人至密碼保護的檔案：

1. 開啓 Privacy Manager，並按一下「**移轉 (Migration)**」。
2. 按一下「**匯入移轉檔案 (Import migration file)**」。
3. 在「選取資料 (Select Data)」頁面中，選擇要包括在移轉檔案中的資料類別，然後按「**下一步 (Next)**」。
4. 在「移轉檔案 (Migration File)」頁面中，輸入檔名或按一下「**瀏覽 (Browse)**」以搜尋位置，然後按「**下一步 (Next)**」。
5. 在「移轉檔案匯入 (Migration File Import)」頁面中按一下「**完成 (Finish)**」。

6 File Sanitizer for HP ProtectTools

File Sanitizer 是可供您安全地拆解電腦上的資產（個人資訊或檔案、記錄或 Web 相關資料或其他資料元件），並且定期清理硬碟的工具。

附註： File Sanitizer 目前只能在硬碟上作業。

關於拆解

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

拆解不同於標準的 Windows® 刪除方式（在 File Sanitizer 中又叫做單純刪除），因爲當您拆解資產時，會叫用模糊資料的演算法，以免他人取得原始資產。

當您選擇一種拆解設定檔（高安全性、中安全性或低安全性），會自動選用一個適用於拆解的預先定義資產清單及清除方法。您也可以自訂拆解設定檔，讓您指定拆解週期的數目，哪些資產需要拆解，哪些資產拆解前需要先確認，以及哪些資產不必拆解等等。

您可以設定自動拆解排程，也可以隨時手動拆解資產。

關於可用空間清理

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

附註： 可用空間清理功能適用於使用 Windows「資源回收筒」刪除或手動刪除的資產。可用空間清理並未對已拆解的資產提供額外的安全性。

您可以設定自動可用空間清理排程，或者使用工作列最右邊通知區中的「HP ProtectTools」圖示，啓動可用空間清理功能。

設定程序

開啓 File Sanitizer

若要開啓 File Sanitizer：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 按一下「**File Sanitizer**」。

－ 或 －

- 在「**File Sanitizer**」圖示上連按兩下。

－ 或 －

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

設定可用空間清理排程

附註： 可用空間清理功能適用於使用 Windows「資源回收筒」刪除或手動刪除的資產。可用空間清理並未對已拆解的資產提供額外的安全性。

若要設定可用空間清理排程：

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

附註： 可用空間清理作業可能需要很長的時間。即使在背景中執行可用空間清理，您的電腦還是可能因爲處理器使用量增加而執行速度變慢。

選取或建立拆解設定檔

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

選取預先定義的拆解設定檔

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

若要選取預先定義的拆解設定檔：

1. 開啓 **File Sanitizer**，然後按一下「**設定 (Settings)**」。
2. 按一下預先定義的拆解設定檔。
3. 按一下「**檢視詳細資料 (View Details)**」以檢視所選取要拆解的資產清單。

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

5. 按一下「**套用**」，然後按一下「**確定**」。

自訂拆解設定檔

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

1. 開啓 File Sanitizer，按一下「**設定 (Settings)**」，按一下「**進階安全性設定 (Advanced Security Settings)**」，然後按一下「**檢視詳細資料 (View Details)**」。

2. 指定拆解週期的數目。

附註： 各項資產會執行所選取的拆解週期數目。例如，如果您選擇 3 個拆解週期，則模糊資料的演算法會分 3 次執行。如果您選擇較高安全性的拆解週期，可能要耗費很長的時間進行拆解；然而，您指定的拆解週期數目越高，電腦就越安全。

3. 選取您要拆解的資產：

   a. 在「**可用的拆解選項 (Available shred options)**」下方，按一下該資產，然後按一下「**新增 (Add)**」。

   b. 若要新增自訂資產，按一下「新增自訂選項」，輸入檔案名稱或資料夾名稱，然後按一下「**確定 (OK)**」。按一下自訂資產，然後按一下「**新增 (Add)**」。

   附註： 若要從可用拆解選項中刪除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

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

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

5. 在「**請勿拆解下列項目 (Do not shred the following)**」下方，按一下「**新增 (Add)**」以選取您要排除在拆解之外的特定資產。

附註： 只有副檔名能排除在拆解之外。例如，如果您新增 .BMP 副檔名，則所有具有 .BMP 副檔名的檔案，都將排除在拆解之外。

若要從排除清單中移除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

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

自訂單純刪除設定檔

單純刪除設定檔執行標準資產刪除而不拆解。在您自訂單純刪除設定檔後，也指定了哪些資產包含在單純刪除中，哪些資產在執行單純刪除前要經過確認，以及哪些資產要從單純刪除中排除：

附註： 如果使用單純刪除，強烈建議您定期執行可用空間清理。

1. 開啓 **File Sanitizer**，按一下「**設定 (Settings)**」，按一下「**單純刪除設定 (Simple Delete Setting)**」，然後按一下「**檢視詳細資料 (View Details)**」。
2. 選取您要刪除的資產：
   a. 在「**可用的刪除選項 (Available delete options)**」下方，按一下該資產，然後按一下「**新增 (Add)**」。
   b. 若要新增自訂資產，按一下「**新增自訂選項 (Add Custom Option)**」，輸入檔案名稱或資料夾名稱，然後按一下「**確定 (OK)**」。按一下自訂資產，然後按一下「**新增 (Add)**」。

   附註： 若要從可用刪除選項中刪除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。
3. 在「**刪除下列項目 (Delete the following)**」下方，選取在您要在刪除前做確定的各項資產旁邊的核取方塊。

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

4. 在「**請勿拆解下列項目 (Do not shred the following)**」下方，按一下「**新增 (Add)**」以選取您要排除在刪除之外的特定資產。

附註： 只有副檔名可以排除在刪除之外。例如，如果您新增 .BMP 副檔名，則所有具有 .BMP 副檔名的檔案，都將排除在刪除之外。

若要從排除清單中移除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

5. 您完成設定單純刪除設定檔後，按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

設定銷毀排程

1. 開啓 File Sanitizer，按一下「**拆解 (Shred)**」。
2. 選取拆解選項：
   - **Windows 啓動 (Windows startup)** — 選擇此選項可以在 Windows 啓動時拆解所有選取的資產。
   - **Windows 關閉 (Windows shutdown)** — 選擇此選項可以在 Windows 關閉時拆解所有選取的資產。

     附註： 選取此選項後，在關機時會出現對話方塊，詢問您是否要繼續拆解選取的資產，或者要略過這個程序。按一下「是 (Yes)」以略過拆解程序，或者按一下「否 (No)」以繼續進行拆解。
   - **Web 瀏覽器開啓 (Web browser open)** — 選擇此選項可以在您開啓 Web 瀏覽器時拆解所有選取的 Web 相關資產，例如瀏覽器 URL 歷程記錄。
   - **Web 瀏覽器關閉 (Web browser quit)** — 選擇此選項可以在您關閉 Web 瀏覽器時拆解所有選取的 Web 相關資產，例如瀏覽器 URL 歷程記錄。
   - **排程器 (Scheduler)** — 選取「啓動排程器 (Activate Scheduler)」核取方塊，輸入您的 Windows 密碼，然後輸入拆解選取資產的日期和時間。
3. 按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

設定可用空間清理排程

附註： 可用空間清理功能適用於使用 Windows「資源回收筒」刪除或手動刪除的資產。可用空間清理並未對已拆解的資產提供額外的安全性。

若要設定可用空間清理排程：

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

附註： 可用空間清理作業可能需要很長的時間。即使在背景中執行可用空間清理，您的電腦還是可能因爲處理器使用量增加而執行速度變慢。

選取或建立拆解設定檔

選取預先定義的拆解設定檔

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

若要選取預先定義的拆解設定檔：

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

自訂拆解設定檔

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

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

附註： 各項資產會執行所選取的拆解週期數目。例如，如果您選擇 3 個拆解週期，則模糊資料的演算法會分 3 次執行。如果您選擇較高安全性的拆解週期，可能要耗費很長的時間進行拆解；然而，您指定的拆解週期數目越高，電腦就越安全。

3. 選取您要拆解的資產：

   a. 在「**可用的拆解選項 (Available shred options)**」下方，按一下該資產，然後按一下「**新增 (Add)**」。

   b. 若要新增自訂資產，按一下「新增自訂選項 (Add Custom Option)」，輸入檔案名稱或資料夾名稱，然後按一下「**確定 (OK)**」。按一下自訂資產，然後按一下「**新增 (Add)**」。

   附註： 若要從可用拆解選項中刪除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

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

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

5. 在「**請勿拆解下列項目 (Do not shred the following)**」下方，按一下「**新增 (Add)**」以選取您要排除在拆解之外的特定資產。

附註： 只有副檔名能排除在拆解之外。例如，如果您新增 .BMP 副檔名，則所有具有 .BMP 副檔名的檔案，都將排除在拆解之外。

若要從排除清單中移除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

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

自訂單純刪除設定檔

單純刪除設定檔執行標準資產刪除而不拆解。在您自訂單純刪除設定檔後，也指定了哪些資產包含在單純刪除中，哪些資產在執行單純刪除前要經過確認，以及哪些資產要從單純刪除中排除：

附註： 如果使用單純刪除，強烈建議您定期執行可用空間清理。

1. 開啓 **File Sanitizer**，按一下「**設定 (Settings)**」，按一下「**單純刪除設定 (Simple Delete Setting)**」，然後按一下「**檢視詳細資料 (View Details)**」。

2. 選取您要刪除的資產：

   - 在「**可用的刪除選項 (Available delete options)**」下方，按一下該資產，然後按一下「**新增 (Add)**」。

   - 若要新增自訂資產，按一下「**新增自訂選項 (Add Custom Option)**」，輸入檔案名稱或資料夾名稱，然後按一下「**確定 (OK)**」。按一下自訂資產，然後按一下「**新增 (Add)**」。

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

3. 在「**刪除下列項目 (Delete the following)**」下方，選取在您要在刪除前做確定的各項資產旁邊的核取方塊。

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

4. 在「**請勿刪除下列項目 (Do not delete the following)**」下方，按一下「**新增 (Add)**」以選取您要排除在刪除之外的特定資產。

附註： 只有副檔名可以排除在刪除之外。例如，如果您新增 .BMP 副檔名，則所有具有 .BMP 副檔名的檔案，都將排除在刪除之外。

若要從排除清單中移除資產，按一下該資產，然後按一下「**刪除 (Delete)**」。

5. 您完成設定單純刪除設定檔後，按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

一般工作

使用按鍵順序啓動拆解

若要要指定按鍵順序，請依照下列步驟執行：

1. 開啓 **File Sanitizer**，按一下「**拆解 (Shred)**」。
2. 選取「**按鍵順序 (Key sequence)**」核取方塊。
3. 在可用方塊中輸入字元，然後選取「**CTRL**」、「**ALT**」或「**SHIFT**」方塊，或者三個都選。

   例如，若要使用 S 鍵和 Ctrl+Shift 鍵，在方塊中輸入 S，然後選取「**Ctrl**」和「**Shift**」選項。

附註： 請確定選取的按鍵順序與您已經設定的其他按鍵順序不同。

若要使用按鍵順序啓動拆解：

1. 按下選擇的字元時，按住 Ctrl、Alt 或 Shift 鍵（或任何您指定的組合鍵）。
2. 如果確認對話方塊開啓，請按一下「**是 (Yes)**」。

使用 File Sanitizer 圖示

△ 注意： 拆解過的資產無法復原。選取哪些項目要進行手動拆解前請仔細考慮。

1. 瀏覽至您要拆解的文件或資料夾。
2. 將資產拖曳至桌面上的 File Sanitizer 圖示。
3. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。
4. 按一下「**是 (Yes)**」以確認您要移除所選的使用者。

手動拆解一項資產

△ 注意： 拆解過的資產無法復原。選取哪些項目要進行手動拆解前請仔細考慮。

1. 在工作列最右邊通知區中的「**HP ProtectTools**」圖示上按一下滑鼠右鍵，按一下「**File Sanitizer**」，然後按一下「**拆解一項 (Shred One)**」。
2. 當「瀏覽」對話方塊開啓時，請瀏覽至您想拆解的資產，然後按一下「**確定 (OK)**」。

附註： 您選取的資產可爲單一檔案或資料夾。

3. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

－ 或 －

1. 在桌面的「**File Sanitizer**」圖示上按一下滑鼠右鍵，然後按一下「**拆解一項 (Shred One)**」。
2. 當「瀏覽」對話方塊開啓時，請瀏覽至您想拆解的資產，然後按一下「**確定 (OK)**」。
3. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

－ 或 －

1. 開啓 File Sanitizer，按一下「**拆解 (Shred)**」。
2. 按一下「**瀏覽 (Browse)**」按鈕。
3. 當「瀏覽」對話方塊開啓時，請瀏覽至您想拆解的資產，然後按一下「**確定 (OK)**」。
4. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

手動拆解所有選取的項目

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

－ 或 －

1. 在桌面的「**File Sanitizer**」圖示上按一下滑鼠右鍵，然後按一下「**立即拆解 (Shred Now)**」。
2. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

手動啓動可用空間清理

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

－ 或 －

1. 開啓 File Sanitizer，按一下「**可用空間清理 (Free Space Bleaching)**」。
2. 按一下「**立即清理 (Bleach Now)**」。
3. 當確認對話方塊開啓時，按一下「**是 (Yes)**」。

中止拆解或可用空間清理作業

當銷毀或釋放空間的整理作業正在進行時，會在通知區域的 HP ProtectTools Security Manager for Administrators 圖示上方顯示一個訊息。訊息會提供銷毀或釋放空間的整理過程的詳細資訊（完成百分比），並讓您有放棄作業的選擇。

若要中止作業：

▲ 按一下訊息，然後按一下「**停止 (Stop)**」以取消作業。

檢視記錄檔

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

附註： 成功拆解或清理的檔案不會出現在記錄檔中。

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

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

7 Java Card Security for HP ProtectTools

Java Card Security for ProtectTools 會管理 Java Card 安裝及設定，以便與 HP Smart Card 鍵盤一起使用。HP 的 Java Card 是保護驗證資料的個人安全性裝置，需要同時具有介面卡及 PIN 碼才能獲准存取，如同使用含 PIN 的 ATM 提款卡。Java Card 可以用於存取 Credential Manager、Drive Encryption、HP BIOS 或任何數量的協力廠商存取點。

擁有 Java Card Security，您將可以完成下列工作：

- 存取 Java Card Security 功能
- 與電腦設定 (Computer Setup) 公用程式一起使用，在開機的環境下啓用 Java Card 驗證。
- 爲管理員及使用者設定不同的 Java Card。使用者必須插入 Java Card，並在作業系統載入前輸入 PIN。
- 設定並變更原先用來驗證 Java Card 使用者的 PIN

一般工作

「一般 (General)」頁面允許您執行下列工作：

- 變更 Java Card PIN
- 選取讀卡機或智慧卡鍵盤

附註： 讀卡機可使用 Java Card 及智慧卡。只有在電腦擁有超過一部以上的讀卡機時，才可使用此功能。

變更 Java Card PIN

若要變更 Java Card PIN：

附註： Java Card PIN 必須爲介於 4 到 8 個的數字字元。

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。
2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**一般 (General)**」。
3. 將 Java Card（含現有 PIN）插入讀卡機。
4. 在右邊窗格中，按一下「**變更 (Change)**」。

5. 在「**變更 PIN (Change PIN)**」對話方塊的「**目前的 PIN (Current PIN)**」方塊中，輸入目前的 PIN。

6. 在「**新的 PIN (New PIN)**」方塊中輸入新的 PIN，然後於「**確認新的 PIN (Confirm New PIN)**」方塊中再次輸入 PIN。

7. 按一下「**確定 (OK)**」。

選取讀卡機

使用 Java Card 之前，請確認已在「Java Card 安全性」中選取正確的讀卡機。如果未選取正確的讀卡機，則可能無法使用或無法正確顯示某些功能。此外，也必須正確安裝讀卡機驅動程式，安裝後會出現在 Windows「裝置管理員」中。

若要選取讀卡機：

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。

2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**一般 (General)**」。

3. 將 Java Card 插入讀卡機。

4. 在右邊窗格中，按一下「**選取的讀卡機 (Selected card reader)**」下的正確讀卡機。

進階的工作（僅限管理員）

「進階 (Advanced)」頁面允許您執行下列工作：

- 指派 Java Card PIN
- 指派一個名稱給 Java Card
- 設定開機驗證
- 備份與復原 Java Card

附註： 您必須擁有 Windows 管理員權限才能看得到「進階」頁面的顯示。

指派 Java Card PIN

您必須爲 Java Card 指派一個名稱及 PIN，才能將其用於「Java Card 安全性」中。

若要指派 Java Card PIN：

附註： Java Card PIN 必須爲介於 4 到 8 個的數字字元。

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。

2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**進階 (Advanced)**」。

3. 將新的 Java Card 插入讀卡機。

4. 當「**新卡 (New Card)**」對話方塊開啓時，在「**新的顯示名稱 (New display name)**」方塊中輸入新名稱，在「**新的 PIN (New PIN)**」方塊中輸入 PIN，然後於「**確認新的 PIN (Confirm New PIN)**」方塊中再次輸入 PIN。

5. 按一下「**確定 (OK)**」。

指派一個名稱給 Java Card

您必須爲 Java Card 指派一個名稱及 PIN，才能將其用於開機驗證。

若要指派一個名稱給 Java Card：

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。
2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**進階 (Advanced)**」。
3. 將 Java Card 插入讀卡機。

附註： 如果您尚未爲此卡指派 PIN，則「**新卡 (New Card)**」對話方塊會開啓，以便您輸入新的名稱及 PIN。

4. 在右邊窗格中，按一下「**顯示名稱 (Display name)**」下的「**變更 (Change)**」。
5. 在「**名稱**」方塊中爲 Java Card 輸入名稱。
6. 在「**PIN**」方塊中輸入目前的 Java Card PIN。
7. 按一下「**確定 (OK)**」。

設定開機驗證

啓用後，開機驗證會要求您使用 Java Card 啓動電腦。

啓用 Java Card 開機驗證的程序包括下列步驟：

1. 在「BIOS 組態 (BIOS Configuration)」或「電腦設定 (Computer Setup)」中啓用 Java Card 開機驗證支援。
2. 在「Java Card 安全性」中啓用 Java Card 開機驗證。
3. 建立並啓用管理員 Java Card。

啓用 Java Card 開機驗證，並建立管理員 Java Card

若要啓用 Java Card 開機驗證：

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。
2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**進階 (Advanced)**」。
3. 將 Java Card 插入讀卡機。

附註： 如果您尚未爲此卡指派名稱及 PIN，則「**新卡 (New Card)**」對話方塊會開啓，以便您輸入新的名稱及 PIN。

4. 在右邊窗格的「**開機驗證 (Power-on authentication)**」下，勾選「**啓用 (Enable)**」核取方塊。
5. 在「**電腦設定密碼 (Computer Setup Password)**」中輸入您的「電腦設定 (Computer Setup)」密碼，然後按一下「**確定 (OK)**」。
6. 如果您沒有啓用磁碟機鎖，請輸入 Java Card PIN，然後按一下「**確定 (OK)**」。

   - 或 -

   如果您已經啓用磁碟機鎖：

   a. 按一下「**讓 Java card 擁有獨特身份 (Make Java card identity unique)**」。

      - 或 -

      按一下「**讓 Java card 的身份與磁碟機鎖密碼相同 (Make the Java card identity the same as the DriveLock password)**」。

      附註： 如果電腦的磁碟機鎖已啓用，則您可以將 Java card 的身份與磁碟機鎖使用者密碼設爲相同，這可讓您在啓動電腦時僅需使用 Java Card 即可驗證磁碟機鎖與 Java Card。

   b. 如果適用，請在「**磁碟機鎖密碼 (DriveLock password)**」方塊中輸入您的磁碟機鎖使用者密碼，然後於「**確認密碼 (Confirm password)**」方塊中再次輸入該密碼。

   c. 輸入 Java Card PIN。

   d. 按一下「**確定 (OK)**」。

7. 當您收到建立復原檔的提示時，按一下「**取消 (Cancel)**」於稍後建立復原檔，或按一下「**確定 (OK)**」，並依照「HP ProtectTools 備份精靈」的螢幕上指示，立即建立復原檔。

附註： 請參閱「9 頁的備份和還原 HP ProtectTools 認證」以取得詳細資訊。

建立使用者 Java Card

附註： 必須安裝開機驗證及管理員卡才能建立使用者 Java Card。

若要建立使用者 Java Card：

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。
2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**進階 (Advanced)**」。
3. 插入將用作使用者卡的 Java Card。
4. 在右邊窗格的「**開機驗證 (Power-on authentication)**」下，按一下**使用者卡身份 (User card identity)**」旁邊的「**建立 (Create)**」。
5. 爲使用者 Java Card 輸入 PIN，然後按一下「**確定 (OK)**」。

停用 Java Card 開機驗證

一旦您停用 Java Card 開機驗證，即不再需要使用 Java Card 存取電腦。

1. 選取「**開始**」>「**所有程式**」>「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。
2. 在左邊窗格中，按一下「**Java Card 安全性 (Java Card Security)**」，然後按一下「**進階 (Advanced)**」。
3. 插入管理員 Java Card。
4. 在右邊窗格中的「**開機驗證 (Power-on authentication)**」下，取消勾選「**啓用 (Enable)**」核取方塊。
5. 爲 Java Card 輸入 PIN，然後按一下「**確定 (OK)**」。

8 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools 提供電腦設定 (Computer Setup) 公共程式安全性與組態設定的存取，並提供使用者進入電腦設定 (Computer Setup) 管理的系統安全性功能所需的 Windows 存取。BIOS Configuration for HP ProtectTools 中的選項有：

- 檔案 (File)
- 儲存 (Storage)
- 安全性 (Security)
- 電源 (Power)
- 進階 (Advanced)

附註： 對特定電腦設定 (Computer Setup) 選項的支援，視硬體組態而有所不同。

「BIOS 組態 (BIOS Configuration)」讓您管理多項電腦設定 (Computer Setup)，除此之外您僅能在啟動時及進入「電腦設定 (Computer Setup)」按下 F10 存取。透過「BIOS 組態 (BIOS Configuration)」，您將可以完成下列目標：

- 管理開機密碼和系統管理員密碼。
- 設定其他開機驗證功能，例如啓用嵌入式安全性驗證支援。
- 啓用和停用硬體功能，例如可抽換式媒體開機或不同的硬體連接埠。
- 設定開機選項，包括啓用多重開機和變更開機順序。

附註： 「F10 設定」擁有 BIOS Configuration for ProtectTools 中所有的功能。如需使用「F10 設定」的詳細指示，請參閱包含於於您電腦或 BIOS 更新中的《電腦設定 (F10) 公用程式指南》。

一般工作

BIOS Configuration 可讓您管理只有在啓動時，按下 F10 鍵後進入「電腦設定 (Computer Setup)」中，才能存取的各項電腦設定。

存取 BIOS 組態

若要存取 BIOS Configuration：

1. 按一下「**開始**」，按一下「**設定**」，然後按一下「**控制台**」。
2. 按一下「**HP ProtectTools Security Manager for Administrators**」，然後按一下「**BIOS 組態 (BIOS Configuration)**」。

   您也可以從工作列最右邊的通知區域中的圖示存取 BIOS Configuration。

   附註： 若要顯示 HP ProtectTools Security Manager for Administrators 圖示，您可能需要按一下通知區域中的「**顯示隱藏圖示**」圖示（「**<**」或「**<<**」）。

   - 在通知區域中的「**HP ProtectTools Security Manager for Administrators**」圖示上按一下滑鼠右鍵。
   - 按一下「**BIOS 組態 (BIOS Configuration)**」。
3. 如果您是 HP ProtectTools 使用者，請輸入您的 Windows 密碼。
   - 如果您正確輸入 Windows 密碼，但卻不是 BIOS 管理員，您可以進行變更的能力依據安全性等級設定會有所不同。

     附註： HP ProtectTools 使用者可以是或者不是 BIOS 管理員。
   - 如果輸入的 Windows 密碼錯誤，您只能檢視 BIOS 組態 (BIOS CONFIGURATION) 設定，但無法進行變更。
4. 如果您不是 HP ProtectTools 使用者，BIOS Configuration 軟體會檢查是否已經設定 BIOS 管理員密碼。
   - 如果已經設定 BIOS 管理員密碼，您必須輸入該密碼。
     - 如果輸入的 BIOS 管理員密碼正確，您可以檢視及變更 BIOS 組態 (BIOS CONFIGURATION) 設定。
     - 如果已經設定 BIOS 管理員密碼，卻沒有輸入該密碼，或是密碼輸入錯誤時，您可以檢視 BIOS 組態 (BIOS CONFIGURATION) 設定，但無法進行變更。
   - 如果未設定 BIOS 管理員密碼，您可以檢視並且變更 BIOS 組態 (BIOS CONFIGURATION) 設定。

檢視或變更設定

若要檢視或變更組態設定：

1. 按一下「BIOS 組態 (BIOS CONFIGURATION) 」頁面的其中一頁。
2. 進行變更，然後按一下「**套用 (Apply)**」儲存變更。
3. 結束後重新啓動電腦。

   當電腦重新啓動時，您的變更便會生效。

附註： 密碼變更會立刻生效，無需重新啓動電腦。

檔案

BIOS Configuration for HP ProtectTools 中的「檔案 (File)」會提供系統資訊，例如處理器類型、系統 BIOS 名稱及版本、機箱、序列號碼等。唯一能編輯的「檔案 (File)」資料是資產追蹤號碼。所有其他資料都是唯讀。

附註： 如需「檔案 (File)」選項的詳細資訊，請參閱《電腦設定 (F10) 公用程式指南》。

儲存

BIOS Configuration for HP ProtectTools 中的「儲存 (Storage)」選項提供關於所有設定於電腦系統中可開機裝置的資訊，可讓您指定這些裝置的設定。「儲存 (Storage)」中可存取的設定包括：

- 裝置組態 (Device Configuration)
- 儲存體選項 (Storage Options)
- DPS 自動測試 (DPS Self-Test)
- 開機順序 (Boot Order)

附註： 如需「儲存 (Storage)」選項的詳細資訊，請參閱《電腦設定 (F10) 公用程式指南》。

安全性

BIOS Configuration for HP ProtectTools 中的「安全性 (Security)」選項是所與安全性與密碼等設定有關的集中位置。設定包括：

- 設定密碼 (Setup Password)
- 開機密碼 (Power-On Password)
- 密碼選項(Password Options)
- 智慧型外殼 (Smart Cover)（某些機型）
- 裝置安全性 (Device Security)
- 網路服務啓動 (Network Service Boot)
- 系統 ID (System IDs)

- 磁碟機鎖安全性 (DriveLock Security) 功能
- 系統安全性 (System Security)（某些機型）
- 設定安全性等級 (Setup Security Level)

附註： 如需「安全性 (Security)」選項的詳細資訊，請參閱《電腦設定 (F10) 公用程式指南》。

電源

BIOS Configuration for HP ProtectTools 中的「電源 (Power)」選項提供在硬體層級控制電源管理的設定。設定包括：

- OS 電源管理 (OS Power Management)
- 硬體電源管理 (Hardware Power Management)
- 溫度 (Thermal)

附註： 如需「電源 (Power)」選項的詳細資訊，請參閱《電腦設定 (F10) 公用程式指南》。

進階

BIOS Configuration for HP ProtectTools「進階 (Advanced)」選項中的設定是專爲進階使用者準備。這些設定包括：

- 開機選項 (Power-On Options)
- 執行記憶體測試 (Execute Memory Test)（某些機型）
- BIOS 開機 (BIOS Power-On)
- 內建裝置 (Onboard Devices)
- PCI 裝置 (PCI Devices)
- PCI VGA 組態 (PCI VGA Configuration)
- 匯流排選項 (Bus Options)
- 裝置選項 (Device Options)
- 管理裝置 (Management Devices)
- 管理作業 (Management Operations)

附註： 如需「進階 (Advanced)」選項的詳細資訊，請參閱《電腦設定 (F10) 公用程式指南》。

9 Embedded Security for HP ProtectTools

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

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

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

TPM 嵌入式安全晶片可增強並啓用其他 HP ProtectTools Security Manager for Administrators 的安全性功能。例如，Credential Manager for HP ProtectTools 可以在使用者登入 Windows 時，使用嵌入式晶片做爲驗證方式。在選定的機型上，TPM 嵌入式安全晶片也能啓用經由 BIOS Configuration for HP ProtectTools 而存取的增強 BIOS 安全性功能。

設定程序

△ **注意：** 爲了降低安全性風險，強烈建議您的 IT 管理員立即初始化嵌入式安全晶片。沒有初始化嵌入式安全晶片可能會使得未獲授權的使用者、電腦病毒或病毒取得電腦的控制權，並控制擁有者的工作，如處理緊急復原封存，以及設定使用者的存取設定。

遵循以下兩節的步驟來啓用和初始化嵌入式安全晶片。

在「電腦設定 (Computer Setup)」中啓用嵌入式安全晶片

嵌入式安全晶片可以依下列說明，於「快速初始化精靈」或「電腦設定 (Computer Setup)」公用程式中啓用。此程序無法在 BIOS Configuration for HP ProtectTools 中執行。

若要在「電腦設定 (Computer Setup)」中啓用嵌入式安全晶片：

1. 啓動或重新啓動電腦以開啓電腦設定 (Computer Setup)，然後在螢幕左下角顯示 "F10 = ROM Based Setup" 訊息時，按下 F10 鍵。
2. 若尚未設定管理員密碼，使用方向鍵選擇「**安全性 (Security)**」，選擇「**設定密碼 (Setup password)**」，然後按下 Enter 鍵。
3. 在「**新密碼 (New Password)**」與「**確認新密碼 (Verify New Password)**」方塊中鍵入您的密碼，接著按下 F10 鍵。
4. 在「**安全性 (Security)**」功能表中，使用方向鍵來選擇「**TPM 嵌入式安全性 (TPM Embedded Security)**」，再按下 Enter 鍵。
5. 在「**嵌入式安全性 (Embedded Security)**」下，如果有隱藏的裝置，請選擇「**可用 (Available)**」。
6. 請選擇「**嵌入式安全性裝置狀態 (Embedded Security Device State)**」，然後將它變更爲「**啓用 (Enable)**」。
7. 按下 F10 鍵，即可接受對「嵌入式安全性 (Embedded Security)」組態所做的變更
8. 若要儲存您的偏好設定並離開「電腦設定 (Computer Setup)」，請使用方向鍵選擇「**檔案 (File)**」，然後按一下「**儲存變更並離開 (Save Changes and Exit)**」。然後依照螢幕上的指示進行。

初始化嵌入式安全晶片

在嵌入式安全性 (Embedded Security) 的初始化過程中，您將執行下列工作：

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

若要初始化嵌入式安全晶片：

1. 在工作列最右邊之通知區域內的 HP ProtectTools Security Manager for Administrators 圖示上按一下滑鼠右鍵，然後選取「**嵌入式安全性初始化 (Embedded Security Initialization)**」。

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

2. 請依照螢幕上的說明繼續執行。

設定基本使用者帳戶

設定嵌入式安全性 (Embedded Security) 的基本使用者帳戶，以完成下列工作：

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

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

若要設定基本使用者帳戶和啓用使用者安全性功能：

1. 如果「嵌入式安全性使用者初始化精靈」沒有啓動，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。

2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**使用者設定 (User Settings)**」。

3. 在右側窗格中，於「**嵌入式安全性功能 (Embedded Security Features)**」下，按一下「**設定 (Configure)**」。

   嵌入式安全性使用者初始化精靈 (Embedded Security Initialization Wizard) 將會開啓。

4. 請依照螢幕上的說明繼續執行。

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

一般工作

設定基本使用者帳戶後，可執行下列工作：

- 加密檔案和資料夾
- 傳送與接收加密的電子郵件

使用 Personal Secure Drive

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

加密檔案和資料夾

使用加密的檔案時，請考慮下列規則：

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

若要加密檔案和資料夾：

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

傳送與接收加密的電子郵件

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

變更基本使用者金鑰密碼

若要變更基本使用者金鑰密碼：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**使用者設定 (User Settings)**」。
3. 在右側窗格中，於「**基本使用者金鑰密碼 (Basic User Key Password)**」下，按一下「**變更 (Change)**。」
4. 鍵入舊密碼，然後設定和確認新密碼。
5. 按一下「**確定 (OK)**」。

進階工作

備份和還原

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

建立備份檔

若要建立備份檔：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**備份 (Backup)**」。
3. 在右側窗格中，請按一下「**備份 (Backup)**」。「HP ProtectTools 嵌入式安全性備份精靈 (HP Embedded Security for ProtectTools Backup Wizard)」將會開啟。
4. 請依照螢幕上的說明繼續執行。

從備份檔還原憑證資料

若要從備份檔還原資料：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**備份 (Backup)**」。
3. 在右側窗格中，請按一下「**還原 (Restore)**」。「HP ProtectTools 嵌入式安全性備份精靈 (HP Embedded Security for ProtectTools Backup Wizard)」將會開啟。
4. 請依照螢幕上的說明繼續執行。

變更擁有者密碼

若要變更擁有者密碼：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**進階 (Advanced)**」。
3. 在右側窗格中，於「**擁有者密碼 (Owner Password)**」下，按一下「**變更 (Change)**」。
4. 鍵入舊的擁有者密碼，然後設定和確認新的擁有者密碼。
5. 按一下「**確定 (OK)**」。

重設使用者密碼

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

啓用與停用嵌入式安全性

若不想使用安全性功能運作，可以停用「嵌入式安全性 (Embedded Security)」功能。

您可以在 2 個不同的等級上啓用或停用「嵌入式安全性 (Embedded Security)」功能：

- 暫時停用 (Temporary disabling) — 利用這個選項，會在重新啓動 Windows 時自動重新啓用嵌入式安全性。所有使用者預設都能使用這個選項。
- 永遠停用 (Permanent disabling) — 利用這個選項，需要使用擁有者密碼來重新啓用「嵌入式安全性 (Embedded Security)」。這個選項僅適用於管理員。

永遠停用嵌入式安全性 (Embedded Security)

若要永遠停用嵌入式安全性 (Embedded Security)：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**進階 (Advanced)**」。
3. 在右側窗格中，於「**嵌入式安全性 (Embedded Security)**」下，按一下「**停用 (Disable)**」。
4. 在提示上輸入您的擁有者密碼，再按一下「**確定 (OK)**」。

永遠停用後啓用嵌入式安全性

若要在永遠停用嵌入式安全性 (Embedded Security) 後啓用它：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**嵌入式安全性 (Embedded Security)**」，然後再按一下「**進階 (Advanced)**」。

3. 在右側窗格中，於「**嵌入式安全性 (Embedded Security)**」下，按一下「**啓用 (Enable)**」。
4. 在提示上輸入您的擁有者密碼，再按一下「**確定 (OK)**」。

以轉移精靈 (Migration Wizard) 轉移金鑰

轉移是一項進階的管理員工作，可管理、還原和轉移金鑰和憑證。

如需移轉的詳細資訊，請參閱嵌入式安全性的軟體說明。

10 Device Access Manager for HP ProtectTools

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

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

啓動背景服務

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

簡易組態

這項功能可以讓您拒絕下列裝置類別的存取：

- 所有非管理員的 USB 裝置
- 所有非管理員的所有可抽換式媒體（磁片、隨身碟等）
- 所有非管理員的所有 DVD/CD-ROM 光碟機
- 所有非管理員的所有序列埠和並列埠

若要拒絕存取所有非管理員的某種裝置類別：

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**裝置存取管理員 (Device Access Manager)**」，然後再按一下「**簡易組態 (Simple Configuration)**」。
3. 在右側窗格中，選擇要拒絕存取之裝置的核取方塊。
4. 按一下「**套用 (Apply)**」。

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

5. 按一下「**確定 (OK)**」。

裝置類別組態（進階）

您還可以使用其他選項，准許或拒絕特定使用者或使用者群組存取裝置類型。

新增使用者或群組

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**裝置存取管理員 (Device Access Manager)**」，然後再按一下「**裝置類別組態 (Device Class Configuration)**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 按一下「**新增 (Add)**」。「**選擇使用者或群組 (Select Users or Groups)**」對話方塊便會開啓。
5. 按一下「**進階 (Advanced)**」，然後按一下「**立刻尋找 (Find Now)**」以搜尋要新增的使用者或群組。
6. 按一下使用者或群組以便新增至可用的使用者與群組清單中，然後按一下「**確定 (OK)**」。
7. 按一下「**確定 (OK)**」。

移除使用者或群組

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**裝置存取管理員 (Device Access Manager)**」，然後再按一下「**裝置類別組態 (Device Class Configuration)**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 按一下您要移除的使用者或群組，再按一下「**移除 (Remove)**」。
5. 按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

拒絕存取使用者或群組

1. 在 Windows XP 中，按一下「**開始**」，按一下「**所有程式**」，然後按一下「**HP ProtectTools Security Manager for Administrators**」。
2. 在左側窗格中，按一下「**裝置存取管理員 (Device Access Manager)**」，然後再按一下「**裝置類別組態 (Device Class Configuration)**」。
3. 在裝置清單中，按一下您要設定的裝置類別。
4. 在「**使用者/群組 (User/Groups)**」之下，按一下要拒絕存取的使用者或群組。
5. 按一下要拒絕存取之使用者或群組旁邊的「**拒絕 (Deny)**」。
6. 請按一下「**套用 (Apply)**」，然後按一下「**確定 (OK)**」。

11 疑難排解

Credential Manager for HP ProtectTools

簡短說明	細節	解決方式
您可以使用認證管理員網路帳戶 (Credential Manager Network Accounts) 選項，選取要登入的網域帳戶。當您使用 TPM 驗證時，就無法使用這個選項。所有其它的驗證方法都能正確運作。	當您使用 TPM 驗證，只能登入到本機電腦中。	您可以使用認證管理員單一登入 (Credential Manager Single Sign On) 工具來驗證其他帳戶。
如果安裝 Credential Manager 後才安裝智慧卡和 USB Token，則智慧卡和 USB Token 無法在 Credential Manager 中使用。	爲了使智慧卡和 USB Token 可以在 Credential Manager 中使用，必須在安裝 Credential Manager 之前先安裝支援軟體（驅動程式、PKCS#11 提供者等）。 如果您已經先安裝了 Credential Manager，在安裝智慧卡或 Token 支援軟體後請執行下列步驟：	登入 Credential Manager。 在 HP ProtectTools Security Manager 中，按一下「**Credential Manager**」，按一下「**進階設定 (Advanced Settings)**」，然後按一下「**智慧卡及 Token (Smart Cards and Tokens)**」標籤。在「本機 Token」中會顯示可用的 Token 清單。 在「本機 Token」節點中按一下滑鼠右鍵以顯示快顯功能表，然後選擇「掃描新的智慧卡及 Token」。 如果出現提示，請重新啓動電腦。
某些應用程式網頁會產生錯誤，導致使用者無法執行或完成工作。	某些網頁應用程式會因爲單一登入 (Single Sign On) 的停用功能模式而停止運作並報告錯誤。例如，如果 Internet Explorer 中出現含有 **!** 符號的黃色三角形，代表出現錯誤。	Credential Manager 單一登入並不支援所有軟體 Web 介面。關閉「單一登入 (Single Sign On)」支援以停用特定 Web 頁面的單一登入支援。請參閱 Credential Manager 軟體說明檔案中，有關「單一登入 (Single Sign On)」的完整文件。 如果您無法針對指定應用程式停用特定的單一登入 (Single Sign On) 功能，請聯絡 HP 技術支援部門，並透過 HP 客服中心聯絡人要求提供第三級支援。
登入期間您無法看到「**瀏覽虛擬 Token (Browse for Virtual Token)**」選項。	使用者無法移動認證管理員 (Credential Manager) 中已註冊之虛擬 Token 的位置，這是爲了降低安全性風險而將瀏覽選項移除所致。	將瀏覽選項移除的原因爲：它能讓非使用者刪除並重新命名檔案，進而掌控整個 Windows 系統。
網域系統管理員即使擁有授權，仍無法變更 Windows 密碼。	當網域系統管理員登入網域，並以具有網域和本機 PC 的系統管理員權限的帳戶，而使用 Credential Manager 登錄網域識別時，就會發生這個情況。當網域系統管理員嘗試從 Credential Manager 變更 Windows 密碼時，系統管理員便會收到錯誤登入失敗的訊息：**使用者帳戶限制**。	Credential Mana 無法透過「**變更 Windows 密碼**」來變更網域使用者的帳戶密碼。Credential Manager 只能變更本機電腦的帳戶密碼。網域使用者可以透過「**Windows 安全性**」中的「**變更密碼**」選項變更其密碼，但是由於網域使用者在本機電腦上沒有實體帳戶，因此 Credential Manager 只能變更用來登入的密碼。

簡短說明	細節	解決方式
認證管理員 (Credential Manager) 與 Corel WordPerfect 12 密碼 GINA 之間有不相容的問題存在。	假設使用者登入認證管理員 (Credential Manager)，然後使用 WordPerfect 建立一個文件並加上密碼進行儲存，則認證管理員將無法自動地偵測或經由使用者手動來識別密碼 GINA。	HP 正在尋找做爲未來產品增強的方法。
Credential Manager 無法辨認螢幕上的「**連線 (Connect)**」按鈕。	如果遠端桌面連線 (RDP) 的單一登入 (Single Sign On) 認證設爲「**連線 (Connect)**」，在重新啓動單一登入時，則一律進入「**另存爲 (Save As)**」模式，而不是「**連線 (Connect)**」模式。	HP 正在尋找做爲未來產品增強的方法。
使用者可能會遺失所有 TPM 保護的認證管理員 (Credential Manager) 認證。	如果 TPM 模組被移除或損壞，使用者則會失去所有 TPM 保護的認證。	這是依照設計而發生的結果。 TPM 模組主要是用來保護認證管理員 (Credential Manager) 認證。HP 建議使用者將認證管理員 (Credential Manager) 中的身份識別備份起來，再移除 TPM 模組。
在 Windows XP Service Pack 1 中會發生一種特定狀況，一旦從睡眠模式轉換到休眠模式，使用者將無法登入認證管理員 (Credential Manager)。	在允許系統轉換至休眠與睡眠模式之後，系統管理員或使用者將無法登入到認證管理員 (Credential Manager) 中，而且不管選取了哪個登入認證（密碼、指紋或 Java 卡），都只會顯示 Windows 登入畫面。	透過 Windows Update 將 Windows 更新爲 Service Pack 2。如需造成原因的詳細資訊，請參閱 Microsoft 知識庫第 813301 號文章，網址爲：http://www.microsoft.com。 登入時，使用者必須選取認證管理員 (Credential Manager) 才能登入。在登入認證管理員 (Credential Manager) 之後，使用者會收到登入 Windows 的提示（可能需要選取 Windows 登入選項）以完成登入程序。 如果使用者先登入 Windows 系統，就必須手動登入認證管理員 (Credential Manager)。

簡短說明	細節	解決方式
還原嵌入式安全性造成 Credential Manager 失敗。	在 ROM 還原成原廠設定後，Credential Manager 無法登錄任何認證。	在安裝完認證管理員 (Credential Manager) 之後，如果將 ROM 重設爲原廠設定，則認證管理員將無法存取 TPM。 TPM 嵌入式安全晶片可以經由 F10 電腦設定 (Computer Setup) 公用程式、BIOS 組態 (BIOS Configuration)，或是 HP 用戶端管理員 (HP Client Manager) 加以啓用。請遵循下列步驟，使用電腦設定 (Computer Setup) 來啓用 TPM 嵌入式安全晶片： 1. 啓動或重新啓動電腦以開啓電腦設定 (Computer Setup)，然後在螢幕左下角顯示「**F10 = ROM Based Setup**」訊息時，按下 F10 鍵。 2. 使用方向鍵按一下「**安全性 (Security)**」，然後按一下「**設定密碼 (Setup Password)**」。設定密碼。 3. 選取「**嵌入式安全性裝置 (Embedded Security Device)**」。 4. 使用方向鍵選取「**嵌入式安全性裝置 － 停用 (Embedded Security Device – Disable)**」。使用方向鍵將其變更爲「**嵌入式安全性裝置 － 啓用 (Embedded Security Device – Enable)**」。 5. 按一下「**啓用 (Enable)**」，然後按一下「**儲存變更並離開 (Save changes and exit)**」。 HP 正在調查未來客戶軟體版本的解決方法選項。
安全性功能的「**還原身份識別 (Restore Identity)**」程序會失去與虛擬 Token 的關聯性。	在使用者還原身份識別時，認證管理員 (Credential Manager) 會在登入畫面時失去與虛擬 Token 位置的關聯性。就算認證管理員 (Credential Manager) 已經註冊使用了虛擬 Token，使用者還是需要重新註冊 Token 以還原關聯性。	目前這是依照設計而發生的結果。 如果在解除安裝認證管理員 (Credential Manager) 時沒有保存身份識別，則 Token 的系統（伺服器）部分就會損毀，導致登入時無法繼續使用。就算 Token 的用戶端部分已經透過身份識別還原方法還原回來，也還是一樣無法使用。 HP 正在調查解決方法的長期選項。

Embedded Security for HP ProtectTools

簡短說明	細節	解決方式
對 PSD 上的資料夾、子資料夾與檔案進行加密處理會導致錯誤訊息的出現。	如果使用者將檔案與資料夾複製到 PSD 並嘗試對資料夾/檔案或資料夾/子資料夾進行加密處理，則會顯示「**套用屬性錯誤 (Error Applying Attributes)**」的訊息。使用者可以在 C:\ 磁碟或是額外安裝的硬碟上加密相同的檔案。	這是依照設計而發生的結果。 加到 PSD 的檔案/資料夾會自動加密處理。您無須「重複加密」檔案/資料夾。如果您嘗試使用 EFS 對 PSD 上的這些檔案/資料夾重複進行加密的話，就會出現這個錯誤訊息。
無法在多重開機平台上以其他作業系統取得所有權。	如果設定磁碟機爲多重作業系統開機，那麼所有權就只能以一個作業系統的平台初始化精靈取得。	基於安全理由，這是依照設計而發生的結果。
未獲授權的系統管理員可以檢視、刪除、重新命名，或是移除加密 EFS 資料夾中的內容。	對於具有系統管理員權限而未經授權的使用者，加密資料夾並不會停止其進行資料夾內容的檢視、刪除或移動。	這是依照設計而發生的結果。 這是 EFS 的功能，而不是嵌入式安全性 TPM 的功能。嵌入式安全性使用 Microsoft EFS 軟體，而 EFS 則會爲所有系統管理員保留檔案/資料夾的存取權。
當使用者嘗試使用 FAT32 還原硬碟，就不會有加密選項。	如果使用者嘗試使用 FAT32 還原硬碟，就不會有任何使用 EFS 的檔案/資料夾加密選項。	這是依照設計而發生的結果。軟體不應該安裝在使用 FAT32 進行還原的系統上。 Microsoft EFS 僅支援在 NTFS 上使用，而無法在 FAT32 上運作，而這是 Microsoft EFS 本身的特性，與 HP ProtectTools 軟體無關。
使用者可以對復原封存 XML 檔案進行加密或刪除處理。	此資料夾的 ACL 預設值爲不設定；因此，使用者可以隨性或是有計劃地加密或刪除該檔案，讓他人無法存取。一旦此檔案經過加密或被刪除，任何人都無法使用 TPM 軟體。	這是依照設計而發生的結果。 使用者可以存取緊急封存，以便儲存/更新自己的基本使用者金鑰 (Basic User Key) 備份。使用者應該了解：絕對可對復原封存檔進行加密或加以刪除。
Embedded Security EFS 與 Symantec Antivirus 或 McAfee Total Protection 的互動會造成較長的加密/解密及掃描時間。	加密的檔案會干擾 Symantec Antivirus 或 McAfee Total Protection 的病毒掃描。當 Symantec Antivirus 或 McAfee Total Protection 正在執行時，使用 Embedded Security EFS 加密檔案需要較長的時間。	若要減少掃描嵌入式安全性 EFS (Embedded Security EFS) 檔案所需的時間，使用者可以在掃描之前先行鍵入加密密碼，或是先解密再進行掃描。 若要減少使用 Embedded Security EFS 加密/解密資料所需的時間，使用者應該停用 Symantec Antivirus 或 McAfee Total Protection 的自動防護。
緊急復原封存無法儲存至可抽換式媒體上。	如果使用者在嵌入式安全性 (Embedded Security) 初始化階段建立緊急復原封存路徑時，插入 MultiMediaCard 或 Secure Digital (SD) 記憶卡，就會出現錯誤訊息。	這是依照設計而發生的結果。 不支援在可抽換式媒體上儲存復原封存。復原封存可以存放在網路磁碟或是除了 C 磁碟以外的本機磁碟上。
如果因爲電源中斷而影響嵌入式安全性 (Embedded Security) 初始化作業，則會出現錯誤。	如果嵌入式安全 (Embedded Security) 化作業中出現電源中斷狀況，就會發生下列問題： • 當您嘗試啓動嵌入式安全性初始化精靈 (Embedded Security Initialization Wizard) 時，就會顯示下列錯誤訊息：「**由於嵌入式安全晶片已有嵌入式安全性擁有者，因此無法進行初始化。(The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.)**」 • 當您嘗試啓動使用者初始化精靈 (User Initialization Wizard) 時，就	執行下列程序以從電源中斷進行修復： **附註：** 使用方向鍵來選取各種功能表、功能表項目，以及變更數值（除非另有指定）。 1. 啓動或重新啓動電腦。 2. 當螢幕上出現「**F10=Setup**」的訊息時，按下 F10。 3. 選取適當的語言選項。 4. 按 Enter。 5. 選擇「**安全性 (Security)**」，然後按一下「**嵌入式安全性 (Embedded Security)**」。

簡短說明	細節	解決方式
	會顯示下列錯誤訊息：「**嵌入式安全性尚未初始化。若要使用精靈，必須先初始化嵌入式安全性。(The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.)**」	6. 設定「**嵌入式安全性裝置 (Embedded Security Device)**」選項爲「**啓用 (Enable)**」。 7. 按下 F10 接受變更。 8. 選擇「**檔案 (File)**」，然後按一下「**儲存變更並離開 (Save Changes and Exit)**」。 9. 按 Enter。 10. 按下 F10，儲存變更並結束公用程式。
電腦設定 (Computer Setup) (F10) 公用程式的密碼可在啓用 TPM 模組之後移除。	啓用 TPM 模組時需要用到電腦設定 (Computer Setup) (F10) 公用程式密碼。一旦啓用了模組，使用者就可以移除密碼。這樣一來，任何人只要能夠直接存取系統，就能重設 TPM 模組，進而導致資料遺失。	這是依照設計而發生的結果。 只有知道密碼的使用者才能移除電腦設定 (Computer Setup) (F10) 公用程式的密碼。然而，HP 強烈建議隨時保護好電腦設定 (Computer Setup) (F10) 公用程式的密碼。
當系統由待命狀態回到作用中狀態時，就不會再顯示 PSD 密碼方塊	當使用者建立了 PSD 並順利登入系統後，TPM 會要求提供基本使用者 (Basic User) 的密碼。如果使用者沒有鍵入密碼，而且系統進入了「待命」狀態，則當使用者再度使用時，就不會再顯示密碼對話方塊。	這是依照設計而發生的結果。 使用者必須登出然後登入，以再度檢視 PSD 密碼方塊。
變更安全性平台政策 (Security Platform Policies) 時不需要任何密碼。	擁有系統管理員權限的使用者在存取安全性平台原則（電腦和使用者）時不需要 TPM 密碼。	這是依照設計而發生的結果。 無論是否有進行 TPM 使用者初始化，任一位系統管理員都可以修改安全性平台原則。
當系統檢視過憑證之後，就會顯示爲不信任。	當使用者設定好 HP ProtectTools 並執行使用者初始化精靈 (User Initialization Wizard) 之後，就能夠檢視所發行的憑證；然而，當系統檢視過憑證之後，就會顯示爲不信任。雖然您可以在這個階段按一下安裝按鈕來安裝憑證，安裝動作仍舊無法使其受到信任。	自行簽署的憑證不會被信任。在一個設定適當的企業環境裡，EFS 憑證是由線上憑證授權單位所簽署，而受到信任。
不定時出現下列的加密與解密錯誤：「**程序無法存取檔案，因爲檔案正由另一個程序使用。(The process cannot access the file because it is being used by another process.)**」	每當另一個程序正在使用檔案時，如果對該檔案進行加密或解密，就會出現這個典型的間歇性錯誤，就算作業系統或其他應用程式目前並未處理該檔案或資料夾亦然。	若要解決此失敗： 1. 重新啓動系統。 2. 登出。 3. 重新登入。
如果在產生新資料或轉移過程中移除可抽換式儲存媒體的話，則存放在其上的資料就會遺失。	移除諸如 MultiBay 硬碟之類的儲存媒體之後，仍舊會顯示 PSD 爲可用，而且在新增/修改 PSD 的資料時，也不會出現錯誤。系統重新啓動後，PSD 不會將當可抽換式儲存媒體無法使用時所發生的檔案變更情況反映出來。	請勿在資料產生或轉移過程中移除 PSD。只有當使用者存取 PSD，並在新資料的產生或轉移過程中移除硬碟，才會出現這個問題。如果使用者在可抽換式硬碟已經被移除的情況下嘗試存取 PSD，則會出現「**裝置尚未就緒 (the device is not ready)**」的錯誤訊息。
在解除安裝的過程中，如果使用者沒有初始化基本使用者 (Basic User) 就逕行開啓管理工具 (Administration tool)，則必須等到管理工具已經關閉才能使用「**停用**	使用者可以選擇在不停用 TPM 的情況下解除安裝，或是透過管理工具 (Administration tool) 先停用 TPM，然後再解除安裝。存取管理工具 (Administration tool) 時需要初始化基本使用者金鑰 (Basic User Key)。如果沒有執行基本初始化動作，則使用者將無法使用所有的選項。	管理工具 (Administration tool) 主要是用來停用 TPM 晶片，但是除非基本使用者金鑰 (Basic User Key) 已經初始化，否則使用者將無法使用此選項。如果它尚未初始化，則選取「**確定 (OK)**」或「**取消 (Cancel)**」，繼續解除安裝作業。

簡短說明	細節	解決方式
(Disable)」選項並繼續執行解除安裝程式。	由於使用者已經明確地選擇要開啓管理工具 (Administration tool)（當對話方塊提示「**按一下「是」以開啓嵌入式安全性管理工具 (Click Yes to open Embedded Security Administration tool)**」時按一下「**是 (Yes)**」），解除安裝作業就會等到管理工具已經關閉之後才會繼續執行。如果使用者在該對話方塊提示下按一下「**否 (No)**」，則管理工具 (Administration tool) 將不會開啓，並且繼續執行解除安裝作業。	
在爲兩個使用者帳戶建立了 PSD 並在 128-MB 系統組態中採用快速使用者切換模式之後，就會發生不定時的系統當機。	在記憶體不足的情況下使用快速切換模式時，可能會出現螢幕變黑，以及沒有回應的鍵盤與滑鼠等系統當機狀況，而不是顯示歡迎登入畫面。	可能的原因是記憶體不足所導致的調度問題。 整合式顯示晶片使用 UMA 架構並用去了 8 MB 的記憶體，只剩下 120 MB 可用記憶體給使用者使用。當兩位已登入系統並使用快速使用者切換模式的使用者同時共用這 120 MB 的記憶體時，就會出現這個錯誤。 解決辦法就是重新啓動系統以增加記憶體（HP 並未生產包含安全性模組的 128-MB 記憶體）。
EFS 使用者驗證（要求密碼）時間終止，且出現「**拒絕存取**」。	EFS 使用者驗證密碼 (EFS User Authentication) 密碼會在使用者按一下「**確定 (OK)**」，或是當系統結束「待命」狀態時重新開啓。	這是依照設計 － 以避免 Microsoft EFS 出現問題，我們建立了 30 秒的看門狗計時器 (Watchdog Timer) 來產生錯誤訊息。
設定日文版時，出現小部分的功能說明截斷情況。	安裝精靈的自訂安裝選項功能說明被截斷。	HP 將會在未來的版本中更正此問題。
就算是在提示狀態下未鍵入密碼，EFS 加密 (EFS Encryption) 機制仍舊可以運作。	就算要求鍵入使用者密碼 (User password) 的提示已經逾時，仍舊可以在檔案或資料夾上進行加密。	由於這是 Microsoft 的 EFS 加密機制，因此加密功能不需要經過密碼驗證。解密時則需要提供使用者密碼。
支援安全電子郵件，就算使用者初始化精靈 (User Initialization Wizard) 當中並未指定安全電子郵件或是使用者政策已停用安全電子郵件組態亦然。	嵌入式安全性軟體與精靈無法控制電子郵件用戶端（Outlook、Outlook Express，或 Netscape）的設定。	這是依照設計的行爲模式。TPM 電子郵件設定的組態無法禁止直接在電子郵件用戶端編輯加密設定。安全電子郵件的使用是由協力廠商的應用程式所設定與控制的。HP 精靈可供連結三個參照的應用程式，以便立即進行自訂作業。
第二次在相同 PC 或先前已初始化的 PC 中執行大規模部署，會覆寫緊急復原和緊急權杖檔案。新檔案無法做爲復原用途。	在已經初始化的 HP ProtectTools 嵌入式安全性 (HP ProtectTools Embedded Security) 系統中執行大規模的部署作業，會覆寫這些 XML 檔案而讓現有的復原封存 (Recovery Archive) 與復原 Token (Recovery Token) 失效。	HP 正努力解決 XML 檔案覆寫的問題，並將於未來的 SoftPaq 中提供解決方案。
當嵌入式安全性 (Embedded Security) 進行使用者還原作業時，自動化登入指令檔無法運作。	當使用者執行下列動作時，就會發生這個錯誤： • 在嵌入式安全性中初始化所有者和使用者（使用預設位置 －「**我的文件**」）後。 • 在 BIOS 中重設晶片爲原廠設定後。 • 重新啓動電腦後。 • 開始還原嵌入式安全性 (Embedded Security)。在還原過程中，認證管理員 (Credential Manager) 會詢問	按一下螢幕上的「**瀏覽**」按鈕以選擇位置，還原處理程序便會繼續。

簡短說明	細節	解決方式
	系統是否能自動化 Infineon TPM 使用者驗證 (Infineon TPM User Authentication) 的登入作業。如果使用者選取「**是 (Yes)**」，則 SPEmRecToken 的位置就會自動顯示在文字方塊中。 雖然此位置正確，但仍會顯示下列錯誤訊息：**沒有提供緊急復原權杖。選取抓取緊急復原權杖的權仗位置 (No Emergency Recovery Token is provided. 選取抓取緊急復原權杖的權仗位置。)**	
多重使用者的 PSD 無法在快速使用者切換環境中運作。	一旦建立了多個使用者並給予具有相同磁碟機代號的 PSD 之後，就會出現這個錯誤。如果在載入 PSD 時嘗試於使用者之間進行快速使用者切換，則第二個使用者的 PSD 將會無法使用。	第二個使用者的 PSD 必須重新設定使用另一個磁碟機代號，或是當第一個使用者登出時，才能使用。
如果產生 PSD 的硬碟已經格式化，則 PSD 將會停用而且無法刪除。	PSD 圖示仍舊看得見，但是當使用者嘗試存取 PSD 時，出現「**磁碟機無法存取 (drive is not accessible)**」的錯誤訊息。 使用者無法刪除 PSD，並顯示下列訊息：「**您的 PSD 仍舊爲使用狀態，請確定 PSD 內的檔案皆已關閉，而且沒有被其他程序存取 (your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process)**」。使用者必須重新啓動系統以刪除 PSD，而 PSD 在重新啓動後就不會載入。	依照設計：如果客戶強迫刪除，或從 PSD 資料的儲存位置中斷，嵌入式安全性 PSD 磁碟模擬就會繼續運作，並將基於缺乏與遺失資料的通訊而製造錯誤。 解決方法：下次重新開機後，模擬無法載入，使用者可以刪除舊的 PSD 模擬並建立新的 PSD。
當使用者嘗試從自動備份封存 (Automatic Backup Archive) 中還原，就會偵測到內部錯誤。	在嵌入式安全性 (Embedded Security) 中，如果使用者按一下「**使用備份來還原 (Restore under Backup)**」選項，從自動備份的封存 (Archive) 中還原，然後選取「**SPSystemBackup.xml**」，則還原精靈 (Restore Wizard) 會失敗，並顯示下列錯誤訊息：「**選取的備份封存與還原理由不符。請選取另一個封存再繼續。(Backup Archive does not match the restore reason. Please select another archive and continue.)**」	如果使用者在系統要求提供 SpBackupArchive.xml 時選取了「**SpSystemBackup.xml**」，則嵌入式安全性精靈 (Embedded Security Wizard) 就會失敗，並顯示下列訊息：「**偵測到內部的嵌入式安全性錯誤。(An internal Embedded Security error has been detected.)**」 使用者必須選取正確的 XML 檔案，以符合要求的理由。 處理程序依設計進行且運作正常；然而，內部嵌入式安全性的錯誤訊息並不清楚，且應該陳述更適當的訊息。HP 正努力在未來的產品中增強這一點。
安全性系統出現多重使用者的還原錯誤。	在還原處理程序中，如果系統管理員選取要還原的使用者，那麼未選取的使用者就無法在稍後試著還原時還原金鑰。將顯示「**解碼處理程序失敗 (Decryption process failed)**」錯誤訊息。	您可藉由重新設定 TPM、執行還原程序，並在執行下一個預設的每日備份作業之前選好所有的使用者，來還原非選取的使用者。如果自動化備份開始執行，會覆寫非還原的使用者，導致這些使用者的資料遺失。如果還原了新系統備份，則先前未選取的使用者就無法還原。 使用者同時必須還原整個系統備份。封存備份 (Archive Backup) 可以個別還原。
將系統 ROM (System ROM) 重設爲預設值會將 TPM 隱藏起來。	重新設定系統 ROM 爲預設值，會使 TPM 隱藏至 Windows。這使安全性軟體不能正常作業，且讓 TPM 加密的資料無法存取。	在 BIOS 中解除隱藏 TPM： 開啓電腦設定 (F10) 公用程式，瀏覽至「**安全性 > 裝置安全性**」(Security Device security)，然後將欄位從「**隱藏 (Hidden)**」修改爲「**可用 (Available)**」。

簡短說明	細節	解決方式
自動化備份作業無法與對應磁碟一同運作。	當管理員在「嵌入式安全性」中設定「自動備份 (Automatic Backup)」時，會在「**Windows > 工作 > 排程工作**」中建立一個項目。會將 Windows 排程工作設定爲使用 NT AUTHORITY\SYSTEM 作爲執行備份的權限。這適用於所有本機磁碟機。 當系統管理員沒有這麼執行，而是設定自動備份儲存到對應磁碟機上，那麼處理程序便會失敗，因爲 NT AUTHORITY\SYSTEM 沒有使用對應磁碟機的權限。 如果將自動備份 (Automatic Backup) 排定在登入時發生，則嵌入式安全性 (Embedded Security) 的工作列通知區圖示就會顯示下列訊息：「**目前無法存取備份封存位置。如果您想要在恢復存取備份封存之前先備份暫存封存的話，按一下這裡。(The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.)**」儘管自動備份 (Automatic Backup) 已排定在特定時間執行，但是，備份作業仍舊失敗，而且沒有顯示失敗訊息。	解決方法爲變更 NT AUTHORITY\SYSTEM 至（電腦名稱）\（系統管理員名稱）。如果排定的工作是以手動建立，那麼這就是預設設定。 HP 正努力在未來的產品版本中，提供包括「電腦名稱\系統管理員名稱」的預設設定。
嵌入式安全性 (Embedded Security) 無法透過嵌入式安全性圖形化介面 (Embedded Security GUI) 暫時停用。	目前的 4.0 軟體是設計供 HP 筆記型電腦 1.1B 執行，並支援 HP 桌上型電腦 1.2 的執行。 TPM 1.1 平台的軟體介面中仍支援此停用選項。	HP 將在未來的版本中處理此問題。

HP ProtectTools 的裝置存取管理員 (Device Access Manager for HP ProtectTools)

簡短說明	細節	解決方案
使用者已經被拒絕存取裝置存取管理員 (Device Access Manager) 中的裝置，但是仍舊可以存取裝置。	已經使用裝置存取管理員 (Device Access Manager) 中的簡易組態 (Simple Configuration) 與/或裝置類別組態 (Device Class Configuration) 來拒絕使用者存取裝置。儘管已經被拒絕存取，使用者仍舊可以存取裝置。	確定 HP ProtectTools 裝置鎖定 (HP ProtectTools Device Locking) 服務已經啓動。 以管理員使用者身份瀏覽至「**控制台 > 系統管理工具 > 服務**」。在「**服務**」視窗中，搜尋「**HP ProtectTools 裝置鎖定/稽核 (HP ProtectTools Device Locking/Auditing)**」服務。確定服務已經啓動且啓動類型爲「**自動 (Automatic)**」。
使用者意外存取某個裝置，或使用者意外被拒絕存取某個裝置。	裝置存取管理員 (Device Access Manager) 用來拒絕使用者存取某些裝置，並允許使用者存取其他裝置。在使用者使用系統時，可以存取他們認爲已經遭到裝置存取管理員 (Device Access Manager) 拒絕的裝置，而且被拒絕存取他們認爲裝置存取管理員 (Device Access Manager) 應該會允許存取的裝置。	您應該使用裝置存取管理員 (Device Access Manager) 中的裝置類別組態 (Device Class Configuration) 來調查使用者裝置設定。 按一下「**Security Manager**」，按一下「**Device Access Manager**」，然後按一下「**裝置類別組態 (Device Class Configuration)**」。展開「裝置類別 (Device Class)」樹的等級，並檢視使用者適用的設定。檢查可能設定於使用者或使用者所屬任何 Windows 群組（例如使用者、管理員）的「拒絕」權限。
允許或拒絕 — 哪個具有優先順序？	在裝置類別組態 (Device Class Configuration) 中，已經設定下列組態： • 以位於裝置類別階層（例如 DVD/CD-ROM 光碟機）同一階層爲基準，「允許 (Allow)」權限給予某個 Windows 群組（例如 BUILTIN\Administrators）存取權限，而「拒絕 (Deny)」權限則給了另一個 Windows 群組（例如 BUILTIN\Users）拒絕存取的權限。 如果使用者同時是這兩個群組的成員（例如：系統管理員 (Administrator) 群組），則哪一個群組的權限將大於另一個群組權限？	使用者被拒絕存取裝置。「拒絕 (Deny)」權限優先於「允許 (Allow)」權限。 無法存取的原因在於 Windows 解決裝置有效權限的方式。如果某個群組爲拒絕存取，而另一個群組爲允許存取，但是使用者同時屬於兩個群組的成員。由於拒絕存取優先於允許存取，因此使用者會被拒絕存取。 解決辦法之一就是在 DVD/CD-ROM 磁碟機層級拒絕「使用者 (Users)」群組存取，然後在 DVD/CD-ROM 磁碟機層級以下的層級允許「系統管理員 (Administrators)」群組存取。 更好的解決辦法則是建立特定的 Windows 群組，一個用來允許存取 DVD/CD，另一個則是用來拒絕存取 DVD/CD。這時必須將特定的使用者加入到適當的群組當中。

其他事項

受影響的軟體 – 簡短說明	細節	解決方式
安全管理員 (Security Manager) — 收到警告：「**安全性應用程式必須等到 HP Protect Tools 的安全管理員已經安裝完畢，才能開始安裝 (The security application can not be installed until the HP Protect Tools Security Manager is installed)**」。	所有的安全性應用程式，例如嵌入式安全性 (Embedded Security)、Java 卡安全性 (Java Card Security)，以及生物測定都是安全管理員 (Security Manager) 介面的可延伸外掛程式。安全管理員 (Security Manager) 必須先安裝完畢，才能載入 HP 核准的安全性外掛程式。	安全管理員 (Security Manager) 軟體必須先安裝完畢，才能安裝任何的安全性外掛程式。
TPM 韌體升級工具 (TPM Firmware Update Utility) 用於包含 Broadcom 技術的 TPM 機型上 — 這項透過 HP 支援網站提供的工具會回應「**需要擁有權 (ownership required)**」的訊息。	當使用者將 TPM 韌體升級工具 (TPM Firmware Update Utility) 運用在包含 Broadcom 技術的 TPM 機型時，預期會發生的狀況。 韌體升級工具允許使用者升級韌體，不論有沒有簽署金鑰（Endorsement Key，EK）。當沒有 EK 時，就不需要授權來完成韌體升級。 具有 EK 時，TPM 所有者必須存在，因爲升級需要所有者的授權。成功升級後，您必須重新啓動平台以讓新韌體生效。 如果 BIOS TPM 爲原廠重設，那麼系統就會移除所有權並防止韌體更新，直到設定嵌入式安全性軟體平台和使用者初始化精靈爲止。 **附註：** 一旦執行了韌體更新，建議您重新啓動機器。韌體版本必須等到機器重新啓動後才能夠正確識別。	1. 重新安裝嵌入式安全性 (Embedded Security) 軟體。 2. 執行平台與使用者組態精靈 (Platform and User Configuration Wizard)。 3. 請確定系統已經安裝了 Microsoft .NET Framework 1.1： **a.** 按一下「**開始**」。 **b.** 按一下「**控制台**」。 **c.** 按一下「**新增或移除程式**」。 **d.** 請確定系統列出了「**Microsoft .NET Framework 1.1**」的安裝項目。 4. 檢查硬體和軟體組態： **a.** 按一下「**開始**」。 **b.** 按一下「**所有程式**」。 **c.** 按一下「**HP ProtectTools Security Manager for Administrators**」(Windows Vista) 或「**HP ProtectTools Security Manager**」(Windows XP)。 **d.** 從樹狀功能表中選取「**嵌入式安全性 (Embedded Security)**」。 **e.** 按一下「**詳細資料**」。系統應有下列組態： • 產品版本 = V4.0.1 • 嵌入式安全性狀態：晶片狀態 = 啓用，所有者狀態 = 已初始，使用者狀態 = 已初始 • 元件資訊：TCG 規格 版本 = 1.2 • 廠商 = Broadcom Corporation

受影響的軟體 – 簡短說明	細節	解決方式
		• FW 版本 = 2.18（或更新） • TPM 裝置驅動程式程式庫版本 2.0.0.9（或更新） 5. 如果 FW 版本不是 2.18，請下載並更新 TPM 韌體。TPM Firmware SoftPaq 是一個支援下載，可在 HP 網站中 http://www.hp.com 取得。
HP ProtectTools Security Manager – 關閉 Security Manager 介面時會間歇傳回錯誤。	在所有插件應用程式完成載入前使用螢幕右上方的關閉按鈕，會產生間歇性（1/12 的機會）的錯誤。	這與在關閉並重新啓動 Security Manager 時的插件服務載入時間計時依存性相關。由於 PTHOST.exe 是儲藏其他應用程式（插件）的殼層，因此會依賴插件完成其載入時間（服務）的能力。在插件有足夠時間完成載入前關閉殼層是根本原因。 允許安全管理員 (Security Manager) 完成服務載入訊息（可在安全管理員 (Security Manager) 視窗上方看到），並在左側欄位中列示所有的外掛程式。爲了預防錯誤發生，請給予充足的時間，讓這些外掛程式全部載入。
HP ProtectTools — 未限制的存取或未控制的系統管理員權限造成安全上的風險。	許多風險都是因爲未限制用戶端電腦的存取行爲而導致，包括下列幾項： • 刪除 PSD • 惡意修改使用者設定 • 停用安全性政策與功能	HP 建議系統管理員遵循「最佳方式」，限制一般使用者權限並限制使用者存取。 不應給予未授權的使用者系統管理特殊權限。
BIOS 以及作業系統的嵌入式安全性 (Embedded Security) 密碼沒有同步。	假使使用者沒有對新密碼進行驗證以成爲有效的 BIOS 嵌入式安全性 (BIOS Embedded Security) 密碼，則 BIOS 嵌入式安全性密碼就會經由 F10 BIOS 回頭使用原始的嵌入式安全性密碼。	此功能是依照設計；這些密碼可藉由變更作業系統基本使用者密碼，並於 BIOS 嵌入式安全性密碼提示中進行驗證來重新同步化。
只有一位使用者可以在 TPM 預啓動驗證於 BIOS 啓用後登入系統。	TPM BIOS PIN 碼會與第一位對使用者設定進行初始化作業的使用者進行關聯。假使電腦含有多位使用者，則第一位使用者基本上就是系統管理員。第一位使用者必須將其 TPM 使用者 PIN 碼提供給其他使用者，以便登入系統。	此功能是依照設計；HP 建議客戶的 IT 部門採用良好的安全性原則來進行安全性解決方案，並確認 BIOS 系統管理員密碼是由系統層級保護的 IT 管理員設定。
在將 TPM 重設爲原廠設定之後，使用者必須變更自己的 PIN 碼，才能讓 TPM 預先開機作業正常運作。	使用者必須變更自己的 PIN 碼，或是建立另一個使用者來初始化使用者設定，以便在重設之後，讓 TPM BIOS 驗證正常運作。這是讓 TPM BIOS 驗證正常運作的唯一方式。	這是依照設計而發生的結果；回復原廠設定的動作會清除基本使用者金鑰 (Basic User Key)。使用者必須變更其使用者 PIN 碼或是建立新使用者以重新初始化基本使用者金鑰 (Basic User Key)。
使用嵌入式安全性 (Embedded Security)「**重設爲原廠設定 (Reset to Factory Settings)**」時，預設不會設爲「**開機驗證支援 (Power-on authentication support)**」	電腦設定 (Computer Setup) 中，在使用嵌入式安全性裝置選項「**重設爲原廠設定**」時沒有將「**開機驗證支援**」選項重設爲原廠設定。依照預設，「**開機驗證支援**」是設定爲「**停用**」。	「**重設爲原廠設定 (Reset to Factory Settings)**」選項會停用嵌入式安全性裝置 (Embedded Security Device)，進而隱藏其他嵌入式安全性選項（包括「**開機驗證支援 (Power-on authentication support)**」）。然而，在重新啓用了嵌入式安全性裝置 (Embedded Security Device) 之後，「**開機驗證支援 (Power-on authentication support)**」仍然會維持啓用狀態。 HP 正在尋找解決方法，並在未來的網路 ROM SoftPaq 產品中提供。
在開機順序中，安全性開機驗證 (Security Power-On Authentication) 將與	開機驗證 (Power-On Authentication) 會提示使用者使用 TPM 密碼登入系統，但是假使使用者按下 F10 來存取 BIOS，則系統只會賦予使用者「讀取」權限。	爲了能夠寫入 BIOS，使用者必須在開機驗證 (Power-On Authentication) 視窗中鍵入 BIOS 密碼，而不是 TPM 密碼。

受影響的軟體 – 簡短說明	細節	解決方式
BIOS 密碼 (BIOS Password) 同時發生。		
一旦擁有者 (Owner) 的密碼變更，BIOS 就會藉由電腦設定 (Computer Setup) 要求同時鍵入新舊密碼。	一旦嵌入式安全性 Windows (Embedded Security Windows) 軟體中的擁有者 (Owner) 密碼變更，BIOS 就會藉由電腦設定 (Computer Setup) 要求同時鍵入新舊密碼。	這是依照設計而發生的結果。這是因爲一旦作業系統啓動而且正常運作後，爲了確認 TPM 驗證字串 (pass phrase)，但是 BIOS 又無法與 TPM 溝通而導致的結果。

辭彙

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

BIOS 安全性模式。 Java 卡安全性 (Java Card Security) 的設定，啓用時，需要使用 Java 卡和有效的 PIN 碼進行使用者驗證。

BIOS 設定檔。 BIOS 組態 (BIOS CONFIGURATION) 設定的群組，可儲存和套用到其他帳戶。

BIOS 管理員密碼。 電腦設定 (Computer Setup) 的「**設定**」密碼。

Drive Encryption 金鑰復原服務。 SafeBoot Recovery 服務。可儲存加密金鑰的副本，以便您在忘記密碼且無法存取本機備份金鑰時，仍然可以存取電腦。您必須建立包含此服務的帳戶，以便爲您的備份金鑰設定線上存取權限。

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

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

Personal Secure Drive (PSD)。 提供受保護的儲存區以儲存敏感性資料。

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

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

Token。 請參閱「安全登入法」。

TXT。 受信任的執行技術。提供安全性，讓電腦軟體及資料不受攻擊的硬體及韌體。

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

Windows 使用者帳戶。 有權登入網路或個人電腦的個人設定檔。

Windows 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。

公開金鑰基礎架構 (Public Key Infrastructure, PKI) 一種可用來定義介面以建立、使用和管理憑證及密碼編譯金鑰的標準。

手動拆解。 略過自動拆解排程，立刻拆解資產或選取的資產。

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

加密檔案系統 (EFS)。 用來加密選定資料夾中所有檔案和子資料夾的系統。

可用空間清理。 硬碟已刪除資源的隨機資料安全寫入會扭曲已刪除的資源，這會讓資料的復原更不易。

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

生物測定。 使用實體功能的驗證認證類別（如指紋）來識別使用者身份。

安全登入法。 用來登入電腦的方法。

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

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

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

拆解。 執行一個演算法以模糊資產中的資料。

拆解設定檔。 指定的清除方法和資產清單。

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

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

信任的平台模組 (TMP) 嵌入式安全晶片。 HP ProtectTools 嵌入式安全晶片的一般詞彙。TPM 藉由儲存主機系統特有的資訊，例如加密金鑰、數位憑證和密碼等，來驗證電腦，而不是驗證使用者。TPM 可將電腦中的資訊被小偷破壞或被外部駭客攻擊的風險降到最小。

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

信任的連絡人 (Trusted Contact) 清單。 列出信任的連絡人。

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

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

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

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

按鍵順序。 特定鍵的組合，按下時會啓動自動拆解，例如 Ctrl+Alt+S。

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

重新開機。 電腦的重新啓動程序。

密碼編譯。 加密和解密資料的實務，目的是只允許特定的個人解碼該資料。

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

啓用。 必須先完成工作，才能存取任何 Drive Encryption 功能。使用 HP ProtectTools Security Manager for Administrators 安裝精靈啓用 Drive Encryption。僅有管理員可以啓用 Drive Encryption。啓用程序包括啓用軟體、加密磁碟機、建立使用者帳戶，以及在卸除式儲存裝置上建立初始背景加密金鑰。

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

聊天記錄。 加密的檔案，包含聊天工作階段中雙方交談的記錄。

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

單一登入。 爲一種功能，可儲存驗證資料，並讓您使用認證管理員，來存取需要密碼驗證的網際網路和 Windows 應用程式。

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

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

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

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

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

解密。 密碼編譯所使用的程序，可將加密的資料轉換成純文字。

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

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

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

管理員。 請參閱「Windows 管理員」。

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

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

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

認證。 使用者用來證明其具有驗證程序中的特定工作權限之方法。

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

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

憑證授權單位。 發出執行公開金鑰基礎架構所需之憑證的服務。

整理。 請參閱「**釋放空間整理**」。

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

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

嚴密安全性。 BIOS Configuration 中的安全性功能，可增強對開機密碼和管理員密碼的防護，並提供其他形式的開機驗證。

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

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

索引