Dell Data Protection

主控台使用者指南

加密狀態
驗證註冊
密碼管理員

目錄

1

簡介

Dell Data Protection | Security Tools 提供您簡單易用的工具以提高電腦的安全性。

下列功能可透過 的 DDP 主控台取得：

- 註冊使用 DDP|E 所需的認證
- 充分利用多面向認證方式，包括密碼、指紋與智慧卡。
- 如果忘記密碼，無需致電服務台或請求系統管理員的協助，即可恢復存取您的電腦
- 備份及還原您的程式資料
- 輕鬆變更您的 Windows 密碼
- 設定個人偏好
- 檢視加密狀態 (在使用自行加密磁碟機的電腦上)

DDP Security Console

DDP Security Console 這個介面可讓您註冊、管理認證及設定自我復原問題。

您可以存取這些應用程式：

- Encryption Status 工具可讓您檢視電腦磁碟機的加密狀態。
- Enrollments 工具可讓您設定並管理認證、設定自我復原問題，以及檢視其認證註冊狀態。系統管理員會設定您註冊各類型認證的能力。
- Password Manager 可讓您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 可讓您從應用程式變更登入密碼，確保 Password Manager 維護的登入密碼與目標資源的內容同步。

本指南說明如何使用這幾個應用程式。

務必定期查看 www.dell.com/support ，瞭解是否有更新的文件。

2

要求條件

- DDP|Security Tools (包含 DDP 安全性主控台) 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。也可以 DDP | Enterprise 版與 DDP | Personal 版的部分方式安裝它且總是以 DDP | Endpoint Security Suite 一同安裝。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。

DDP 主控台最低需求如下：

- 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 TPM。
- 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。

用戶端必備項目

- Security Tools 一次性密碼 (OTP) 功能需要有信賴平台模組 (TPM) 的存在、啓用與擁有。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。
- SED 不需要 TPM 來提供進階認證或加密。

註： 執行 HCA 原則後，絕對不要清除 TPM 或 DDP|HCA 的所有權。執行原則後如果略過 BIOS 警告並清除 TPM 或 HCA，會失去加密硬碟機的存取權限，必須完成復原程序才能重新取得存取權限。

- 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。

硬體

最低硬體需求需符合作業系統的最低規格。

下表詳細說明支援的 Dell 硬體。指紋讀取器與智慧卡的驅動程式位於用戶端安裝套件。其他硬體廠商可能需要自己的驅動程式。

指紋與智慧卡讀卡機
• 安全模式的 Validity VFS495
• Broadcom ControlVault Swipe Reader
• 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 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。
• CSP 卡片
• 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。
• Class B/SIPR 網卡

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

Dell 電腦型號 - UEFI 支援
• 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**重新啓動**後，電腦會重新啓動，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。

Opal 相容 SED

雖然 SED 管理支援有 「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)	✓	Opal 1
Seagate ST500LT015 (Yarra 1D FIPS 500)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D non-FIPS 500)	X	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS)	✓	Opal 2
Travelstar 5K750 系列	X	Opal
Travelstar 7K750 系列	X	Opal
Travelstar Z5K320 系列	X	Opal
MKxx61GSYD 系列	X	
MKxx61GSYG 系列	X	
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
Samsung SM841 OPAL SSD	✓	Opal 2
Samsung SM841N OPAL SSD	✓	Opal 2
Samsung PM851 OPAL SSD	✓	Opal 2
Samsung PM871 256GB M.2 2280 SED	✓	Opal 2
Samsung PM871 256GB mSATA SED	✓	Opal 2
Samsung PM871 512GB mSATA SED	✓	Opal 2
Samsung PM871 512G M.2 2280 SATA SED	✓	Opal 2
Samsung PM871 512G 7mm SED	✓	Opal 2
SanDisk X300s	X	Opal 2
LiteOn L9M OPAL SSD	✓	Opal 2
LiteOn M3 series SSD	✓	Opal 1

硬碟機	供貨狀況	標準
LiteOn M6 series SSD	✓	Opal 2
LiteOn V2M series SSD	✓	Opal 2
Micron RealSSD C400 SSD	X	Opal 1

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」變更爲 「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」變更爲 「AHCI」時，將會出現藍色畫面。

作業系統

Windows 作業系統

下表詳細說明支援的作業系統。

Windows 作業系統 (32 和 64 位元)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional - Ultimate
• Microsoft Windows 8 - Enterprise - Pro
• Microsoft Windows 8.1 - Windows 8.1 Update 1 - Enterprise - Pro
• Microsoft Windows 10 - Education 版 - Enterprise 版 - Pro 版

下表詳細說明搭配支援的 Opal 相容 SED 與 Dell 電腦型號 - UEFI 支援 使用時，UEFI 模式支援的作業系統。

UEFI 模式 (32 與 64 位元) 支援的 Windows 作業系統
• Microsoft Windows 8 - Enterprise - Pro

• Microsoft Windows 8.1 - Windows 8.1 Update 1 - Enterprise 版 - Pro 版
• Microsoft Windows 10 - Education 版 - Enterprise 版 - Pro 版

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

語言支援

進階驗證用戶端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不支援 UEFI 模式與開機前驗證。

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 - Personal Edition 與 Security Tools

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 網卡 與 UEFI 電腦上的驗證。下列選項需要組態：有 Windows 驗證與 一次性密碼 的智慧卡。下表依作業系統顯示符合硬體和組態需求時，Personal Edition 與 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[2]	X	X[2]	X[2]
Windows 8	X[1]					X	X[2]	X	X[2]	X[2]
Windows 8.1 - Windows 8.1 更新 1	X[1]					X	X[2]	X	X[2]	X[2]
Windows Embedded 8.1						X		X		
Windows 10	X[1]					X	X[2]	X	X[2]	X[2]

1. 僅限搭配 Hardware Crypto Accelerator 或支援的 OPAL SED 使用。

2. 使用子安裝程式時，以主安裝程式、ESS 主安裝程式或進階驗證與驅動程式套件安裝時可以使用。

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 SP0-SP1										
Windows 8	X[3]					X	X[2]	X	X[2]	X[2]
Windows 8.1 - Windows 8.1 更新 1	X[3]					X	X[2]	X	X[2]	X[2]
Windows 10	X[3]					X	X[2]	X	X[2]	X[2]

2. 使用子安裝程式時，以主安裝程式、ESS 主安裝程式或進階驗證與驅動程式套件安裝時可以使用。

3. 在支援的 UEFI 電腦含支援的 OPAL SED 時可用。

驗證選項 - Enterprise Edition

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 網卡 與 UEFI 電腦上的驗證。下列選項需要組態：有 Windows 驗證的智慧卡以及有開機前驗證與 一次性密碼 的智慧卡。組態說明請參閱 *DDP | Enterprise Edition 進階安裝指南*。下表依作業系統顯示符合硬體和組態需求時，Dell Data Protection 產品提供的驗證選項。

加密用戶端驗證選項

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[1]			X	X[2]	X	X[2]	X[2]
Windows Embedded 7						X		X		
Windows 8	X[1]		X[1]			X	X[2]	X	X[2]	X[2]
Windows 8.1 - Windows 8.1 更新 1	X[1]		X[1]			X	X[2]	X	X[2]	X[2]
Windows Embedded 8.1						X		X		
Windows 10	X[1]		X[1]			X	X[2]	X	X[2]	X[2]
VMWare Workstation 5.5 和以上版本						X		X		

1. 僅限搭配 Hardware Crypto Accelerator 使用。

2. 使用子安裝程式時，以主安裝程式、ESS 主安裝程式或進階驗證與驅動程式套件安裝時可以使用。

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 SP0-SP1										
Windows 8						X	X[2]	X	X[2]	X[2]
Windows 8.1 - Windows 8.1 更新 1						X	X[2]	X	X[2]	X[2]
Windows 10						X	X[2]	X	X[2]	X[2]

2. 使用子安裝程式時，以主安裝程式、ESS 主安裝程式或進階驗證與驅動程式套件安裝時可以使用。

SED 加密用戶端驗證選項

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[3]		X[3]		X[3]	X	X	X	X	X
Windows 8	X[3]		X[3]		X[3]	X	X	X	X	X
Windows 8.1	X[3]		X[3]		X[3]	X	X	X	X	X
Windows 10	X[3]		X[3]			X	X	X	X	X

3. 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[4]					X	X	X	X	X
Windows 8.1	X[4]					X	X	X	X	X
Windows 10	X[4]					X	X	X	X	X

4. 在支援的 UEFI 電腦含支援的 OPAL SED 時可用。

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[1]			X	X[2]	X	X[2]	X[2]
Windows 8	X[1]		X[1]			X	X[2]	X	X[2]	X[2]
Windows 8.1 - Windows 8.1 更新 1	X[1]		X[1]			X	X[2]	X	X[2]	X[2]
Windows 10	X[1]		X[1]			X	X[2]	X	X[2]	X[2]

1. 僅限搭配 Hardware Crypto Accelerator 使用。

2. 使用子安裝程式時，以主安裝程式、ESS 主安裝程式或進階驗證與驅動程式套件安裝時可以使用。

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，在安裝加密用戶端、SED 或進階驗證之**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. 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

   當電腦完成取消提供之後，DDP|A 將重新啟動電腦以恢復 Windows 預設的認證提供者。

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： 如果使用的是自行加密磁碟機，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。

3

DDP 安全性主控台

DDP Security Console 可讓電腦的所有使用者存取應用程式、檢視及管理電腦磁碟機與分割的加密狀態，以及根據系統管理員設定的原則，管理網站、程式和網路資源的登入，並且輕輕鬆鬆註冊驗證認證。

若要開啓 DDP 主控台，請從*桌面*按兩下 **DDP 主控台**圖示。

DDP Security Console 啓動時，首頁會顯示 Security Tools 應用程式：

- 加密狀態
- 註冊
- 密碼管理員

若要首次設定認證，請在 Enrollments (註冊) 動態磚上選取 **Getting Started** (開始使用) 連結。精靈會逐步帶領您完成簡短的註冊程序。請參閱 首次註冊認證 以獲得詳細資訊。

瀏覽

若要存取應用程式，請按一下合適之動態磚。

標題列

若要從應用程式返回首頁，請按一下使用中應用程式名稱旁的標題列左邊的返回箭頭。

若要直接瀏覽至另一個應用程式，按一下作用中應用程式名稱旁的向下箭號，然後選取應用程式。

若要最小化、最大化或關閉 DDP 主控台，請按一下標題列右邊的適當圖示。

若要在最小化之後還原 DDP 主控台，請在其系統匣圖示上連按兩下滑鼠鍵。

若要開啓說明，請按一下標題列上的 ?。

DDP 主控台詳細資料

若要檢視關於 DDP 主控台、原則、使用中服務與記錄檔的詳細資訊，請按一下標題列左側的齒輪圖示。系統管理員可能需要此資訊以提供技術支援。

從功能表選取項目。

功能表項目	用途
About (**關於**)	包含版本與著作權資訊。
Show Info (**顯示資訊**)	包含下列資訊： • 產品版本與日期資訊 • DDP 主控台在此電腦上是由企業還是本機系統管理員管理 • 作業系統、BIOS、主機板及 TPM 的版本編號。
MS Info (MS **資訊**)	執行 Microsoft Windows System Information 公用程式顯示詳細的硬體、元件及軟體環境資訊。
Copy Info (**複製資訊**)	將所有系統資訊複製至剪貼簿、貼至給系統管理員或 Dell ProSupport 的電子郵件。
Feedback (**回饋意見**)	顯示表格讓您可以提供關於此產品的回饋意見給 Dell。
Policies (**原則**)	顯示套用於此電腦的原則階層。
Services (**服務**)	顯示正在執行的服務詳細資料。
Support (**支援**)	連接至 Dell ProSupport 網站。
Log (**記錄**)	顯示詳細的記錄事件清單，以進行疑難排解。

4

加密狀態

Encryption (加密) 頁面會顯示電腦的加密狀態。如果磁碟、磁碟區或分割未加密，其狀態爲 ***Unprotected*** (未保護)。加密的磁碟機或分割會顯示 *Protected* (受保護) 的狀態。

若要更新加密狀態，在合適的磁碟、磁碟區或分割上按滑鼠右鍵，然後選取 **Refresh** (重新整理)。

5

註冊

註冊工具可讓您根據系統管理員設定的原則，註冊、修改及檢查註冊狀態。

首次以 DDP 主控台註冊認證時，精靈會逐步引導您註冊密碼變更、復原問題、指紋、行動裝置及智慧卡。視原則而定，您可註冊或略過各個認證。完成初始註冊後，您可按一下 Enrollment (註冊) 標題，新增或修改認證。

首次註冊認證

首次註冊認證：

1. 在 DDP 安全性主控台首頁，按一下 Enrollments (註冊) 動態磚上的 **Getting Started** (開始使用) 連結。
2. 在 Welcome (歡迎) 頁面，按一下 **Next** (下一步)。
3. 在 Authentication Required (所需驗證) 對話方塊中，以您的 Windows 密碼登入，然後按一下 **OK** (確定)。
4. 在 Password (密碼) 頁面，若要變更您的 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)。
5. 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)。
6. 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 新增、修改或檢視註冊。

新增、修改或檢視註冊

若要新增、修改或檢視註冊，請按一下 **Enrollments** (註冊) 動態磚

左窗格內的標籤會列出可用的註冊。結果因平台或硬體類型而有所不同。

Status (狀態) 頁面會顯示支援的認證、其原則設定 (必要或 N/A) 及其註冊狀態。使用者可從此頁面，根據系統管理員設定的原則，管理其註冊：

- 若是首次註冊認證，請在認證的那行上，按一下 **Enroll** (註冊)。
- 若要刪除現有已註冊的認證，請按一下 **Delete** (刪除)。
- 如果原則不允許您註冊或修改自己的認證，Status (狀態) 頁面上的 **Enroll** (註冊) 與 **Delete** (刪除) 連結則會停用。
- 若要變更現有註冊，請按一下左窗格中的合適標籤。

  如果原則不允許註冊或修改認證，則會在認證的註冊頁面上顯示訊息 「Credentials modification is not allowed by policy (原則不允許認證修改)」。

密碼

變更您的 Windows 密碼：

1. 按一下 **Password**（密碼）標籤。
2. 輸入目前的 Windows 密碼。
3. 輸入新密碼，然後再輸入一次確認，再按一下 **Change**（變更）。

   密碼變更隨即生效。
4. 在 Successful Enrollment（成功註冊）對話方塊中，按一下 **OK**（確定）。

註： 您只能在 DDP Security Console 變更 Windows 密碼，不可在 Windows 中變更。如果在 DDP Security Console 以外的地方變更 Windows 密碼，將會發生密碼不符的情況，因而需要進行復原作業。

復原問題

Recovery Questions（復原問題）頁面可讓您建立、刪除或變更復原問題與答案。Recovery Questions（復原問題）爲您提供在密碼過期或遺忘密碼時，存取 Windows 帳戶的問答方法。

註： 復原問題僅限用於恢復存取電腦。復原問題與答案無法用於登入。

如果您沒有已註冊的 Recovery Questions（復原問題）：

1. 按一下 **Recovery Questions**（復原問題）標籤。
2. 從預先定義的問題中選取問題，然後輸入並確認答案。
3. 按一下 **Enroll**（註冊）。

註： 按一下 **Reset**（重設）按鈕，清除此頁面上的選擇，並重新開始。

已註冊復原問題

如果已註冊復原問題，您可刪除或重新註冊復原問題。

1. 按一下 **Recovery Questions**（復原問題）標籤。
2. 按一下合適的按鈕：
   - 若要移除復原問題，請按一下 **Delete**（刪除）。
   - 若要重新定義復原問題與答案，按一下 **Re-enroll**（重新註冊）。

指紋

註： 若要使用此功能，您的電腦必須具有指紋掃描器。

請遵循下述指示註冊指紋：

1. 按一下 **Fingerprints**（指紋）標籤。
2. 在 Fingerprint（指紋）頁面上，按一下想要註冊的手指。
3. 依照畫面上的指示註冊指紋。

註： 必須成功掃描手指四次，才能完成註冊。完成指紋註冊所需的掃描次數，取決於每次掃描的品質而定。系統管理員定義指紋數量下限和上限。

4. 逐一按每一個要掃描的手指，直到註冊完原則要求的指紋數量下限爲止。

若註冊的指紋數量未達下限要求，將會顯示對話方塊提醒。按一下 **OK** (確定) 繼續。

5 完成要求的指紋數量掃描，按一下 **Save** (儲存)。

若要刪除掃描的指紋，請在 Fingerprint enrollment (指紋註冊) 頁面上，按一下反白顯示的指紋，以取消註冊，然後按一下 **Yes** (是) 確認刪除，再按一下 **Save** (儲存)。

行動裝置

行動裝置註冊提供一次性密碼 (OTP) 功能。有了 OTP，使用者便可使用與電腦配對的行動裝置，透過 Security Tools Mobile 應用程式產生的密碼，登入 Windows。或者，若原則許可，OTP 功能也可在密碼過期或忘記密碼的情況下，用於恢復存取電腦。

註： 如果 Mobile Device (行動裝置) 標籤未在 DDP Security Console 中顯示，表示您的電腦組態不支援，或系統管理員設定的原則不允許。

註： 原則設定值決定 OTP 功能的使用方式 - 用於登入或用於密碼過期或您忘記密碼時恢復存取您的電腦。OTP 功能無法同時適用於登入與還原。

若要使用 OTP 功能，您必須在電腦上註冊行動裝置，或使行動裝置與電腦配對。在有多個使用者的電腦上，每一名使用者可在電腦上註冊一部行動裝置。行動裝置可在多部電腦上註冊。

已註冊裝置時，註冊新裝置會自動將上一台裝置解除配對。

在 DDP 安全性主控台上：

1 在 DDP Security Console Enrollments (註冊) 頁面，按一下 **Mobile Device** (行動裝置) 標籤。

2 在右上方，按一下 **Enroll** (註冊)。

Enroll One-time Password (註冊一次性密碼) 頁面即開啓。

3 如果這是第一部要配對的電腦，請選取 **Yes** (是)。

a 在行動裝置上，從應用程式商店下載 Dell Data Protection | Security Tools Mobile 應用程式。

b 在電腦按一下 **Next** (下一步)。

設定 Security Tools Mobile

1 開啓 Security Tools Mobile 應用程式。

2 建立並輸入用於存取 Security Tools Mobile 應用程式的 PIN。

註： 行動裝置未鎖定時，可能需要輸入原則要求的 PIN。如未使用 PIN 解除行動裝置鎖定，必須設定 PIN 才能存取 Security Tools Mobile 應用程式。

3 選取 **Enroll a Computer** (註冊電腦)。(必要時，點選行動畫面左上角存取命令。)

密碼會在行動裝置上顯示。密碼長度與英數字元組合以系統管理員設定的原則爲基礎。

配對行動裝置與電腦

1 在電腦的 DDP Security Console Mobile Code (行動密碼) 頁面上：

a 於欄位上輸入行動裝置顯示的代碼。

b 按一下 **Next** (下一步)。

c 在 Pair Device (裝置配對) 頁面上，選取一個選項：

QR Code (QR 碼) - 顯示 QR 碼。

或

Manual Entry (手動輸入)- 顯示 24 位數的配對碼。

2 在行動裝置上：

a 輕按 **Pair Devices** (配對裝置)。

b 選取您在電腦上已選取的同一個配對選項 (**掃描 QR Code** (QR 碼) 或 **Manual Entry** (手動輸入))。

c 選擇其中一種方法：

- 若爲 **QR Code** (QR 碼)，請將行動裝置放在電腦螢幕前，以便掃描 QR 碼。
  請記下顯示在行動裝置上的數字驗證碼，然後輕按 **Next** (下一步)。

註：如果顯示 *Trouble Scanning?* (遇到掃描問題嗎？) 列，再試一次，或選取 **Manual Entry** (手動輸入)。

- 若爲 **Manual Entry** (手動輸入)，請輸入電腦畫面顯示的 24 位數配對代碼，然後輕按 **Done** (完成)。
  請記下顯示在行動裝置上的數字驗證碼，然後輕按 **Next** (下一步)。

3 在電腦的 DDP 安全性主控台上：

a 按一下 **Next** (下一步)。

b 輸入行動裝置所顯示的驗證碼，然後按一下 **Next** (下一步)。

c 或者修改行動裝置的名稱。

d 按一下 **Apply** (套用)。
裝置便完成配對。

4 在行動裝置上：

a 輕按 **Continue** (繼續)。

b 或者修改電腦的名稱，然後輕按 **Done** (完成)。

c 輕按 **Finish** (完成)。

註冊其他行動裝置

註冊新的裝置會導致之前的裝置自動取消配對。不需另外執行取消配對的操作步驟。

解除配對電腦與行動裝置

若要在不註冊其他裝置的情況下，取消電腦與行動裝置的配對，請選擇一種方式：

- 在 DDP 安全性主控台：在 Enrollments Status (註冊狀態) 頁面的 Mobile Device (行動裝置) 認證旁，按一下 **Delete** （刪除）。
- 在行動裝置上：
  1 執行 Security Tools Mobile 應用程式。
  2 輕按左上方的功能表列，開啓滑動選單。
  3 輕按 **Remove Computers** (移除電腦)。
  4 選擇要取消配對的電腦。
  5 選取 **Remove** (移除) (Android) 或輕按 **Done** (完成) (iOS)。
  確認訊息隨即出現。
  6 選取 **Remove All** (全部移除)，從裝置移除所有註冊的電腦。
  移除多部電腦，以及移除唯一配對的電腦時，會出現 Remove All (全部移除) 選項。
  選取 **Restore Default Settings** (還原爲預設值)，移除註冊的電腦及移除 PIN。
  選取 **Cancel** (取消)，讓電腦保持註冊。

智慧卡

註： 若要使用此功能，您的電腦必須具有智慧卡讀卡機。

請遵循下述指示註冊智慧卡：

1. 按一下 **Smartcard**（智慧卡）標籤。
2. 根據卡片類型註冊智慧卡：
   - 將智慧卡插入讀卡機。
   - 將非接觸式卡拿到讀卡機上方或附近之處。
3. 偵測到此卡片時，會顯示綠色核取方塊與 ***Enroll the card***（註冊卡片）訊息。選取 **Enroll the card**（註冊卡片）。
4. 在 Successful Enrollment（成功註冊）對話方塊中，按一下 **OK**（確定）。

若要取消註冊與使用者關聯的所有智慧卡，請在 Smartcard enrollment（智慧卡註冊）頁面，選取 **Remove enrolled cards from your account**（從您的帳戶移除註冊的卡片）。

6

密碼管理員

Password Manager (密碼管理員) 可讓您以單一工具自動登入網站、Windows 程式及網路資源並管理登入認證。Password Manager 可讓使用者從應用程式變更登入密碼，確保 Password Manager 維護的登入密碼與目標資源的內容同步。

Password Manager 支援 Internet Explorer 與 Mozilla Firefox。Password Manager 不支援 Microsoft 帳戶 (之前爲 Windows Live ID)。

註： 如果執行於 Firefox，您必須安裝並註冊 Password Manager 擴充套件。如需在 Mozilla Firefox 安裝擴充套件的說明，請參閱 https://support.mozilla.org/。

註： 在 Mozilla Firefox，Password Manager 圖示的使用方法 (包含訓練前與訓練圖示) 不同於 Microsoft Internet Explorer：

- 無法使用在 Password Manager 圖示上按兩下的功能。
- 預設動作不會顯示在下拉式內容功能表中。
- 如果頁面有多個登入表單，您可能會看見一個以上的 Password Manager 圖示。

註： 由於網路登入頁面瞬息萬變，因此密碼管理員可能無法隨時支援所有網站。

開始使用 Password Manager 密碼管理員

Password Manager (密碼管理員) 會在您工作時收集與儲存登入認證。安裝 Security Tools 後，馬上可以開始使用 Password Manager (密碼管理員)。在登入頁面上輸入認證時，Password Manager 便會偵測登入表單，讓您選擇是否要 Password Manager 儲存您的認證。

您有三個選項：

- 按一下 **Save Logon** (儲存登入)，將登入認證儲存於 Password Manager。
- 如果您 ***不想要*** 儲存您的登入，每次登入網站或程式時，會提示您再次儲存登入認證。若不希望顯示提示，請選取 **Never for this site** (永遠不在此網站顯示提示)。網站排除清單上將會建立記錄。請參閱 排除網站 以獲得詳細資料。
- 如果不想要儲存認證，請按一下 **Don't Save Logon** (不要儲存登入)。

此對話方塊也會在之前已儲存網站或程式的認證，但卻輸入不同的使用者名稱或密碼時顯示。使用新的使用者名稱時，如果您選取 **Save Logon** (儲存登入)，則會以儲存新一組的認證。使用之前儲存的使用者名稱與新密碼時，如果您選取 **Save Logon** (儲存登入)，則會以新的密碼更新原本的認證。

管理登入

Logon Manager (登入管理員) 簡化並集中管理所有您的網站、Windows 程式及網路資源登入。

開啓 Logon Manager：

1. 在 DDP Security Console 首頁，按一下 **Password Manager** (密碼管理員) 動態磚。
2. 按一下 **Logon Manager** (登入管理員) 標籤。

您可新增登入與類別，並排序與篩選類別：

- 新增登入 - 可讓您新增一組新的登入認證。視原則而定，您可能必須輸入儲存在 Security Tools 的認證，才能新增登入。
- 新增類別 - 可讓您新增用於排序與篩選的新類別（如電子郵件、儲存、新聞、企業資源、社群媒體）。

Sort（排序）：依帳戶、使用者名稱或類別排序登入。按一下欄標題依欄排序。

Filter（篩選）：從 ***View***（檢視）清單選取類別，以隱藏所有登入，但不包括在所選類別中的登入。若要移除篩選條件，請選取 ***All***（全部）。

您可管理登入：

- Launch（啓動）- 開啓網站或程式，並根據使用者設定提交登入認證。
- Edit（編輯）- 可讓您變更網站或程式儲存的登入資料。
- Delete（刪除）- 可讓您從 Password Manager（密碼管理員）移除儲存的登入資料。
- Add（新增）- 可讓您新增新的登入、類別或新的登入資料。

新增類別

新增登入前，請建立類別（如電子郵件、儲存、新聞、企業資源、社群媒體），以隨著登入建立時，將登入分類。然後您可依類別排序與篩選登入。

若要新增類別，在 Logon Manager（登入管理員）頁面上，按一下 **Add category**（新增登入）、輸入類別名稱，然後按一下 **Save**（儲存）。

新增登入

1. 在 Logon Manager（登入管理員）頁面上，按一下 **Add Logon**（新增登入）。

   您可能需要根據原則驗證，以新增登入。
2. 開啓要登入的網站或程式。
3. 在 Add Logon（新增登入）對話方塊中，按一下 **Continue**（繼續）。
4. 在下一個對話方塊中，請輸入以下項目：
   - **Category**（類別）- 爲您正在儲存之網站或程式登入，選擇類別。如果尚未新增類別，這份清單會完全空白。
   - **Account Name**（帳戶名稱）- 保留現狀，以接受預先填入的名稱，或輸入網站或程式的名稱。
   - **Undetected Title**（未偵測的標題）- 這些欄位是 Password Manager 在登入頁面上偵測到要輸入登入資訊的欄位。這些欄位一般包括使用者名稱或電子郵件及密碼。
5. 若欄位名稱顯示 Undetected Title（未偵測的標題），或登入欄位包括錯誤的欄位，請按一下 **More Fields**（更多欄位）按鈕，以編輯欄位名稱或移除欄位。
6. 在 More Fields（更多欄位）對話方塊中，按一下 **Undetected Title**（未偵測的標題），並輸入各欄位正確的欄位名稱。

   顯示 More Fields（更多欄位）對話方塊時，在 Add Logon（新增登入）對話方塊中使用的欄位會反白顯示，協助您重新命名欄位。

   如果是登入不需要的欄位，請清除其核取方塊，以將此欄位自登入資訊排除。
7. 若要儲存變更，請按一下 **OK**（確定）。
8. 在 Add Logon（新增登入）對話方塊中，請填寫登入必填欄位。

註： 因為您要儲存的是現有的登入，所以只能前往網站或程式的 Change Password（變更密碼）功能才能變更密碼。

9 如果您想要 Password Manager 自動填入並提交登入資訊，請選取 **Automatically submit log in data**（自動提交登入資料）。

10 按一下 **Save**（儲存）。

網站或程式登入會在 Logon Manager（登入管理員）頁面上顯示。

匯入認證

您可以將儲存在網頁瀏覽器的認證匯入 Password Manager（密碼管理員）。

1 在 Password Manager 工具中，選取 **Import Credentials**（匯入認證）。

2 選取要匯入的瀏覽器，按一下 **Scan**（掃描）。

3 出現提示時，請輸入所選瀏覽器的密碼。

註： 如果匯入動作並未匯入密碼，請查看瀏覽器是否具有要匯入的儲存資料。如果您正在使用 Firefox，請登入以同步化。請再次嘗試匯入認證。

圖示內容功能表

造訪網站或程式時，會顯示 Password Manager 圖示。

表示可訓練的登入表單。

未出現 時，表示已訓練登入表單。在圖示上連按兩下，登入程式或網站。

按一下圖示時，內容功能表會根據是否已訓練或未訓練登入表單，來顯示不同的選項。

尚未訓練目前的登入欄位時，內容功能表會顯示下列選項：

Add to Password Manager（新增至密碼管理員）	開啓 Add Logon（新增登入）對話方塊。
Icon Settings（圖示設定）	可讓使用者在可訓練登入頁面設定 Password Manager 圖示的顯示。
Open Password Manager（開啓密碼管理員）	啓動 ***Password Manager Administration*** 工具並開啓 Logon Manager 頁面。
Help（說明）	開啓線上說明。

已訓練目前的登入欄位時，內容功能表會顯示下列選項：

Fill in logon data（填入登入資料）	視您在訓練登入表單時所做的選擇而定，會自動登入或填入使用者名稱與密碼欄位，可讓您提交登入資料。
Edit logon（編輯登入）	開啓 Edit logon（編輯登入）對話方塊。
Add logon（新增登入）	開啓 Add logon（新增登入）對話方塊。
Open Password Manager（開啓密碼管理員）	開啓 Logon Manager 頁面。
Help（說明）	開啓線上說明。

如果 Password Manager 圖示未隨著登入表單出現，請關閉瀏覽器的密碼儲存功能：

- 在 Mozilla Firefox：選單圖示 > Options（選項）> Security（安全）> 清除 **Remember passwords for sites**（記住網站的密碼）核取方塊
- 在 Internet Explorer：齒輪圖示 > 網際網路選項 > 內容標籤 > 自動完成設定 > 取消選取 **User names and passwords on forms**（表單上的使用者名稱與密碼）核取方塊

登入訓練的登入頁面

開啓網站或程式登入時，Password Manager 會偵測是否已訓練此頁面。如果已訓練，Password Manager 圖示會在登入區域內顯示。如果尚未訓練，Password Manager 圖示便會顯示 – 除非已停用尚未訓練表單的提示。

若要登入，請選取其中一種方法：

- 掃描註冊的認證。如果已註冊指紋或智慧卡，您可用註冊的指紋觸碰指紋讀取器，或是在讀卡器出示註冊的卡片。
- 按一下 Password Manager 圖示並從內容功能表選取 **Fill in logon data** (填入登入資料)。
- 按下 Password Manager 快速鍵組合：**Ctrl+Win+H**。Password Manager 快顯畫面會顯示您已訓練的網站，可讓您迅速啓動網站。

註： 您可在 DDP Security Console > Password Manager > Settings (設定) 中變更快速鍵組合。

如果該網站或程式不只儲存一個登入，將提示您選擇要使用的帳戶。

網域支援

如果您已針對特定網域訓練登入頁面，但是後來想從不同的登入頁面存取其在該網域的帳戶，請瀏覽至新的登入頁面。系統會提示您使用現有的登入，或是新增登入至密碼管理員。

- 如果按一下 ***Use logon*** (使用登入)，就會登入先前建立的帳號。下次從新的登入頁面存取該帳戶時，即自動登入之前建立的帳戶。
- 如果按一下 ***Add logon (新增登入)***，新增登入 對話方塊便會顯示。

填入 Windows 認證

某些程式允許使用 Windows 認證登入。

請從 ***Add Logon*** (新增登入) 和 ***Edit Logon*** (編輯登入) 對話方塊提供的下拉式功能表選擇 Windows 認證，不用輸入您的使用者名稱和密碼。

若爲使用者名稱，請從下列類型選擇：

- Windows 使用者名稱
- Windows 使用者主體名稱
- Windows 網域 \ 使用者名稱
- Windows 網域

若爲密碼，請使用您的 Windows 密碼。

無法修改這些選項。

使用舊密碼

Password Manager (密碼管理員) 內的密碼可能已變更，程式於是拒絕新密碼。在這個情況下，程式可讓您使用先前的密碼 (先前爲這個登入頁面輸入的密碼)，而不是最新的密碼。

選取 **Password History** (密碼記錄)。驗證後會出現提示，要求您從 Password History (密碼記錄) 清單選擇舊密碼。清單內有七個密碼。

排除網站

若要網站不受 Password Manager 管理，請按一下 **Website Exclusions** (排除網站) 標籤。

排除的網站有這些特性：

- 不會喚起 Password Manager 圖示。
- 不會自動登入使用者。
- 不會顯示密碼提醒。

若要新增網站至排除清單：

1. 按一下 **Website Exclusions** (排除網站) 標籤。
2. 按一下 **Add Website** (新增網站)。
3. 輸入欲排除網站的 URL。
4. 按一下 **Save** (儲存)。

網站一旦排除，便不受 Password Manager 管理。僅須從 Website Exclusions (排除網站) 清單刪除網站，即可取消排除。從排除清單中移除網站：按一下 ✕。

新增數個網站後，您可：

- 若要依網站排上行或下行次序清單，請按一下 Website (網站) 欄標題。
- 若要在清單內搜尋，請將部分 URL 輸入搜尋欄位。清單隨著您輸入進行篩選。

停用訓練登入表單的提示

雖然可保留現有的訓練登入，但可停用訓練登入表單的提示。

停用新登入的提示：

1. 開啓 DDP Security Console。
2. 按一下 **Password Manager** 動態磚。
3. 按一下 **Settings** (設定) 標籤。
4. 清除 **Prompt to add a logon when on a logon screen** (在登入畫面時提示新增登入) 核取方塊。

備份與還原 Password Manager (密碼管理員) 憑證

Password Manager (密碼管理員) 可讓您安全備份由 Password Manager (密碼管理員) 管理的登入資料。有 Password Manager 保護的電腦可以還原這份資料。

註： 備份的 Password Manager (密碼管理員) 資料不包括作業系統或 PBA 登入認證或特定認證資訊，例如指紋。

備份認證

若要備份認證：

1. 按一下 **Backup Credentials** (備份認證) 標籤，以設定備份程序。
2. 按一下 **Browse** (瀏覽) 並瀏覽至所需的備份位置。
   如果您嘗試將資料備份至本機磁碟機，隨即會顯示建議，請您將資料備份至可攜式儲存裝置或網路磁碟機。
3. 輸入並確認密碼。如果必須在之後還原這些備份的認證，必須使用此密碼。
4. 按一下 **Backup** (備份)。
5. 輸入 Windows 密碼。

6 在 Success (成功) 對話方塊中，按一下 **OK** (確定)。

註： 若要檢視已執行之備份作業的文字記錄，請按一下 並選取 **Log** (記錄)。

還原認證

備份位置必須可用，才能還原認證。

若要還原認證：

1 按一下 **Restore Credentials** (還原認證) 標籤。

2 按一下 **Browse** (瀏覽) 瀏覽至備份檔，然後輸入檔案的密碼。

3 按一下 **Restore** (還原)。

警告：還原 Password Manager (密碼管理員) 資料將會覆寫任何現有資料。在建立備份後新增的登入與其他資料將會遺失。

4 按一下 **Next** (下一步)。

註： 若要檢視還原作業的文字記錄，請按一下標題列中的 圖示，然後選取 **Log** (記錄)。

使用一次性密碼登入

註： OTP 驗證僅適用於 Windows 登入。

OTP 可用於復原、重新取得遭鎖定的電腦存取權限或 Windows 登入。無法同時適用於兩種用途。

如果原則允許且 OTP 符號 在登入畫面上顯示，則可使用 OTP 登入 Windows。

以 OTP 登入：

1 在電腦的 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。
- 如果您不只擁有一個 Windows 使用者帳戶，表示 DDP | Security Tools 未安裝在您正在嘗試存取的電腦上，或您正在登入的使用者帳戶不同於用於配對電腦與行動裝置的帳戶。

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**。

若您曾使用 OTP 進行復原，則在您取得電腦存取權限後，請依照畫面指示重設密碼。

Security Tools Mobile 管理工作

這些工作以行動裝置上的 Security Tools Mobile 應用程式執行。

重設 Security Tools Mobile 應用程式 PIN

若要重設 Security Tools Mobile 應用程式 PIN：

1. 輕按右上方的選單選項。
2. 選取 **Reset Pin** (重設 PIN)。
3. 輸入並確認新的 PIN。

還原 Security Tools Mobile 應用程式的預設值

若還原爲預設值，將移除所有已註冊的電腦以及您用於存取 Security Tools Mobile 應用程式的 PIN。

若要還原 Security Tools Mobile 應用程式的預設值：

1. 輕按右上方的選單選項。
2. 選取 **Restore Default Settings** (還原爲預設值)。
3. 確認您要移除所有已註冊的電腦。

從行動裝置解除配對電腦

從行動裝置解除配對電腦：

1. 在左上方，輕敲箭號可開啓拖曳視窗。
2. 在拖曳視窗中，輕敲 **Remove Computers** (移除電腦)。
3. 輕敲電腦名稱旁的核取方塊，然後輕敲 **Remove** (移除)。
4. 在確認對話方塊中，輕敲 **Continue** (繼續)。
5. 若您有多台電腦，請重複上述步驟。

解除安裝 Security Tools Mobile 應用程式

在行動裝置上：

1. 取消裝置與電腦的配對。
2. 輕按右上方的選單選項。
3. 選取 **Uninstall/disable apps** (解除安裝 / 停用應用程式)。
4. 選取 Security Tools Mobile。
5. 在確認對話方塊中，按一下 **OK** (確定)。

詞彙表

一次性密碼 (OTP) – 一次性密碼為僅可使用一次，且在有限時間內有效的密碼。OTP 需要有 TPM，而且必須啟用及擁有。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。

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。DDPlE 因其安全儲存功能，而使用 TPM。TPM 亦可為 DDPlE 軟體保存庫提供加密的容器，並保護 DDPlE HCA 加密金鑰。TPM 為搭配 DDPlE HCA 與一次性密碼功能使用所需。Dell 建議佈建 TPM。

受保護 – 若為自行加密磁碟機 (SED)，啟動 SED 並部署開機前驗證 (PBA) 後，電腦便受到保護。

自行加密磁碟機 (SED) - 內建加密機制的硬碟機，會自動加密儲存在媒體的所有資料，解密離開媒體的所有資料。使用者完全無法察覺到這類加密。

認證 - 認證是某種可證明身份的東西，例如指紋或 Windows 密碼。

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