Dell Data Protection | Security Tools

Security Tools Installation Guide

Dell Data Protection | Security Tools Installation Guide

Installation Guide v1.12

DELL EMC

註、警示與警告

註:「註」表示可以幫助您更有效地使用產品的重要資訊。

警示:「警示」表示有可能會損壞硬體或導致資料遺失，並告訴您如何避免發生此類問題。

警告:「警告」表示可能的財產損失、人身傷害或死亡。

2017- 02

Rev. A01

Contents

1

簡介

Dell Data Protection | Security Tools 為 Dell 電腦管理員與使用者提供安全和身分保護。DDP | Security Tools 前置安裝於所有 Dell Latitude、Optiplex 和 Precision 電腦，以及特定 Dell XPS 筆記型電腦。若需要 *reinstall* (重新安裝) DDP | Security Tools，請遵循本指南中的指示。如需其他支援，請參閱 www.dell.com/support > Endpoint Security Solutions。

概觀

DDP | Security Tools 屬於端對端安全解決方案，設計可提供進階驗證支援，並支援開機前驗證 (PBA) 與自行加密磁碟機管理。

DDP | Security Tools 支援以密碼、指紋掃描器及智慧卡進行 Windows 多重因素驗證 -「非接觸式」與「接觸式」，以及自我註冊、One-Step Logon (單一登入 [SSO])，以及 一次性密碼 (OTP)。

提供 Security Tools 給使用者使用前，系統管理員可能想要以 DDP 安全性主控台的 Administrator Settings 工具設定 Security Tools 功能，例如：啟用開機前驗證與驗證原則。但預設設定可讓系統管理員與使用者，在安裝與啟動之後，立即開始使用 Security Tools。

DDP 安全性主控台

根據系統管理員設定的原則，使用者可透過使用 DDP 安全性主控台此 Security Tools 介面來註冊與管理其認證，並設定自我復原問題。使用者可存取這些 Security Tools 應用程式：

- Encryption 工具可讓使用者檢視電腦磁碟機的加密狀態。
- Enrollments 工具可讓使用者設定並管理認證、設定自我復原問題，以及檢視其認證註冊狀態。這些權限是以系統管理員設定的原則為準。
- Password Manager 可讓使用者自動填寫及提交用以登入網站、Windows 應用程式和網路資源所需的資料。Password Manager 還提供使用者從應用程式變更登入密碼的功能，確保 Password Manager 維護的密碼與目標資源的內容同步。

系統管理員設定

Administrator Settings 工具可為電腦所有使用者設定 Security Tools，讓系統管理員設定驗證原則、管理使用者，以及設定可用於 Windows 登入的認證。

系統管理員可藉由 Administrator Settings 工具啟用加密與開機前驗證 (PBA)，以及設定 PBA 原則並自訂 PBA 畫面文字。

繼續至 Requirements (需求)。

2

要求條件

- 在所有 Dell Latitude、Optiplex 和 Precision 電腦，以及特定 Dell XPS 筆記型電腦上，皆已預先安裝 DDP | Security Tools，而且符合下列最低要求。若您需要重新安裝 DDP | Security Tools，請確認電腦仍符合這些要求。請參閱 www.dell.com/support > Endpoint Security Solutions（端點安全性解決方案）以獲得詳細資訊。
- 請勿將 Windows 8.1 安裝在自行加密磁碟機的磁碟機 1 上。此作業系統組態不受支援，因為 Windows 8.1 會建立復原分割區磁碟機 0，而導致開機前驗證中斷。請改將 Windows 8.1 安裝在設定為磁碟機 0 的磁碟機上，或者將 Windows 8.1 以映像檔方式還原到任意磁碟機上。
- DDP | Security Tools 不支援動態磁碟。
- 配備自我加密磁碟機的電腦，無法搭配 Hardware Crypto Accelerator 使用。不相容性存在時將阻礙 HCA 佈建。請注意，Dell 所銷售的電腦並未配備支援 HCA 模組的自我加密磁碟機。此不支援的組態可能是售後組態。
- DDP | Security Tools 不支援多重開機磁碟組態。
- 在用戶端安裝新作業系統前，先在 BIOS 清除 Trusted Platform Module (TPM) 可信賴平台模組。
- SED 不需要 TPM 來提供進階認證或加密。

驅動程式

- 支援的 Opal 相容 SED 需要已更新的 Intel Rapid Storage Technology (快速儲存技術) 驅動程式，位於 http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

  註:

  由於 RAID 與 SED 的本質，SED 管理不支援 RAID。SED 的「RAID=On」問題在於，RAID 需要存取磁碟，以在 High 磁區讀寫 RAID 相關資料，但此功能在已鎖上的 SED 上從一開始便不可得，且無法等到使用者登入後再讀取此資料。在 BIOS 中將 SATA 運作從「RAID=On」變更為「AHCI」可解決此問題。若作業系統未預先安裝 AHCI 控制器驅動程式，從「RAID=On」變更為「AHCI」時，將會出現藍色畫面。

用戶端必備項目

- Security Tools 需要使用完整版的 Microsoft .Net Framework 4.5（或以上版本）。所有自 Dell 原廠出貨的電腦已預先安裝完整版的 Microsoft .Net Framework 4.5。然而，如果不是安裝在 Dell 硬體上，或是打算在舊型 Dell 硬體上升級 Security Tools，您應先驗證已安裝的 Microsoft .Net 版本並將其更新再安裝 Security Tools，以免安裝 / 升級失敗。若要安裝完整版 Microsoft .Net Framework 4.5，請造訪 https://www.microsoft.com/en-us/download/details.aspx?id=30653

  若要驗證安裝的 .Net 版本，請遵循準備要安裝的電腦所提供的指示：http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- 在您電腦上欲驗證的硬體之驅動程式與韌體，必須是最新版本。如欲取得適用 Dell 電腦的驅動程式與韌體，請前往 http://www.dell.com/support/home/us/en/19/Products/?app=drivers 並選取您的電腦機型。視您欲驗證的硬體而定，下載下列適用的軟體：
  - NEXT Biometrics 指紋讀取驅動程式
  - Validity 指紋讀取器 495 驅動程式
  - O2Micro 智慧卡驅動程式
  - Dell ControlVault

  其他硬體廠商可能需要自己的驅動程式。

如果電腦尚未安裝此元件，安裝程式會加以安裝：

必備項目

- Microsoft Visual C++ 2012 Update 4 或以上版本的可轉散發套件 (x86/x64)

Software

Windows Operating Systems

The following table details supported software.

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 7 SP0-SP1
  - Enterprise
  - Professional

  NOTE: Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 (Consumer)

  NOTE: Windows 8 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.
- Microsoft Windows 8.1 - 8.1 Update 1
  - Enterprise Edition
  - Pro Edition

  NOTE: Windows 8.1 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.
- Microsoft Windows 10 through Version 1511 (November Update/Threshold 2)
  - Education Edition
  - Enterprise Edition
  - Pro Edition

NOTE: Windows 10 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

Mobile Device Operating Systems

The following mobile operating systems are supported with Security Tools One-time Password feature.

Mobile Device Operating Systems

Android Operating Systems

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS Operating Systems

- iOS 7.x
- iOS 8.x

Mobile Device Operating Systems
Windows Phone Operating Systems
• Windows Phone 8.1 • Windows 10 Mobile

Hardware

Authentication

The following table details supported authentication hardware.

Authentication
Fingerprint Readers
• Validity VFS495 in Secure Mode • Broadcom Control Vault Swipe Reader • UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379 • Authentec Eikon and Eikon To Go USB Readers **NOTE: When using an external fingerprint reader, you must download and install the latest drivers required for your specific reader.**
Contactless Cards
• Contactless Cards using Contactless Card Readers built-in to specified Dell laptops
Smart Cards
• PKCS #11 Smart cards using the ActivIdentity client **NOTE: The ActivIdentity client is not pre-loaded and must be installed separately.** • Common Access Cards (CAC) **NOTE: With multi-cert CACs, at logon, the user selects the correct certificate from a list.** • CSP Cards • Class B/SIPR Net Cards

The following table details Dell computer models supported with SIPR Net cards.

Dell Computer Models - Class B/SIPR Net Card Support		
• Latitude E6440 • Latitude E6540	• Precision M2800 • Precision M4800 • Precision M6800	• Latitude 14 Rugged Extreme • Latitude 12 Rugged Extreme • Latitude 14 Rugged

Dell Computer Models - UEFI Support

Authentication features are supported with UEFI mode on select Dell computers running Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 with qualified Opal Compliant SEDs. Other computers running Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 support Legacy Boot mode.

The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 Tower, Small Form Factor, Micro
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 5050 Tower, Small Form Factor, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- OptiPlex 7050 Tower, Small Form Factor, Micro
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

NOTE: Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.

NOTE: On a supported UEFI computer, after selecting Restart from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture. Some models display the PBA logon screen; other models display the Windows logon screen. Both logon screens are equally secure.

NOTE:

Ensure that the Enable Legacy Option ROMs setting is disabled in the BIOS.

To disable Legacy Option ROMs:

1. Restart the computer.
2. As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.
3. Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.
4. Select **Settings** > **General** > **Advanced Boot Options**.
5. Clear the **Enable Legacy Option ROMs** checkbox and click **Apply**.

Opal Compliant SEDs

For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

International Keyboards

- The following table lists international keyboards supported with Preboot Authentication on UEFI and non-UEFI computers.

International Keyboard Support - UEFI

- DE-CH - Swiss German
- DE-FR - Swiss French

International Keyboard Support - Non-UEFI

- AR - Arabic (using Latin letters)
- DE-CH - Swiss German
- DE-FR - Swiss French

語言支援

DDP | Security Tools 與多語系使用者介面 (MUI) 相容，支援下列語言。

註:

在 UEFI 電腦上，俄文、繁體中文或簡體中文未支援 PBA 當地語系化。

語言支援

- EN - 英文
- FR - 法文
- IT - 義大利文
- DE - 德文
- ES - 西班牙文
- JA - 日文
- KO - 韓文
- ZH-CN - 簡體中文
- ZH-TW - 繁體中文/台灣
- PT-BR - 巴西葡萄牙文
- PT-PT - 葡萄牙 (伊比利亞) 葡萄牙文
- RU - 俄文

驗證選項

下列驗證選項需要特定硬體 ：Fingerprints (指紋)、Smart Cards (智慧卡)、 Contactless Cards (非接觸式卡)、Class B/SIPR Net Cards (Class B/SIPR 網卡) 和 **authentication on UEFI computers** (UEFI 電腦上驗證)。

一次性密碼功能需要有 TPM，而且必須啟用及擁有。如需更多資訊，請參閱 Clear Ownership and Activate the TPM (清除所有權及啟動 TPM)。TPM 2.0 不支援 OTP。

下表依作業系統顯示符合硬體和組態需求時，Security Tools 提供的驗證選項。

非 UEFI

	PBA					Windows 驗證				
	密碼	指紋	接觸式智慧卡	OTP	SIPR 卡	密碼	指紋	智慧卡	OTP	SIPR 卡
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 更新 1	X[1]					X	X	X	X	X

非 UEFI

	PBA					Windows 驗證				
	密碼	指紋	接觸式智慧卡	OTP	SIPR 卡	密碼	指紋	智慧卡	OTP	SIPR 卡
Windows 10	X[1]					X	X	X	X	X

1. 有支援的 Opal SED 時可用。

UEFI

	支援的 Dell 電腦上的 PBA					Windows 驗證				
	密碼	指紋	接觸式智慧卡	OTP	SIPR 卡	密碼	指紋	智慧卡	OTP	SIPR 卡
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 更新 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. 在支援的 UEFI 電腦含支援的 OPAL SED 時可用。

互通性

取消提供及解除安裝 Dell Data Protection | Access

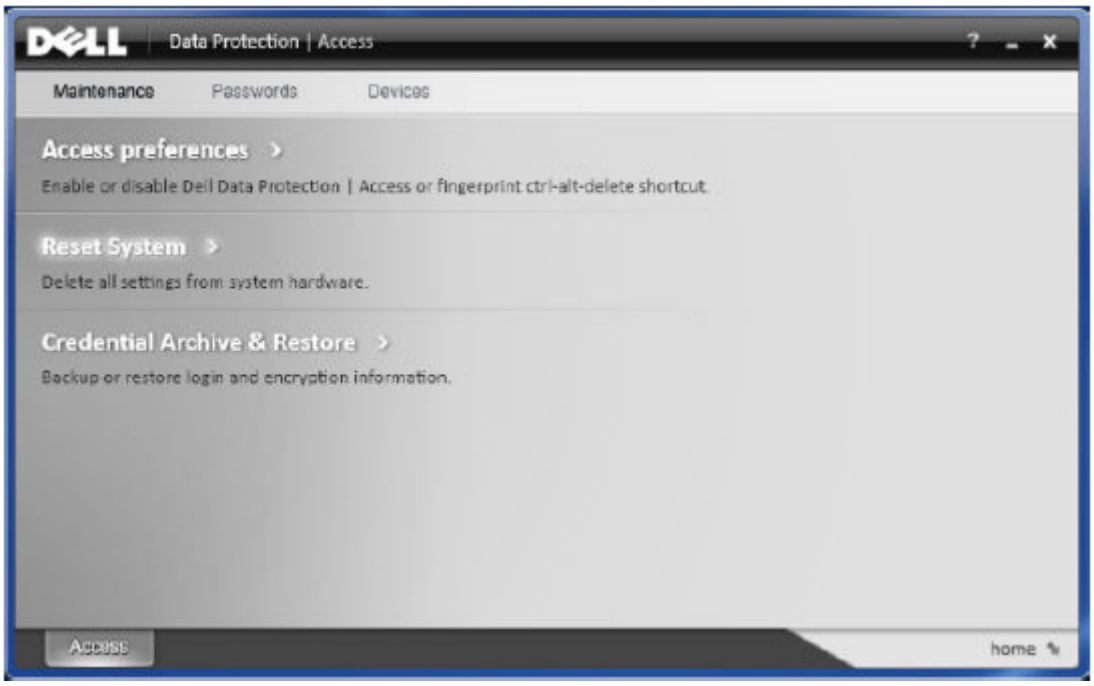
如果您的電腦上現在已安裝或過去曾安裝 DDP|A，在安裝 Security Tools 之**前**，必須取消提供 DDP|A 管理的硬體，然後解除安裝 DDP|A。如果不曾使用 DDP|A，您可能只需解除安裝 DDP|A，然後重新啟動安裝程序。

取消提供 DDP|A 管理的硬體包括指紋讀取器、智慧卡讀卡機、BIOS 密碼、TPM 及自行加密磁碟機。

註: 如果執行 DDP|E 加密產品，請停止或暫停加密掃描。如果執行 Microsoft BitLocker，請暫止加密原則。一旦 DDP|A 解除安裝，且 Microsoft BitLocker 原則已取消暫止後，請遵循 http://technet.microsoft.com/en-us/library/cc753140.aspx 的指示，初始化 TPM。

取消提供 DDP|A 管理的硬體

1. 啟動 DDP|A 並按一下 **Advanced**（進階）標籤。



2. 選取 **Reset System**（重設系統）。這將需要您輸入任何提供的認證以驗證您的身分。在 DDP|A 驗證認證之後，DDP|A 將執行下列動作：
   - 從 Dell ControlVault 移除所有取消提供的認證 (如果有)
   - 移除 Dell ControlVault 擁有者密碼 (如果有)
   - 從內建的指紋讀取器移除所有提供的指紋 (如果有)
   - 移除所有 BIOS 密碼 (BIOS 系統、BIOS 管理員及硬碟機密碼)
   - 清除信賴平台模組
   - 移除 DDP|A 認證供應者

   電腦一取消佈建後，DDP|A 隨即啟動電腦，以還原 Windows 預設認證提供者。

解除安裝 DDP|A

當認證硬體完成取消提供之後，請解除安裝 DDP|A。

1. 啟動 DDP|A 並執行 Reset System（重設系統）。

   此將移除所有受 DDP|A 管理的認證與密碼，並將清除信賴平台模組 (TPM)。
2. 按一下 **Uninstall**（解除安裝）啟動安裝程式。
3. 解除安裝完成後，按一下 **Yes**（是）重新啟動。

註: 移除 DDP|A 也將解鎖 SED 並移除開機前驗證。

初始化 TPM

- 您必須是本機系統管理員群組成員或同等身分。
- 電腦必須配備相容的 BIOS 和 TPM。

如果使用一次性密碼 (OTP)，就必須執行這項工作。

- 請遵循 http://technet.microsoft.com/en-us/library/cc753140.aspx 中的指示。

清除所有權及啟動 TPM

若要清除及設定 TPM 的所有權，請參閱 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2。

繼續至 Installation and Activation (安裝與啟動)。

3

安裝與啟動

本章節詳細說明在本機電腦安裝 DDP | Security Tools 的程序。若要安裝與啟動 DDP | Security Tools，您必須以系統管理員的身分登入電腦。

註:

安裝時，請勿對電腦進行任何變更，包括插入及取出外接式 (USB) 磁碟機。

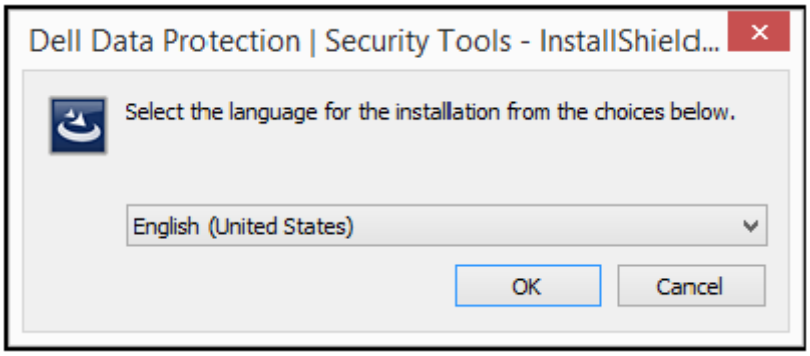
安裝 DDP | Security Tools

安裝 Security Tools：

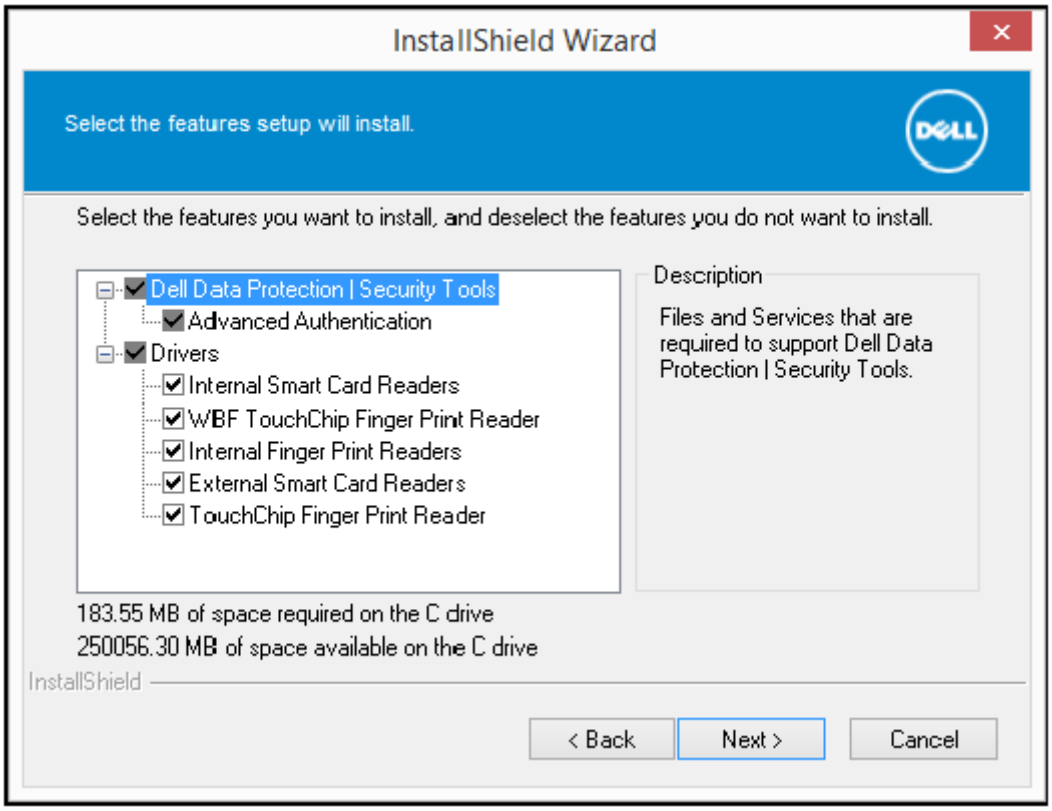
1. 在 DDP | Security Tools 安裝媒體中找出安裝檔案。將安裝檔案複製至本機電腦。

   註: 安裝媒體位於 www.dell.com/support > Endpoint Security Solutions（端點安全性解決方案）。

2. 連按兩下檔案，啟動安裝程式。
3. 選取適當的語言，然後按一下 **OK**（確定）。



4. 顯示 Welcome（歡迎）頁面時，請按一下 **Next**（下一步）。
5. 閱讀授權協議書，同意條款，然後按一下 **Next**（下一步）。
6. 按一下 **Next**（下一步）將 Security Tools 安裝在預設位置 `C:\Program Files\Dell\Dell Data Protection`。選取



7. 按一下 **Install**（安裝）開始安裝。
8. 安裝完成時，需要重新啟動電腦。選取 **Yes**（是）重新啟動，然後按一下 **Finish**（完成）。

   安裝隨即完成。

啟動 DDP | Security Tools

首次執行 DDP 安全性主控台並選取 Administrator Settings 時，啟動精靈會引導您進行啟動程序。

如果尚未啟動 DDP 安全性主控台，一般使用者仍可執行此 Console。在系統管理員啟動 DDP | Security Tools 並自訂設定前，如果使用者為第一個使用 DDP 安全性主控台 的人，預設值將被使用。

啟動 Security Tools：

1. 以系統管理員身分從桌面捷徑啟動 Security Tools。

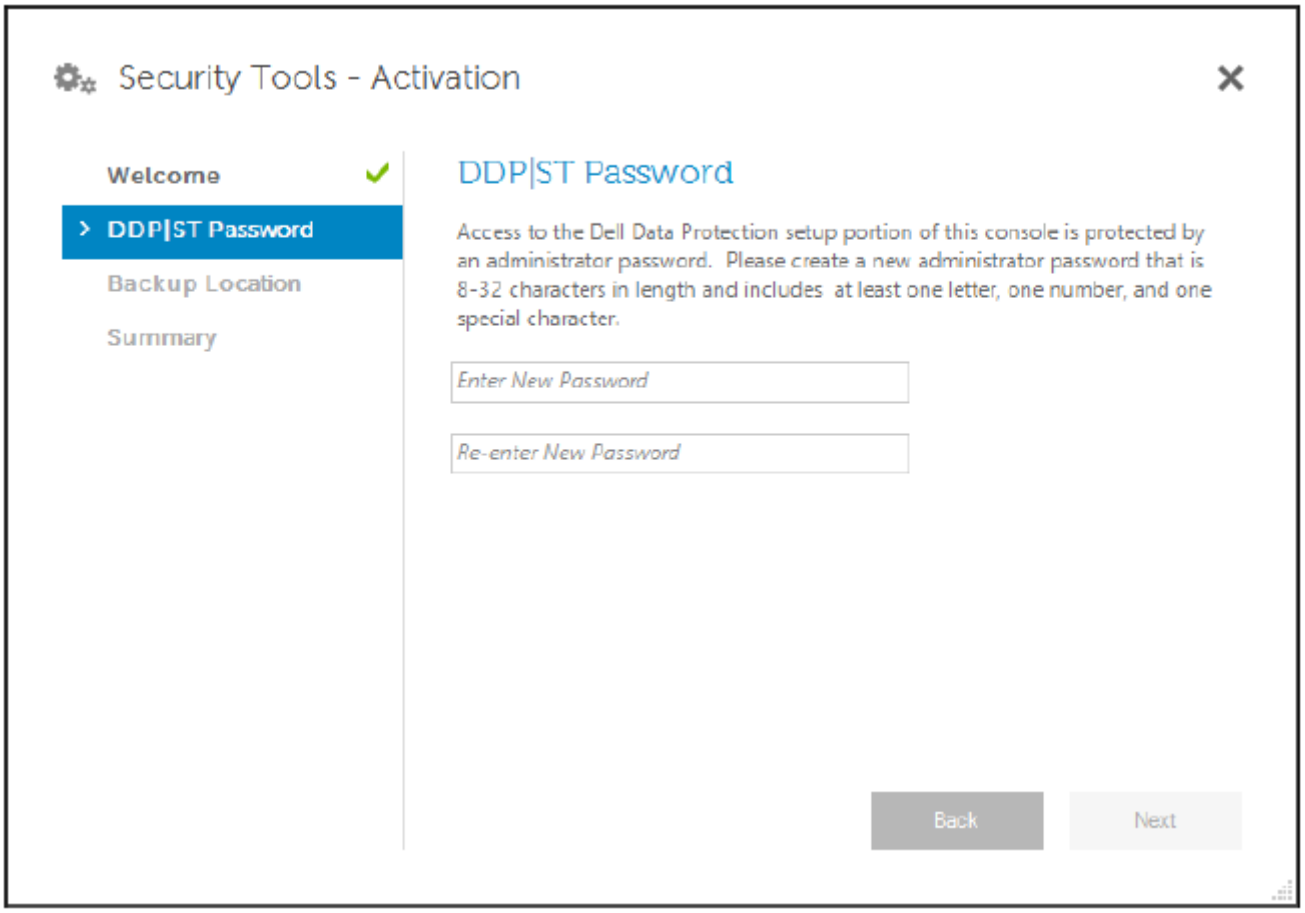
註: 如果以一般使用者身分登入（使用標準 Windows 帳戶），Administrator Settings 工具將需要 UAC 提高權限才可啟動。一般使用者必須先輸入系統管理員認證，以登入工具，並在第二次出現提示時，輸入系統管理員的密碼（密碼儲存於 Administrator Settngs 之中）。

2. 按一下 **Administrator Settings**（系統管理員設定）圖標。

3. 在歡迎頁面，按一下 **Next**（下一步）。

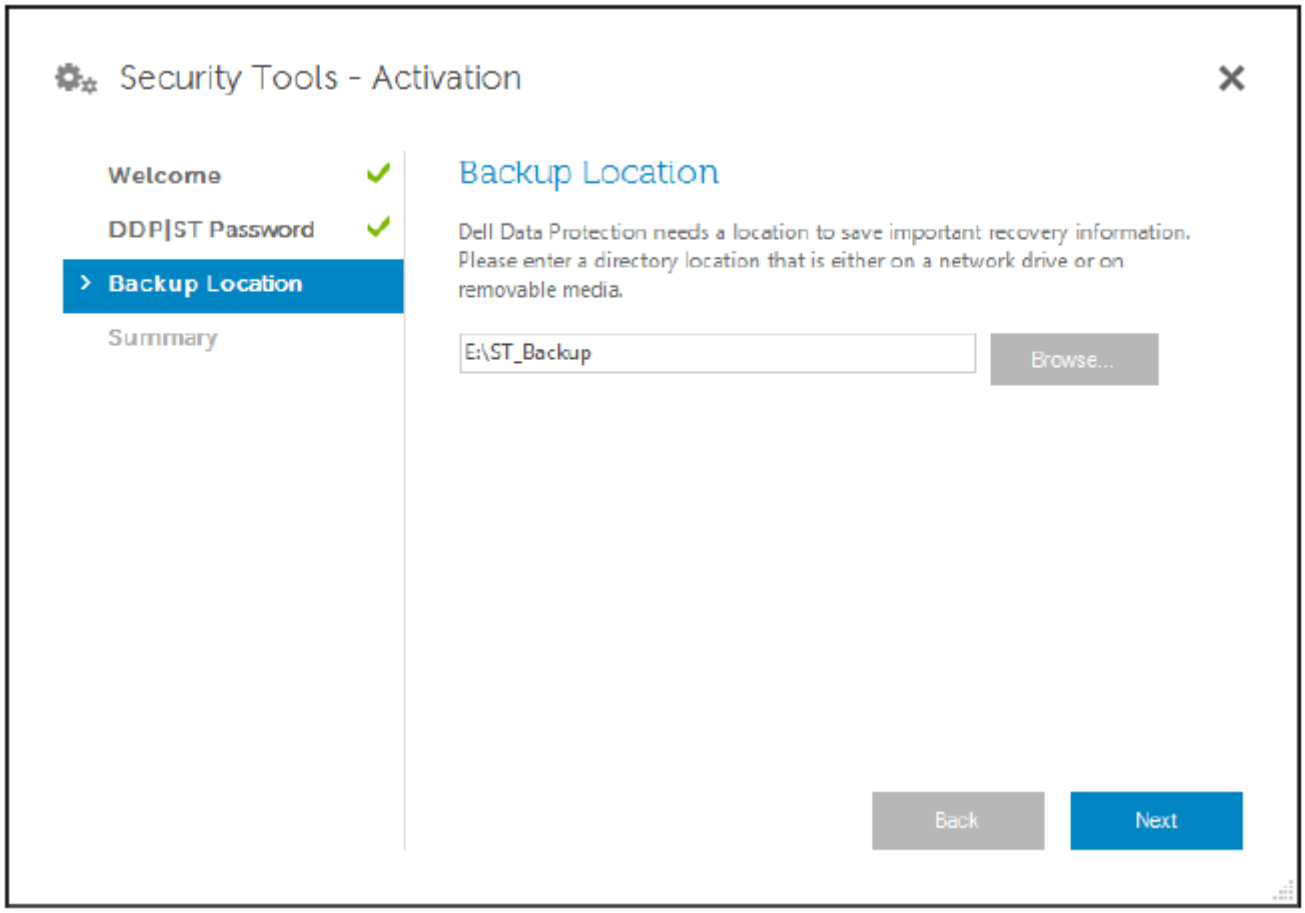
4. 建立 DDP | Security Tools 密碼，並按一下 **Next**（下一步）。

   您必須在設定 Security Tools 之前，建立 DDP | Security Tools 系統管理員的密碼。執行 Administrator Settings 工具時，將須隨時使用此密碼。密碼長度必須在 8-32 個字元之間，其中必須包含至少一個字母、一個數字及一個特殊字元。



5. 在 **Backup Location**（備份位置）中，指定將寫入備份檔案的位置，然後按一下 **Next**（下一步）。備份檔案必須儲存於網路磁碟機或卸除式媒體上。備份檔案包含復原此電腦資料所需的金鑰。Dell Support 需要存取此檔案，才能協助您復原資料。

   復原資料將自動備份至指定位置。若無法取得位置 (例如，若未插入備份 USB 磁碟機)，DDP | Security Tools 會顯示訊息，提示您選擇資料備份位置。需有復原資料的存取權限才可開始加密。



6. 在 Summary (摘要) 頁面，按一下 **Apply** (套用)。

   Security Tools 啟動完成。

   系統管理員與使用者可開始根據預設設定，立即使用 Security Tools 的各種功能。

4

適用 Administrators

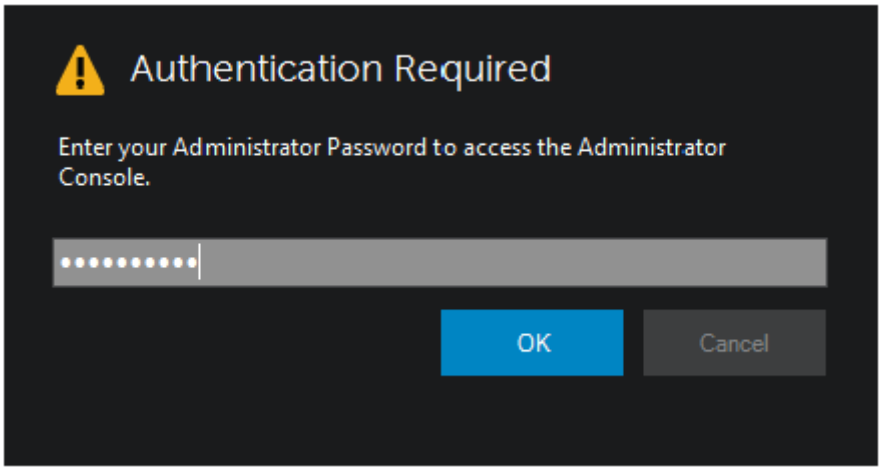
Security Tools 預設設定可讓系統管理員及使用者在啟動後立即使用 Security Tools ，無須其他設定。使用者在以其 Windows 密碼登入電腦時，自動會被新增為 Security Tools 使用者，但預設設定為不啟用多重因素 Windows 驗證。加密與開機前認證的預設設定為停用。

若要設定 Security Tools 功能，您必須是電腦上的系統管理員。

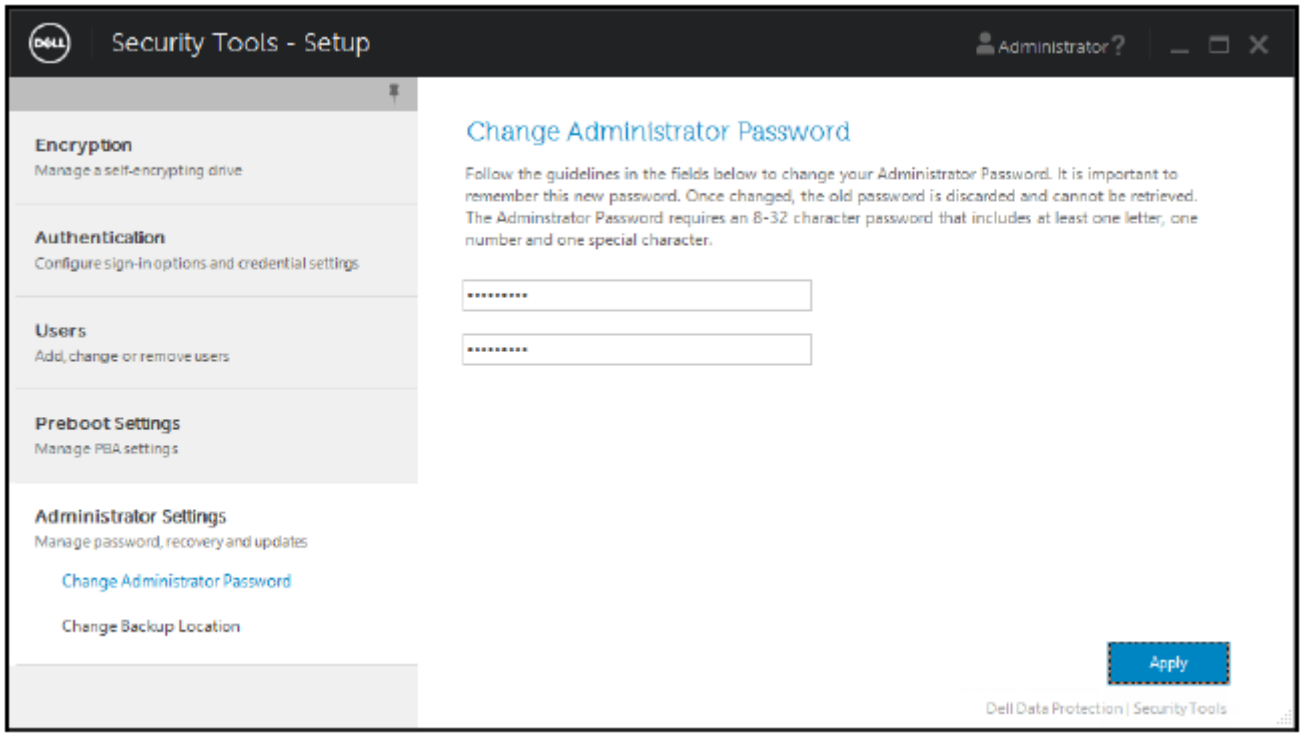
Change the Administrator Password and Backup Location

After Security Tools activation, the Administrator Password and Backup Location can be changed, if necessary.

1. As an administrator, launch Security Tools from the Desktop shortcut.
2. Click the **Administrator Settings** tile.
3. In the Authentication dialog, enter the administrator password that was set up during activation, and click **OK.**



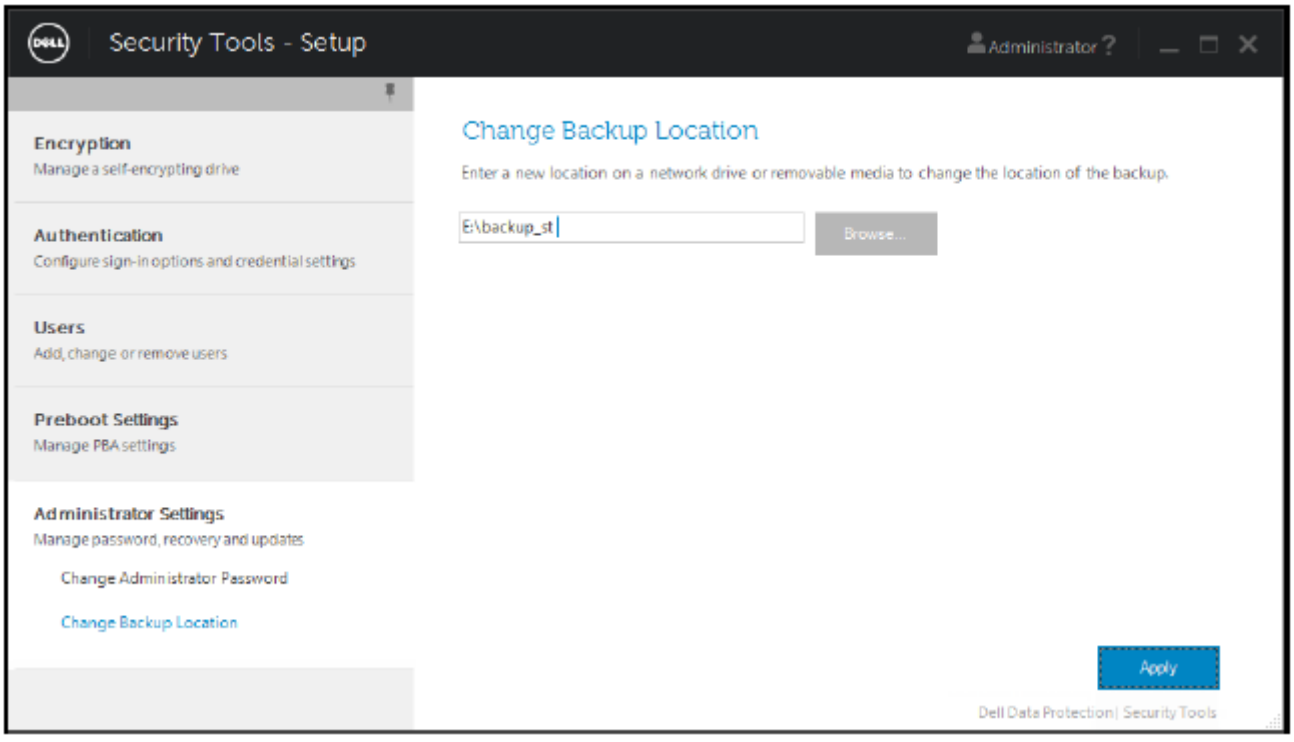
4. Click the **Administrator Settings** tab.
5. In the Change Administrator Password page, if you want to change the password, enter a new password that is between 8-32 characters and includes at least one letter, one number, and one special character.



6. Enter the password a second time to confirm it, then click **Apply**.
7. To change the location where the recovery key is stored, in the left pane, select **Change Backup Location**.
8. Select a new location for the backup, and click **Apply**.

   The backup file must be saved either on a network drive or onto removable media. The backup file contains the keys that are needed to recover data on this computer. Dell ProSupport must have access to this file to help you recover data.

   Recovery data will be automatically backed up to the specified location. If the location is not available (for instance, if your backup USB drive is not inserted), Security Tools prompts for a location to back up your data. Access to recovery data will be required in order to begin encryption.



設定加密與開機前驗證

如果您的電腦配備自我加密磁碟機 (SED)，可使用加密與開機前驗證 (PBA)。上述功能皆可透過 Encryption (加密) 標籤設定。此標籤唯有在電腦配備自我加密磁碟機 (SED) 時才可看見。啟用加密或 PBA 時，另一選項亦會啟用。

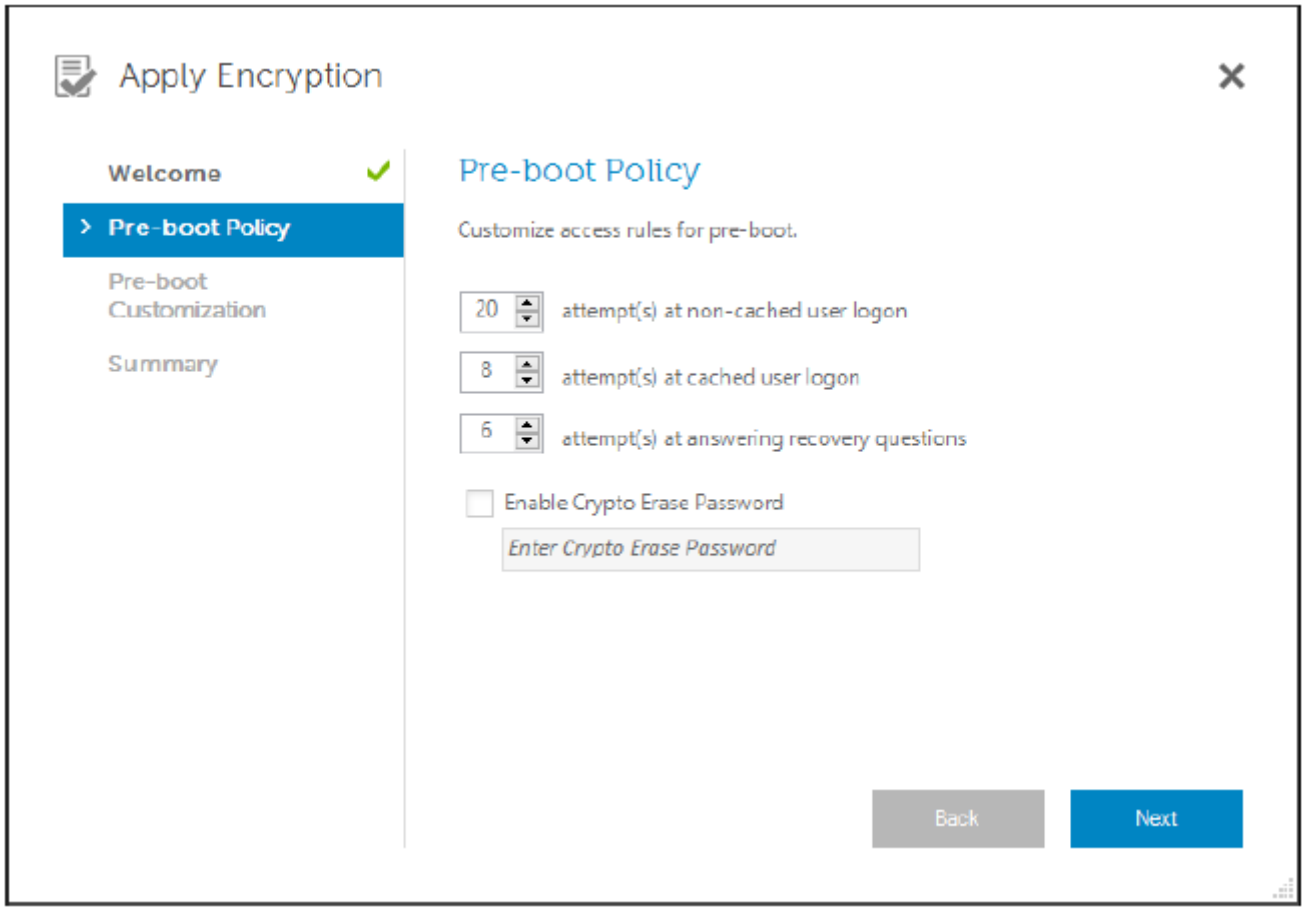
啟用加密與 PBA 前，Dell 建議註冊並將 Recovery Questions (復原問題) 作為 Recovery Option (復原選項) 使用，以在密碼遺失時復原密碼。如需更多資訊，請參閱 Configure Sign-in Options (設定登入選項)。

設定加密與開機前驗證：

1. 在 DDP 安全性主控台中，按一下 **Administrator Settings** (系統管理員設定) 動態磚。
2. 確定可從電腦存取備份位置。

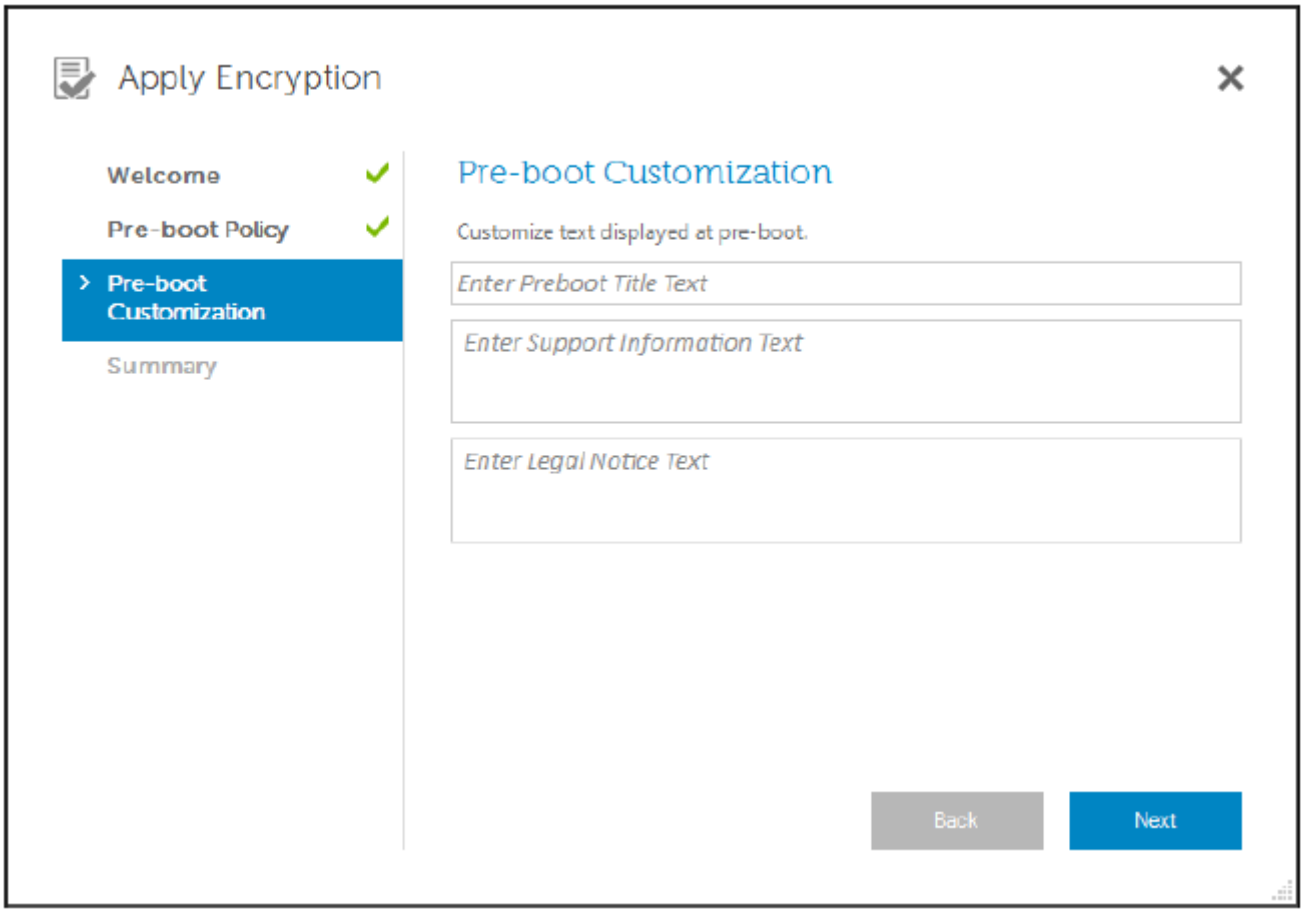
   註: 如果在啟用加密時顯示「Backup Location not found (未找到備份位置)」訊息，且備份位置位於 USB 磁碟機上，則表示尚未連接您的磁碟機，或您的磁碟機連接的插槽不同於備份時使用的插槽。如果顯示此訊息，且備份位置位於網路磁碟機上，則表示無法從電腦存取網路磁碟機。如果需要變更備份位置，請從 Administrator Settings (系統管理員設定) 標籤選取 Change Backup Location (變更備份位置)，將位置變更為目前的插槽或可存取的磁碟機。重新指派位置數秒後，即可繼續啟用加密的程序。
3. 按一下 **Encryption** (加密) 標籤，然後按一下 **Encrypt** (加密)。
4. 在歡迎頁面，按一下 **Next** (下一步)。
5. 請在 Preboot Policy (開機前原則) 頁面中，變更或確認以下數值，然後按一下 **Next** (下一步)。

非快取使用者登入的嘗試次數	未知使用者可嘗試登入的次數 (也就是使用者之前從未登入此電腦 [所以從未對認證進行快取])。
快取使用者登入的嘗試次數	已知使用者可嘗試登入的次數。
回答復原問題的嘗試次數	使用者可嘗試輸入正確答案的次數。
啟用 Crypto Erase Password (密碼編譯清除密碼) 功能	選取可啟用。
輸入 Crypto Erase Password (密碼編譯清除密碼)	使用最多 100 個字元的字詞或代碼，作為故障防護安全性機制。於 PBA 驗證期間在使用者名稱或密碼欄位輸入此文字或代碼，會刪除所有使用者的驗證權杖的並鎖定 SED。如此一來，只有管理員可以強制解除鎖定裝置。 若您不想要在緊急情況時有可用的加密清除密碼，請將此欄位空白。



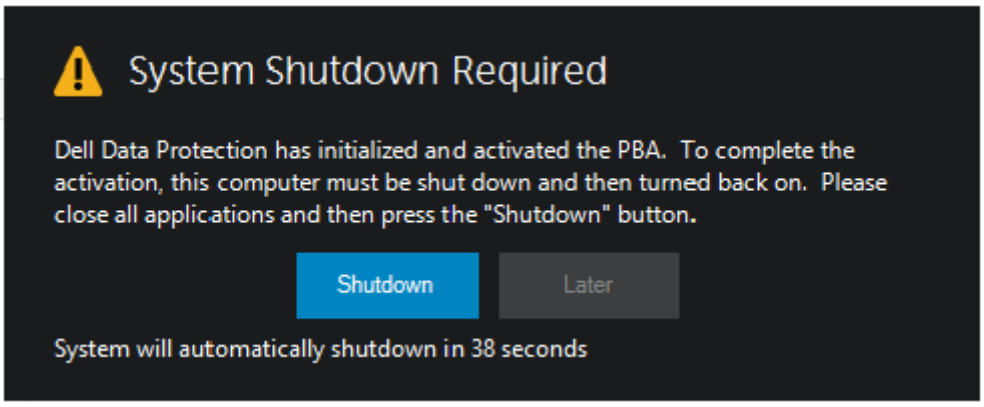
6. 在 Preboot Customization (開機前自訂) 頁面，輸入要在開機前驗證 (PBA) 畫面上顯示的自訂文字，然後按一下 **Next** (下一步)。

開機前動態磚文件	此文字在 PBA 畫面上方顯示。如果讓此欄位留白，將不會顯示任何標題。文字不會自動換行，因此輸入超過 17 個字元可能會切斷文字。
支援資訊文字	此文字在 PBA 支援資訊畫面上顯示。Dell 建議您在自訂訊息中加入關於如何聯絡「Help Desk」(服務台) 或「Security Administrator」(安全系統管理員) 的特定指示。若未在此欄位輸入文字，會導致使用者無法取得支援聯絡資訊。自動換行是在字詞層級執行，而非字元層級。例如，如果單一字詞的字元長度超過約 50 個字元，將不會換行也不會顯示捲軸，因此該文本將會被切斷。
法律聲明文字	此文字在允許使用者登入裝置前顯示。例如 :「按一下「確定」, 即表示您同意遵守可接受的電腦使用原則」。未在此欄位輸入文字結果為無出現文字或即顯示「確定」/「取消」按鈕。自動換行是在字詞層級執行，而非字元層級。例如，如果單一字詞的字元長度超過約 50 個字元，將不會換行也不會顯示捲軸，因此該文本將會被切斷。



7. 在 Summary (摘要) 頁面，按一下 **Apply** (套用)。
8. 提示時，請按一下 **Shutdown** (關機)。

   必須完全關機後，才可開始加密。



9. 關機後，請重新啟動電腦。

   現在以 Security Tools 管理驗證。使用者必須在開機前驗證畫面以 Windows 密碼登入。

變更加密與開機前驗證設定

先啟用加密並設定開機前原則與自訂後，則可從 Encryption (加密) 標籤執行下列動作：

- 變更開機前原則與自訂 - 按一下 **Encryption** (加密) 標籤，然後按一下 **Change** (變更)。
- 將 SED 解密，例如為了解除安裝 - 按一下 **Decrypt** (解密)。

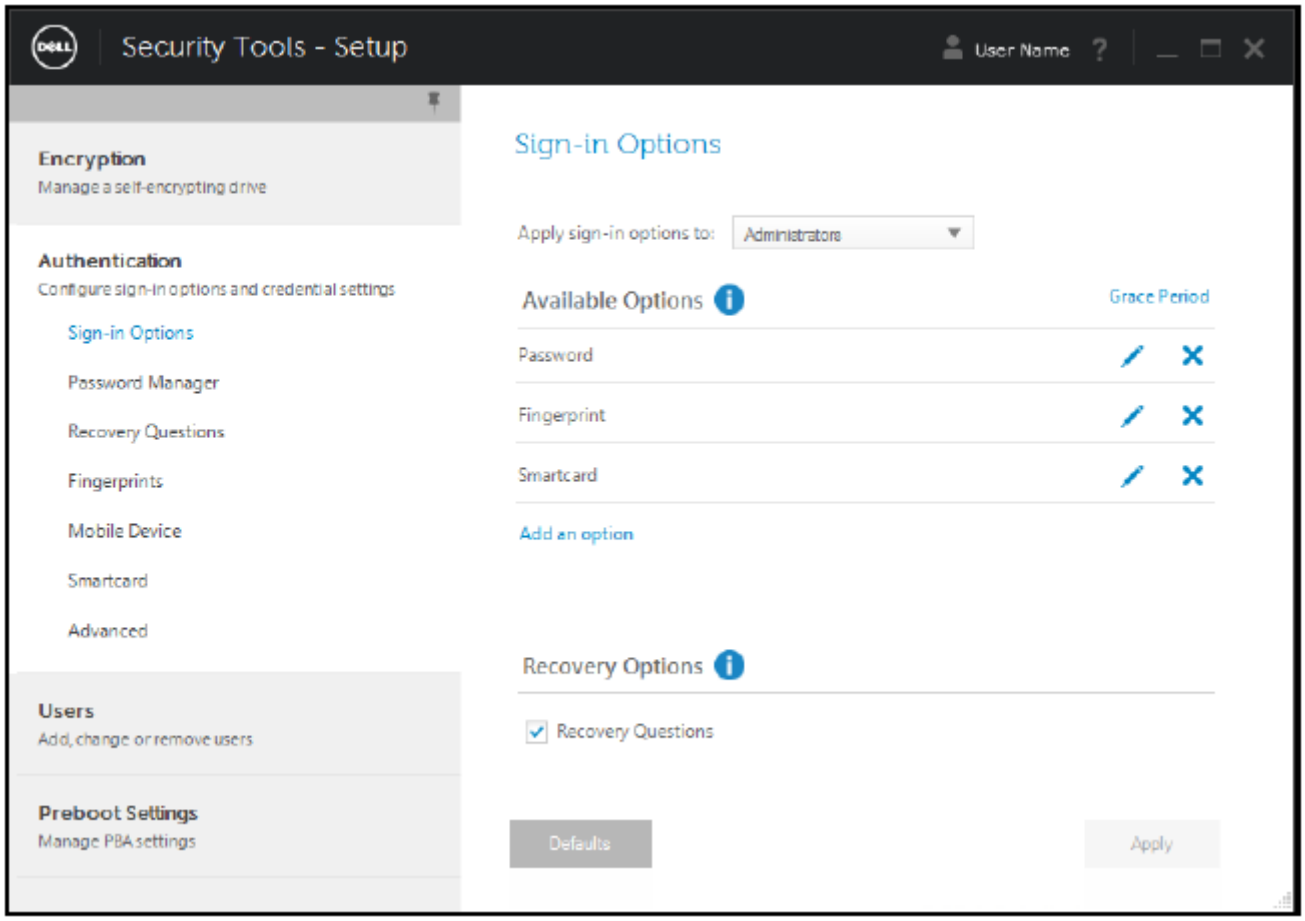
先啟用加密並設定開機前原則與自訂後，則可從 Preboot Settings (開機前設定) 標籤執行下列動作：

- 變更開機前原則與自訂 - 按一下 **Preboot Settings** (開機前設定) 標籤 並選取 **Preboot Customization** (開機前自訂) 或 **Preboot Logon Policies** (開機前登入原則)。

如需解除安裝指示，請參閱 Uninstallation Tasks (解除安裝工作)。

Configure Authentication Options

The controls on the Administrator Settings Authentication tab let you set user sign-in options and customize the settings for each.



NOTE: The One-time Password option does not display under Recovery Options if the TPM is not present, owned, and enabled.

Configure Sign-in Options

On the Sign-in Options page, you can configure logon policies. By default, all supported credentials are listed in Available Options.

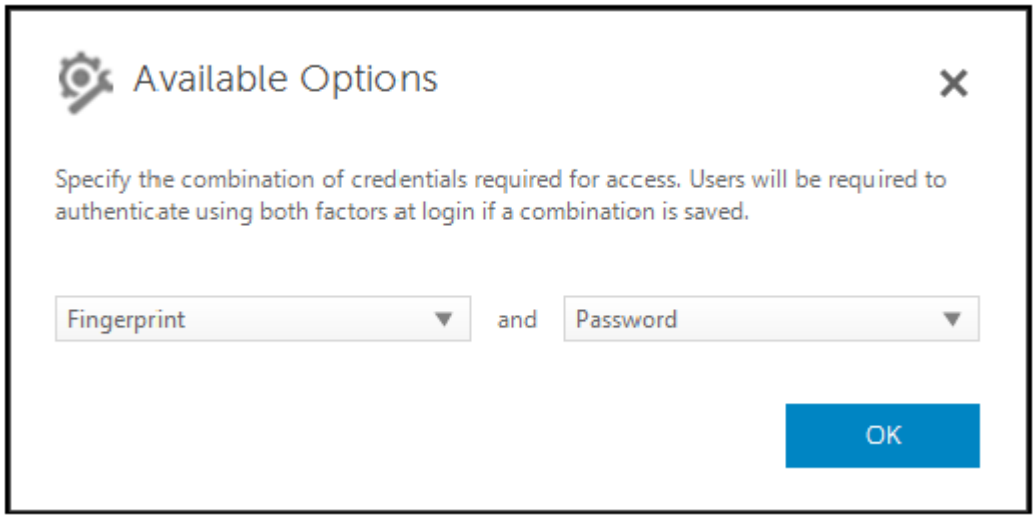
To configure sign-in options:

1. In the left pane, under Authentication, select **Sign-in Options**.
2. To choose the role you want to set up, select the role in the **Apply sign-in options to** list: **Users** or **Administrators**. All of the changes that you make on this page will apply only to the role that you select.
3. Set Available Options for authentication.

   By default, each authentication method is configured to be used individually, not in combination with other authentication methods. You can change the defaults in the following ways:

   - To set up a combination of authentication options, under Available Options, click ✎ to select the first authentication method. In the Available Options dialog, select the second authentication method, then click **OK**.

     For example, you can require both a fingerprint and a password as logon credentials. In the dialog, select the second authentication method that must be used with fingerprint authentication.



- To allow each authentication method to be used individually, in the Available Options dialog, leave the second authentication method set to **None**, and click **OK**.
- To remove a sign-in option, under Available Options on the Sign-in Options page, click **X** to remove the method.
- To add a new combination of authentication methods, click **Add an Option**.

4. Set Recovery Options for users to recover their computer access, if they become locked out.
   - To allow users to define a set of questions and answers to be used to regain access to the computer, select **Recovery Questions**.

     To prevent use of Recovery Questions, deselect the option.
   - To allow users to recover access using a mobile device, select **One-time Password**. When One-time Password (OTP) is selected as a recovery method, it is not available as a sign-in option on the Windows logon screen.

     To use the OTP feature for logon, deselect the option in Recovery Options. When deselected as a recovery method, the OTP option appears on a Windows logon page as long as at least one user has enrolled in OTP.

     NOTE: As administrator, you control how One-time Password can be used - for authentication or for recovery. The OTP feature can be used either for authentication or for recovery, but not for both. The configuration affects either all users of the computer or all administrators, based on the selection in the Sign-in Options field, Apply sign-in options to.

     If the One-time Password option is not listed under Recovery Options, your computer's configuration does not support it. For more information, see Requirements.
   - To require the user to make a help desk call if they lose or forget logon credentials, clear both check boxes under Recovery Options: Recovery Questions and One-time Password.
5. To set a length of time to allow users to enroll their authentication credentials, select **Grace Period**.

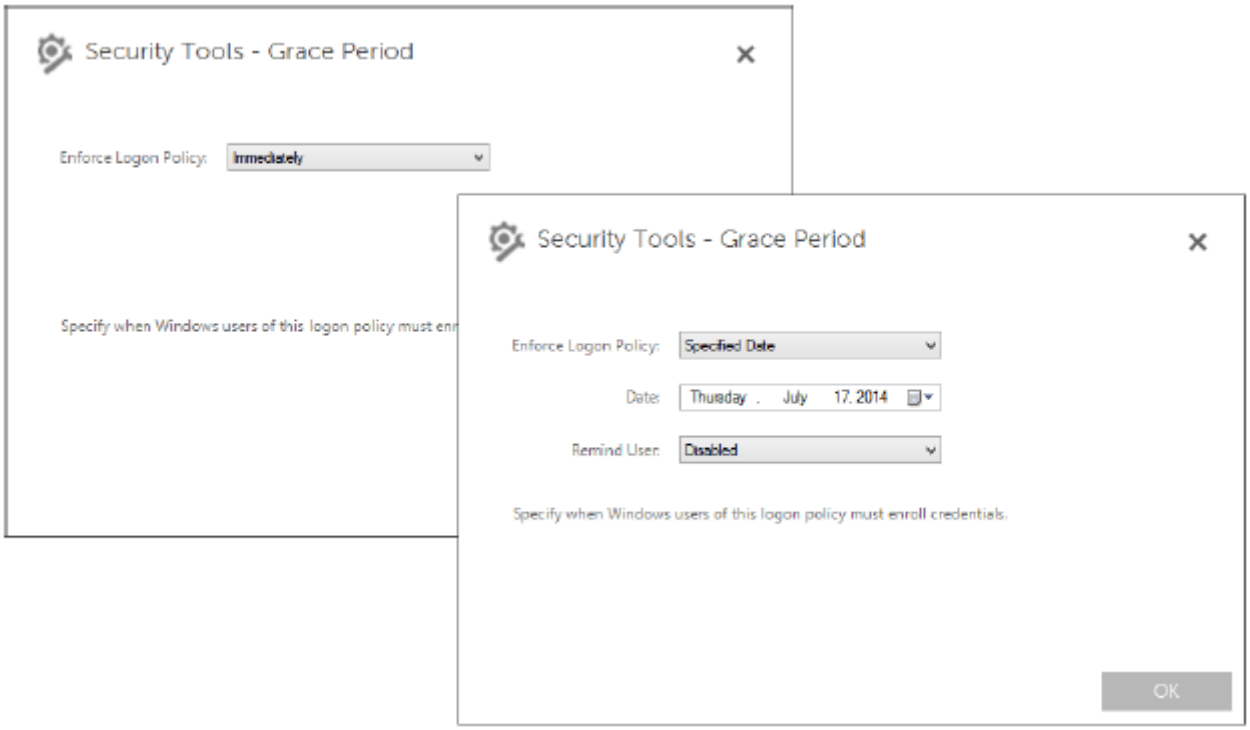
   The Grace Period feature lets you set the date on which a configured Sign-in Option will begin to be enforced. You can configure a Sign-in Option before the date when it will be enforced and set up a length of time to allow users to enroll. By default, the policy is enforced immediately.

   To change the Enforce Sign-in Option date from *Immediately*, in the Grace Period dialog, click the drop-down menu and select **Specified Date**. Click the down arrow at the right side of the date field to display a calendar, then select a date on the calendar. Enforcement of the policy begins at approximately 12:01 AM on the date selected.

   Users can be reminded to enroll their credentials required at their next Windows logon (by default), or you can set up regular reminders. Select the reminder interval from the *Remind User* drop-down list.

   NOTE:

   The reminder that is displayed to the user is slightly different, depending on whether the user is at the Windows Logon screen or within a Windows session when the reminder is triggered. Reminders do not appear on Preboot Authentication logon screens.



Functionality During the Grace Period

During a specified Grace Period, after every log on, the Additional Credentials notification displays when the user has not yet enrolled the minimum credentials required to satisfy a changed Sign-in Option. The message content is: *Additional credentials are available for enrollment*.

If additional credentials are available, but are not required, the message displays only once after the policy has been changed.

Clicking the notification has the following results, depending on the context:

- If no credentials have been enrolled, the Setup wizard displays, allowing Administrative Users to configure computer-related settings and offering users the ability to enroll the most common credentials.
- After initial credential enrollment, clicking the notification displays the Setup wizard within the DDP Security Console.

Functionality After Grace Period Expires

In all cases, after the Grace Period has expired, users cannot log on without having enrolled the credentials required by the Sign-in Option. If a user attempts to log on with a credential or credential combination that does not satisfy the Sign-in Option, the Setup wizard displays on top of the Windows Logon screen.

- If the user successfully enrolls the required credentials, they are logged into Windows.
- If a user does not successfully enroll the required credentials, or cancels the wizard, they are returned to the Windows Logon screen.

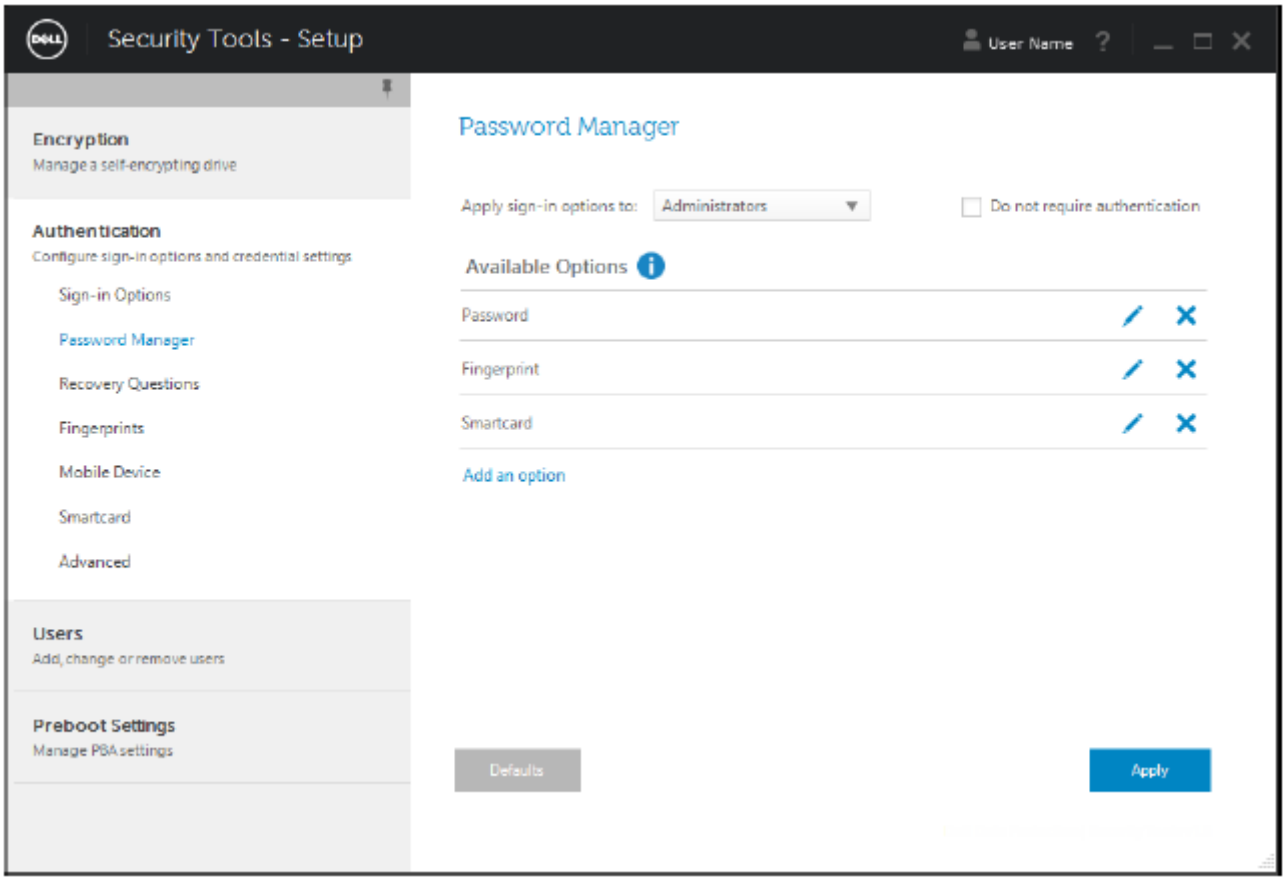
6. To save the settings for the selected role, click **Apply**.

Configure Password Manager Authentication

On the Password Manager page, you can configure how users authenticate to Password Manager.

To configure Password Manager authentication:

1. In the left pane, under Authentication, select **Password Manager**.
2. To choose the role you want to set up, select the role in the **Apply sign-in options to** list: **Users** or **Administrators**. All of the changes that you make on this page will apply only to the role that you select.
3. Optionally, select the **Do not require authentication** check box to allow the selected user role to be automatically logged on to all software applications and Internet websites with credentials stored in Password Manager.

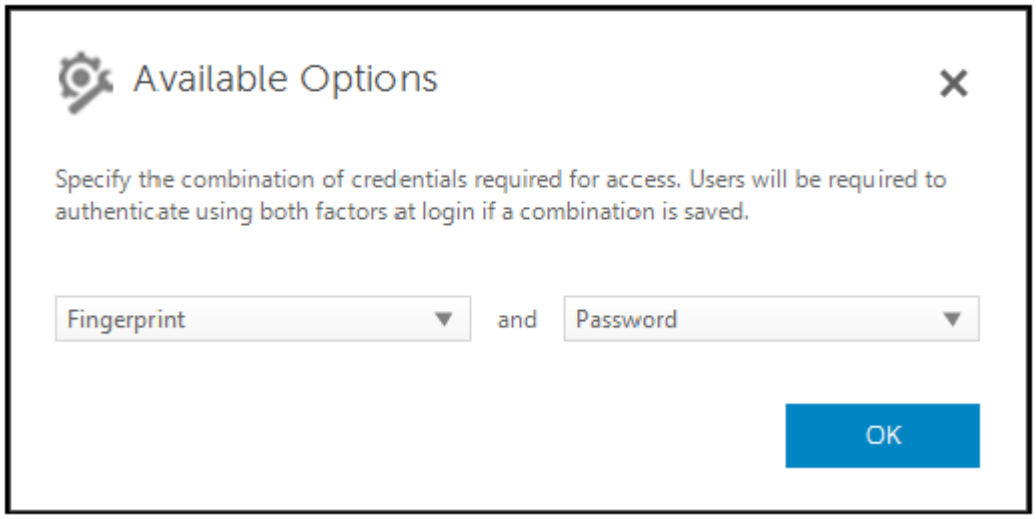


4. Set Available Options for authentication.

   By default, each authentication method is configured to be used individually, not in combination with other authentication methods. You can change the defaults in the following ways:

   - To set up a combination of authentication options, under Available Options, click ✎ to select the first authentication method. In the Available Options dialog, select the second authentication method, then click **OK**.

     For example, you can require both a fingerprint and a password as logon credentials. In the dialog, select the second authentication method that must be used with fingerprint authentication.



   - To allow each authentication method to be used individually, in the Available Options dialog, leave the second authentication method set to **None**, and click **OK**.
   - To remove a sign-in option, under Available Options on the Sign-in Options page, click **X** to remove the method.
   - To add a new combination of authentication methods, click **Add an Option**.

5. To save the settings for the selected role, click **Apply.**

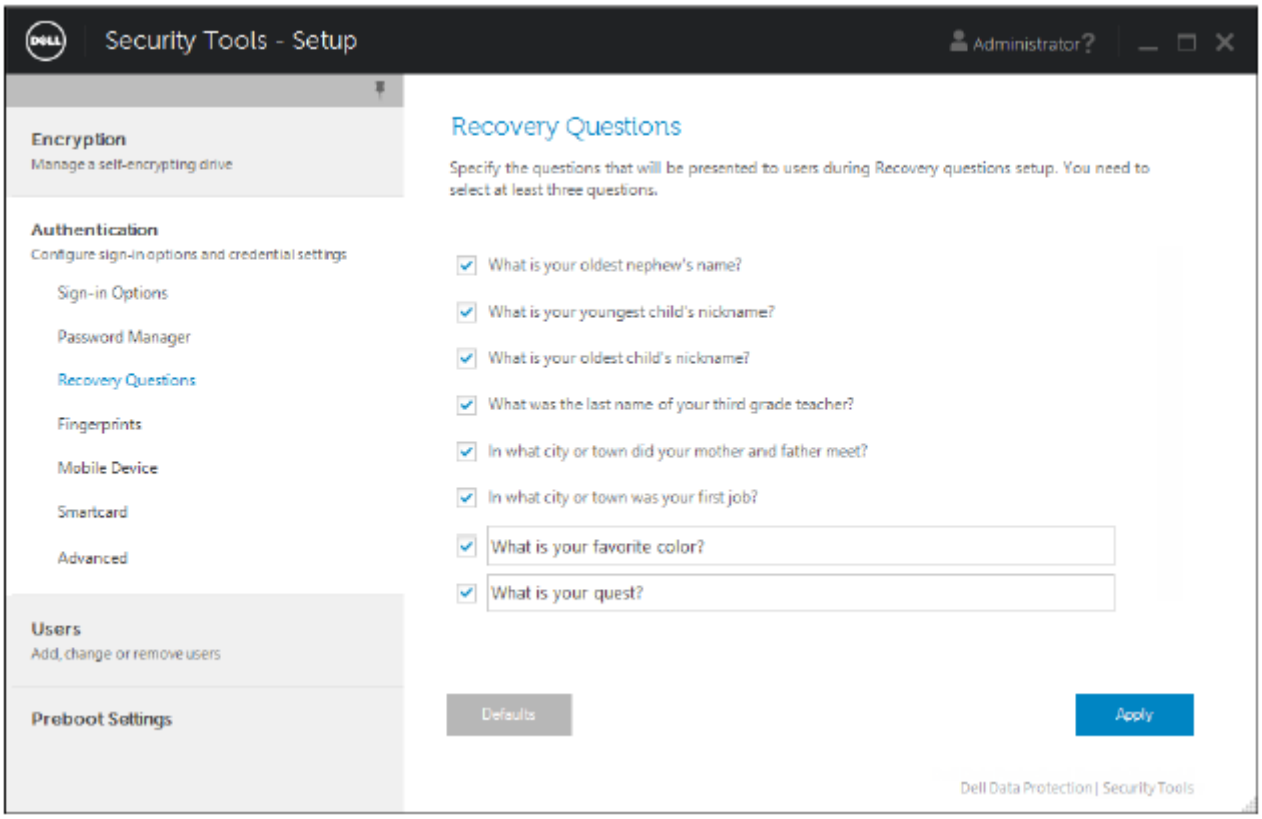
NOTE: Select the Defaults button to restore the settings to their original values.

Configure Recovery Questions

On the Recovery Questions page, you can select which questions will be presented to users when they define personal Recovery Questions and answers. Recovery Questions allow users to recover access to their computers if their passwords are expired or forgotten.

To configure Recovery Questions:

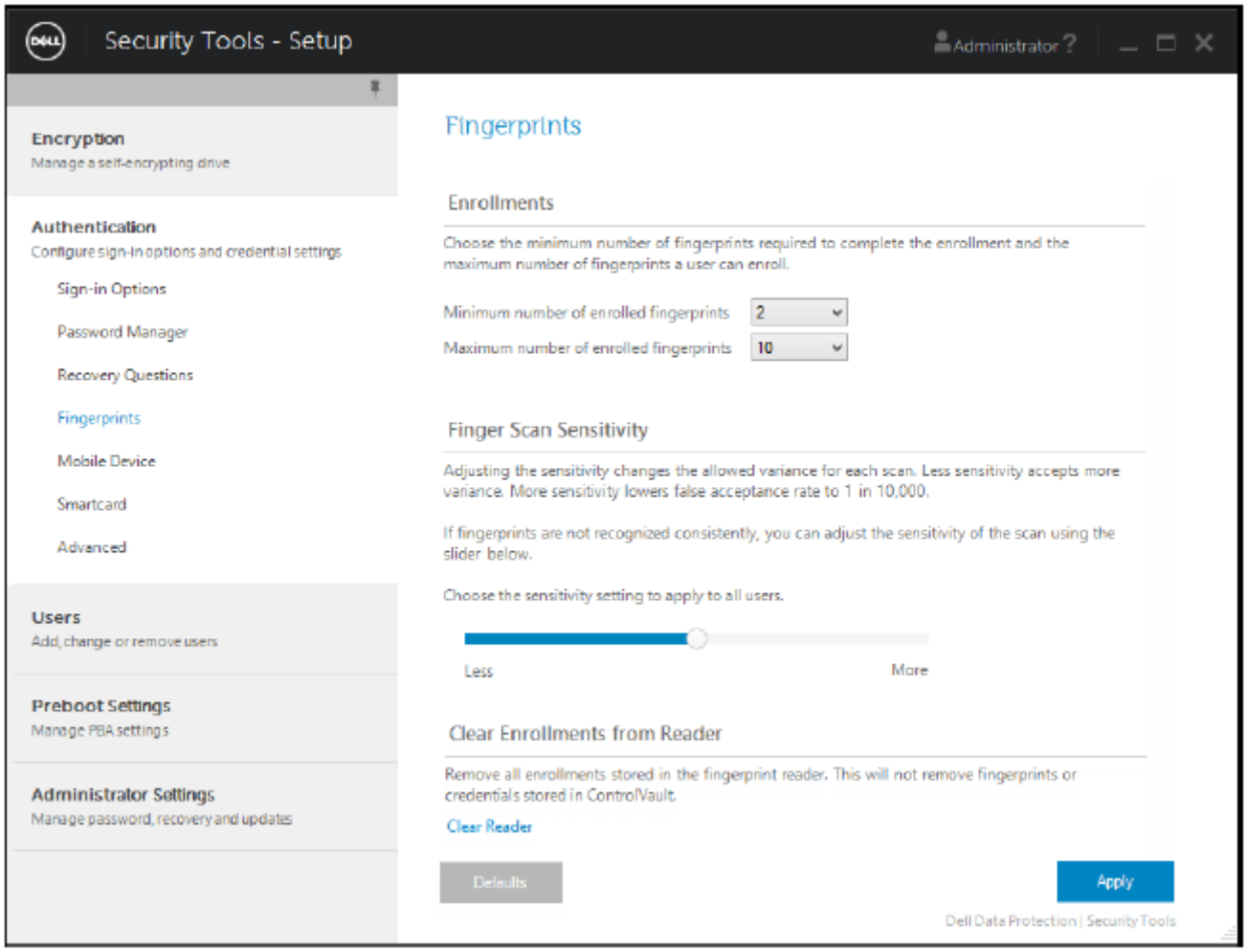
1. In the left pane, under Authentication, select **Recovery Questions**.
2. On the Recovery Questions page, select at least three pre-defined Recovery Questions.
3. Optionally, you can add up to three custom questions to the list that the user selects from.
4. To save the Recovery Questions, click **Apply**.



Configure Fingerprint Scan Authentication

To configure fingerprint scan authentication:

1. In the left pane, under Authentication, select **Fingerprints**.
2. In Enrollments, set the minimum and maximum number of fingers that a user can enroll.



3. Set the Fingerprint Scan sensitivity.

   Lower sensitivity increases the acceptable variance and the probability of accepting a false scan. At the highest setting, the system may reject legitimate fingerprints. The More sensitivity setting lowers the false acceptance rate to 1 in 10,000 scan.
4. To remove all fingerprint scans and credential enrollments from the fingerprint reader's buffer, click **Clear Reader**. This removes only data that you are currently adding. It does not delete scans and enrollments stored from previous sessions.
5. To save the settings, click **Apply**.

Configure One-time Password Authentication

To use the One-time Password feature, the user generates a One-time Password with the Security Tools Mobile application on his mobile device then enters the password on the computer. The password can be used only once, and it is valid for only a limited length of time.

To further improve security, the administrator can ensure that the mobile application is secure by requiring a password.

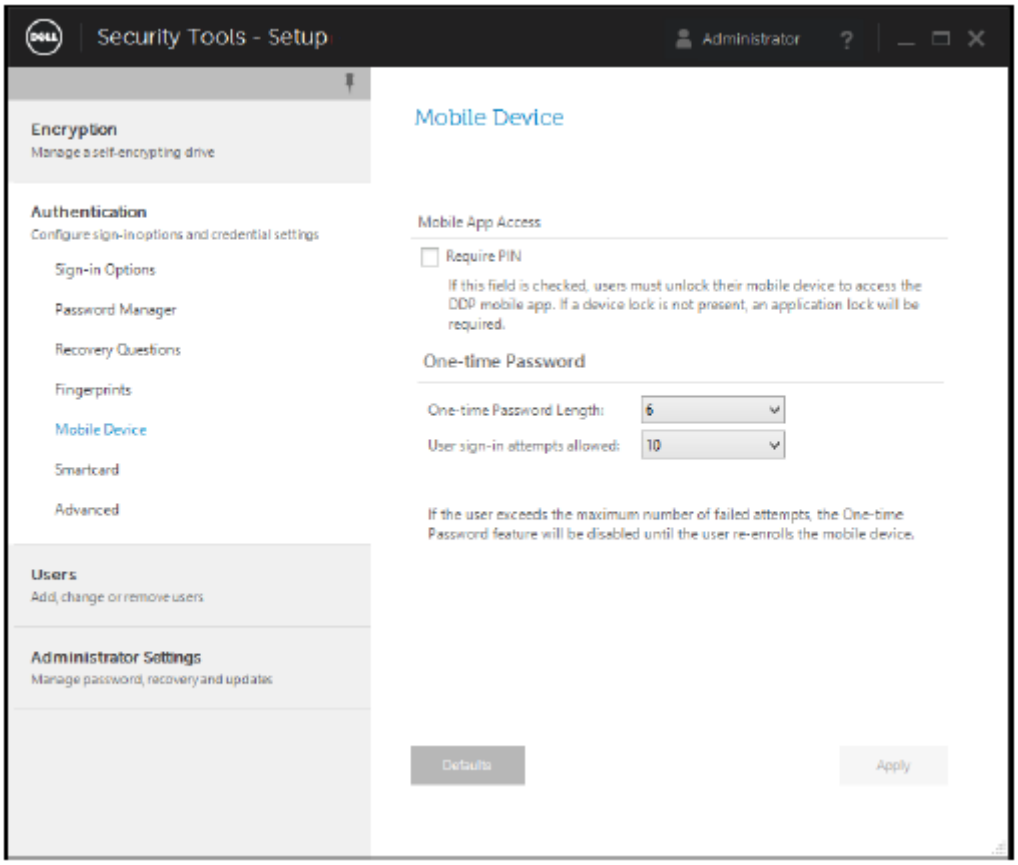
On the Mobile Device page, you can configure settings that further increase the security of the mobile device and One-time Password.

To configure One-time Password authentication:

1. In the left pane, under Authentication, select **Mobile Device**.
2. To require the user to enter a password to access the Security Tools Mobile application on the mobile device, select **Require Password**.

   NOTE: Enabling the *Require Password* policy after mobile devices have been enrolled with a computer causes all mobile devices to be unenrolled. Users will be required to re-enroll their mobile devices once this policy is enabled.

   When the **Require Password** check box is selected, users must unlock their mobile device to access the Security Tools Mobile app. If a device lock is not present on the mobile device, the password will be required.



3. To select the length of the One-time Password (OTP), for **One-time Password Length**, select number of password characters to require.
4. To select the number of chances the user has to enter the One-time Password correctly, for **User Sign-in Attempts Allowed**, select a number from **5** to **30**.

   When the maximum attempts is reached, the OTP feature will be disabled until the user re-enrolls the mobile device.

   NOTE: Dell recommends setting up at least one other authentication method in addition to One-time Password.

Configure Smart Card Enrollment

DDP|Security Tools supports two kinds of smart cards: contacted and contactless.

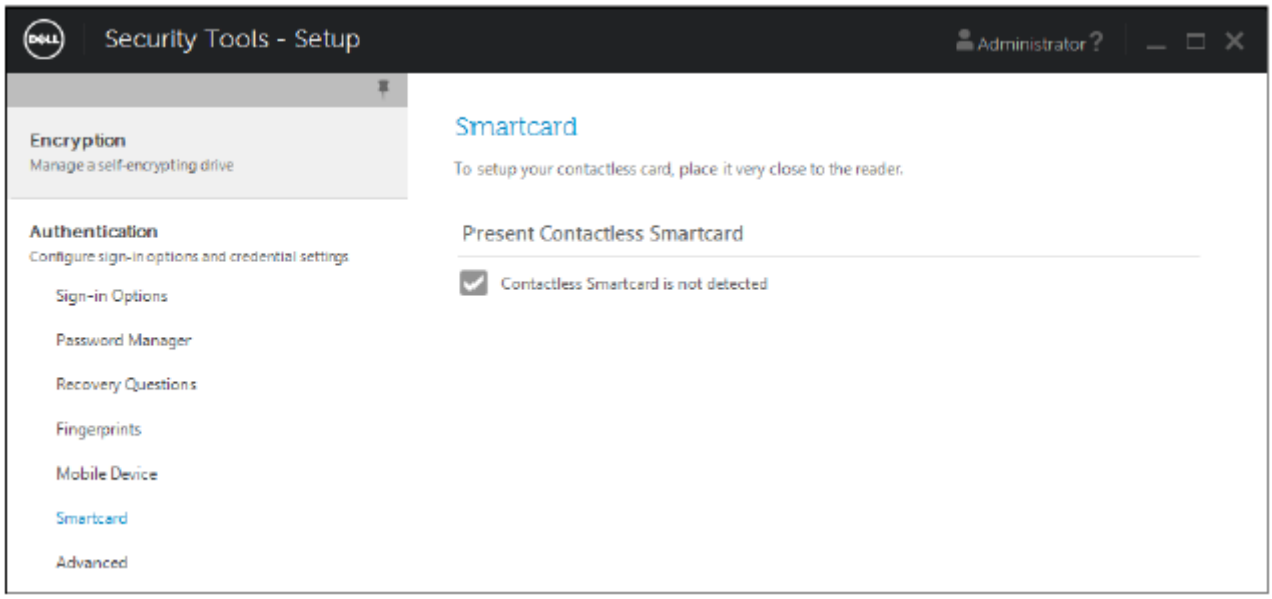
Contacted cards require a smart card reader into which the card is inserted. Contacted cards are only compatible with domain computers. CAC and SIPRNet cards are both contacted cards. Due to the advanced nature of these cards, the user will be required to choose a cert after using inserting his card to log on.

- Contactless cards are supported by non-domain computers and by computers configured with domain specifications.
- Users can enroll one contacted smart card per user account, or multiple contactless cards per account.
- Smart cards are not supported with Preboot Authentication.

NOTE: When removing a smart card enrollment from an account with multiple cards enrolled, all cards are unenrolled at the same time.

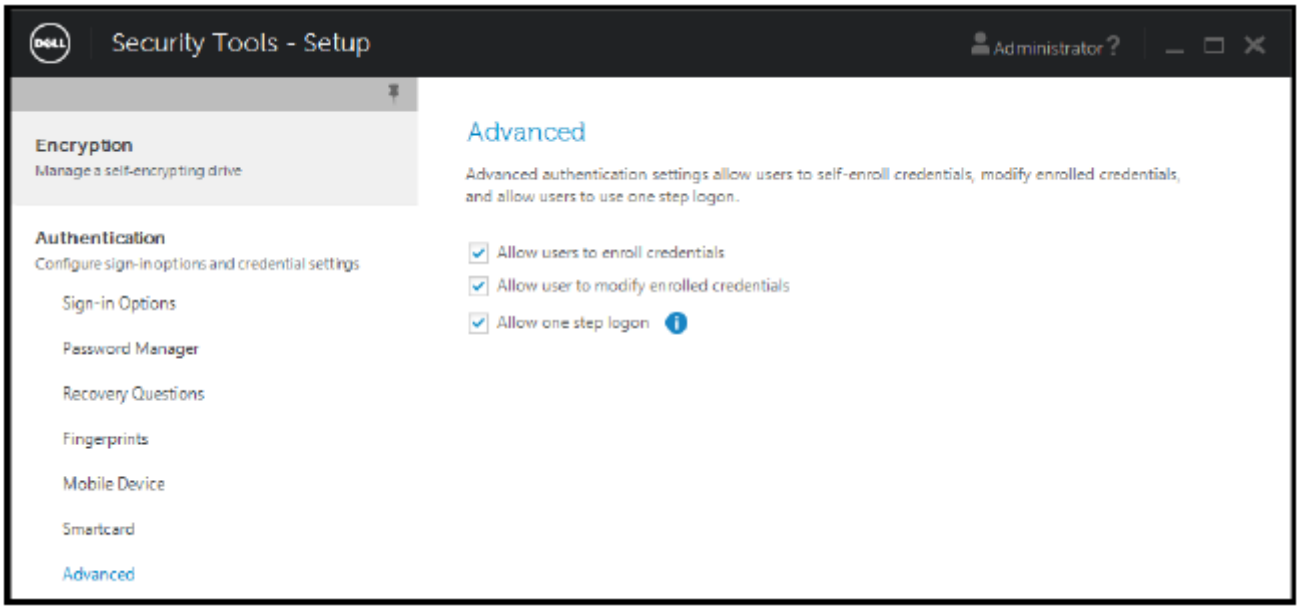
To configure smart card enrollment:

On the Administrator Settings tool's Authentication tab, select **Smartcard**.



Configure Advanced Permissions

1. Click **Advanced** to modify advanced end user options. Under *Advanced*, you can optionally allow users to self-enroll credentials, optionally allow users to modify their enrolled credentials, and enable one step logon.



2. Select or clear the check boxes:

   Allow users to enroll credentials - By default, the check box is selected. Users are permitted to enroll credentials without intervention by an administrator. If you clear the check box, credentials must be enrolled by the administrator.

   Allow user to modify enrolled credentials - By default, the check box is selected. When selected, users are permitted to modify or delete their enrolled credentials without intervention by an administrator. If you clear the check box, credentials cannot be modified or deleted by a regular user but must be modified or deleted by the administrator.

   NOTE: To enroll a user's credentials, go to the *Users* page of the Administrator Settings tool, select a user and click Enroll.

   Allow one step logon - One step logon is Single Sign-on (SSO). By default, the check box is selected. When this feature is enabled, users must enter their credentials only at the Preboot Authentication screen. Users are automatically logged on to Windows. If you clear the check box, the user may be required to log on multiple times.

   NOTE: This option cannot be selected unless the Allow users to enroll credentials setting is also selected.

3. Click **Apply** when finished.

Smart Card and Biometric Services (Optional)

If you do not want Security Tools to change the services associated with smart cards and biometric devices to a startup type of "automatic," the service startup feature can be disabled.

When disabled, Security Tools will not attempt to start these three services:

- SCardSvr - Manages access to smart cards read by the computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.
- SCPolicySvc - Allows the system to be configured to lock the user desktop upon smart card removal.
- WbioSrvc - The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

Disabling this feature also suppresses warnings associated with the required services not running.

Disable the Automatic Service Startup

By default, if the registry key does not exist or the value is set to 0, this feature is enabled.

1. Run **Regedit**.
2. Locate the following registry entry:

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

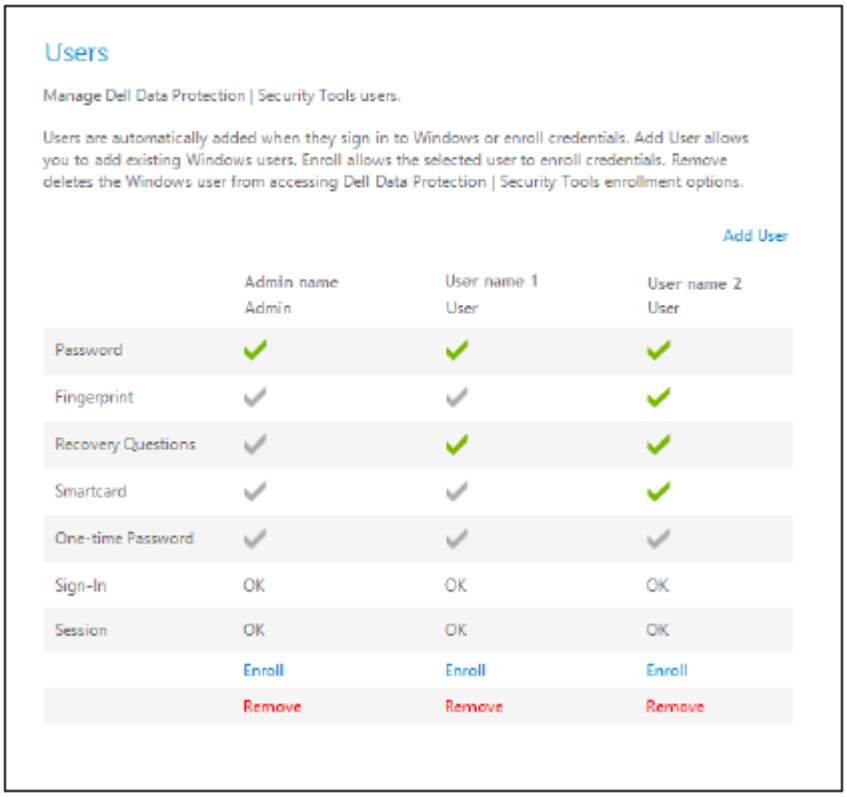
   Set to 0 to Enable. Set to 1 to Disable.

Manage Users' Authentication

The controls on the Administrator Settings Authentication tab let you set user logon options and customize the settings for each.

To manage user authentication:

1. As an administrator, click the **Administrator Settings** tile.
2. Click the **Users** tab to manage users and view user enrollment status. From this tab, you can:
   - Enroll new users
   - Add or change credentials
   - Remove a user's credentials



NOTE:

Sign-in and Session show the enrollment status of a user.

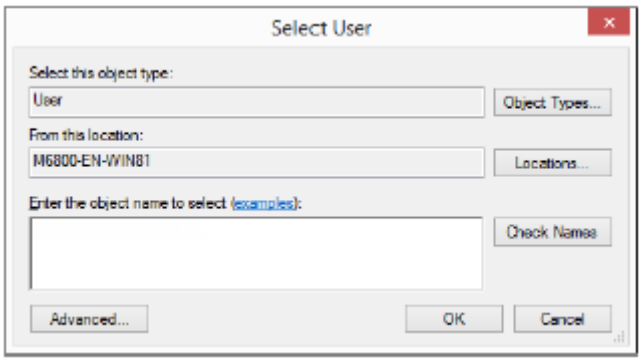
When Sign-in status is OK, all enrollments that the user needs to be able to log on have been completed. When Session status is OK, all enrollments that the user needs to use Password Manager have been completed.

If either status is No, the user needs to complete additional enrollments. To find out which enrollments are still needed, select the Administrator Settings tool and open the Users tab. Gray check mark boxes represent incomplete enrollments. Alternatively, click the Enrollments tile and review the Status tab's Policy column, where the required enrollments are listed.

Add New Users

NOTE: New Windows users are automatically added when they log on to Windows or enroll credentials.

1. Click **Add User** to begin the enrollment process for an existing Windows user.
2. When the *Select User* dialog displays, select **Object Types**.



3. Enter a user's object name in the text box and click **Check Names**.
4. Click **OK** when finished.

The Enrollment wizard opens.

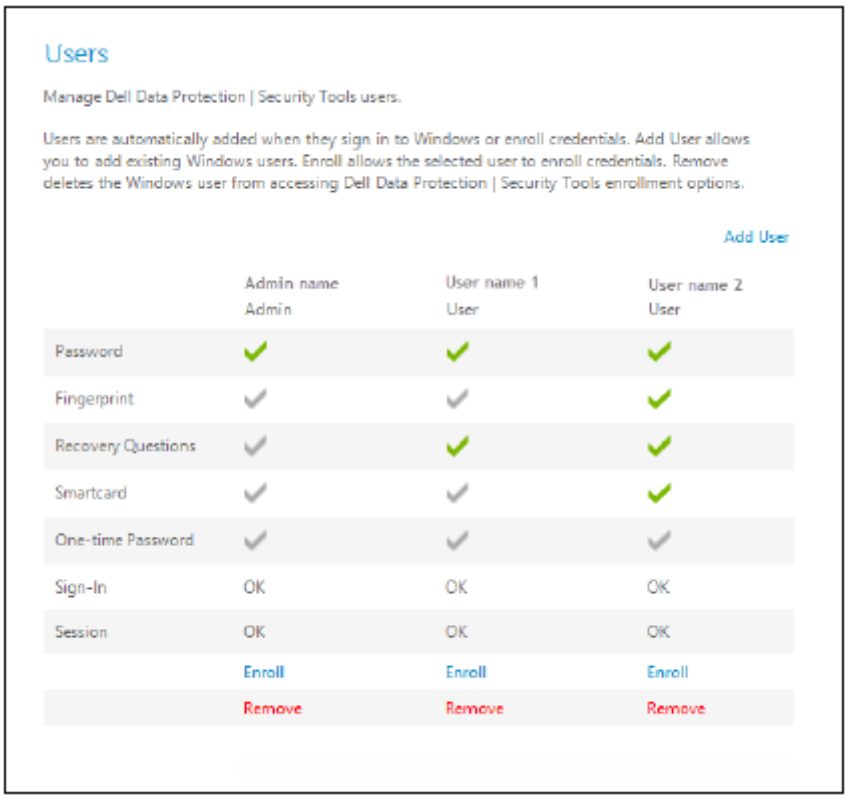
Continue to Enroll or Change User Credentials for instructions.

Enroll or Change User Credentials

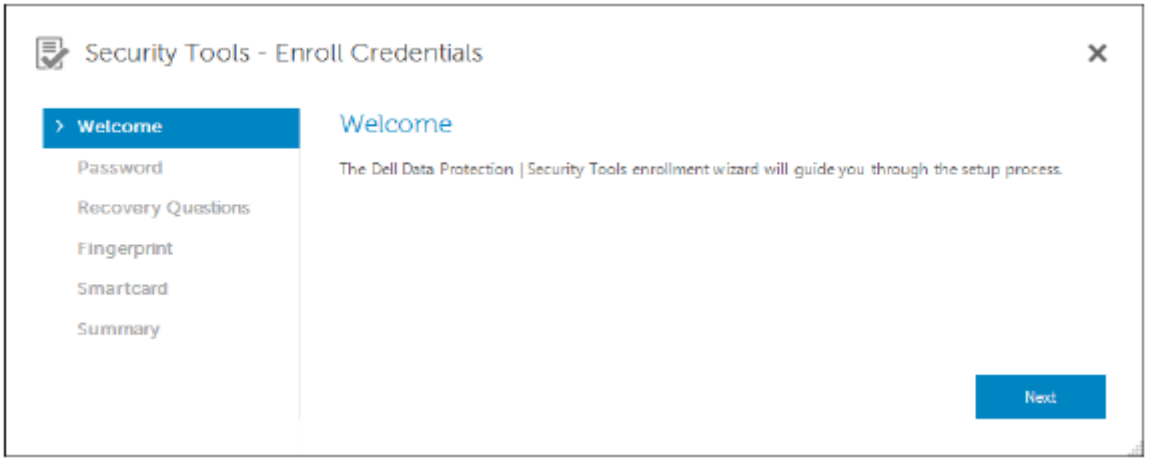
The administrator can enroll or change a user's credentials on behalf of a user, but a few enrollment activities require the user's presence, such as answering recovery questions and scanning the user's fingerprints.

To enroll or change user credentials:

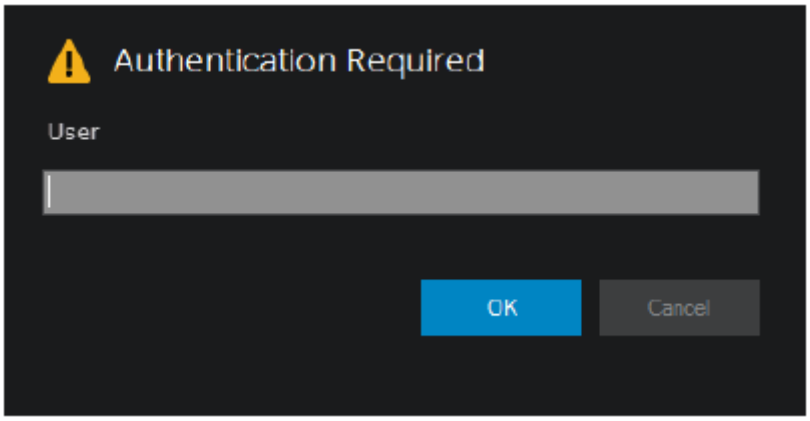
1. In Administrator Settings, click the **Users** tab.
2. On the Users page, click **Enroll**.



3. On the Welcome page, click **Next**.



4. In the Authentication Required dialog, log in with the user's Windows password, and click **OK**.



5. On the Password page, to change the user's Windows password, enter and confirm a new password and click **Next**.

   To skip changing the password, click **Skip**. The wizard allows you to skip a credential if you don't want to enroll it. To return to a page, click **Back**.
6. Follow the instructions on each page, and click the appropriate button: **Next**, **Skip**, or **Back**.
7. On the Summary page, confirm the enrolled credentials and, when finished with enrollment, click **Apply**.

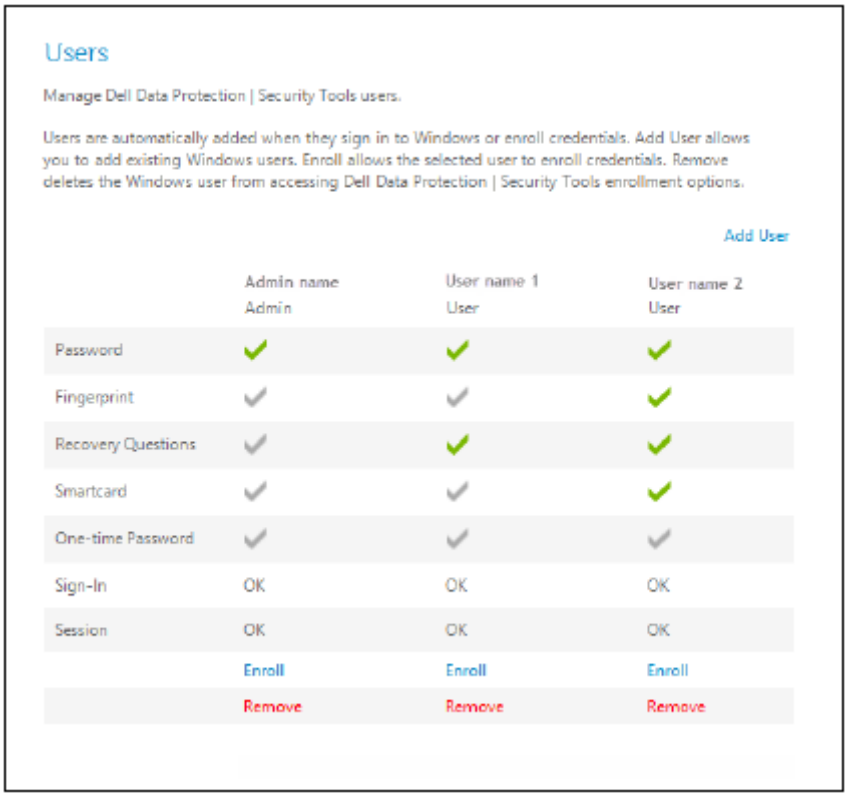
   To return to a credential enrollment page to make a change, click **Back** until you reach the page you want to change.

   For more detailed information about enrolling a credential, or to change a credential, see the *Console User Guide*.

Remove One Enrolled Credential

1. Click the **Administrator Settings** tile.
2. Click the **Users** tab and find the user to change.
3. Hover over the green checkmark of the credential you want to remove. It turns into ⊗.
4. Click the ⊗ symbol and then click **Yes** to confirm the deletion.

   NOTE: A credential cannot be removed this way if it is the user's only enrolled credential. In addition, the Password cannot be removed with this method. Use the Remove command to completely remove a user's access to the computer.



Remove All of a User's Enrolled Credentials

1. Click the **Administrator Settings** tile.
2. Click the **Users** tab and find the user you want to remove.
3. Click **Remove**. (The Remove command appears in red at the bottom of the user's settings).

   After removal, the user will not be able to log on to the computer unless he re-enrolls.

5

解除安裝工作

若要解除安裝 DDP | Security Tools，您必須至少是 **local Admin** (本機系統管理員) 使用者。

解除安裝 DDP | Security Tools

您必須依此順序解除安裝應用程式：

DDP | Client Security Framework

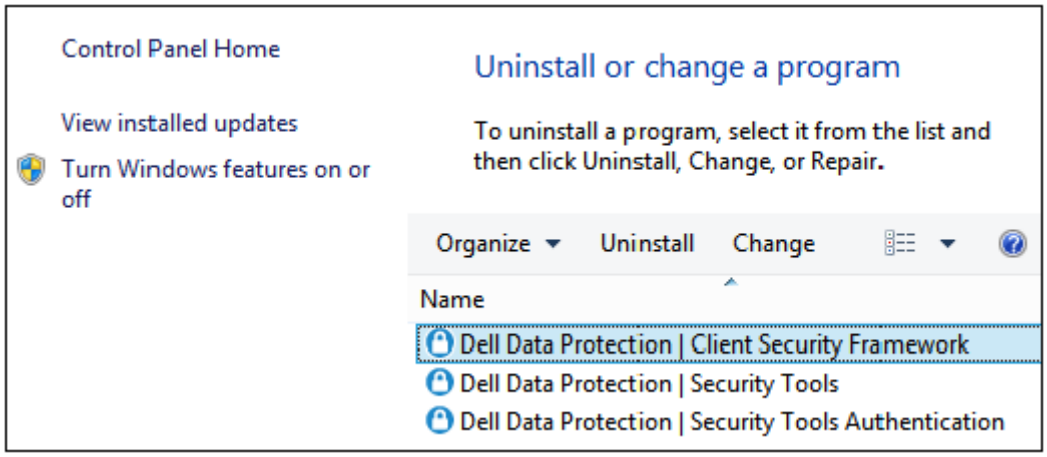
2. DDP | Security Tools Authentication

3. DDP | Security Tools

如果您擁有的電腦配備自我加密磁碟機，請遵循以下指示解除安裝：

1. Deprovision (解除佈建) SED：
   a) 從 Administrator Settings（系統管理員設定）> 按一下 **Encryption**（加密）標籤。
   b) 按一下 **Decrypt**（解密），停用加密。
   c) 將 SED 解除加密後，請重新啟動電腦。
2. 在 Windows 控制台中，前往 **Uninstall a Program**（解除安裝程式）。

   註: 開始 > 控制台 > 程式和功能 > 解除安裝程式。



3. 解除安裝 **Client Security Framework**，然後重新啟動電腦。
4. 從 Windows 控制台，解除安裝 **Security Tools Authentication**。

   將會顯示訊息，提示您是否要保留使用者資料。

   如果計畫重新安裝安全性工具，請按一下 **Yes**（是）。否則按一下 **No**（否）。

   解除安裝完成後，請重新啟動電腦。

5. 從 Windows 控制台，解除安裝 **Security Tools**。

   將會顯示訊息，提示您是否要完全解除此應用程式及其元件。

   按一下 **Yes**（是）。

   即顯示 *Uninstallation Complete*（解除安裝完成）對話方塊。
6. 按一下 **Yes, I want to restart my computer now**（是，我想要重新啟動電腦），然後按一下 **Finish**（完成）。
7. 電腦重新啟動，完成解除安裝作業。

6

復原

復原選項可在使用者認證到期或遺失時使用：

- **One-time Password (OTP) (一次性密碼)：**使用者在註冊的行動裝置上以 Security Tools Mobile 應用程式產生 OTP，並在 Windows 登入畫面輸入 OTP，以取回存取權限。唯有使用者已使用 Security Tools 在電腦上註冊行動裝置後，才可使用此選項。若要將 OTP 功能作為復原之用，使用者不可使用 OTP 登入電腦。

  註: 一次性密碼 (OTP) 功能需要有 TPM，而且必須啟用及擁有。依照 Clear Ownership and Activate the TPM (清除所有權及啟動 TPM) 中的指示。OTP 功能可用於驗證或復原，但上述兩者並非皆同時可用。如需詳細資訊，請參閱 Configure Sign-in Options (設定登入選項)。
- **Recovery Questions (復原問題)：**使用者正確回答一組個人問題，以取回存取電腦的功能。唯有在設定系統管理員並啟用 Recovery Questions (復原問題)，且使用者已註冊 Recovery Questions (復原問題) 後，才可使用此選項。此選項可用於透過開機前驗證畫面與 Windows 登入畫面，取回存取電腦的權限。

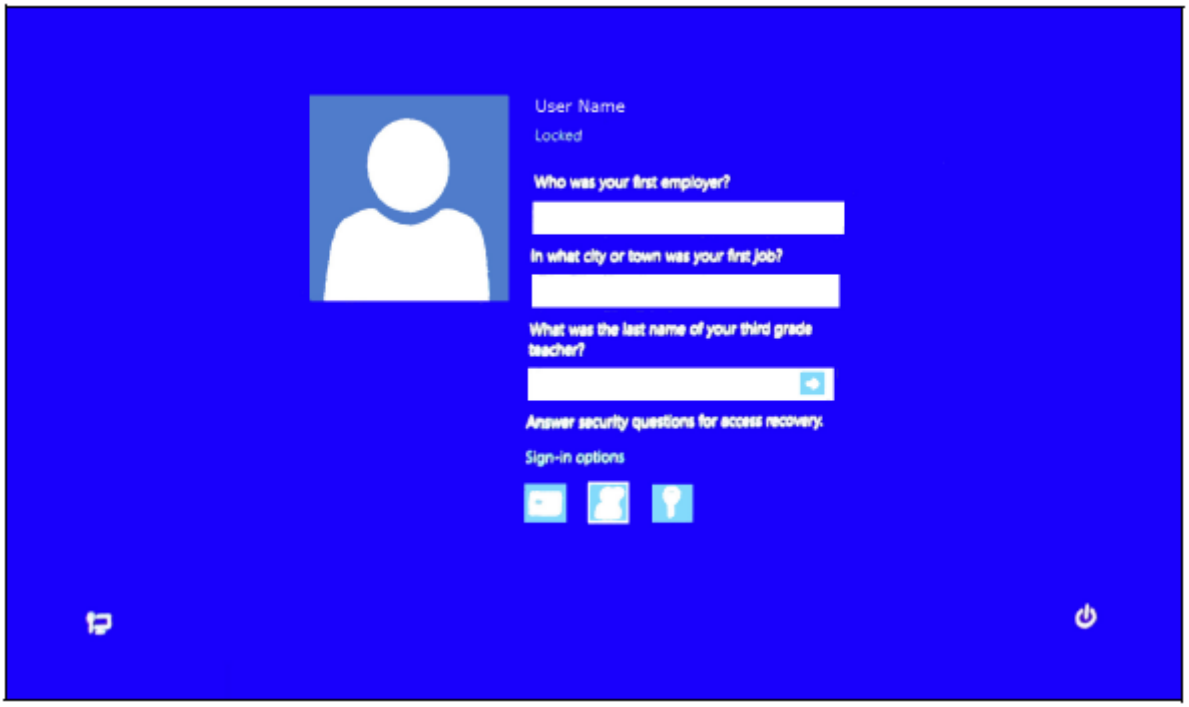
但上述兩種復原方法需要您註冊復原問題，或以電腦上的 Security Tools 註冊行動裝置，做好復原作業準備。

Self-Recovery, Windows Logon Recovery Questions

To answer Recovery Questions to recover access at the Windows logon screen:

1. To use the Recovery questions, click **Can't access your account?**

   The Recovery Questions that you selected during enrollment display.



2. Enter the answers and click **OK**.

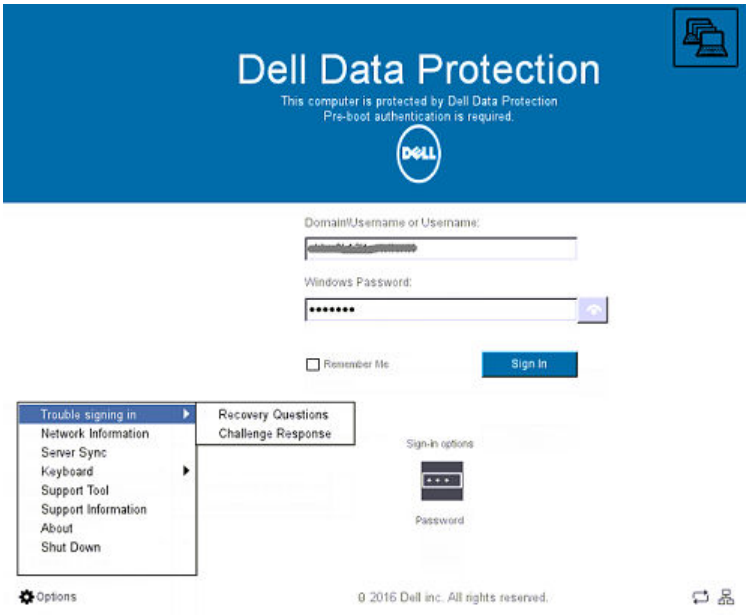
   Upon successful entry of the answers to the questions, you enter Access Recovery mode. What happens next depends upon the credential that failed.

   - If you failed to enter the correct Windows password, then the Change Password screen displays.
   - If a fingerprint failed to be recognized, then the fingerprint enrollment page displays so that you can re-enroll the fingerprint.

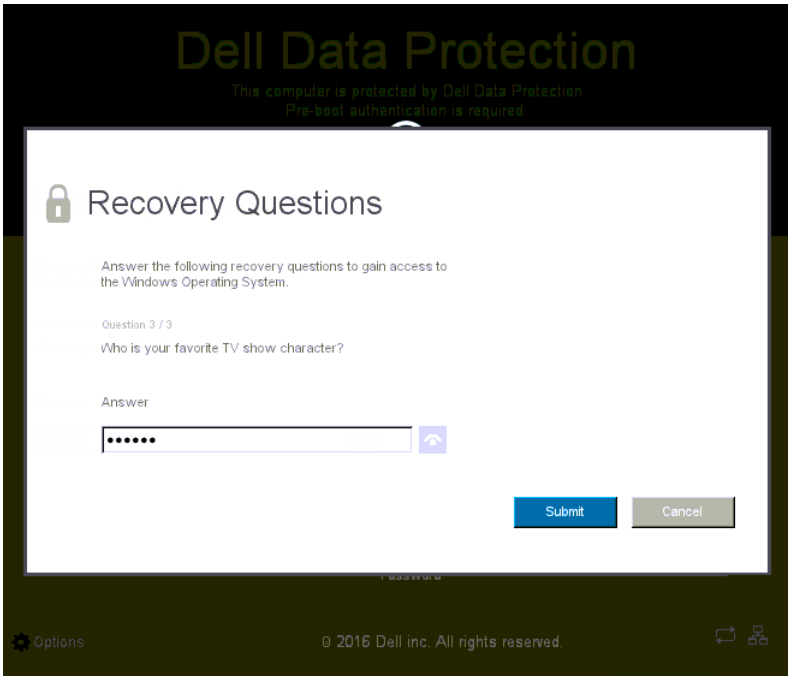
Self-Recovery, PBA Recovery Questions

To answer Recovery Questions to recover access at the Preboot Authentication screen:

1. Enter your user name.
2. At the bottom left side of the screen, click **Options** > **Trouble Signing In**.



3. When the Q&A dialog appears, enter the answers that you supplied when you enrolled in Recovery Questions the first time you signed in.



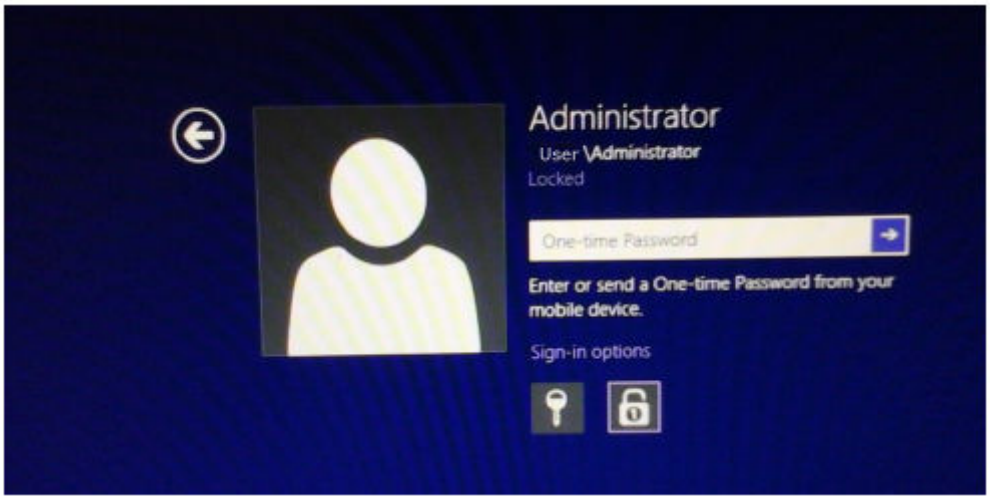
自我復原，一次性密碼

此程序說明如何使用一次性密碼 (OTP) 功能，在 Windows 密碼過期或忘記密碼，或已超過允許的登入嘗試次數上限時，復原存取電腦的權限。一次性密碼 (OTP) 選項唯有在使用者已註冊行動裝置，且 OTP 之前未曾用於登入 Windows 時使用。

註: 一次性密碼功能需要有 TPM，而且必須啟用及擁有。OTP 可用於 Windows 驗證或復原，但上述兩者並非皆同時可用。系統管理員可設定原則允許 OTP 用於復原或驗證，或可停用此功能。

使用 OTP 復原存取電腦的功能：

1. 在 Windows 登入畫面，選取 OTP 圖示 。



2. 在行動裝置上，開啟 Security Tools Mobile 應用程式，然後輸入密碼。
3. 選取要存取的電腦。

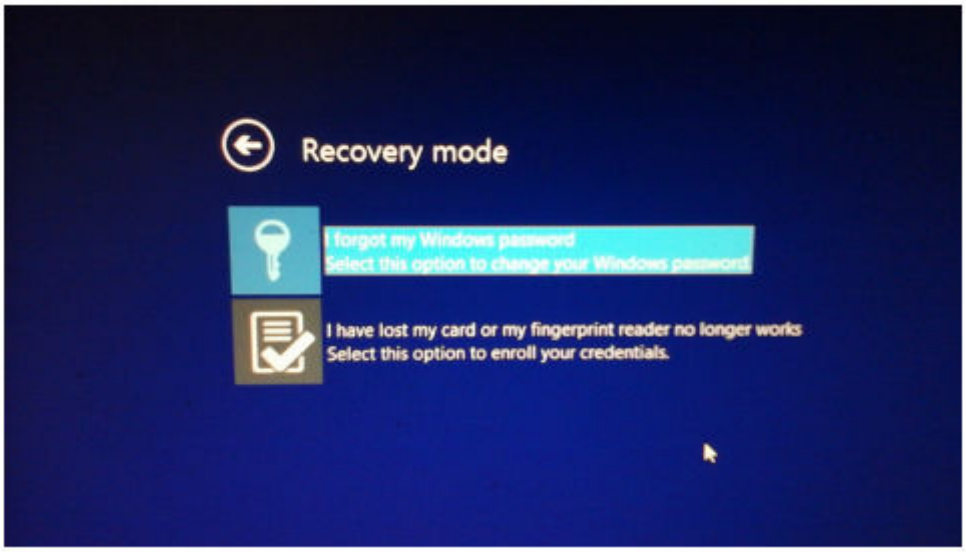
   若行動裝置未顯示電腦名稱，可能有其中一種情況：

   - 行動裝置尚未在您目前嘗試存取的電腦上註冊或與之配對。
   - 若您擁有多個 Windows 使用者帳戶，則可能表示您目前所存取的電腦並未安裝 DDP | Security Tools，或者您並未使用用於配對電腦與行動裝置的使用者帳戶登入。
4. 輕按 **One-time Password** (一次性密碼)。

密碼在行動裝置上顯示。

註: 必要時按一下重新整理符號 ，取得新密碼。OTP 前兩次重新整理後，會延遲 30 秒才產生另一個 OTP。電腦與行動裝置必須同步，以便於同時辨識相同的密碼。如果不斷迅速產生密碼，將造成電腦與行動裝置不同步，且 OTP 功能也會無效。如果發生此問題，請等候 30 秒讓這兩台裝置重新同步，然後再試一次。

5. 在電腦的 Windows 登入畫面上，輸入在行動裝置上顯示的密碼，然後按下 **Enter**。
6. 在電腦的復原模式畫面上，選取 **I forgot my Windows password** (我忘記我的 Windows 密碼)，然後依照螢幕上的指示重設密碼。



7

詞彙表

取消提供 - 取消提供會移除 PBA 資料庫並停用 PBA。解除佈建需要關機才能生效。

一次性密碼 (OTP) - 一次性密碼只能使用一次，效期有限。OTP 需要有 TPM，而且必須啟用及擁有。透過 Security Console (安全性主控台) 和 Security Tools Mobile 應用程式，讓行動裝置與電腦配對，即可啟用 OTP。Security Tools Mobile 應用程式會在行動裝置上產生密碼，以便使用者於電腦的 Windows 登入畫面登入。根據原則，若密碼過期或忘記密碼，且使用者尚未使用過 OTP 登入電腦，則 OTP 功能可用於恢復存取電腦。OTP 功能可用於驗證或復原，但無法同時適用於兩者。OTP 所產生的密碼僅限使用一次，並將於短時間內過期，因此安全性高於其他若干驗證法。

開機前驗證 (PBA) - 開機前驗證是 BIOS 或開機韌體的延伸，此受信任的驗證層可確保作業系統以外的環境安全防竄改。確認使用者認證正確無誤前，PBA 會防止硬碟讀取作業系統等環境。

單一登入 (SSO) - 在開機前和 Windows 登入同時啟用多重因素驗證的情況下，SSO 會簡化登入程序。如果啟用，則僅需在開機前驗證，就會將使用者自動登入至 Windows。如未啟用，則可能需要驗證數次。

信賴平台模組 (TPM) - TPM 為具有三大主要功能的安全性晶片：安全儲存、測量及證明。加密用戶端使用 TPM 是因為其安全儲存功能。TPM 亦可為軟體保存庫提供加密容器。若要搭配使用一次性密碼功能，也必須使用 TPM。