Dell Data Protection | Security Tools

安装指南

1.9 版

2016-01

目錄

1

簡介

Dell Data Protection | Security Tools (DDP|ST) 爲 Dell 電腦管理員與使用者提供安全和身分保護。DDP|ST 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*重新安裝* DDP|ST，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|ST 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|ST 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 Security Console 的 Administrator Settings 工具設定 Security Tools 功能，例如：啓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，在安裝與啓動之後，立即開始使用 Security Tools。

DDP Security Console

根據系統管理員設定的原則，使用者可透過使用 DDP Security Console 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爲準。
- 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 工具可爲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 工具啓用加密與 開機前驗證 (PBA)，以及設定 PBA 原則並自訂 PBA 畫面文字。

繼續至 要求條件。

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|ST，而且符合下列最低要求。若您需要重新安裝 DDP|ST，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，因爲 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 安裝在設定爲磁碟機 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|ST 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|ST 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 可信賴平台模組 (TPM) 。
- SED 不需要 TPM 來提供進階認證或加密。
- 使用 DDP|Hardware Crypto Accelerator 時，PBA 支援**筆記型電腦內建的 Intel RAID**。含自行加密磁碟機的系統不支援 RAID。請參閱 驅動程式 以獲得詳細資訊。

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。

重要事項： 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 4.0 （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 4.0。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 4.0，請造訪 http://www.microsoft.com/en-us/download/details.aspx?id=17851。

  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)

軟體

Windows 作業系統

下表詳細說明支援的軟體。

Windows 作業系統 (32 和 64 位元)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional
註： Windows 7 支援傳統開機模式。Windows 7 不支援 UEFI。
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 （消費者）
註： 搭配 Opal 相容 SED 與 Dell 電腦型號 - UEFI 支援 使用時，Windows 8 支援 UEFI 模式。
• Microsoft Windows 8.1 - 8.1 Update 1 - Enterprise Edition - Pro Edition
註： 搭配 Opal 相容 SED 與 Dell 電腦型號 - UEFI 支援 使用時，Windows 8.1 支援 UEFI 模式。

Windows 作業系統 (32 和 64 位元)
• Microsoft Windows 10 - Education 版 - Enterprise 版 - Pro 版

註： 搭配 Opal 相容 SED 與 Dell 電腦型號 - UEFI 支援 使用時，Windows 10 支援 UEFI 模式。

行動裝置作業系統

下列行動作業系統支援 Security Tools 一次性密碼功能。

Android 作業系統
• 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 作業系統
• iOS 7.x
• iOS 8.x
Windows Phone 作業系統
• Windows Phone 8.1
• Windows 10 Mobile

硬體

驗證

下表詳細說明支援的驗證硬體。

指紋讀取器
• 安全模式的 Validity VFS495
• Broadcom Control Vault 掃動式讀取器
• UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
• Authentec Eikon 與 Eikon To Go USB 讀取器

註： 使用外接式指紋讀取器時，您必須下載及安裝特定讀取器所需的最新驅動程式。

非接觸式卡
• 非接觸式卡使用指定之 Dell 筆記型電腦內建的非接觸式卡讀取器
智慧卡
• PKCS #11 智慧卡使用 ActivIdentity 用戶端

註： ActivIdentity 用戶端未預先載入，必須另行安裝。

• 通用存取卡 (CAC)

註： 使用者在開機時，以多重憑證的 CAC，從清單選取正確的憑證。

• CSP 卡片
• Class B/SIPR Net 卡

下表詳細說明支援 SIPR Net 卡的 Dell 電腦型號。

Dell 電腦型號 - Class B/SIPR 網路卡支援
• Latitude E6440
• Latitude E6540
• Precision M2800
• Precision M4800
• Precision M6800
• Latitude 14 Rugged Extreme
• Latitude 12 Rugged Extreme
• Latitude 14 Rugged

Dell 電腦型號 - UEFI 支援

在若干執行 Microsoft Windows 8、Microsoft Windows 8.1 與 Microsoft Windows 10 且有 Opal 相容 SED 的 Dell 電腦支援以 UEFI 模式進行驗證功能。其他執行 Microsoft Windows 7、Microsoft Windows 8、Microsoft Windows 8.1 及 Microsoft Windows 10 的電腦支援傳統開機模式。

下表詳細說明支援 UEFI 的 Dell 電腦。

Dell 電腦型號 - UEFI 支援
• Latitude E7240
• Latitude E7250
• Latitude E7350
• Latitude E7440
• Latitude E7450
• Precision M4800
• Precision M6800
• Precision T7810
• OptiPlex 7020
• OptiPlex 9020 Micro
• Venue Pro 11 (型號 7139)

註： 在支援的 UEFI 電腦上，從主功能表選取**重新啟動**後，電腦會重新啟動，然後顯示兩個可能的登入畫面之一。出現的登入畫面取決於電腦平台架構的差異。有些型號會顯示 PBA 登入畫面；有些型號則顯示 Windows 登入畫面。兩個登入畫面一樣安全。

註： 請確認 Enable Legacy Option ROMs （啓用傳統選項 ROMs）設定於 BIOS 中是停用的。

如欲停用傳統選項 ROMs：

1. 將電腦重新開機。
2. 在電腦重新開機時，重複按下 **F12** 鍵以叫出 UEFI 電腦的開機設定。
3. 按下向下箭號，, 反白 **BIOS 設定**選項，然後按下 **Enter**（輸入鍵）。
4. 選擇 **Settings**（設定）**> General**（一般）**> Advanced Boot Options**（進階開機選項）。
5. 清除 **Enable Legacy Option ROMs**（啓用傳統選項 ROMs）核取方塊上的勾選，然後按一下 **Apply**（套用）。

Opal 相容 SED

雖然支援有「X」的磁碟機，但這些磁碟機不符合 Dell 系統資格，Dell 系統出廠時也沒有預先安裝。

硬碟機	供貨狀況	標準
Seagate ST320LT009 (FIPS Julius 320GB)	✓	Opal 1
Seagate ST320LT014 (Julius 320GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000GB)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D non-FIPS 500GB)	✓	Opal 2/eDrive
Seagate ST500LT015 (Yarra 1D FIPS 500GB)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS 500GB)	✓	Opal 2/eDrive
Seagate ST1000LM028 (Kahuna V FIPS 1000GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS 500GB)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5 inch 1000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5 inch 2000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5 inch 3000GB)	X	Opal 2/eDrive
Travelstar 5K750 系列	X	Opal 1
Travelstar 7K750 系列	X	Opal 1
Travelstar Z5K320 系列	X	Opal 1
Toshiba MKxx61GSYD 系列	X	Opal 1
Toshiba MKxx61GSYG 系列	X	Opal 1
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
Samsung SM841 OPAL SSD	✓	Opal 2
Samsung SM841N OPAL SSD	✓	Opal 2
Samsung SM850 PRO 2.5 英吋 MZ-7KE128 – MZ-7KE2T0 (2.5 英吋 SED SSD 128GB 至 2000GB)	X	Opal 2/eDrive
Samsung SM850 PRO 2.5 英吋 MZ-75E120 – MZ-75E2T0 (2.5 英吋 SED SSD 120GB 至 2000GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 – MZ-M5E1T0 (mSATA SED SSD 120GB 至 1000GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2 MZ-N5E120 – MZ-N5E500 (M.2.SED SSD 120GB 至 500GB)	X	Opal 2/eDrive
Samsung PM851 OPAL SSD – 2.5 英吋 (2.5 英吋 128GB - 512GB)	✓	Opal 2/eDrive
Samsung PM851 OPAL SSD – mSATA (mSATA 128GB - 512GB)	✓	Opal 2/eDrive

硬碟機	供貨狀況	標準
Samsung PM851 OPAL SSD - M.2. (M.2.128GB - 512GB)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD - 2.5 英吋 (2.5 英吋 256GB - 512GB)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD - mSATA (mSATA 256GB - 512GB)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD - M.2. (M.2.256GB - 512GB)	✓	Opal 2/eDrive
SanDisk X300s	X	Opal 2
LiteOn L9M OPAL SSD	✓	Opal 2
LiteOn M3 series SSD	✓	Opal 1
LiteOn M6 series SSD	✓	Opal 2
LiteOn V2M series SSD	✓	Opal 2
Crucial RealSSD C400 SSD	X	Opal 1
Micron RealSSD C400 SSD	X	Opal 1
Micron M500 SSD 2.5 英吋 (120GB - 960GB)	X	Opal 2/eDrive
Micron M500 SSD mSATA (120GB - 480GB)	X	Opal 2/eDrive

語言支援

DDP|ST 與多語系使用者介面 (MUI) 相容，支援下列語言。

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

驗證選項

下列驗證選項需要特定硬體：指紋、智慧卡、非接觸式卡、Class B/SIPR 網路卡 與 UEFI 電腦上驗證。

一次性密碼功能需要有 TPM，而且必須啓用及擁有。如需更多資訊，請參閱 清除所有權及啓動 TPM。

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
Windows 10	X[1]					X	X	X	X	X

1. 有支援的 Opal SED 時可用。

UEFI

	PBA - 開啓 支援的 Dell 電腦					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，可以只解除安裝 DDP|A，然後重新啓動安裝程序。

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. 啓動 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 隨即啓動電腦，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. 啓動 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）啓動安裝程式。
3. 解除安裝完成後，按一下 **Yes** （是）重新啓動。

註： 移除 DDP|A 也將解鎖 SED 並移除開機前驗證。

初始化 TPM

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

清除所有權及啓動 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。

繼續進行 安裝與啓動。

3

安裝與啓動

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

最佳作法： 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|ST

安裝 Security Tools：

1. 在 DDP|ST 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，啓動安裝程式。
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。在 Select Feature （選取功能）頁面選取 **Next** （下一步）。
7. 按一下 **Install** （安裝）開始安裝。
8. 安裝完成時，需要重新啓動電腦。選取 **Yes** （是）重新啓動，然後按一下 **Finish** （完成）。

   安裝隨即完成。

啓動 DDP|ST

首次執行 DDP Security Console 並選取 Administrator Settings 時，啓動精靈會引導您進行啓動程序。

如果尚未啓動 DDP Security Console，一般使用者仍可執行此 Console。在系統管理員啓動 DDP|ST 並自訂設定前，如果使用者爲第一個使用 DDP Security Console 的人，預設值將被使用。

啓動 Security Tools：

1. 以系統管理員身分從桌面捷徑啓動 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 提高權限才可啓動。一般使用者必須先輸入系統管理員認證，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**。
4. 建立 DDP|ST 密碼，並按一下 **Next**（下一步）。

   您必須在設定 Security Tools 之前，建立 DDP|ST 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|ST 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 啓動完成。

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

系統管理員的設定工作

Security Tools 預設設定可讓系統管理員及使用者在啓動後立即使用 Security Tools ，無須其他設定。使用者在以其 Windows 密碼登入電腦時，自動會被新增爲 Security Tools 使用者，但預設設定爲不啓用多重因素 Windows 驗證。加密與開機前認證的預設設定爲停用。

若要設定 Security Tools 功能，您必須是電腦上的系統管理員。

變更系統管理員密碼與備份位置

Security Tools 啓動後，必要時可變更系統管理員密碼與備份位置。

1. 以系統管理員身分從桌面捷徑啓動 Security Tools。
2. 按一下 **Administrator Settings** （系統管理員設定）圖標。
3. 在 Authentication (驗證) 對話方塊中，輸入原先在啓動期間設定的系統管理員密碼，然後按一下 **OK** (確定)。
4. 按一下 **Administrator Settings** (系統管理員設定) 標籤。
5. 如要變更密碼，請在 Change Administrator Password (變更系統管理員密碼) 頁面輸入 8 至 32 個字元的新密碼，其中至少需包含一個英文字母、一個數字以及一個特殊字元。
6. 再次輸入密碼以確認，然後按一下 **Apply** (套用)。
7. 若要變更復原金鑰的儲存位置，請在左窗格中選取 **Change Backup Location** (變更備份位置)。
8. 選取新的備份位置，按一下 **Apply** (套用)。

   備份檔案必須儲存在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 ProSupport 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|ST 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。

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。啓用加密或 PBA 時，另一選項亦會啓用。

啓用加密與 PBA 前，Dell 建議註冊並將 Recovery Questions (復原問題) 作爲 Recovery Option (復原選項) 使用，以在密碼遺失時復原密碼。請參閱 設定登入選項 以獲得詳細資訊。

設定加密與開機前驗證：

1. 在 DDP Security Console 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： 如果在啓用加密時顯示「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，即可繼續啓用加密的程序。

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。
啓用 Crypto Erase Password (密碼編譯清除密碼) 功能	選取可啓用。
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，作爲故障防護安全性機制。在 PBA 驗證期間，於使用者名稱或密碼欄位中輸入此文字或代碼，會**永久抹除此裝置**。若未在此欄位輸入文字，會導致在緊急情況下無法使用密碼編譯清除密碼。

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：「By clicking OK, you agree to abide by the acceptable computer use policy. (按一下確定後，您即同意遵循電腦使用原則。)」若未在此欄位輸入文字，就不會顯示文字或 「OK/Cancel」 (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，請重新啓動電腦。

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

先啓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，例如爲了解除安裝 - 按一下 **Decrypt** (解密)。

先啓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)。

  如需解除安裝的指示，請參閱 解除安裝工作。

設定驗證選項

Administrator Settings Authentication (系統管理員設定驗證) 標籤上的控制項可讓您設定使用者登入選項，並自訂各選項的設定。

註： 如果 TPM 不存在，也沒有擁有及啓用，One-time Password (一次性密碼) 選項不會在 Recovery Options (復原選項) 下方顯示。

設定登入選項

在 Sign-in Options (登入選項) 頁面，您可設定登入原則。所有支援的認證預設列於 Available Options (可用選項)。

設定登入選項：

1. 在左窗格的 Authentication (驗證) 下，選取 **Sign-in Options** (登入選項)。
2. 若要選擇您要設定的角色，請選取在 **Apply sign-in options to** (套用登入選項至) 清單中的角色：**Users** (使用者) 或 **Administrators** (系統管理員)。您在此頁面中所做的任何變更只會套用至選取的角色。
3. 設定驗證的 Available Options (適用選項)。

   依預設，每一種驗證法皆設定爲個別使用，無法結合其他驗證法使用。您可以透過以下方式變更預設值：

   - 若要設定驗證選項組合，請在 Available Options (可用選項) 下，按一下 選取第一種驗證方法。在 Available Options (可用選項) 對話方塊中，選取第二個驗證方法，然後按一下 **OK** (確定)。

     例如，您可規定將指紋與密碼作爲登入認證使用。在對話方塊中，選取必須搭配指紋驗證使用的第二種驗證法。
   - 若要個別使用每種驗證方法，在 Available Options Available Options (可用選項) 對話方塊中，將第二種驗證方法設爲 **None** (無) ，然後按一下 **OK** (確定)。
   - 若要移除登入選項，請在 Sign-in Options (登入選項) 頁面上的 Available Options (可用選項) 下方，按一下 **X** 移除該方法。
   - 若要新增新的驗證方法組合，請按一下 **Add an Option** (新增選項)。
4. 設定使用者的 Recovery Options (復原選項)，以在使用者被鎖定時，復原存取電腦的權限。
   - 若要讓使用者定義用於取回存取電腦權限的一組問題與答案，請選取 **Recovery Questions** (復原問題)。

     若要避免使用 Recovery Questions (復原問題)，請取消選取此選項。
   - 若要允許使用者使用行動裝置復原存取權限，請選取 **One-time Password** (一次性密碼)。選取一次性密碼 (OTP) 作爲復原方式時，此密碼無法作爲 Windows 登入畫面的登入選項。

     若要使用 OTP 功能登入，請取消選取 Recovery Options (復原選項) 中的選項。取消以 OTP 作爲復原方式後，只要至少有一名使用者以 OTP 註冊，Windows 登入頁面上便會顯示 OTP 選項。

註： 身為系統管理員，您可控制一次性密哪的使用方式 - 用於驗證或復原。OTP 功能可用於驗證或復原，但上述兩者並非皆同時可用。設定會根據 Sign-in Options (登入選項) 欄位，**Apply sign-in options to** (套用登入選項至) 中的選擇，影響電腦的所有使用者或所有系統管理員。

如果未列出 One-time Password (一次性密碼) 選項，表示您的電腦組態不支援此選項。如需更多資訊，請參閱 要求條件。

- 若規定使用者在遺失或忘記登入認證時必須致電服務台，請取消選取 Recovery Questions (復原問題) 與 One-time Password (一次型密碼)。

5 若要設定一段時間讓使用者註冊其驗證認證，請選取 **Grace Period**（寬限期）。

寬限期功能可讓您設定開始強制執行所設定之 Sign-in Option（登入選項）的日期。您可在強制執行日期之前設定 Sign-in Option（登入選項），並設定允許使用者註冊的一段時間。系統預設爲立即執行此原則。

若要從 ***Immediately***（立即）變更 Enforce Sign-in Option（強制執行登入選項）日期，請在 Grace Period（寬限期）對話方塊中按一下下拉式功能表，然後選取 **Specified Date**（指定的日期）。按一下日期欄位右方的向下箭號，以顯示日曆，然後選取日曆上的日期。原則會在所選取之日期的上午 12:01 左右開始實施。

系統會提醒使用者在下次登入 Windows 時（依預設）註冊指定的認證，您也可以設定一般提醒通知。從 ***Remind User***（提醒使用者）下拉式清單選取提醒間隔。

註： 向使用者顯示的提醒會稍有差異，取決於觸發提醒時使用者是在 Windows 登入畫面，或是在 Windows 工作階段中而定。不會在開機前驗證登入畫面上出現提醒。

寬限期內的功能

在指定的寬限期內，每次登入後，如果使用者尚未註冊符合變更之 Sign-in Option（登入選項）所需的最低認證，就會顯示 Additional Credentials（其他認證）通知。訊息內容：***Additional credentials are available for enrollment.***（其他認證可供註冊）

如果有其他可用但非必要的認證，則訊息只會在變更原則後顯示一次。

按一下通知會產生下列結果，取決於整體情況而定：

- 如果尚未註冊任何認證，便會顯示安裝精靈，讓系統管理員使用者設定電腦相關設定，並讓使用者能註冊最常見的認證。
- 進行初始認證註冊後，按一下通知即會在 DDP Security Console 顯示安裝精靈。

寬限期過期後的功能

在所有情況下，寬限期過期後，若使用者沒有註冊 Sign-in Option（登入選項）要求的認證，將無法登入。如果使用者嘗試用不符合 Sign-in Option（登入選項）的認證或認證組合登入，即會在 Windows 登入畫面頂端顯示安裝精靈。

- 如果使用者成功註冊要求的認證，就會登入 Windows。
- 如果使用者未成功註冊要求的認證，或是取消精靈，就會返回 Windows 登入畫面。

6 若要儲存選取角色的設定，請按一下 **Apply**（套用）。

設定密碼管理員驗證

在 Password Manager（密碼管理員）頁面上，您可設定使用者如何以 Password Manager（密碼管理員）驗證身分。

設定 Password Manager（密碼管理員）驗證：

1 在左窗格的 Authentication（驗證）下，選取 **Password Manager**（密碼管理員）。

2 若要選擇您要設定的角色，請選取在 **Apply sign-in options to**（套用登入選項至）清單中的角色：**Users**（使用者）或 **Administrators**（系統管理員）。您在此頁面中所做的任何變更只會套用至選取的角色。

3 或者，選取 **Do not require authentication**（不需要驗證）核取方塊，讓所選取的使用者角色可以用儲存於 Password Manager（密碼管理員）中的認證，自動登入所有軟體應用程式與網際網路網站。

4 設定驗證的 Available Options（適用選項）。

依預設，每一種驗證法皆設定爲個別使用，無法結合其他驗證法使用。您可以透過以下方式變更預設值：

- 若要設定驗證選項組合，請在 Available Options（可用選項）下，按一下 選取第一種驗證方法。在 Available Options（可用選項）對話方塊中，選取第二個驗證方法，然後按一下 **OK**（確定）。

  例如，您可規定將指紋與密碼作爲登入認證使用。在對話方塊中，選取必須搭配指紋驗證使用的第二種驗證法。

- 若要個別使用每種驗證方法，在 Available Options Available Options (可用選項) 對話方塊中，將第二種驗證方法設爲 **None** (無) ，然後按一下 **OK** (確定)。
- 若要移除登入選項，請在 Sign-in Options (登入選項) 頁面上的 Available Options (可用選項) 下方，按一下 **X** 移除該方法。
- 若要新增新的驗證方法組合，請按一下 **Add an Option** (新增選項)。

5 若要儲存選取角色的設定，請按一下 **Apply** (套用)。

註： 選取 Defaults (預設) 按鈕，將設定還原成其原始數值。

設定復原問題

在 Recovery Questions (復原問題) 頁面上，您可選取在定義個人復原問題與答案時，將向使用者提出那些問題。Recovery Questions (復原問題) 可讓使用者在密碼到期或忘記密碼時，復原存取電腦的權限。

設定復原問題：

1 在左窗格的 Authentication (驗證) 下，選取 **Recovery Questions** (復原問題)。

2 在 Recovery Questions (復原問題) 頁面上，選取至少三個預先定義的復原問題。

3 或者，您最多可新增三個自訂問題至使用者選取的清單。

4 若要儲存復原問題，按一下 **Apply** (套用)。

設定指紋掃描驗證

設定指紋掃描驗證：

1 在左窗格的 Authentication (驗證) 下，選取 **Fingerprints** (指紋)。

2 在 Enrollments (註冊) 中，設定使用者可註冊的指紋數目上限與下限。

3 設定指紋掃描的敏感度。

降低敏感度會使可接受的變異與接受誤掃描的機率提高。使用最高設定時，系統可能會拒絕合法的指紋。敏感度設定越高，會將誤接受率降低至每 10,000 次掃描僅 1 次誤接受。

4 若要從指紋掃描器的緩衝區移除所有指紋掃描與認證註冊，請按一下 **Clear Reader** (清除掃描器)。此僅會移除您正在新增的資料。不會刪除上一個工作階段儲存的掃描與註冊資料。

5 若要儲存設定值，請按一下 **Apply** (套用)。

設定一次性密碼驗證

若要使用一次性密碼功能，使用者需使用行動裝置的 Dell Data Protection | Security Tools Mobile 應用程式產生一次性密碼，然後在電腦上輸入該密碼。密碼僅可使用一次，且僅在有限時間內有效。

若要進一步提升安全性，系統管理員可要求 PIN 碼，以確保行動應用程式的安全。

在 Mobile Device (行動裝置) 頁面上，您可進行提高行動裝置與一次性密碼安全性的設定。

設定一次性密碼驗證：

1. 在左窗格的 Authentication (驗證) 下，選取 **Mobile Device** (行動裝置)。
2. 若要求使用者輸入 PIN 碼才能存取行動裝置的 Security Tools Mobile 應用程式，請選取 **Require PIN** (要求輸入 PIN 碼)。

註： 在行動裝置註冊電腦後才啓用 *Require PIN* (要求輸入 PIN 碼) 原則，會導致所有行動裝置都取消註冊。一旦啓用此原則，使用者就必須重新註冊行動裝置。

若選取 **Require PIN** (要求輸入 PIN 碼) 核取方塊，使用者必須先解鎖行動裝置，才能存取 Security Tools Mobile 應用程式。若行動裝置無裝置鎖定功能，則將需要輸入 PIN 碼。

3. 若要選取一次性密碼 (OTP) 的長度，請爲 **One-time Password Length** (一次性密碼長度) 選取所需的密碼字元數。
4. 若要選取使用者正確輸入所需一次性密碼的機會次數，請爲 **User Sign-in Attempts Allowed** (允許使用者的登入嘗試次數) 選取 **5** 至 **30** 的數字。

   嘗試次數達到上限時，在使用者重新註冊行動裝置之前，將停用 OTP 功能。

最佳作法： 除了一次性密碼之外，Dell 建議至少設定另一項驗證方法。

設定智慧卡註冊

DDP|Security Tools 支援兩種智慧卡：接觸式與非接觸式。

接觸式卡需要使用插入卡片的智慧卡讀卡機。接觸式卡片僅相容於網域電腦。CAC 與 SIPRNet 卡皆爲接觸式卡片。由於此類卡片搭載先進功能，使用者插入卡片後，需選擇認證才可登入。

- 非網域電腦與採用網域規格設定的電腦支援非接觸式卡。
- 每個使用者帳戶可註冊一張接觸式智慧卡，或每個帳戶註冊多張非接觸式卡。
- 智慧卡不支援開機前驗證。

註： 從註冊多張卡片的帳戶移除智慧卡註冊時，所有卡片皆會同時取消註冊。

設定智慧卡註冊：

1. 在 Administrator Settings 工具的 Authentication (驗證) 標籤上，選取 **Smartcard** (智慧卡)。

設定進階權限

1 按一下 **Advanced** (進階) 修改進階使用者選項。在 ***Advanced*** (進階) 下，您可以選擇允許使用者自行註冊認證，或是選擇允許使用者自行修改其註冊認證，並啓用單一登入。

2 選取或清除核取方塊：

Allow users to enroll credentials (允許使用者註冊認證)- 預設設定爲選取此核取方塊。允許在沒有管理員介入的情況下，註冊認證。如果清除核取方塊，必須由系統管理員註冊認證。

Allow user to modify enrolled credentials (允許使用者修改註冊的認證) - 預設設定爲選取此核取方塊。選取時，允許使用者在沒有管理員介入的情況下，修改或刪除其註冊的認證。如果清除此核取方塊，一般使用者無法修改或刪除認證，而須由系統管理員修改或刪除認證。

註： 若要註冊使用者的認證，請至 Administrator Settings 工具的 ***Users*** (使用者) 頁面，選取使用者並按一下 **Enroll** (註冊)。

Allow one step logon (允許單一登入)- One-Step Logon 即單一登入 (SSO)。預設設定爲選取此核取方塊。啓用此功能後，使用者只能夠在 Preboot Authentication (開機前驗證) 畫面輸入其認證。使用者會自動登入 Windows。若取消勾選核取方塊，使用者可能需要登入多次。

註： 除非也選取 **Allow users to enroll credentials** (允許使用者註冊認證) 設定，否則無法選取此選項。

3 完成時按一下 **Apply** (套用)。

智慧卡與生物辨識服務 (選用)

如果您不想要 Security Tools 變更將智慧卡與生物辨識裝置關聯至 「自動」啓動類型的服務，可停用此服務。

停用時，Security Tools 將不會嘗試啓動這三項服務：

- SCardSvr - 管理電腦讀取智慧卡的權限。如果已停止這項服務，這台電腦就無法讀取智慧卡。如果這項服務已停用，凡是明確仰賴它的服務都無法啓動。
- SCPolicySvc - 讓系統可以設定成在取出智慧卡時鎖定使用者桌面。
- WbioSrvc - Windows 生物辨識服務讓用戶端應用程式能擷取、比較、操控與儲存生物辨識資料，無須直接存取任何生物辨識硬體或樣本。這項服務由特許的 SVCHOST 程序代管。

停用此功能亦會隱藏與未執行之所需服務關聯的警告。

停用自動服務啓動

如果登錄機碼不存在或數值設爲 0，預設設定爲啓用此功能。

1 執行 **Regedit**。

2 找出以下登錄項目：

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

設爲 0 可啓用。
設爲 1 可停用。

管理使用者的驗證

Administrator Settings Authentication (系統管理員設定驗證) 標籤可讓您設定使用者登入選項，並自訂各選項的設定。

管理使用者驗證：

1. 以系統管理員身分 , 按一下 **Administrator Settings** (系統管理員設定) 動態磚。
2. 按一下 **Users** (使用者) 標籤管理使用者與檢視使用者註冊狀態。從此標籤您可以：
   - 註冊新使用者
   - 新增或變更認證
   - 移除使用者的認證

註： **Sign-in** (登入) 與 **Session** (工作階段) 顯示使用者的註冊狀態。

Sign-in (登入) 狀態為 **OK** (正常) 時，表示已完成使用者必須能夠登入的所有註冊。
Session (工作階段) 狀態為 **OK** (正常) 時，表示已完成使用者必須使用 Password Manager (密碼管理員) 的所有註冊。

若任一狀態為 **No** (不正常)，使用者必須完成其他註冊。若要找出仍需進行的註冊，請選取 **Administrator Settings** (系統管理員設定) 工具並開啓 **Users** (使用者) 標籤。灰色核取記號方塊表示尚未完成的註冊。或者按一下 **Enrollments** (註冊) 動態磚，並檢閱其中列出所需註冊的 **Status** 標籤的 **Policy** (政策) 欄。

新增新使用者

註： 新 Windows 使用者登入 Windows 或註冊認證時，便會自動新增該名使用者。

1. 按一下 **Add User** (新增使用者)，開始現有 Windows 使用者的註冊程序。
2. ***Select User*** (選取使用者) 對話方塊顯示時，請選取 **Object Types** (物件類型)。
3. 在文字方塊中輸入使用者的物件名稱，然後按一下 **Check Names** (檢查名稱)。
4. 完成時按一下 **OK** (確定)。

   開啓註冊精靈。

   繼續進行 註冊或變更使用者認證，以獲得相關指示。

註冊或變更使用者認證

系統管理員可代表使用者註冊或變更使用者的認證，但有些註冊活動仍需使用者在場，例如回答復原問題與掃描使用者的指紋。

註冊或變更使用者認證：

1. 在 Administrator Settings (系統管理員設定) 中，按一下 **Users** (使用者) 標籤。
2. 在 Users (使用者) 頁面上，按一下 **Enroll** (註冊)。
3. 在 Welcome (歡迎) 頁面，按一下 **Next** (下一步)。
4. 在 Authentication Required (所需驗證) 對話方塊中，以使用者的 Windows 密碼登入，然後按一下 **OK** (確定)。
5. 在 Password (密碼) 頁面，若要變更使用者的 Windows 密碼，請輸入並確認新密碼，然後按一下 **Next** (下一步)。

   若要略過密碼變更的步驟，請按一下 **Skip** (略過)。如果您不想要註冊認證，精靈可讓您略過認證。若要回到頁面，請按一下 **Back** (返回)。
6. 請遵循每一頁的指示，然後按一下合適的按鈕：**Next** (下一步)、**Skip** (略過) 或 **Back** (返回)。

7 在 Summary (摘要) 頁面上，確認已註冊的認證，並在完成註冊後，按一下 Apply (套用)。

若要返回認證註冊頁面進行更改，按一下 Back (返回) 直到回到欲更改資料的頁面爲止。

如需註冊認證或變更認證的詳細資訊，請參閱 *Dell Data Protection | Console User Guide* （Dell 資料保護丨主控台使用者指南）。

移除一個已註冊的認證

1 按一下 Administrator Settings （系統管理員設定）圖標。

2 按一下 Users (使用者) 標籤，然後找出要變更的使用者。

3 將滑鼠暫留在您要移除之認證的綠色核取記號上。該核取記號即變成 ⊗。

4 按一下 ⊗ 符號，然後按一下 Yes (是) 確認刪除。

註： 如果此為使用者唯一註冊的認證，便無法透過此方式移除認證。此外，亦無法透過此方法移除密碼。請使用 Remove (移除) 命令徹底移除使用者對該部電腦的存取權限。

移除使用者註冊的所有認證

1 按一下 Administrator Settings （系統管理員設定）圖標。

2 按一下 Users (使用者) 標籤，然後找出想要移除的使用者。

3 按一下 Remove (移除)。(Remove (移除) 命令會以紅色顯示在使用者設定的底部)。

移除後，除非重新註冊，否則該名使用者將無法登入電腦。

5

解除安裝工作

若要解除安裝 DDP|ST，您必須至少是**本機系統管理員**使用者。

解除安裝 DDP|ST

您必須依此順序解除安裝應用程式：

1.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. 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**，然後重新啓動電腦。
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，請重新啓動電腦。
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，我想要重新啓動電腦），然後按一下 **Finish**（完成）。
7. 電腦重新啓動，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：

- **一次性密碼 (OTP)：**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 功能作爲復原之用，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，而且必須啓用及擁有。請遵循 清除所有權及啓動 TPM 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。請參閱 設定登入選項 以獲得詳細資訊。

- **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啓用 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。

自我復原，Windows 登入復原問題

回答復原問題，以復原在 Windows 登入畫面的存取權限：

1. 若要使用復原問題，請按一下 **Can't access your account?** (無法存取您的帳戶嗎？)
   您在註冊顯示時選取的復原問題。
2. 輸入答案，然後按一下 **OK** (確定)。
   成功輸入問題答案後，便進入 Access Recovery (存取復原) 模式。接下來會發生的情況取決於失效的認證。
   - 如果未能輸入正確的 Windows 密碼，則會顯示 Change Password (變更密碼) 畫面。
   - 如果未能辨識指紋，則會顯示指紋註冊頁面，以便重新註冊指紋。

自我復原，PBA 復原問題

回答復原問題，以復原在開機前驗證畫面的存取權限：

1. 在開機前驗證畫面，輸入您的使用者名稱。
2. 在畫面左下方，選取 **Options** (選項)。
3. 在 Options (選單) 功能表，選取 **Forgot Password** (忘記密碼)。
4. 回答復原問題並按一下 **Sign In** (登入)。

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，而且必須啓用及擁有。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，開啓 Security Tools Mobile 應用程式，然後輸入 PIN。
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。

詞彙表

一次性密碼 (OTP) －一次性密碼爲僅可使用一次，且在有限時間內有效的密碼。OTP 需要有 TPM，而且必須啓用及擁有。透過 DDP Security Console (安全性主控台) 和 Security Tools Mobile 應用程式，使行動裝置與電腦配對，即可啓用 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。OTPsecurity 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。

信賴平台模組 (TPM) － TPM 爲具有三大主要功能的安全性晶片：安全儲存、測量及證明。DDP|E 因其安全儲存功能，而使用 TPM。TPM 亦可爲 DDP|E 軟體保存庫提供加密的容器，並保護 DDP|E HCA 加密金鑰。Dell 建議佈建 TPM。TPM 爲搭配 DDP|E HCA 與一次性密碼功能使用所需。

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

單一登入 (SSO) －開機前驗證與 Windows 登入啓用多因素驗證功能時，SSO 則可簡化登入流程。如果啓用，則僅需在開機前驗證，就會將使用者自動登入至 Windows。如未啓用，則可能需要驗證數次。

開機前驗證 (PBA) - 開機前驗證 (PBA) 是 BIOS 或開機韌體的延伸，這個受信任的驗證層保證是作業系統外的安全防竄改環境。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。


0XXXXXA0X