Dell Data Protection | Access 首頁

Dell Data Protection | Access
首頁是存取應用程式各項功能的起點。 您可以從此視窗存取以下項目：

System Access Wizard
存取選項
Self-Encrypting Drive
進階選項

視窗右下角有**進階**的連結，按一下可以存取進階選項。

從**進階選項**視窗按一下右下角的**首頁**連結，即可返回首頁。

System Access Wizard

System Access Wizard 會在 **Dell Data Protection | Access**
應用程式第一次啟動時自動啟動。精靈將引導您逐步完成系統的各項安全設定，包括您希望登入系統的方式 (例如僅進行密碼驗證，或指紋和密碼) 以及登入的時機 (進入 Windows 系統時、進入 Windows
前畫面時，或二者) 。此外，若您的系統有自行加密磁碟，您也可以使用此精靈進行設定。

管理員功能

在系統中擁有 Windows 管理員權限的使用者有權在 **Dell Data Access | Protection** 中執行以下功能，一般標準使用者則不行：

- 設定/變更系統 (Windows 前) 密碼
- 設定/變更硬碟密碼
- 設定/變更管理員密碼
- 設定/變更 TPM 所有者密碼
- 設定/變更 ControlVault 管理員密碼
- 重設系統
- 存檔並還原憑證
- 設定/變更 Smartcard 管理員 PIN
- 清除/重設 Smartcard
- 啟用/停用 Dell Secure 登入 Windows
- 設定 Windows 登入政策
- 管理 Self-Encrypting Drive，包括：
    - 啟用/停用 Self-Encrypting Drive 鎖住
    - 啟用/停用 Windows 密碼同步化 (WPS)
    - 啟用/停用 Single Sign On (SSO)
    - 執行以密碼刪除

遠端管理

您的組織可以設定一個環境，在這個環境下集中管理數個平台上的 **Dell Data Protection | Access** 應用程式的安全功能 (這也就是 遠端管理)。 在此情況下，即可運使用 Windows 安全基礎架構，例如 Active Directory，以安全的方式管理 **Dell Data Protection | Access** 的特定功能。

當電腦接受遠端管理時 (例如由遠端管理員「擁有」)，將停用 **Dell Data Protection | Access** 功能中的本機管理功能，您將無法從本機存取應用程式的管理視窗。您可從遠端管理下列功能：

- Trusted Platform Module (TPM)
- ControlVault
- Windows 前登入
- 重設系統
- BIOS 密碼
- Windows 登入政策
- Self-Encrypting Drive
- 指紋和 Smartcard 登記

如需要有關使用 Wave Systems 的 EMBASSYAR Remote Administration Server (ERAS) 進行遠端管理的詳細資訊，請聯繫 Dell 銷售人員，或至 dell.com。

存取選項

您可以從「存取選項」視窗設定存取系統的方式。

您已設定的 **Dell Data Protection | Access** 選項將在首頁顯示可使用的選項 (例如變更 Windows 前登入密碼)。 這些可使用的選項是捷徑，在您點選時會進入對應的視窗執行特定工作 (例如變更 Windows 前登入密碼或登記另一枚指紋)。

一般

首先，您可以指定登入 (Windows、Windows 前、或二者) 的時間以及登入的方式 (例如指紋和密碼)。您可以選擇一或二種登入方式，登入方式包括指紋、Smartcard 與密碼的組合。 列出的選項是以適用於您環境的登入政策以及平台支援的方式為依據。

指紋

若您的系統有指紋讀取機，您可以登記或更新用來登入系統的指紋。
當您登記的指紋後，可以在系統的指紋讀取機上敲擊已登記的指紋，在 Windows 、Windows 前、或二者皆可的情況下存取您的系統 (需視您在「一般存取選項」中指定的項目而定)。
如需詳細資訊，請參閱登記使用者指紋。

Windows 前登入

若指定使用者必須在 Windows 前登入，您必須針對 Windows 前的存取設定系統密碼 (有時候稱為 Windows 前密碼) 。 密碼設定好之後，系統管理員可以隨時更改。

您也可以從這個畫面停用 Windows 前登入。若要停用，需要輸入您目前的系統密碼，確認密碼正確，然後按一下**「停用」**按鈕。

Smartcard

若您指定使用者必須使用 Smartcard 登入，則必須登記一或多個傳統 (接觸式) Smartcard 或 Contactless Smartcard。按一下**「登記另一個 Smartcard」**連結啟動 Smartcard 登記精靈。登記表示設定您的 Smartcard 以用於登入。

登記 Smartcard 之後，可以透過**「變更或設定我的 Smartcard PIN」**連結變更或設定卡片的 PIN。

Windows 前登入

設定 Windows 前登入之後，在系統開機後、Windows 系統載入之前必須提供驗證 (密碼、指紋或 Smartcard)。Windows 前登入功能為系統提供額外的安全性，保持 Windows 不受未經授權使用者登入而存取電腦 (例如當電腦遭竊時)。

管理員可從「Windows 前登入」視窗設定 Windows 前登入，或者建立或變更 Windows 前 (系統) 密碼。若密碼已經設定，則可以從這個視窗停用 Windows 前登入。設定 Windows 前登入將會啟動精靈執行以下動作：

- 系統密碼： 設定 Windows 前存取權限的系統密碼 (也稱為 Windows 前密碼)。當使用者有其他驗證因子時，此密碼也可以做為備用密碼 (例如當指紋感應器發生問題時，用來進入系統)。
- 指紋或 Smartcard： 設定 Windows 前登入使用的指紋或 Smartcard，並指定是否以此驗證因子取代 Windows 前登入密碼，或作為密碼之外的額外驗證機制。
- Single Sign On： 依預設，您的 Windows 前驗證 (密碼、指紋或 Smartcard) 也會讓您自動登入 Windows (這稱為「Single Sign On」)。若要停用此功能，請選取「我想在 Windows 載入時再次登入」核取方塊。
- 若是除了 Windows 前密碼之外，您還設定了 BIOS 硬碟密碼，您也可以選擇變更或停用硬碟密碼。

注意： 並非所有指紋讀取機皆可在 Windows 前驗證啟用。若您的讀取機不相容，則您只能登記 Windows 登入的指紋。若要知道特定指紋讀取機是否與系統相容，請聯絡您的系統管理員，或至 support.dell.com 取得受支援的指紋讀取機清單。

停用 Windows 前登入

您也可以從這個視窗停用 Windows 前登入。若要停用，您必須輸入目前的 Windows 前 (系統) 密碼，確認密碼正確，然後按一下**「停用」**按鈕。請注意，當您停用 Windows 前登入時，已登記的指紋或 Smartcard 將保持在登記狀態。

登記/移除指紋

使用者可以註冊或更新指紋，其可使用於 Windows 前登入或 Windows 登入時的系統驗證。在「指紋」標籤中，雙手的影像會顯示已登記的手指 (若有已登記手指)。按一下**登記其他**連結會啟動「指紋登記精靈」，它將引導您完成登記流程。「登記」表示儲存用來登入的指紋。您必須已適當安裝及設定有效的指紋讀取機，才能登記指紋。

注意： 並非所有指紋讀取機皆可使用於 Windows 前登入。若您嘗試以不相容的讀取機登記 Windows 前的登入指紋，將出現錯誤訊息。若要知道裝置是否與系統相容，請聯絡您的系統管理員，或至 support.dell.com 取得受支援的指紋讀取機清單。

登記指紋時，系統將提示您輸入 Windows 密碼以驗證您的身分。若您的政策有要求，系統也將提示您輸入 Windows 前 (系統) 密碼。若是指紋讀取機發生問題，可使用 Windows 前密碼取得系統的存取權。

注意：

- 在登記的程序中，強烈建議您登記至少兩組指紋。
- 您必須確認在啟用指紋驗證功能前已正確地登記指紋。
- 若您變更系統中的指紋讀取機，則必須以新的讀取機重新登記指紋。不建議您在兩個不同的指紋讀取機之間來回切換。
- 若您在登記指紋時重複看見「感應器無法對焦」訊息，可能是電腦無法辨識指紋讀取機。若指紋讀取機是外部裝置，通常拔除連線並重新連線即可解決這個問題。

清除登記的指紋

您可以移除已登記的指紋，方法為按一下**移除指紋**連結，或在「指紋登記精靈」中按一下 (取消選取) 已登記的指紋。

若要移除已登記 Windows 前驗證指紋的特定使用者，管理員可以取消選取該使用者所有已登記的指紋。

注意：若您在指紋登記過程中發生任何錯誤，可以參閱 wave.com/support/Dell 以取得詳細資訊。

登記 Smart Card

Dell Data Protection | Access 讓您選擇使用傳統 (接觸式) 或非接觸式 Smartcard，在 Windows 前登入您的 Windows 帳號進行驗證。 在「Smartcard」標籤按一下**登記另一個 Smartcard** 連結，啟動 Smartcard 登記精靈，由精靈引導您完成登記流程。「登記」表示設定使用您的 Smartcard 以用於登入。

您必須已適當安裝及設定有效的 Smartcard 驗證裝置，才能執行登記。

注意： 若要知道特定的裝置是否與系統相容，請聯絡您的系統管理員，或至 support.dell.com 取得受支援的 Smartcard 清單。

登記
登記 Smartcard 時，系統將提示您輸入 Windows 密碼以驗證您的身分。若您的政策有要求，系統也將提示您輸入 Windows 前 (系統) 密碼。若是 Smartcard 讀卡機發生問題，可使用 Windows 前密碼取得系統的存取權。

在登記的過程中，系統將提示您輸入 Smartcard PIN (若已設有 Smartcard PIN)。若您的政策要求 PIN，而您尚未設定 PIN，系統將提示您建立 PIN。

注意：

- 當使用者完成在 Windows 前使用的 Smartcard 登記，將無法移除該使用者。
- 標準使用者可以在 Smartcard 變更使用者 PIN，而系統管理員可變更管理員 PIN 和使用者 PIN。
- 系統管理員也可以重設 Smartcard，一旦重設後，即無法使用 Smartcard 進行 Windows 登入驗證或 Windows 前驗證，直到重新登記 Smartcard 為止。

注意：有關於 TPM 證書驗證，管理員可以透過 Microsoft Windows Smartcard 登記程序來登記 TPM 證書。管理員必須選取 「Wave TCG-Enabled CSP」作為 Cryptographic Service Provider，取代 Smartcard CSP 以便與應用程式相容。 此外，必須啟用 Dell Secure 登入，並採用適合用戶端的驗證類型政策。

注意： 若您收到錯誤訊息指出 Smartcard Service 不在執行中，您可以執行以下動作來啟動/重新啟動此服務：

- 從「控制台」瀏覽至「系統管理工具」視窗，選取「服務」，然後以滑鼠右鍵點選 Smartcard，然後選取「啟動」或「重新啟動」。
- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

Self-Encrypting Drive

Dell Data Protection | Access 可管理 Self-Encrypting Drive 的硬體式安全功能，該磁碟機在硬碟中內嵌資料加密功能。這種功能可確保當磁碟鎖住功能啟用時，只有經過授權的使用者可以存取加密的資料。

按一下「**Self-Encrypting Drive**」底部標籤，可存取「Self-Encrypting Drive」視窗。此標籤只有在系統中有一或多個自行加密磁碟 (SED) 存在時才會顯示。

按一下「**設定**」連結開始 Self-Encrypting Drive 設定精靈。在此精靈中，您將建立磁碟管理員密碼，請將密碼備份，並套用您的磁碟加密設定。只有系統管理員可以存取 Self-Encrypting Drive 設定精靈。

重要！ 磁碟設定完成之後，資料保護以及磁碟鎖住功能會變成「啟用」。當磁碟鎖住時，以下行為將適用：

- 只要磁碟的電源關閉，磁碟便進入*鎖住*模式。
- 除非使用者在 Windows 前登入畫面中輸入正確的使用者名稱和密碼 (或指紋)，否則不會啟動磁碟。在磁碟鎖住啟用之前，電腦的任何使用者皆可存取磁碟中的資料。
- 磁碟即使插入另一台機器做為次要磁碟，仍可受到安全保護，存取磁碟資料必須要通過驗證。

磁碟設定之後，「Self-Encrypting Drive」視窗會顯示磁碟和連結，供使用者變更磁碟密碼。若您是磁碟管理員，您也可以在這個視窗新增或移除磁碟使用者。 若已經設定外部磁碟，外部磁碟也會在此視窗中顯示，且可以將其解鎖。

注意： 若要鎖住次要外部磁碟，必須從電腦將磁碟電源個別關閉。

磁碟管理員可以在「**進階>裝置**」中管理磁碟設定。如需詳細資訊，請參閱裝置管理 - Self-Encrypting Drive。

磁碟設定

Self-Encrypting Drive 設定精靈會引導您完成磁碟的設定。在此過程中，請務必牢記以下觀念。

磁碟管理員

擁有系統管理員權限、設定磁碟存取權 (以及磁碟管理員密碼) 的第一位使用者會成為磁碟管理員，只有這位使用者有權可以變更磁碟存取權。為了確定特別將第一位使用者設定為磁碟管理員，您必須選取「我了解」核取方塊才能繼續此步驟。

磁碟管理員密碼

精靈會提示您建立「磁碟管理員」密碼，並重新輸入密碼確認。您必須先輸入 Windows 密碼建立身分，才可以建立「磁碟管理員」密碼。目前的 Windows 使用者必須有管理員權限才能建立密碼。

備份磁碟憑證

若要儲存一份磁碟管理員憑證備份，請輸入位置，或按一下「**瀏覽**」按鈕選取位置。

重要！

- 我們非常建議您進行憑證備份，並且請備份在主要硬碟以外的磁碟 (例如可移除式媒體)。否則，若您失去磁碟的存取權，將無法取得備份。
- 磁碟備份完成後，所有使用者都必須在 Windows 載入前輸入正確的使用者名稱和密碼 (或指紋)，才能在系統下次開機時存取系統。

新增磁碟使用者

磁碟管理員可將有效的 Windows 使用者的其他使用者新增到磁碟。將使用者新增到磁碟時，管理員可選擇要求使用者在第一次登入時重設密碼。使用者將在 Windows 前驗證畫面中被要求重設密碼，才能使磁碟解鎖。

進階設定

- *Single Sign On* - 依預設，您在 Windows 前輸入進行磁碟驗證的 Self-Encrypting Drive 密碼會用來將您自動登入 Windows (這稱為「Single Sign On」)。若要停用此功能，請在進行磁碟設定時選取「我要在 Windows 開始時再次登入」核取方塊。
- *指紋登入* - 在支援的平台上，您可以指定要使用指紋而不使用密碼進行自行加密磁碟的驗證。
- *待命/睡眠 (S3) 支援* (若在平台支援) - 若是啟用，您的自行加密磁碟可安全地切換至「待命/睡眠」模式 (也稱為「S3」模式)，當從「待命/睡眠」模式恢復時必須經過 Windows 前驗證。

注意：

- 啟用「S3 支援」時，磁碟加密密碼會受到可能存在的 BIOS 密碼的限制。如需系統可能存在的任何特定 BIOS 密碼限制的詳細資訊，請洽系統硬體製造商。
- 並非所有的自行加密磁碟都支援 S3 模式。在磁碟安裝過程中，系統將通知您磁碟是否支援「待命/睡眠」模式。對於不支援此模式的磁碟，若是已啟用休眠功能，「Windows S3」要求會自動轉換為休眠要求 (強烈建議您啟用電腦的休眠模式)。
- Single Sign On (SSO) 選項設定後，當您第一次登入時，程序會在 Windows 登入提示暫停。您將需要填入「Windows 驗證」表單，系統會安全儲存表單，供進一步嘗試「Windows 登入」之用。下一次系統開機時，SSO 會自動將您登入 Windows。當使用者的 Windows 驗證 (密碼、指紋、Smartcard PIN) 變更時，必須經過相同過程。 若電腦 位於相同網域，而該網域的政策為必須使用「ctrl+alt+del」進行登入，程序將遵守此政策。

小心！若您要解除安裝 **Dell Data Protection | Access** 應用程式，必須先停用自行加密磁碟資料保護，並將磁碟解鎖。

Self-Encrypting Drive 使用者功能

Self-Encrypting Drive
管理員負責執行磁碟安全性與使用者的所有管理功能。非磁碟管理員的使用者只能執行以下工作：

- 變更自己的磁碟密碼
- 解鎖磁碟

這些工作可從 **Dell Data Protection | Access** 的「**Self-Encrypting Drive**」標籤存取。

變更密碼
這可讓登記的使用者建立新的磁碟驗證密碼。您必須輸入目前的 Self-Encrypting Drive 密碼，才能將磁碟密碼設為新值。

注意：

- 應用程式將強制執行 Windows 密碼長度與密碼複雜性政策 (若此二者已啟用)。如果未啟用 Windows 密碼政策，則 Self-Encrypting Drive 密碼的長度上限為 32 個字元。請注意，若未啟用 S3 (睡眠/待命)，則長度上限為 127 字元。
- 使用者的 Self-Encrypting Drive 密碼與 Windows 密碼是分開的。 當使用者的 Windows 密碼變更或重設時，除非已啟用「Windows 密碼同步化」，否則不會對使用者的磁碟密碼有任何影響。如需詳細資訊，請參閱裝置： Self-Encrypting Drive。
- 有些非英文鍵盤的部分字元受到限制，無法作為 Self-Encrypting Drive 的密碼。如果 Windows 密碼包含任何受到限制的字元，且「Windows 密碼同步化」已啟用，則會無法同步化，並會產生錯誤訊息。

磁碟解鎖
「磁碟解鎖」可供已登記的磁碟使用者將磁碟解鎖。如果已啟用磁碟鎖定，則每當電腦電源關閉時，磁碟就會進入鎖定狀態。當系統電源恢復時，您必須在 Windows 前畫面輸入密碼，進行磁碟驗證。

注意：

- 若在電腦上同時啟用多個 Self-Encrypting Drive 使用者帳號，電腦可能無法進入省電模式 (也就是睡眠/待命或休眠)。
- 在下列語言版本的應用程式的 Windows 前驗證畫面上，User 1、User 2 等會由磁碟使用者名稱取代：中文、日文、韓文與俄文。

進階選項

Dell Data Protection | Access
中的「進階」選項讓擁有管理員權限的使用者得以管理應用程式的以下項目：

維護
密碼
裝置

注意： 只有擁有管理員權限的使用者可以在「進階」選項中進行修改。一般標準使用者可以檢視設定，但無法做任何變更。

維護

「維護」視窗可供管理員設定 Windows
登入喜好設定、重設以讓系統重新轉換、或者存檔或復原儲存於系統安全硬體中的使用者憑證。如需詳細資訊，請參閱以下主題：

存取喜好設定
重設系統
憑證存檔 & 還原

存取喜好設定

「存取喜好設定」視窗可供管理員為系統的所有使用者指定 Windows 登入的喜好設定。

啟用 Dell Secure 登入
此選項取代了標準的 Windows ctrl-alt-delete 畫面，讓您可以使用 Windows 密碼以外的不同驗證因子進入 Windows 系統。您可以選擇加入指紋做為第二個驗證因子，以加強 Windows 登入程序的安全性。您也可以加入其他登入 Windows 的驗證因子，包括 Smartcard 或 TPM 證書。

注意：

- 啟用 Dell Secure 登入會影響系統的所有使用者。
- 建議在使用者登記指紋或 Smartcard「之後」 再啟用此選項。
- 當您在設定此選項後首次登入時，系統將提示您根據標準政策在 Windows 進行驗證，之後在下次開機時，您將需要使用新的驗證因子登入。

停用 Dell Secure 登入
此選項停用 **Dell Data Protection | Access** 所有登入 Windows 的功能。此選項選取時，您將回到標準的 Windows 登入政策。

注意：

- 當您試圖登入時若發生 Secure Windows 登入錯誤，請停用並重新啟用 Dell Secure 登入選項。
- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

重設系統

「重設系統」功能可用來清除平台中所有安全硬體的所有使用者資料，例如當電腦要變更用途時即可使用此功能。此選項可清除系統中除了 Windows
使用者密碼以外的所有密碼，以及清除硬體裝置的所有資料 (也就是 ControlVault、TPM
和指紋讀取機)。此功能也會針對 Self-Encrypting Drive
停用資料保護功能，讓您可存取磁碟資料。

您必須確認您知道自己正在重設系統，然後按一下**「下一步」**。若要重設系統，您必須為每一個已設定的安全裝置輸入密碼：

- TPM 所有者
- ControlVault 管理員
- BIOS 管理員
- BIOS 系統 (Windows 前)
- 硬碟 (BIOS)
- Self-Encrypting Drive 管理員

注意：Self-Encrypting Drive 僅需磁碟管理員密碼，不需磁碟所有使用者的密碼。

重要事項！若要復原在重設系統時清除掉的資料，唯一的方法是從事先儲存的存檔中還原。若您沒有存檔，資料將無法復原。針對 Self-Encrypting
Drive，只會刪除設定資料，而不會刪除磁碟中的個人資料。

憑證存檔與還原

「憑證存檔與還原」功能可以備份和還原儲存於 ControlVault 和 Trusted Platform Module (TPM) 的所有使用者憑證
(登入和加密資訊)。發生硬體故障時，若須重新提供電腦或必須還原資料，此時資料備份便很重要。在這種情況下，您可以從存檔的檔案將所有的憑證還原到新電腦。

您可以選擇存檔或還原系統中單一使用者或所有使用者的憑證。

使用者憑證包含使用於 Windows 前的資料，例如登記的指紋和 Smartcard 資料，以及儲存於 TPM 的金鑰。TPM 會依照安全應用程式提出的要求建立金鑰，例如產生數位證書即可在 TPM 建立金鑰。

注意： 請查詢安全應用程式文件以決定 **Dell Data Protection | Access** 是否可以存檔 TPM 金鑰。 一般來說，以 Wave TCG-Enabled CSP 產生金鑰的應用程式都受到支援。

存檔憑證
若要將憑證存檔，必須執行以下動作：

- 指定只存檔自己的憑證，或是存檔系統中所有使用者的憑證。
- 輸入系統 (Windows 前) 密碼、ControlVault 管理員密碼、以及 TPM 所有者密碼，以向安全硬體進行驗證。
- 建立憑證備份密碼。
- 使用「**瀏覽**」按鈕指定存檔位置。 存檔位置應該是可移除的媒體，例如 USB 隨身碟或網路硬碟，以避免硬碟故障。

重要事項：

- 請注意存檔位置，因為使用者將需要此資訊才能還原憑證資訊。
- 請注意憑證備份密碼，確定可還原資訊。由於密碼無法復原，因此這點非常重要。
- ?若您不知道「TPM 所有者」密碼，請聯絡系統管理員或參考電腦的 TPM 設定指示。

還原憑證
若要將憑證還原，必須執行以下動作：

- 指定您只還原自己的憑證，或是還原存檔系統中所有使用者的憑證。
- 瀏覽至存檔位置，並選取存檔檔案。
- 輸入設定存檔時建立的憑證備份密碼。
- 輸入系統 (Windows 前) 密碼、ControlVault 管理員密碼、以及 TPM 所有者密碼，以向安全硬體進行驗證。

注意：

- 若您收到錯誤訊息，指出憑證還原失敗，且您已經多次嘗試執行還原，請試著還原另一個存檔檔案。若是不成功，請建立另一個憑證存檔並嘗試從新的存檔還原。
- 若您收到錯誤訊息，指出無法還原 TPM 金鑰，請建立憑證存檔，然後清除 BIOS 中的 TPM。若要清除 TPM，請將電腦重新開機，在電腦開始時按 **F2** 鍵進入 BIOS 設定，然後瀏覽至「安全」>「TPM 安全」。之後，重新建立 TPM 的所有權，並再次嘗試還原憑證。
- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

密碼管理

管理員可從「密碼管理」視窗建立或變更系統中的所有安全密碼：

- 系統 (也稱為「Windows 前」)*
- 管理員*
- 硬碟*
- ControlVault
- TPM 所有者
- TPM 主要
- TPM 密碼保險庫
- Self-Encrypting Drive

注意：

- 只會顯示適用於目前平台組態的密碼，因此視窗內容會根據系統組態和狀態變更。
- 上述密碼中帶有星號 (*) 者是 BIOS 密碼，也可透過系統 BIOS 更改。
- 若是 BIOS 管理員拒絕密碼變更，則無法建立或變更 BIOS 層級的密碼。
- 按一下 Self-Encrypting Drive 的**設定**連結會啟動 Self-Encrypting Drive 設定精靈；按一下**管理**可讓使用者變更一或多個 Self-Encrypting Drive 密碼。
- 按一下「TPM 密碼保險庫」的**管理**連結會顯示一個視窗，您可以在視窗中檢視或變更保護 TPM 金鑰的密碼。在建立需要密碼的 TPM 金鑰時，密碼會隨機產生並放置在保險庫中。在您建立 TPM 主要密碼之前，無法管理 TPM 密碼保險庫。

Windows 密碼 複雜性規則

Dell Data Protection | Access 可確保以下密碼符合 Windows 電腦的密碼複雜性規則：

- 「TPM 所有者」密碼

若要決定電腦的 Windows 密碼複雜性政策，請遵循下列步驟：

1. 存取「控制台」。
2. 按兩下「系統管理工具」。
3. 按兩下「本機安全性原則」。
4. 展開「帳戶原則」，並選取「密碼原則」。

裝置

「裝置」視窗供系統管理員管理安裝於系統中的所有安全裝置。 您可以檢視每個裝置的狀態和其它詳細資訊，例如韌體版本。按一下**「顯示」**可以檢視每個裝置的資訊，或者按一下**「隱藏」**摺疊該區段。以下為可管理的裝置，視您的平台所包含的項目而定：

Trusted Platform Module (TPM)
ControlVault[AR]
Self-Encrypting Drive
驗證裝置資訊

Trusted Platform Module (TPM)

您必須啟用 TPM 安全晶片並且建立 TPM 所有權，才能使用 **Dell Data Protection | Access** 和 TPM 所提供的進階安全功能。

裝置管理中的 Trusted Platform Module 視窗只在您的系統偵測到 TPM 時才會顯示。

TPM 管理
這些功能使得系統管理員能夠管理 TPM。

狀態
顯示 TPM 的*作用中*或*非使用中*狀態。 「作用中」狀態表示 TPM 已在 BIOS 中啟用，且可以進行設定 (也就是可以設定所有權)。 若是 TPM 不在作用中 (未啟用)，則無法管理 TPM 或存取其安全功能。

若在系統偵測到 TPM，但 TPM 不在作用中 (未啟用)，您可以按一下這個視窗中的**「啟動」**連結將其啟用，不須要進入系統 BIOS。
在使用此功能啟用 TPM 後，電腦必須重新開機。
在重新開機的過程中，某些情況下會出現系統提示，要求您接受變更。

注意： 不一定所有的平台都支援從此應用程式啟用 (啟動) TPM。 若平台不支援，您必須在系統 BIOS 中啟動它。 若要這麼做，請重新啟動系統，在 Windows 載入前按 **F2** 按鍵進入 BIOS 設定，然後瀏覽到安全>TPM 安全，啟動 TPM。

您也可以按一下**「停用」**連結，*停用* TPM。停用 TPM 會使 TPM 無法提供進階安全功能使用。但是，停用 TPM 不會變更任何 TPM 設定，或者刪除或改變儲存於 TPM 的任何資訊或金鑰。

已擁有
顯示所有權 (也就是「已擁有」) 狀態，且可讓您建立或變更 TPM 所有者。
TPM 的安全功能必須在建立所有權之後才能使用。 TPM 必須先啟用 (啟動)，才可以建立 TPM 所有權。

建立所有權的過程包含 (擁有管理員權限的) 使用者 建立「TPM 所有者」密碼。
一旦定義密碼，表示已建立所有權並可使用 TPM。

注意： 「TPM 所有者」密碼必須符合您系統的 Windows 密碼複雜性規則。

重要！ 由於存取 **Dell Data Protection | Access** 中的 TPM 進階安全功能必須有「TPM 所有者」密碼，請留意不要遺失或忘記「TPM 所有者」密碼。

鎖住
顯示 TPM 的*鎖住*或*解鎖*狀態。 「鎖住」是 TPM 的安全功能。當輸入錯誤的「TPM 所有者」密碼達指定次數後，TPM 會進入鎖住狀態。
TPM 所有者可以從這裡將 TPM 解鎖，必須輸入「TPM 所有者」密碼。

注意：

- 若您接到的錯誤訊息指出無法建立 TPM 的所有權，請在系統 BIOS 中清除 TPM，並再次嘗試建立所有權。 若要清除 TPM，請將電腦重新開機，在電腦開始時按 **F2** 鍵進入 BIOS 設定，然後瀏覽至「安全」>「TPM 安全」。
- 若您接到的錯誤訊息指出無法變更「TPM 所有者」密碼，請將 TPM 資料 (憑證存檔) 存檔，清除 BIOS 中的 TPM，重新建立 TPM 所有權並還原 TPM 資料 (還原憑證)。

- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

Dell ControlVault®

Dell ControlVault™ (CV) 是儲存 Windows 前登入使用者憑證 (例如使用者密碼或登記的指紋資料) 的安全硬體儲存庫。**裝置管理**中的 ControlVault 視窗只在您的系統偵測到 ControlVault 時才會顯示。

ControlVault 管理

這些功能讓系統管理員能夠管理系統的 ControlVault。

狀態

顯示 ControlVault 的*作用中*或*非使用中*狀態。「非使用中」狀態 表示您的系統無法使用 ControlVault 儲存裝置。請查閱 Dell 系統文件以判斷系統是否包含 ControlVault。

密碼

指出是否已設定 ControlVault 管理員密碼，並可讓您在此設定密碼，或變更密碼 (若已設定密碼) 。只有系統管理員可以設定或變更密碼。執行以下工作前，必須先設定 ControlVault 管理員密碼：

- 執行憑證存檔或還原。
- 清除使用者資料 (所有的使用者) 。

注意： 若是未設定 ControlVault 管理員密碼而嘗試進行憑證存檔或還原，系統會提示使用者必須建立密碼 (若使用者是系統管理員)。

登記的使用者

指出是否有任何使用者登記了目前儲存於 ControlVault 的登入憑證 (例如密碼、指紋或 Smartcard 資料)。

清除使用者資料

ControlVault 的資料在某個時間點可能需要清除。例如，當使用者使用或登記 Windows 前憑證進行驗證發生問題時。可以在此視窗中清除儲存於 ControlVault 的所有資料，包括單一使用者或所有使用者的資料。

必須輸入 ControlVault 管理員密碼，才能清除平台中所有使用者的資料。若有任何登記的 Windows 前憑證，系統也將提示您輸入系統 (Windows 前) 密碼。當您清除所有使用者資料時，ControlVault 管理員密碼和系統密碼將自動重設。請注意，這是清除 ControlVault 管理員密碼的唯一方法。

注意： 當您清除所有使用者資料，系統將提示您重新開機。請務必重新開機以便系統能正常運作。

若是要清除單一使用者的憑證，不需要設定 ControlVault 管理員密碼。當您按一下**「清除使用者資料」**，系統將提示您選取要清除哪些使用者的 ControlVault 憑證。選取使用者之後，系統將提示您輸入系統密碼 (只有在已登記 Windows 前憑證時)。

注意：

- 若您收到錯誤訊息指出無法建立 ControlVault 管理員密碼，則您必須將您的憑證存檔，清除 ControlVault 的所有使用者資料，重新開機，然後重新嘗試建立密碼。

- 若您收到錯誤訊息指出無法清除 ControlVault 的單一使用者憑證，則您必須將您的憑證存檔，試著清除所有使用者的資料，接著再重新嘗試清除該單一使用者的資料。
- 若您收到錯誤訊息指出無法清除 ControlVault 的所有使用者憑證，則您應考慮執行**系統重設**。**重要！** 請在執行重設之前檢閱「重設系統」說明主題，因為此操作會清除所有使用者的安全資料。
- 若您收到錯誤訊息指出無法備份 ControlVault 和 TPM 資料，請停用系統 BIOS 的 TPM。 進行的方式為將電腦重新開機，在電腦開機時按 **F2** 鍵進入 BIOS 設定，然後瀏覽至「安全」>「TPM 安全」。接著，重新啟用 TPM，然後重新嘗試將您的 ControlVault 資料存檔。
- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

Self-Encrypting Drive： 進階

Dell Data Protection | Access可管理自行加密磁碟的硬體式安全功能。自行加密磁碟在硬體中嵌入資料加密機制。這種管理可確保當磁碟鎖住功能啟用時，只有經過授權的使用者可以存取加密的資料。

裝置管理中的「Self-Encrypting Drive」視窗只有當系統中有一或多個自行加密磁碟 (SED) 時才會顯示。

重要！ 磁碟設定完成之後，自行加密磁碟資料保護以及磁碟鎖住功能會變成「啟用」。

磁碟管理

這些功能使磁碟管理員能夠管理磁碟安全設定。磁碟安全設定的變更會在磁碟關閉後生效。

資料保護

顯示自行加密磁碟資料保護的*啟用*或*停用*狀態。「啟用」狀態表示已設定磁碟安全，但是只要磁碟的*鎖住*功能沒有開啟，使用者不需要在存取 Windows 前階段進行磁碟的驗證。

您可以從這裡停用自行加密磁碟資料保護。此功能停用時，自行加密磁碟的所有進階安全功能會關閉，磁碟的功能將只限於標準磁碟。?停用資料保護也會刪除所有安全設定，包括磁碟管理員和磁碟使用者的憑證。但是此功能不會改變或移除磁碟上的任何使用者資料。

鎖住

顯示自行加密磁碟的*啟用*或*停用*狀態。如需有關鎖住磁碟行為的詳細資訊，請參閱 Self-Encrypting Drive 主題。

您可能需要從這裡暫時停用磁碟鎖住功能。我們不建議您這麼做，因為當磁碟鎖住停用時，不須要任何憑證即可存取磁碟，因此任何平台使用者皆可存取磁碟資料。停用磁碟鎖住不會刪除任何安全設定，包括磁碟管理員和使用者的憑證，或磁碟的任何使用者資料在內。

小心！若您要解除安裝 **Dell Data Protection | Access** 應用程式，必須先停用自行加密磁碟資料保護，並將磁碟解鎖。

磁碟管理員

顯示目前的磁碟管理員。磁碟管理員可從這裡變更要由哪一位使用者擔任磁碟管理員。新的管理員必須是系統中有效的 Windows 使用者，並具有管理員權限。系統中只能有一位磁碟管理員。

磁碟使用者

顯示已登記的磁碟使用者，以及目前已登記的使用者人數。能夠支援的最多使用者人數是以自行加密磁碟為依據 (目前 Seagate 磁碟支援 4 位使用者，Samsung 磁碟支援 24 位使用者)。

Windows 密碼 同步化

Windows 密碼同步化 (WPS) 功能將使用者的 Self-Encrypting Drive 密碼自動設定為與 Windows 密碼相同。不強制對磁碟管理員啟用此功能，它只適用於磁碟使用者。WPS 功能可用於必須定期變更密碼的企業環境 (例如每 90 天)。啟用此選項時，若 Windows 密碼發生變更，所有使用者的自行加密磁碟密碼將隨之自動更新。

注意： 當 Windows 密碼同步化 (WPS) 啟用時，使用者的 Self-Encrypting Drive 密碼無法變更，必須變更其 Windows 密碼才能使磁碟密碼自動更新。

記住上一次的使用者名稱
啟用此選項時，上一次輸入的使用者名稱將按預設顯示於 Windows 前驗證畫面的「**使用者名稱**」欄位中。

使用者名稱選項
啟用此選項時，使用者可以在 Windows 前驗證畫面的「**使用者名稱**」欄位中檢視所有的磁碟使用者名稱。

密碼刪除
此選項可用來「擦掉」 自行加密磁碟上的所有資料。 實際上資料並沒有刪除，而是刪除用來將資料加密的金鑰，使得資料無法使用。密碼經過刪除後，便無法再復原磁碟資料，此外， 自行加密磁碟資料保護會停用，而磁碟可以轉作其他用途。

注意：

- 若發生與自行加密磁碟管理功能有關的錯誤，請關閉電腦 (不要重新啟動系統)，然後重新開機。
- 如果您想要取得有關特定錯誤訊息的詳細資訊，請移至 wave.com/support/Dell。

驗證裝置資訊

裝置管理中的「驗證裝置資訊」視窗顯示系統中所有已連線驗證裝置 (例如指紋讀取機、傳統 Smartcard 或 Contactless Smartcard 讀取機) 的資訊與狀態。

技術支援

Dell Data Protection | Access

軟體的技術支援可於以下網站取得：http://www.wave.com/support.dell.com。

Wave TCG-Enabled CSP

Dell Data Protection | Access 應用程式包含 Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP)，只要需要 CSP 時即可使用，可選擇直接從應用程式呼叫或可從已安裝的 CSP 清單中選取。 在可行的情況下，選取 Wave TCG-Enabled CSP 以確定 TPM 產生金鑰，且金鑰與其密碼由 **Dell Data Protection | Access** 管理。

Wave Systems TCG-enabled CSP 使應用程式得以透過 MSCAPI 直接使用 TCG 相容平台所提供的功能。 此為增強的 TCG MSCAPI CSP 模組，不論特定廠商對於 Trusted Software Stack (TSS) 提供者的需求，在 TPM 上提供非對稱式金鑰功能並使用由 TPM 所提供的增強安全性。

注意： 若由 Wave TCG-enabled CSP 產生的 TPM 金鑰需要密碼，且使用者已建立了 TPM 主要密碼，則個別的金鑰密碼將隨機產生並儲存於 TPM 密碼保險庫中。