參考指南
ProtectTools Security Manager

文件編號：389171-AB1

2005 年 5 月

Microsoft 及 Windows 是 Microsoft Corporation 在美國的註冊商標。

參考指南
ProtectTools Security Manager
第 1 版 2005 年 5 月
文件編號：389171-AB1

目錄

1 簡介

2 ProtectTools 的智慧卡安全性

3 ProtectTools 的嵌入式安全性

4 ProtectTools 的 BIOS 配置

5 ProtectTools 的認證管理員

辭彙

索引

1

簡介

ProtectTools 安全管理員

ProtectTools 安全管理員 (ProtectTools Security Manager) 軟體提供了安全性功能，有助於防止未授權者存取電腦、網路及重要資料。進階安全性功能由下列軟體模組提供：

- ProtectTools 的智慧卡安全性 (Smart Card Security for ProtectTools)
- ProtectTools 的嵌入式安全性 (Embedded Security for ProtectTools)
- ProtectTools 的 BIOS 配置 (BIOS Configuration for ProtectTools)
- ProtectTools 的認證管理員 (Credential Manager for ProtectTools)

您電腦所適用的軟體機型可能隨著您的模型而變。例如，「ProtectTools 的嵌入式安全性」將要求您的電腦安裝「信任平台模組」(TPM) 內建式安全晶片（僅限特定機型）」，而「ProtectTools 的智慧卡安全性」需要搭配使用選購的智慧卡和讀取器。

您可以預先安裝、預先載入，或從 HP 網站下載 ProtectTools 軟體模組。有關其他資訊，請造訪 http://www.hp.com。

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

存取 ProtectTools 安全管理員

若要從 Microsoft® Windows® 的「控制台」存取「ProtectTools 安全管理員 (ProtectTools Security Manager)」：

» 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」**。

設定「認證管理員」模組後，您也可以從 Windows 登入螢幕中，直接登入「認證管理員」，以開啓 ProtectTools。有關詳細資訊，請參閱第 5 章〈ProtectTools 的認證管理員〉的「以認證管理員登入 Windows」。

瞭解安全性角色

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。

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 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，並決定安全性功能，以部署智慧卡、生物測定讀取器或 USB Token 等裝置。

  安全性主管可與 HP 合作，自訂 ProtectTools 的許多功能。有關其他資訊，請造訪 http://www.hp.com。

- 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，若安全性主管已決定部署智慧卡，IT 管理員就能啓用智慧卡 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智慧卡，則使用者可設定智慧卡 PIN 和使用智慧卡進行驗證。

管理 ProtectTools 密碼

大多數 ProtectTools 安全管理員 (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。

ProtectTools 密碼	在此 ProtectTools 模組中設定	功能
電腦設定的管理員密碼 ✎ 也稱為 BIOS 管理員、**F10** 設定或安全性設定密碼	BIOS 組態，由 IT 管理員設定	保護對「電腦設定 (Computer Setup)」公用程式的存取。
磁碟機/光碟機鎖 (DriveLock) 主要密碼	BIOS 組態，由 IT 管理員設定	保護存取受磁碟機/光碟機鎖 (DriveLock) 保護的內建式硬碟。也可用來移除磁碟機/光碟機鎖 (DriveLock) 保護。
磁碟機/光碟機鎖 (DriveLock) 使用者密碼	BIOS 組態	保護存取受磁碟機/光碟機鎖 (DriveLock) 保護的內建式硬碟。
開機密碼 (Power-On Password)	BIOS 組態	當電腦啟動、重新啟動或從休眠狀態回復時，可保護對電腦內容的存取。
設定檔密碼	BIOS 組態，由 IT 管理員設定	加密（與解除鎖定）儲存了 BIOS 系統設定的設定檔。
智慧卡管理員密碼 ✎ 也稱為 BIOS 管理員卡密碼	智慧卡安全性， 由 IT 管理員設定	將智慧卡連結到電腦以執行識別作業。 允許電腦管理員啟用或停用「電腦設定 (Computer Setup)」密碼、產生新的管理員卡，並建立復原檔案來還原使用者或管理員卡。

（續）

ProtectTools 密碼	在此 ProtectTools 模組中設定	功能
智慧卡 PIN 碼	智慧卡安全性	使用選購的智慧卡和讀取器時，保護智慧卡內容和電腦的存取。
智慧卡復原檔密碼	智慧卡安全性	保護內含 BIOS 密碼的復原檔存取。
智慧卡使用者密碼 ✎ 也稱為 BIOS 使用者卡密碼	智慧卡安全性	將智慧卡連結到電腦以進行識別。 允許使用者建立復原檔來還原使用者卡。
基本使用者金鑰密碼 ✎ 也稱為：嵌入式安全性密碼	嵌入式安全性	在啟用做為 BIOS 開機驗證支援密碼後，當電腦啟動、重新啟動或從休眠狀態還原時，可保護對電腦內容的存取。
緊急復原記號 (Token) 密碼 ✎ 也稱為：緊急復原記號 (Token) 金鑰密碼	嵌入式安全性， 由 IT 管理員設定	保護緊急復原記號 (Token) 內建式安全晶片的備份檔案之存取。
擁有者密碼	嵌入式安全性， 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」的全部擁有者功能。
認證管理員登入密碼	認證管理員	這個密碼可提供 2 個選項： ■ 登入 Microsoft 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」。 ■ 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。

（續）

ProtectTools 密碼	在此 ProtectTools 模組中設定	功能
認證管理員復原檔密碼	認證管理員，由 IT 管理員設定	保護認證管理員復原檔的存取。
Windows 登入密碼	Windows 控制台	可使用於手動登入或儲存在智慧卡上。

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。
- 請勿使用字典裡有的字做爲密碼。
- 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。

2

ProtectTools 的智慧卡安全性

基本概念

「ProtectTools 的智慧卡安全性」可管理具選購智慧卡讀取器的電腦之智慧卡設定和組態。

使用智慧卡安全性，您可以

- 存取智慧卡安全性功能。
- 初始化智慧卡，以便與其他 ProtectTools 模組，例如 ProtectTools 的認證管理員 (Credential Manager for ProtectTools)，一起搭配使用。
- 在預先開機的環境中，使用「電腦設定」(Computer Setup) 公用程式來啓用智慧卡驗證，以及爲管理員和使用者設定不同的智慧卡。這個動作將要求使用者插入智慧卡，並選擇先輸入 PIN 碼，再允許作業系統載入。
- 設定及變更密碼，以便使用該密碼來驗證智慧卡之使用者。
- 備份及還原智慧卡所儲存的智慧卡 BIOS 密碼。

初始化智慧卡

使用智慧卡前必須先初始化該智慧卡。

若要初始化智慧卡：

1. 將智慧卡插入讀取器。
2. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
3. 選擇加號 **(+)** 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「智慧卡 (Smart Card)」**。
4. 按一下 **「初始化 (Initialize)」**。
5. 在 **「初始化智慧卡 (Initialize the smart card)」**對話方塊的第一個方塊中鍵入您的名稱。
6. 在適當的方塊中設定及確認智慧卡 PIN。PIN 密碼必須有 4 到 8 個數字字元。

   △ 為免失去電腦的存取權限，請牢記智慧卡 PIN。如果忘了智慧卡 PIN，就無法操作電腦。除非在 5 次嘗試內正確輸入智慧卡 PIN，否則該智慧卡將被鎖定且無法使用。輸入正確的 PIN 後，嘗試輸入的計數會被重設歸零。

7. 按一下 **「確定」**完成初始化。

智慧卡 BIOS 安全性模式

啓用後，智慧卡 BIOS 安全性模式將要求您使用智慧卡來登入電腦。

智慧卡 BIOS 安全性模式的啓用程序包含下列步驟：

1. 在 BIOS 組態中啓用智慧卡開機驗證支援。請參閱第 4 章〈ProtectTools 的 BIOS 配置〉的「啓用與停用智慧卡開機驗證支援」。

   ✎ 您可以啓用此設定，使用智慧卡進行開機驗證。啓用智慧卡開機驗證支援後，才能使用智慧卡 BIOS 安全性模式功能。

2. 在「智慧卡安全性 (Smart Card Security)」中啓用智慧卡 BIOS 安全性模式。請參閱本章稍後的「啓用智慧卡 BIOS 安全性模式與設定智慧卡管理員密碼」。
3. 設定智慧卡管理員密碼。

   ✎ 在啓用智慧卡 BIOS 安全性模式的過程中，會設定智慧卡管理員密碼。

智慧卡管理員密碼與「電腦設定 (Computer Setup)」管理員密碼不同。智慧卡管理員密碼可將智慧卡連結到電腦以進行識別，您也可以使用該密碼來執行下列工作：

- 啓用或停用「電腦設定 (Computer Setup)」密碼
- 建立新管理員和使用者智慧卡
- 建立復原檔來還原使用者或管理員智慧卡

在「智慧卡安全性 (Smart Card Security)」中啓用智慧卡 BIOS 安全性模式後，才能設定智慧卡管理員密碼。

啟用智慧卡 BIOS 安全性模式與設定智慧卡管理員密碼

若要啓用智慧卡 BIOS 安全性模式及設定智慧卡管理員密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。
3. 在 **「BIOS 安全性模式 (BIOS Security Mode)」**下，按一下 **「啟用 (Enable)」**。
4. 按一下 **「下一步」**。
5. 在提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「下一步」**。
6. 插入新的管理員智慧卡，並遵循螢幕上的指示。指示可能會改變，且可能包含下列工作：
   - ❑ 初始化智慧卡。請參閱「初始化智慧卡」以取得詳細說明。
   - ❑ 設定智慧卡管理員密碼。請參閱「儲存管理員或使用者卡密碼」以取得詳細說明。
   - ❑ 建立復原檔。請參閱「建立復原檔」以取得詳細說明。

停用智慧卡 BIOS 安全性模式

停用智慧卡 BIOS 安全性模式時，也會停用智慧卡管理員和使用者密碼，且不再需要使用智慧卡，就能存取電腦。

若先前已啓用智慧卡 BIOS 安全性模式，「智慧卡安全性 BIOS (Smart Card Security BIOS)」頁面的按鈕將會變爲「停用 (Disable)」。

若要停用智慧卡安全性：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。
3. 在 **「BIOS 安全性模式 (BIOS Security Mode)」**下，按一下 **「停用 (Disable)」**。
4. 插入內含現行智慧卡管理員密碼的卡，再按一下 **「下一步」**。
5. 在提示上輸入智慧卡 PIN，再按一下 **「完成 (Finish)」**。

變更智慧卡管理員密碼

在啓用智慧卡 BIOS 安全性模式的過程中，會設定智慧卡管理員密碼。設定智慧卡管理員密碼後，您可以變更它。請參閱本章稍早的「智慧卡 BIOS 安全性模式」，瞭解智慧卡管理員密碼的詳細資訊。

下列程序會更新智慧卡及「電腦設定」(Computer Setup) 所儲存的智慧卡管理員密碼。

變更智慧卡管理員密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。
3. 在 **「BIOS 安全性模式 (BIOS Security Mode)」**的 **「BIOS 管理員卡 (BIOS administrator card)」**旁，按一下 **「變更」**。
4. 輸入智慧卡 PIN，再按一下 **「下一步」**。
5. 插入新的管理員卡，再按一下 **「下一步」**。
6. 輸入智慧卡 PIN，再按一下 **「完成 (Finish)」**。

設定與變更智慧卡使用者密碼

若要設定或變更智慧卡使用者密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。
3. 在 **「BIOS 安全性模式 (BIOS Security Mode)」**的 **「BIOS 使用者卡 (BIOS user card)」**旁，按一下 **「設定 (Set)」**按鈕。

   ✎若「電腦設定 (Computer Setup)」已有使用者密碼，請按一下 **「變更」**按鈕。

4. 輸入智慧卡 PIN，再按一下 **「下一步」**。
5. 插入新的使用者卡，再按一下 **「下一步」**。
   - ❏ 如果卡上已有使用者密碼，則會顯示 **「完成 (Finish)」**對話方塊。省略步驟 6 到 8，並移至步驟 9。
   - ❏ 若卡上沒有使用者密碼，則會開啓「BIOS 密碼精靈 (BIOS Password Wizard)」。
6. 在「BIOS 密碼精靈 (BIOS Password Wizard)」中，您可以
   - ❏ 手動輸入密碼。
   - ❏ 產生隨機的 32 位元組密碼。

   ✎使用已知的密碼，如此您就能建立重複的卡而不必使用復原檔。產生隨機的密碼可提供更強的安全性；不過，您必須具有復原檔才能製作備份卡。

7. 在 **「開機需求 (Boot Requirements)」**下，如果您需要在啓動時輸入智慧卡 PIN，請選擇此核取方塊。

   ✎ 若不需要在啓動時輸入智慧卡 PIN，請清除此核取方塊。

8. 輸入智慧卡 PIN，再按一下 **「確定」**。系統會提示您建立復原檔。

   ✎ 強烈建議您建立復原檔。有關其他資訊，請參閱本章中的「建立復原檔」。

9. 在 **「完成」**對話方塊中輸入智慧卡 PIN，然後按一下 **「完成」**。

儲存管理員或使用者卡密碼

如果您要建立備份卡，而且已設定管理員密碼，則可在新卡上儲存密碼。

⚠ **注意：**這個程序只會更新卡上的密碼，而不會更新「電腦設定」(Computer Setup) 上的密碼。您不能以新卡存取電腦。

若要儲存管理員或使用者卡密碼：

1. 將智慧卡插入讀取器。
2. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
3. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。

4. 在 **「智慧卡上的 BIOS 密碼 (BIOS Password on Smart Card)」**下，按一下 **「儲存 (Store)」**。
5. 在「BIOS 密碼精靈 (BIOS Password Wizard)」中，您可以
   - ❏ 手動輸入密碼。
   - ❏ 產生隨機的 32 位元組密碼。

   ✎ 使用已知的密碼，如此您就能建立重複的卡而不必使用復原檔。產生隨機的密碼可提供更強的安全性；不過，您必須具有復原檔才能製作備份卡。

6. 在 **「存取權限 (Access Privilege)」**下，按一下 **「管理員」**或 **「使用者」**做爲卡的類型。
7. 在 **「開機需求 (Boot Requirements)」**下，如果您需要在啓動時輸入智慧卡 PIN，請選擇此核取方塊。

   ✎ 若不需要在啓動時輸入智慧卡 PIN，請清除此核取方塊。

8. 輸入智慧卡 PIN，再按一下 **「確定」**。
9. 在 **「完成」**對話方塊中重新輸入智慧卡 PIN，然後按一下 **「完成」**。系統會提示您建立復原檔。

✎ 強烈建議您建立智慧卡復原檔。有關其他資訊，請參閱本章中的「建立復原檔」。

一般工作

更新 BIOS 智慧卡設定

若需智慧卡 PIN 來重新啓動電腦：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 按一下加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「BIOS」**。
3. 在 **「智慧卡 BIOS 密碼內容 (Smart Card BIOS Password Properties)」** 下，按一下 **「設定」**。
4. 選擇核取方塊，要求重新開機所需的 PIN。

   ✎若要排除此需求，請清除核取方塊。

5. 輸入智慧卡 PIN，再按一下 **「確定」**。

選擇智慧卡讀取器

確定先在「智慧卡安全性 (Smart Card Security)」中選擇正確的智慧卡讀取器，再使用智慧卡。若未在「智慧卡安全性 (Smart Card Security)」中選擇正確的讀取器，則可能無法使用或正確顯示部份功能。

若要選擇智慧卡讀取器：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「一般」**。
3. 在 **「智慧卡讀取器 (Smart Card Reader)」** 下，選擇正確的讀取器。
4. 將智慧卡插入讀取器。會自動更新讀取器資訊。

變更智慧卡 PIN

若要變更智慧卡 PIN：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「智慧卡 (Smart Card)」**。
3. 按一下 **「變更 PIN (Change PIN)」**。
4. 鍵入您目前的智慧卡 PIN。
5. 設定及確認新 PIN。
6. 在確認對話方塊中按一下 **「確定」**。

備份和還原智慧卡

初始化智慧卡並準備好使用卡後，強烈建議您建立智慧卡復原檔。您可以使用復原檔在智慧卡之間傳送智慧卡資料。也可使用該檔案來備份原始的智慧卡，或在智慧卡遺失或遭竊時還原資料。

注意：若要避免復原檔與具有更新資訊的智慧卡不符，請立即建立新的復原檔並存放在安全的地點。如果您保存備份智慧卡，則也必須將新的復原檔還原到備份智慧卡，以更新備份智慧卡的資訊。

建立復原檔

若要建立復原檔：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「智慧卡 (Smart Card)」**。
3. 在 **「復原」** 下，按一下 **「建立 (Create)」**。
4. 輸入智慧卡 PIN，再按一下 **「確定」**。
5. 在 **「檔名 (Filename)」** 欄位中輸入檔案路徑和檔名。

   △ **若要避免遺失電腦的存取，請勿在電腦硬碟上儲存復原檔；您必須使用智慧卡才能存取檔案。此外，他人可存取硬碟所儲存的復原檔，而這可能會有安全上的風險。**

6. 設定和確認復原檔密碼，再按一下 **「確定」**。

△ **注意：為了避免遺失智慧卡復原檔資料，請記住復原檔密碼。如果您忘記密碼，則無法從復原檔重建卡。**

還原智慧卡資料

您可以從復原檔還原智慧卡資料。如果卡已遺失或遭竊，或想要建立備份智慧卡時，則這個動作特別有用。如果您使用卡與其先前所儲存的資料，則會覆寫該資料。

開始之前，您需要執行下列動作：

- 存取到安裝「智慧卡安全性」(Smart Card Security) 軟體的電腦
- 智慧卡復原檔
- 智慧卡復原檔密碼
- 智慧卡

若要還原智慧卡：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「智慧卡安全性 (Smart Card Security)」**。
2. 選擇加號 (+) 以展開「智慧卡安全性 (Smart Card Security)」功能表，然後選擇 **「智慧卡 (Smart Card)」**。
3. 插入磁片或包含智慧卡復原檔的其他媒體。
4. 將智慧卡插入讀取器。若未對卡進行初始化，系統會提示您初始化該卡。如需初始化智慧卡的詳細說明，請參閱本章前面的「初始化智慧卡」。
5. 在 **「復原」**區段中，按一下 **「還原」**。
6. 確定選擇正確的復原檔名稱，並輸入復原檔密碼。
7. 輸入智慧卡 PIN。
8. 按一下 **「確定」**。原始的智慧卡內容會還原到新的智慧卡。

建立備份智慧卡

強烈建議您建立多張一樣的智慧卡，做爲備份。您可使用兩個方法來建立備份卡，依據智慧卡密碼是手動或隨機產生而定。

若要以隨機產生的智慧卡密碼來建立更換的智慧卡：

» 將智慧卡插入讀取器，然後將適當的復原檔載入其中。有關其他資訊，請參閱本章前面的「還原智慧卡資料」。

若要以手動產生的智慧卡密碼來建立更換的智慧卡：

1. 初始化新的智慧卡。如需相關說明，請參閱本章前面的「初始化智慧卡」。
2. 在新的智慧卡上儲存管理員或使用者卡密碼。如需相關說明，請參閱本章前面的「儲存管理員或使用者卡密碼」。

3

ProtectTools 的嵌入式安全性

基本概念

您必須在電腦中安裝整合的「信任平台模組 (TPM)」內建式安全晶片，才能使用「ProtectTools 的嵌入式安全性」。

「ProtectTools 的嵌入式安全性」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」軟體時，針對受保護的數位認證作業，提供支援協力廠商應用程式（例如 Microsoft Outlook 與 Internet Explorer）的支援

TPM 內建式安全晶片可增強並啓用 ProtectTools 安全管理員 (ProtectTools Security Manager) 的其他安全性功能。例如，ProtectTools 的認證管理員 (Credential Manager for ProtectTools) 可使用嵌入式晶片，做爲使用者登入 Windows 時的驗證因素。在選擇機型上，TPM 內建式安全晶片也可透過 ProtectTools 的 BIOS 配置，來存取增強的 BIOS 安全性功能。

安裝程序

注意：為了降低安全性風險，強烈建議您的 IT 管理員立即初始化內建式安全晶片。沒有初始化內建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內建式安全晶片。

啟用內建式安全晶片

必須在「電腦設定」(Computer Setup) 公用程式中啓用內建式安全晶片。這個程序無法在「ProtectTools 的 BIOS 配置 (BIOS Configuration for ProtectTools)」中執行。

若要啓用內建式安全晶片：

1. 若要開啓「電腦設定 (Computer Setup)」，請啓動或重新啓動電腦，然後在螢幕左下角顯示「F10 = ROM Based Setup」訊息時，按 **F10** 鍵。
2. 若尚未設定管理員密碼，請使用方向鍵以選擇 **「安全性 (Security)」 > 「管理員密碼 (Administrator Password)」**，然後按 **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 **F10** 鍵。
4. 在 **「安全性 (Security)」**功能表中，使用方向鍵來選擇 **「嵌入式安全性 (Embedded Security)」**，再按 **ENTER** 鍵。
5. 在 **「嵌入式安全性 (Embedded Security)」**下，選擇 **「嵌入式安全性裝置狀態 (Embedded security device state)」**，再變爲 **「啟用 (Enable)」**。
6. 按 **F10** 來接受對「嵌入式安全性 (Embedded Security)」組態所做的變更。
7. 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)」 > 「儲存變更後離開 (Save Changes and Exit)」**。然後依照螢幕上的指示進行。

初始化內建式安全晶片

在嵌入式安全性的初始化過程中，您將

- 設定內建式安全晶片的擁有者密碼，保護內建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。

若要初始化內建式安全晶片：

1. 在工作列最右邊的通知區中，在「嵌入式安全性 (Embedded Security)」圖示上按一下滑鼠右鍵，再選擇 **「嵌入式安全性初始化 (Embedded Security Initialization)」**。「ProtectTools 嵌入式安全性初始化精靈 (ProtectTools Embedded Security Initialization Wizard)」將會開啓。
2. 按一下 **「下一步」**。
3. 設定和確認擁有者密碼，再按一下 **「下一步」**。**「設定緊急復原 (Setup Emergency Recovery)」**對話方塊開啓。
4. 按一下 **「下一步」**接受預設的復原封存位置，或按一下 **「瀏覽 (Browse)」**按鈕來選擇不同的位置，再按一下 **「下一步」**。
5. 設定和確認緊急復原記號 (Token) 密碼，再按一下 **「下一步」**。
6. 按一下 **「瀏覽 (Browse)」**並選擇緊急復原封存的位置，再按一下 **「下一步」**。

7. 按一下「摘要 (Summary)」頁面的 **「下一步」**。
   - ❑ 如果您不想在這個時候設定基本使用者帳戶，請清除 **「啟動嵌入式安全性使用者初始化精靈 (Start the Embedded Security User Initialization Wizard)」**核取方塊，再按一下 **「完成」**。您可以遵循下一節的說明，隨時設定基本使用者帳戶來手動啓動精靈。
   - ❑ 如果您想設定基本使用者帳戶，請選擇 **「啟動嵌入式安全性使用者初始化精靈 (Start the Embedded Security User Initialization Wizard)」**核取方塊，再按一下 **「完成」**。「嵌入式安全性使用者初始化精靈 (Embedded Security Initialization Wizard)」將會開啓。詳細資訊，請參閱下一節的說明。

設定基本使用者帳戶

在「嵌入式安全性 (Embedded Security)」設定基本使用者帳戶

- 產生基本使用者金鑰來保護加密的資料，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. 若未開啓「嵌入式安全性使用者初始化精靈 (Embedded Security User Initialization Wizard)」，請選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「使用者設定 (User Settings)」**。

2. 在 **「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。
3. 按一下 **「下一步」**。
4. 設定和確認基本使用者金鑰密碼，再按一下 **「下一步」**。
5. 按一下 **「下一步」**確認設定。
6. 選擇所要的安全性功能，再按一下 **「下一步」**。
7. 再按一下 **「下一步」**。

   ✎ 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。若無法使用數位憑證，您必須從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相關說明，請參閱電子郵件用戶端線上說明。

8. 若存在多個加密憑證，請選擇適當的憑證，再按一下 **「下一步」**。
9. 選擇您 PSD 的磁碟機代號和標籤，再按一下 **「下一步」**。
10. 選擇 PSD 的大小和位置，再按一下 **「下一步」**。
11. 按一下「摘要 (Summary)」頁面的 **「下一步」**。
12. 按一下 **「完成」**。

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輸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

在 Windows XP Professional 中使用加密的檔案時，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」**。

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。有關其他資訊，請參閱嵌入式安全性的線上說明，及您電子郵件的線上說明。

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. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「使用者設定 (User Settings)」**。
2. 在 **「基本使用者金鑰密碼 (Basic User Key password)」** 下，按一下 **「變更」**。
3. 鍵入舊密碼，然後設定和確認新密碼。
4. 按一下 **「確定」**。

進階工作

備份和還原

「嵌入式安全性」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. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「備份 (Backup)」**。
2. 選擇 **「備份 (Backup)」**。
3. 按一下 **「瀏覽 (Browse)」**來選擇備份檔的儲存位置。
4. 選擇是否將緊急復原封存新增至備份資料。
5. 按一下 **「下一步」**。
6. 按一下 **「完成」**。

從備份檔還原憑證資料

若要從備份檔還原資料：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「備份 (Backup)」**。
2. 按一下 **「還原」**。
3. 按一下 **「瀏覽 (Browse)」**，從儲存的位置選擇備份檔。
4. 按一下 **「下一步」**。
5. 選擇是否啓動「嵌入式安全性使用者初始化精靈 (Embedded Security Initialization Wizard)」。
   - ❑ 如果您選擇啓動初始化精靈，請按一下 **「完成」**，然後遵循螢幕的指示來完成初始化。有關其他資訊，請參閱本章前面的「設定基本使用者帳戶」。
   - ❑ 若選擇不啓動初始化精靈，請按一下 **「完成」**。

變更擁有者密碼

若要變更擁有者密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「進階」**。
2. 在 **「擁有者密碼 (Owner Password)」** 下，按一下 **「變更」**。
3. 鍵入舊的擁有者密碼，然後設定和確認新的擁有者密碼。
4. 按一下 **「確定」**。

啟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」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」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」。這個選項僅適用於管理員。

暫時停用嵌入式安全性

若要暫時停用嵌入式安全性：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「使用者設定 (User Settings)」**。
2. 在 **「嵌入式安全性 (Embedded Security)」** 下，按一下 **「停用」**。

暫時停用後啟用嵌入式安全性

若是透過「使用者設定 (User Settings)」停用「嵌入式安全性 (Embedded Security)」，則在重新啓動 Windows 時會自動重新啓用它。

如果您登出 Windows 帳戶但未重新啓動電腦，則當您或另一名使用者登入 Windows 時，仍將停用「嵌入式安全性」功能，直到電腦重新啓動爲止。

永遠停用嵌入式安全性

若要永遠停用嵌入式安全性：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「進階」**。
2. 在 **「嵌入式安全性 (Embedded Security)」** 下，按一下 **「停用」**。
3. 在提示上輸入您的擁有者密碼，再按一下 **「確定」**。

永遠停用後啟用嵌入式安全性

若要在永遠停用嵌入式安全性後啓用它：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「嵌入式安全性 (Embedded Security)」 > 「進階」**。
2. 在 **「嵌入式安全性 (Embedded Security)」** 下，按一下 **「啟用」**。
3. 在提示上輸入您的擁有者密碼，再按一下 **「確定」**。

以轉移精靈轉移金鑰

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。

如需轉移的詳細資訊，請參閱嵌入式安全性的線上說明。

4

ProtectTools 的 BIOS 配置

基本概念

ProtectTools 的 BIOS 配置可存取「電腦設定 (Computer Setup)」公用程式的安全性和配置設定。它能讓使用者利用 Windows 存取「電腦設定 (Computer Setup)」所管理的系統安全性功能。

利用 BIOS 配置，您可以

- 管理開機密碼和管理員密碼。
- 設定其他預先開機的驗證功能，例如智慧卡密碼和嵌入式安全性驗證。
- 啓用和停用硬體功能，例如光碟開機功能或不同的硬體埠。
- 設定開機選項 (Boot Options)，包括啓用多重開機 (MultiBoot) 和變更開機順序 (Boot Order)。

您也能在「電腦設定 (Computer Setup)」公用程式中，使用「ProtectTools 的 BIOS 配置」的許多功能。

一般工作

BIOS 配置可讓您管理各種電腦設定，否則您只能在啓動時按 **F10**，再進入「電腦設定 (Computer Setup)」公用程式來存取這些設定。

管理開機選項

您可以使用 BIOS 配置來管理開啓或重新啓動電腦時所執行的工作之各種設定。

若要管理開機選項：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 在 BIOS 管理員密碼提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「確定」**。

   ✎ 只有在您已設定「電腦設定 (Computer Setup)」管理員密碼時，才會顯示 BIOS 管理員密碼提示。有關設定「電腦設定 (Computer Setup)」管理員密碼的相關資訊，請參閱本章前面的「設定管理員密碼」。

3. 選擇或清除 **「啟用快速開機 (Enable Quick boot)」**核取方塊。
4. 選擇 **F10** 和 **F12** 的延遲秒數，和 **「快速開機快顯 (Express Boot Popup」**的延遲秒數。
5. 選擇或清除 **「啟用多重開機 (Enable MultiBoot)」**核取方塊。
6. 若已啓用多重開機，請藉由選擇開機裝置來選擇開機順序，然後按一下 **「上移 (Move Up)」**或 **「下移 (Move Down)」**來調整其在清單中的順序。
7. 按一下 **「套用」**，再按一下 ProtectTools 視窗中的 **「確定」**以儲存變更。

啟用與停用裝置或安全性選項

若要啓用或停用裝置或安全性選項：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 在 BIOS 管理員密碼提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「確定」**。
3. 按一下 **「裝置選項 (Device Options)」**。
4. 選擇或清除下列選項的任何組合：
   - ❏ 開機時的 NumLock 鍵
   - ❏ 交換 Fn/Ctrl 鍵
   - ❏ 多個指標裝置
   - ❏ USB 舊版支援
   - ❏ 自動 SpeedStep 功能支援
   - ❏ 使用 AC 電源時永遠啓動風扇
5. 從下拉式方塊中選擇並列埠模式。
6. 按一下 **「安全性」**。
7. 選擇或清除下列選項的任何組合：
   - ❏ 序列埠
   - ❏ 紅外線埠
   - ❏ 並列埠
   - ❏ SD 插槽
   - ❏ CD-ROM 開機
   - ❏ 軟碟開機
   - ❏ 內建網路介面卡開機
8. 按一下 **「套用」**，再按一下 ProtectTools 視窗中的 **「確定」**以儲存變更並結束。

進階工作

管理 ProtectTools 設定

可在「BIOS 配置 (BIOS Configuration)」中管理 ProtectTools 安全管理員 (ProtectTools Security Manager) 的部份功能。

啟用與停用智慧卡開機驗證支援

啓用此選項可讓您使用智慧卡，以便在啓動電腦時進行使用者驗證。

若要啓用智慧卡開機驗證支援：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 在 BIOS 管理員密碼提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「確定」**。
3. 選擇 **「安全性」**。
4. 按一下 **「進階 (Advanced)」**。
5. 在 **「智慧卡安全性 (Smart Card Security)」**下，選擇 **「啟用智慧卡開機驗證支援 (Enable Smart Card Power-on Authentication Support)」**核取方塊。

   ✎若要停用智慧卡開機驗證，請清除此核取方塊。

6. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」**以儲存變更。

為嵌入式安全性啟用及停用開機驗證支援

啓用此選項可讓系統使用 TPM 內建式安全晶片（可用的話），以便在啓動電腦時進行使用者驗證。

若要啓用嵌入式安全性的開機驗證支援：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 在 BIOS 管理員密碼提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「確定」**。
3. 選擇 **「安全性」**。
4. 按一下 **「進階 (Advanced)」**。
5. 在 **「嵌入式安全性 (Embedded Security)」** 下，選擇 **「啟用開機驗證支援 (Enable Power-on Authentication Support)」** 核取方塊。

   ✎ 若要停用嵌入式安全性的開機驗證，請清除此核取方塊。

6. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

啟用及停用自動磁碟機/光碟機鎖硬碟保護

在啓用此選項後，TPM 內建式安全晶片就會產生和保護磁碟機/光碟機鎖密碼。會設定磁碟機/光碟機鎖主密碼來符合電腦設定管理員密碼，而磁碟機/光碟機鎖使用者密碼會由 TPM 隨機產生並加以保護。

無法使用可啓用自動磁碟機/光碟機鎖的選項，除非

- 電腦已安裝和初始化 TPM 安全晶片。有關如何啓用和初始化 TPM 安全晶片的相關說明，請參閱第 3 章〈ProtectTools 的嵌入式安全性〉的「啓用內建式安全晶片」和「初始化內建式安全晶片」。
- 尚未啓用磁碟機/光碟機鎖密碼。

如果您已在電腦上手動設定磁碟機/光碟機鎖密碼，您必須先停用它們，才能設定自動磁碟機/光碟機鎖保護。

若要啓用或停用自動磁碟機/光碟機鎖保護：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 在 BIOS 管理員密碼提示上輸入「電腦設定 (Computer Setup)」管理員密碼，再按一下 **「確定」**。
3. 選擇 **「安全性」**。
4. 按一下 **「進階 (Advanced)」**。
5. 在 **「嵌入式安全性 (Embedded Security)」** 下，選擇 **「啟用自動磁碟機/光碟機鎖保護 (Enable Automatic DriveLock Protection)」** 核取方塊。

   若要停用嵌入式安全性的開機驗證，請清除此核取方塊。

6. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

管理設定檔

在「ProtectTools 的 BIOS 配置」中設定了偏好設定後，您可將這些設定儲存在已命名的設定檔之下。這些設定會儲存在檔案中，並使用您輸入的密碼加密。然後，您就可將此設定檔套用在多個平台上。

您必須重新啓動電腦，這些設定才會生效。

使用指令行管理設定檔

您可以使用指令行介面來管理 BIOS 配置的設定檔。從指令行，您可以

- 在「ProtectTools 的 BIOS 配置」中變更設定來顯示「設定檔」頁面（預設隱藏）
- 存取及開啓設定檔配置
- 在多部電腦之間套用設定檔

若要從指令行存取與修改設定檔設定：

1. 選擇 **「開始」 > 「執行」**。
2. 在 **「開啟 (Open)」**方塊中輸入 cmd.exe 。
3. 按一下 **「確定」**。
4. 在指令提示上，請使用 cd 指令以瀏覽到以下「BIOS 配置 (BIOS Configuration)」公用程式的路徑：

   C:\Program Files\HPQ\HP BIOS Configuration for ProtectTools

5. 輸入 hpqsetup.exe，並新增開關以自訂要求，如下表所示。

開關	功能	範例
/f 及 /k ✎ 可一起使用這 2 個開關。	**/f:** 指定 INI 檔案路徑 **/k:** 指定密碼來解密「BIOS 配置 (BIOS Configuration)」工具所建立的檔案	Hpqsetup.exe /fc:\test.ini /kxxxx （其中 *test* 是 INI 檔案的名稱，而 *xxxx* 是密碼）
/p	在「ProtectTools 的 BIOS 配置」頁面上顯示「設定檔」頁面（預設隱藏） （需要重新啟動 ProtectTools）	Hpqsetup.exe /p

6. 按下 **ENTER** 鍵。

儲存新設定檔配置

若要儲存新設定檔配置：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 按一下 **「設定檔」**。

   ✎ 若看不到「設定檔」頁面，您必須從指令行變更顯示設定。若需指示，請參閱前一節的「使用指令行管理設定檔」。

3. 按一下 **「另存新檔 (Save As)」**。
4. 在對話方塊中，鍵入此設定檔的名稱。
5. 設定和確認密碼以加密檔案。
6. 在 **「新增設定檔 (Add Profile)」**對話方塊中按一下 **「確定」**。
7. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」**以儲存變更。

刪除設定檔配置

若要刪除設定檔配置：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「設定檔」**。
3. 從下拉式清單中選擇您要刪除的設定檔。
4. 按一下 **「刪除 (Delete)」**。
5. 在確認對話方塊中按一下 **「是」**。

會從下列位置刪除該設定檔所建立的 INI 檔案：

C:\Program Files\HPQ\HP BIOS Configuration for ProtectTools \INIFiles

套用設定檔配置

您可透過 HP BIOS Configuration for ProtectTools，將任何設定檔配置套用至新平台上。

若要套用設定檔配置：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「設定檔」**。
3. 從下拉式清單中選擇您要套用的設定檔配置。
4. 請按下 **「套用」**。
5. 按一下 **「確定」**。XXX.ini 檔案儲存在下列位置：

   C:\Documents and Settings\All Users\Application Data\BIOS Configuration\INIFiles

在多部電腦之間套用設定檔配置

IT 管理員可使用 HPQSetup 應用程式和部署工具，在一個網路的多個平台之間套用 BIOS 配置設定檔。HPQSetup 應用程式只能與部署工具搭配使用，且只能從指令行執行。有關其他資訊，請參閱此文件前面的「使用指令行管理設定檔」。

管理電腦設定密碼

您可以使用 BIOS 配置，在「電腦設定 (Computer Setup)」中設定和變更開機及管理員密碼，也可以管理各種密碼設定。

注意：在按下 ProtectTools 視窗的 **「套用」**或 **「確定」**按鈕時，會立即儲存透過 BIOS 配置的「密碼」頁面所設定的密碼。請確定您設定的密碼，因為您必須輸入舊密碼，才能還原密碼設定。

開機密碼可防止他人未經授權使用您的筆記型電腦。

在設定開機密碼後，「密碼」頁面上的「設定」按鈕，將會被「變更」按鈕取代。

「電腦設定 (Computer Setup)」管理員密碼可保護「電腦設定 (Computer Setup)」中的組態設定和系統識別資訊。密碼設定好之後，必須要輸入這個密碼才能存取「電腦設定 (Computer Setup)」。如果您已設定管理員密碼，則在您開啓「ProtectTools 的 BIOS 配置」部份前，會提示您先輸入密碼。

在設定管理員密碼後，「密碼」頁面上的「設定」按鈕，將會被「變更」按鈕取代。

設定開機密碼

若要設定開機密碼 (Power-On Password)：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 在 **「開機密碼 (Power-On Password)」** 下，選擇 **「設定」**。
4. 在 **「輸入密碼 (Enter Password)」** 和 **「確認密碼 (Verify Password)」** 方塊中鍵入和確認密碼。
5. 在 **「密碼」** 對話方塊中按一下 **「確定」**。
6. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

變更開機密碼

若要變更開機密碼 (Power-On Password)：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 在 **「開機密碼 (Power-On Password)」** 下，按一下 **「變更」**。
4. 在 **「舊密碼 (Old Password)」** 方塊中，鍵入目前的密碼。
5. 在 **「輸入新密碼」** 方塊中設定和確認新密碼。
6. 在 **「密碼」** 對話方塊中按一下 **「確定」**。
7. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

設定管理員密碼

若要設定電腦設定的管理員密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 在 **「管理員密碼 (Administrator Password)」** 下，選擇 **「設定」**。
4. 在 **「輸入密碼 (Enter Password)」** 和 **「確認密碼 (Verify Password)」** 方塊中設定和確認密碼。
5. 在 **「密碼」** 對話方塊中按一下 **「確定」**。
6. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

變更管理員密碼 (Administrator Password)

若要變更「電腦設定 (Computer Setup)」的管理員密碼：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 在 **「管理員密碼 (Administrator Password)」** 下，按一下 **「變更」**。
4. 在 **「舊密碼」** 方塊中，鍵入目前的密碼。
5. 在 **「輸入新密碼」** 和 **「確認新密碼」** 方塊中鍵入和確認新密碼。
6. 在 **「密碼」** 對話方塊中按一下 **「確定」**。
7. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

設定密碼選項

您可使用 ProtectTools 的 BIOS 配置來設定密碼選項，以增強系統的安全性。

啟用和停用嚴密安全性

注意：若要電腦永久無法使用，請記下您設定的管理員密碼、開機密碼或智慧卡 PIN 碼，並將它們與電腦分開保存，置於安全的地方。若沒有這些密碼或 PIN 碼，就無法將電腦解除鎖定。

「啓用嚴密安全性」可增強對開機密碼和管理員密碼，及其他開機驗證形式的防護。

若要啓用或停用嚴密安全性：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 選擇 **「啟用嚴密安全性 (Enable Stringent Security)」**核取方塊。

   ✎若要停用嚴密安全性，請清除此核取方塊。

4. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」**以儲存變更。

啟用和停用在 Windows 重新啟動時，進行開機驗證

此選項會在 Windows 重新啓動時，要求使用者輸入開機、TPM、磁碟機/光碟機鎖或智慧卡密碼，以增強安全性。

若要在 Windows 重新啓動時啓用或停用開機驗證：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「BIOS 配置 (BIOS Configuration)」**。
2. 選擇 **「密碼」**。
3. 選擇 **「啟用在 Windows 重新啟動時，進行開機驗證 (Enable Power-on Authentication on Windows restart)」** 核取方塊。

   ✎ 若要在 Windows 重新啓動時停用開機驗證，請清除此核取方塊。

4. 按一下 **「套用」**，再按一下 ProtectTools 視窗的 **「確定」** 以儲存變更。

5

ProtectTools 的認證管理員

基本概念

ProtectTools 的認證管理員 (Credential Manager for ProtectTools) 具有安全性功能，可防止未授權者存取電腦。這些功能包括下列各項：

- 不使用密碼登入 Microsoft Windows 的替代方案，如使用智慧卡或生物測定讀取器登入 Windows。
- 單一登入功能，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，如智慧卡和生物測定讀取器。
- 支援其他安全性設定，如要求以選購的安全性裝置進行驗證來解除電腦的鎖定。

安裝程序

登入認證管理員

根據配置，您可以下列任一方式登入「認證管理員」：

- 認證管理員登入精靈（偏好設定）
- 通知區中的「認證管理員」圖示
- ProtectTools Security Manager

如果您使用「Windows 登入」畫面上的「認證管理員登入 (Credential Manager Logon)」提示登入「認證管理員」，則您會同時登入 Windows。

首次登入

當您首次開啓「認證管理員」時，請使用一般的 Windows 登入密碼登入。然後系統會自動以您的 Windows 登入認證，建立「認證管理員」帳戶。

登入「認證管理員」後，您可以註冊其他認證，如指紋或智慧卡。

在下一次登入時，即可選擇登入原則並使用任何組合的已註冊認證。

使用認證管理員登入精靈

若要使用「認證管理員登入精靈」登入「認證管理員」：

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。
   - ❏ 從通知區連按兩下 ProtectTools 圖示。
   - ❏ 從 ProtectTools Security Manager 的「認證管理員」頁面，方法是，按一下視窗右上角的 **「登入」**連結。
2. 在 **「使用者名稱」**方塊中輸入您的使用者名稱，再按一下 **「下一步」**。
3. 選擇要使用的驗證方法，再按一下 **「下一步」**。
4. 按照螢幕上的指示，以所選取的驗證方法登入。
5. 按一下 **「完成」**。

建立新帳戶

您可以使用「認證管理員登入精靈」來建立新使用者帳戶。開始之前，您必須以管理員帳戶登入 Windows，但不能登入「認證管理員」。

若要建立新帳戶：

1. 連按兩下通知區的圖示來開啓「認證管理員」。「認證管理員登入精靈」便會開啓。
2. 在「自我介紹 (Introduce Yourself)」頁面上，按一下 **「更多 (More)」**按鈕，再按一下 **「登入新帳戶 (Sign Up for a New Account)」**。
3. 按一下 **「下一步」**。
4. 在「註冊 (Registration)」頁面上，鍵入使用者姓名及帳戶說明。然後按一下 **「下一步」**。
5. 在「驗證方法 (Authentication Methods)」頁面上，選擇要註冊的驗證方法（並清除您不想註冊之方法的核取方塊），然後按一下 **「下一步」**。
6. 請依照螢幕上的指示註冊所選取的認證。
7. 按一下 **「完成」**。

註冊認證

您可以使用「我的身份識別 (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」。

註冊指紋

若要註冊指紋：

1. 將指紋讀取器連接到電腦。
2. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
3. 按一下 **「我的身份識別 (My Identity)」**。
4. 在 **「我想要 (I Want To)」** 下，按一下 **「註冊指紋 (Register Fingerprints)」**。
5. 請依照螢幕上的指示完成註冊。

註冊智慧卡或 Token

若要註冊智慧卡或 Token：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，然後按一下 **「註冊認證 (Register Credentials)」**。
4. 按一下要註冊的驗證方法，再按一下 **「下一步」**。
5. 請依照螢幕上的指示完成註冊。

註冊其他認證

若要註冊其他認證：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，然後按一下 **「註冊認證 (Register Credentials)」**。
4. 按一下要註冊的驗證方法，再按一下 **「下一步」**。
5. 請依照螢幕上的指示完成註冊。

一般工作

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

- 建立和註冊驗證認證。
- 管理密碼。
- 管理 Microsoft 網路帳戶。
- 管理單一登入認證。

建立虛擬 Token

虛擬 Token 的運作方式很類似智慧卡或 USB Token。Token 是儲存在電腦硬碟或 Windows 登錄中。當您以虛擬 Token 登入時，系統會要求您提供使用者 PIN 來完成驗證。

若要建立新的虛擬 Token：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，然後按一下 **「註冊認證 (Register Credentials)」**。
4. 按一下 **「下一步」**。
5. 按一下 **「虛擬 Token(Virtual Token)」**，然後按一下 **「下一步」**。
6. 按一下 **「新建 (Create New)」**，然後按一下 **「下一步」**。
7. 輸入虛擬 Token 檔案的名稱和位置（或按一下 **「瀏覽」** 按鈕來尋找檔案位置），然後按一下 **「下一步」**。
8. 設定和確認主 PIN 和使用者 PIN。
9. 按一下 **「完成」**。

變更 Windows 登入密碼

您可以從「認證管理員」的「我的身份識別 (My Identity)」頁面中，變更 Windows 登入密碼。

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」**下，按一下 **「變更 Windows 登入密碼 (Change Windows Logon Password)」**。
4. 在 **「舊密碼」**方塊中鍵入您的舊密碼。
5. 在 **「新密碼 (New Password)」**和 **「確認密碼 (Confirm Password)」**方塊中設定和確認新密碼。
6. 按一下 **「完成」**。

變更 Token PIN

您可以從「認證管理員」的「我的身份識別 (My Identity)」頁面中，變更智慧卡或虛擬 Token 的 PIN。

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」**下，按一下 **「更多 (More)」**，再按一下 **「變更 Token PIN (Change Token PIN)」**。
4. 按一下 **「下一步」**。
5. 選擇要變更 PIN 的 Token，然後按一下 **「下一步」**。
6. 請依照螢幕上的指示完成 PIN 變更。

管理身份識別

備份身份識別

建議您在「認證管理員」中備份您的身份識別，避免資料遺失或意外移除。

若要備份身份識別：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，再按一下 **「備份身份識別 (Backup Identity)」**。
4. 按一下 **「下一步」**。
5. 選擇要備份的元件，再按一下 **「下一步」**。
6. 在「裝置類型 (Device Type)」頁面上，選擇要用來儲存備份的裝置類型，然後按一下 **「下一步」**。

   ✎ 您必須知道選來備份檔案之裝置的密碼或 PIN 密碼。

7. 遵循螢幕上有關選定裝置的指示，然後按一下 **「完成」**。

還原身份識別

若要還原身份識別：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，再按一下 **「還原身份識別 (Restore Identity)」**。
4. 按一下 **「下一步」**。
5. 在「裝置類型 (Device Type)」頁面上，選擇要儲存備份的裝置類型，再按一下 **「下一步」**。
6. 遵循螢幕上有關選定裝置的指示，然後按一下 **「完成」**。
7. 在確認對話方塊上按一下 **「是」**。

從系統移除身份識別

您可以從「認證管理員」中完全刪除您的身份識別。

這不會影響 Windows 使用者帳戶。

若要從系統移除身份識別：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 選擇 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，再按一下 **「從系統移除我的身份識別 (Remove My Identity from the System)」**。
4. 在確認對話方塊中按一下 **「是」**。身份識別會從系統登出並移除。

鎖定電腦

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。

爲了加強安全性，可以設定「鎖定工作站 (Lock Workstation)」功能，如此必須取得智慧卡、生物測定讀取器或 Token 才能解除電腦的鎖定。有關其他資訊，請參閱本章中的「設定認證管理員設定」。

若要鎖定電腦：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「我想要 (I Want To)」** 下，按一下 **「更多 (More)」**，再按一下 **「鎖定工作站 (Lock Workstation)」**。Windows 登入畫面便會顯示出來。您必須使用 Windows 密碼或「認證管理員登入精靈 (Credential Manager Logon Wizard)」才能解除電腦的鎖定。

使用 Microsoft 網路登入

您可以在本機電腦或網路網域上，使用「認證管理員」來登入 Windows。當您第一次登入「認證管理員」時，系統會自動將您的本機 Windows 使用者帳戶新增爲「網路登入 (Network Logon)」服務的網路帳戶。若需詳細資訊，請參閱本章前面的「首次登入」。

以認證管理員登入 Windows

您可以使用「認證管理員」來登入 Windows 網路或本機帳戶。

1. 從 Windows 登入畫面中，選擇 **「登入認證管理員 (Log on to Credential Manager)」**。
2. 按一下「歡迎 (Welcome)」頁面的 **「下一步」**（若出現）。
3. 在 **「使用者名稱」**方塊中鍵入您的使用者名稱。

   ✎ 若要將它當做預設的使用者名稱，請選擇 **「下次登入時使用這個名稱 (Use this name next time you log on)」**。

4. 從 **「登入 (Log on to)」**清單中選擇 **「認證管理員 (Credential Manager)」**。
5. 按一下 **「下一步」**。在「登入原則 (Logon Policy)」頁面上，選擇要使用的驗證方法。

   ✎ 若要將此方法當做預設的方法，請選擇 **「下次登入時使用這個原則 (Use this policy next time you log on)」**。

6. 遵循選定驗證方法的指示進行。若驗證資訊正確，您將登入 Windows 帳戶和「認證管理員」。

新增帳戶

登入「認證管理員」後，您可以新增其他本機或網域帳戶。

若要新增帳戶：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「Microsoft 網路登入 (Microsoft Network Logon)」** 下，按一下 **「新增網路帳戶 (Add a Network Account)」**。
4. 在 **「使用者名稱」** 方塊中，設定新帳戶的使用者名稱。
5. 從可用網域的清單中按一下網域。
6. 鍵入並確認密碼。

   ✎ 若要將其當做預設的使用者帳戶，請選擇 **「預設使用這些認證 (Use these credentials by default)」**。

7. 按一下 **「完成」**。

移除帳戶

登入「認證管理員」後，您可以移除本機或網域帳戶。

若要移除帳戶：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「Microsoft 網路登入 (Microsoft Network Logon)」** 下，按一下 **「管理網路帳戶 (Manage Network Accounts)」**。
4. 按一下您要移除的帳戶，再按一下 **「移除」**。
5. 在確認對話方塊中，按一下 **「是」**。

設定預設使用者

登入「認證管理員」後，您可以設定或變更預設使用者。

若要設定預設使用者：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「Microsoft 網路登入 (Microsoft Network Logon)」** 下，按一下 **「管理網路帳戶 (Manage Network Accounts)」**。
4. 按一下要做爲預設值的帳戶，再按一下 **「內容 (Properties)」**。
5. 在 **「帳戶內容 (Account Properties)」** 對話方塊的 **「設定帳戶 (Set Up Account)」** 標籤上，選擇 **「預設使用這些認證 (Use these credentials by default)」** 核取方塊。
6. 依序按一下 **「套用」** 及 **「確定」**。

使用單一登入

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

安全性和私密性是「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」後才能使用。

您也可以設定 「單一登入 (Single Sign On)」，以便在登入安全站台或應用程式之前，以智慧卡、生物測定讀取器或 Token 來驗證您的驗證認證。當您登入應用程式或包含個人資訊（如銀行帳號）的網站時，這個動作特別有用。有關其他資訊，請參閱本章中的「設定認證管理員設定」。

註冊新應用程式

當您登入「認證管理員」時，「認證管理員」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

若要以自動註冊來註冊應用程式：

1. 開啓需要您登入的應用程式。
2. 在 **「認證管理員單一登入 (Credential Manager Single Sign On)」**對話方塊上，按一下 **「選項」**來設定下列用於註冊的設定：
   - ❏ 不建議您搭配此站台或應用程式使用 SSO。
   - ❏ 僅填寫認證。不提交。
   - ❏ 提交認證前要求確認。
3. 按一下 **「是」**，完成註冊。

使用手動 （拖放）註冊

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」** 下，按一下 **「註冊新應用程式 (Register New Application)」**。
4. 執行要註冊的應用程式，直到看到含有密碼方塊的頁面爲止。
5. 在「SSO 註冊精靈 (SSO Registration Wizard)」的「拖放註冊 (Drag and Drop Registration0」頁面上，選擇要自動化的活動類型。

   ✎ 在大部份情況下，您要自動化的活動將是 **「登入」對話方塊**。

6. 按一下，並將精靈頁面的圖示，拖曳到密碼方塊所在的應用程式區域上。區域反白時放開指標。

   ✎ 您將看不到手指圖示移過頁面，但當您將指標拖曳到應用程式的登入方塊時，會顯示矩形圖示。

7. 在「SSO 註冊精靈 (SSO Registration Wizard)」的「應用程式資訊 (Application Information)」頁面上，輸入應用程式的名稱和說明。
8. 按一下 **「完成」**。
9. 在應用程式方塊中輸入登入認證，例如，使用者名稱和密碼。
10. 在確認對話方塊中，確認或修改認證名稱，再按一下 **「是」**。

管理應用程式和認證

修改應用程式內容

若要修改應用程式內容：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」** 下，按一下 **「管理應用程式及認證 (Manage Applications and Credentials)」**。
4. 按一下要修改的應用程式項目，再按一下 **「內容 (Properties)」**。
   a. 按一下 **「一般」** 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。
   b. 按一下 **「指令檔 (Script)」** 標籤來檢視和編輯 SSO 應用程式指令檔。
5. 按一下 **「確定」** 以儲存變更。

從單一登入移除應用程式

若要從單一登入移除應用程式：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」** 下，按一下 **「管理應用程式及認證 (Manage Applications and Credentials)」**。
4. 按一下要移除的應用程式項目，再按一下 **「移除」**。
5. 在確認對話方塊中按一下 **「是」**。
6. 按一下 **「確定」**。

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. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」**下，按一下 **「管理應用程式及認證 (Manage Applications and Credentials)」**。
4. 按一下要匯出的應用程式項目。然後按一下 **「更多 (More)」**，再按一下 **「匯出應用程式 (Export Application)」**。
5. 依照螢幕上的指示完成匯出。
6. 按一下 **「確定」**。

匯入應用程式

若要匯入應用程式：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」**下，按一下 **「管理應用程式及認證 (Manage Applications and Credentials)」**。
4. 按一下要匯入的應用程式項目。然後按一下 **「更多 (More)」**，再按一下 **「匯入應用程式 (Import Application)」**。
5. 依照螢幕上的指示完成匯入。
6. 按一下 **「確定」**。

修改認證

若要修改認證：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「我的身份識別 (My Identity)」**。
3. 在 **「單一登入 (Single Sign On)」** 下，按一下 **「管理應用程式及認證 (Manage Applications and Credentials)」**。
4. 按一下要修改的應用程式項目，再按一下 **「更多 (More)」**。
5. 請選擇以下任一個選項：
   - ❏ 新增認證 (Add New Credentials)
   - ❏ 刪除認證 (Delete Credentials)
   - ❏ 刪除未使用的認證 (Delete Unused Credentials)
   - ❏ 編輯認證 (Edit Credentials)
6. 請依照螢幕上的指示。
7. 按一下 **「確定」** 以儲存變更。

進階工作 （僅適用於管理員）

「認證管理員」的「驗證及認證 (Authentication and Credentials)」頁面和「進階設定 (Advanced Settings)」頁面僅適用於具有管理員權限的使用者。從這些頁面，您可以

- 指定使用者和管理員如何登入。
- 設定認證內容。
- 設定「認證管理員」程式設定。

指定使用者和管理員如何登入

從「驗證及認證 (Authentication and Credentials)」頁面中，您可以指定使用者或管理員需要哪一種認證類型或認證組合。

若要指定使用者或管理員的登入方式：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「驗證及認證 (Authentication and Credentials)」**。
3. 按一下 **「驗證 (Authentication)」**標籤。
4. 按一下類別清單中的類別 （**「使用者」**或 **「管理員」**）。
5. 按一下清單中的驗證方法類型或驗證方法組合。
6. 按一下 **「確定」**。
7. 按一下 **「套用」**，再按一下 **「確定」**，儲存變更。

確認自訂驗證需求

如果所要的驗證認證組未列在「驗證及認證 (Authentication and Credentials)」頁面的 **「驗證 (Authentication)」**標籤中，您可以建立自訂需求。

若要設定自訂需求：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「驗證及認證 (Authentication and Credentials)」**。
3. 按一下 **「驗證 (Authentication)」**標籤。
4. 按一下類別清單中的類別（**「使用者」**或 **「管理員」**）。
5. 按一下驗證方法清單中的 **「自訂」**。
6. 按一下 **「配置 (Configure)」**。
7. 選擇要使用的驗證方法。
8. 按一下下列任一項來選擇方法組合：
   - ❏ 使用 AND 以組合驗證方法

     （每當使用者登入時，都必須以選擇的方法進行驗證。）
   - ❏ 使用 OR 以組合驗證方法

     （每當使用者登入時，都能夠選擇任何選取的方法。）
9. 按一下 **「確定」**。
10. 按一下 **「套用」**，再按一下 **「確定」**，儲存變更。

設定認證內容

從「驗證及認證 (Authentication and Credentials)」頁面的**「認證 (Credentials)」**標籤中，您可以檢視可用的驗證方法清單，以及修改設定。

若要設定認證：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「驗證及認證 (Authentication and Credentials)」**。
3. 按一下 **「認證 (Credentials)」**標籤。
4. 按一下要修改的認證類型。
   - ❏ 若要註冊認證，請按一下 **「註冊 (Register)」**，然後遵循螢幕上的指示進行。
   - ❏ 若要刪除認證，請按一下 **「清除」**，再按一下確認對話方塊中的 **「是」**。
   - ❏ 若要修改認證內容，按一下 **「內容 (Properties)」**，然後遵循螢幕上的指示進行。
5. 依序按一下 **「套用」**及 **「確定」**。

設定認證管理員設定

從「進階設定 (Advanced Settings)」頁面中，您可以使用下列標籤來存取和修改各種設定：

- 一般 (General) — 可讓您修改基本配置的設定。
- 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。
- 生物測定設定 (Biometric Settings) — 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智慧卡和 Token 的內容。

若要修改「認證管理員」設定：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「進階設定 (Advanced 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. 按一下 **「套用」**，再按一下 **「確定」**，儲存變更。

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

若要從 「認證管理員」登入 Windows：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「進階設定 (Advanced Settings)」**。
3. 按一下 **「一般」**標籤。
4. 選擇 **「使用認證管理員登入 Windows (Use Credential Manager to log on to Windows)」**核取方塊。
5. 按一下 **「套用」**，再按一下 **「確定」**，儲存變更。
6. 重新啓動電腦。

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

若要 「單一登入 (Single Sign On)」先驗證您的認證，再登入到註冊的對話方塊或網頁：

1. 選擇 **「開始」 > 「所有程式」 > 「HP ProtectTools Security Manager」 > 「認證管理員」**。
2. 按一下 **「進階設定 (Advanced Settings)」**。
3. 按一下 **「單一登入 (Single Sign On)」**標籤。
4. 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 (Validate user before submitting credentials)」**核取方塊。
5. 按一下 **「套用」**，再按一下 **「確定」**，儲存變更。
6. 重新啓動電腦。

辭彙

下列術語應用於這份文件與整個 ProtectTools Security Manager。

BIOS 安全性模式 (BIOS security mode) — 智慧卡安全性的設定，啓用時，需要使用智慧卡和有效的 PIN 進行使用者驗證。

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

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

USB Token — 儲存使用者相關身份識別資訊的安全性裝置。如同智慧卡或生物測定讀取器，它能用來驗證電腦的擁有者。

Windows 使用者帳戶 (Windows user account) — 有權登入網路或個人電腦的個人設定檔。

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。

加密 (Encryption) — 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 (Encryption File System, EFS) — 用來加密選定資料夾中所有檔案和子資料夾的系統。

生物測定 (Biometric) — 使用實體功能的驗證認證類別（如指紋）來識別使用者身份。

自動磁碟機/光碟機鎖 (Automatic DriveLock) — 安全性功能，可讓 TPM 內建式安全晶片產生和保護磁碟機/光碟機鎖密碼。當使用者在啓動期間輸入正確的 TPM 基本使用者金鑰密碼，通過 TPM 內建式安全晶片的驗證時，BIOS 就會解除使用者的硬碟鎖定。

身份識別 (Identity) — 「ProtectTools 認證管理員」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。

信任平台模組 (Trusted Platform Module, TPM) 內建式安全晶片 （僅限特定機型） — 整合的安全晶片，可防止惡意的攻擊者入侵高度敏感的使用者資訊。它是指定平台的信任根源。TPM 提供了符合「信任計算群組 (Trusted Computing Group, TCG)」規格的密碼編譯演算法和作業。

重新開機 (Reboot) — 電腦的重新啓動程序。

密碼編譯 (Cryptography) — 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 (Cryptographic service provider, 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。

單一登入 (Single Sign On) — 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。

智慧卡 (Smart card) — 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。用來驗證電腦的擁有者。

智慧卡使用者密碼 (Smart card user password) — 可在「電腦設定 (Computer Setup)」中連結使用者智慧卡與電腦的密碼，目的是在啓動或重新啓動時進行身份識別。這個密碼可由管理員手動設定，也可以隨機產生。

智慧卡管理員密碼 — 可在「電腦設定 (Computer Setup)」中連結管理員智慧卡與電腦的密碼，目的是在啓動或重新啓動時進行身份識別。這個密碼可由管理員手動設定，也可以隨機產生。

虛擬 Token (Virtual token) — 運作方式很像智慧卡和讀取器的安全性功能。Token 是儲存在電腦硬碟或 Windows 登錄中。當您以虛擬 Token 登入時，系統會要求您提供使用者 PIN 來完成驗證。

開機驗證 (Power-on authentication) — 當電腦開機時，需要進行某些驗證形式的安全性功能，如智慧卡、安全晶片或密碼。

解密 (Decryption) — 密碼編譯所使用的程序，可將加密的資料轉換成純文字。

磁碟機/光碟機鎖 (DriveLock) — 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/光碟機鎖密碼。

緊急復原封存 (Emergency recovery archive) — 受保護的儲存區，可將一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 (Domain) — 爲一個網路的電腦群組，其會共用公用的目錄資料庫。網域的名稱是唯一的，且每個網域都有一組公用的規則和程序。

網路帳戶 (Network account) — 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 (Credentials) — 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 (Digital certificate) — 符合個人或公司的識別身份之電子認證，方法是將數位憑證擁有者的識別身份繫結到一對電子金鑰來簽署數位資訊。

數位簽章 (Digital signature) — 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 (Certification authority) — 發出執行公開金鑰基礎架構所需之憑證的服務。

轉移 (Migration) — 可管理、還原和轉移金鑰和憑證的工作。

嚴密安全性 (Stringent security) — 「BIOS 配置」中的安全性功能，可增強對開機密碼和管理員密碼，及其他開機驗證形式的防護。

驗證 (Authentication) — 驗證使用者是否有權執行工作的程序，例如，存取電腦、修改特殊程式的設定，或檢視保護的資料。

索引

十三劃

十四劃

十六劃

十八劃

二十劃以上