Dell Data Protection | Access 主页

Dell Data Protection | Access
主页是访问程序功能的第一站。 您可以从主页窗口访问以下内容：

System Access Wizard
访问选项
Self-Encrypting Drive
高级选项

窗口右下方有一个**高级**链接，单击此链接可访问高级选项。

从高级选项窗口，您可以单击右下方的**主页**链接返回到主页。

System Access Wizard

Dell Protection | Access 应用程序首次启动时，System Access Wizard 会自动启动。用户可以利用该向导对系统进行全方位安全设置，包括登录系统的方式（如仅密码进行登录，还是通过指纹和密码进行登录） 以及时间（Windows 启动时登录、Pre-Windows 登录还是两种情况下都登录）。另外，如果系统配置有 self-encrypting drive，则可以通过该向导对其进行配置。

管理员功能

只有系统上拥有 Windows 管理员权限的用户，才可使用 **Dell Data Access | Protection** 中普通用户无法使用的功能，包括：

- 设置/更改系统 (Pre-Windows) 密码
- 设置/更改硬盘密码
- 设置/更改管理员密码
- 设置/更改 TPM 所有者密码
- 设置/更改 ControlVault 管理员密码
- 重置系统
- 归档和恢复凭证
- 设置/更改 smartcard 管理员 PIN
- 清除/重设 smartcard
- 启用/禁用 Dell Windows 安全登录
- 设置 Windows 登录策略
- 管理 self-encrypting drive，包括：
    - 启用/禁用 self-encrypting drive 锁定
    - 启用/禁用 Windows 密码同步 (WPS)
    - 启用/禁用 Single Sign On (SSO)
    - 删除加密

远程管理

您所在的组织可以设置一个环境，以便于集中管理多个平台上 **Dell Data Protection | Access** 应用程序的安全功能（如远程管理）。 这种情况下，Active Directory 等 Windows 安全结构可用于安全管理 **Dell Data Protection | Access** 的特定功能。

计算机被远程管理（如 由远程管理员所有）时，**Dell Data Protection | Access** 的本地管理功能将被禁用；应用程序的管理窗口将无法在本地访问。下列功能可远程管理：

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows 登录
- 重置系统
- BIOS 密码
- Windows 登录策略
- Self-Encrypting Drive
- 指纹和 Smartcard 登记

有关使用 Wave Systems EMBASSY; Remote Administration Server (ERAS) 进行远程管理的详细信息，请与 Dell 销售人员联系或访问 dell.com。

访问选项

您可以从访问选项窗口设置系统访问权限的获取方式。

如果您设置了任何 **Dell Data Protection | Access**选项，以下标题将会显示在主页上，每个标题下会列出一些可操作选项（例如，更改 pre-Windows 的登录密码）。这些选项是执行特定任务（如更改 pre-Windows 密码或登记其他指纹）的快捷方式，单击会跳转至相应窗口。

常规
可用于指定登录 Windows、pre-Windows 或两个系统的时间和方式（例如通过指纹或密码登录）。您可以选择其中一项或两项作为登录方式，包括指纹、smartcard 和密码的组合。所列选项取决于系统所采用的登录策略，以及平台所支持的功能。

指纹
如果系统配置有指纹读取器，那么您可以登记或更新登录系统使用的指纹。登记完指纹后，您便可以在系统的指纹读取器上扫描已登记的指纹，以访问 Windows 或 pre-Windows 系统或同时访问两个系统（取决于您在“常规访问选项”中指定的系统）。更多信息，请参阅登记用户指纹。

Pre-Windows 登录
如果您已指定用户必须登录 pre-Windows，则必须设置访问 pre-Windows 的系统密码（也称作 pre-Windows 密码）。设置成功后，管理员可随时更改此密码。

您也可以禁用由此屏幕登录 pre-Windows。要执行此操作，您需要输入当前的系统密码，然后单击**禁用**按钮（如果验证该密码正确）。

Smartcard
如果您已指定要求用户必须使用 smartcard 登录，则必须登记一个或多个传统（接触式）或 contactless smartcard。单击**登记另一个 smartcard** 链接可启动 smartcard 登记向导。上述的“登记”指设置 smartcard，以供登录时使用。

登记完 smartcard 后，您可以通过**更改或设置我的 smartcard PIN** 链接更改或设置 PIN 码。

Pre-Windows 登录

设置 pre-Windows 登录时，您必须在系统接通电源、Windows 加载之前提供认证信息（密码、指纹或 smartcard）。Pre-Windows 登录功能增强了系统的安全性，可防止未经授权的用户破坏 Windows 和访问计算机（如计算机失窃时）。

管理员可以通过Pre-Windows 登录窗口设置 pre-Windows 登录、创建或更改 pre-Windows（系统）密码；如果密码已设置，则可以通过该窗口禁用 pre-Windows 登录。设置 pre-Windows 登录时，系统会启动向导以指导用户完成下列设置：

- 系统密码： 设置访问 pre-Windows 使用的系统密码（也称 pre-Windows 密码）。在用户使用其它认证因子的情况下，此密码可用作备份（例如，在指纹传感器出现故障时访问系统）。
- 指纹或 Smartcard： 设置 pre-Windows 登录时使用的指纹或 smartcard，并且指定该认证因子是否会替换 pre-Windows 密码或用作其备份。
- Single Sign On： 默认情况下，您可以使用 pre-Windows 认证（密码、指纹或 smartcard）自动登录到 Windows（称为 "Single Sign On"）。要禁用该功能，请选中我想在 Windows 启动时再次登录复选框。
- 如果除了 pre-Windows 密码之外， BIOS 硬盘密码已设置，您也可以选择更改或禁用硬盘密码。

注意： 并非所有指纹读取器已启用 pre-Windows 认证功能。如果读取器不兼容，则只能登记登录 Windows 使用的指纹。要了解指定的指纹读取器是否兼容，请联系您的系统管理员或访问 support.dell.com，获取支持的指纹读取器列表。

禁用 Pre-Windows 登录

您也可以通过此窗口禁用 pre-Windows 登录；要执行此操作，您需要输入当前的 pre-Windows（系统） 密码，然后单击**禁用**按钮（如验证该密码正确）。请注意，禁用 pre-Windows 登录后，已登记的指纹或 smartcard 仍保持已登记状态。

登记/删除指纹

用户可以注册或更新指纹，以便在 pre-Windows 或 Windows
登录时用其向系统提供身份证明。在指纹选项卡中，手指图像显示已登记的手指（如有）。如单击**登记另一个**链接，系统将启动指纹登记向导，随后将指导用户开始登记过程。登记指保存要用于登录的指纹。要登记指纹，必须正确安装和配置有效的指纹读取器。

注意： 并非所有指纹读取器都可用于 pre-Windows 登录。如果您尝试通过不兼容的读取器登记 pre-Windows
登录时使用的指纹，系统将显示错误消息。要了解设备是否兼容，请联系您的系统管理员或访问 support.dell.com，获取支持的指纹读取器列表。

登记指纹时，系统将提示您输入 Windows
密码以验证身份。如果您的策略有要求，系统将提示您同时输入 Pre-
Windows（系统） 密码。如果指纹读取器出现故障，用户可输入 Pre-Windows
密码以获得系统的访问权限。

注意：

- 建议您在登记过程中至少登记两个指纹。
- 您必须先确保指纹已正确登记，然后才能启用指纹认证功能。
- 如果您更换了系统中的指纹读取器，则必须使用新的读取器重新登记指纹。建议不要在两个不同的指纹读取器之间来回切换。
- 登记指纹时如重复显示传感器丢失焦点消息， 可能意味着计算机无法识别指纹读取器。如果指纹读取器为外置读取器， 可以通过断开读取器与计算机的连接，然后重新连接来解决此问题。

清除已登记的指纹
您可以通过单击指纹登记向导中的**删除指纹**链接或单击（以取消选择） 已登记的手指，来删除已登记的指纹。

如果用户已登记用于 pre-Windows
认证的指纹，管理员取消选择该用户登记的所有指纹可将其从系统中删除。

注意：如果您在指纹登记过程中遇到任何问题，请访问
wave.com/support/Dell，获取更多详细信息。

登记 Smartcard

您可以通过 **Dell Data Protection | Access** 选择使用传统（接触式） 或 contactless smartcard 登录到您的 Windows 帐户， 或在 pre-Windows 进行身份认证。 在 Smartcard 选项卡中，单击**登记另一个 smartcard** 链接可启动Smartcard 登记向导，随后将进入登记过程。登记指设置用于登录的 smartcard。

要执行登记操作，您必须正确安装和配置有效的 smartcard 认证设备。

注意： 要了解指定设备是否兼容，请联系您的系统管理员或访问 support.dell.com，获取支持的 smartcard 列表。

登记

登记 smartcard 时，系统将提示您输入 Windows 密码以验证身份。如果您的策略有要求，系统将提示您同时输入 Pre-Windows（系统） 密码。如果 smartcard 读取器出现故障，用户可输入 Pre-Windows 密码以获得系统的访问权限。

登记过程中，系统将提示您输入 smartcard PIN（如果已设置）。如果您的策略要求输入 PIN 但您尚未设置，系统将提示您创建一个。

注意：

- 无法删除为 pre-Windows 中所使用的 smartcard 登记的用户。
- 普通用户只可以更改 smartcard 上的用户 PIN， 而管理员既可以更改管理员 PIN，又可以更改 用户 PIN。
- 管理员还可以重置 smartcard；重置后，smartcard 在重新登记前，将无法在 Windows 登录或 pre-Windows 时用于身份认证。

注意：对于 TPM 证书认证，管理员可按照 Microsoft Windows smartcard 登记程序登记 TPM 证书。为了让系统与 Dell Data Protection | Access 应用程序兼容，管理员必须选择 "Wave TCG-Enabled CSP"（而不是 smartcard CSP）作为密码服务提供商。 此外，必须使用正确的客户端认证类型策略启用 Dell 安全登录。

注意：如果收到错误信息提示 Smartcard 服务未运行，则可以执行下列操作以启动/重启该服务：

- 导航至控制面板中的管理工具窗口，然后右键单击 Smartcard，选择启动或重启。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

Self-Encrypting Drive

Dell Data Protection | Access 在 self-encrypting drive
硬件内嵌入了数据加密功能，可管理驱动器基于硬件的安全功能。此管理功能可确保启用驱动器锁定后，只有授权用户才能访问加密数据。

单击 **Self-Encrypting Drive** 底部的选项卡可以进入 Self-Encrypting Drive
窗口。只有在系统配置有一个或多个 self-encrypting drive (SED) 时，此选项卡才会显示。

单击**设置**链接启动 Self-Encrypting Drive
设置向导。通过此向导，用户可创建和备份驱动器管理员码，并应用驱动器加密设置。只有系统管理员可以访问 Self-Encrypting Drive 设置向导。

重要！ 驱动器一经设置，即会“启用”数据保护和驱动器锁定功能。锁定驱动器后：

- 无论何时关闭驱动器电源，驱动器都将进入*锁定*模式。
- 如果用户未能在 Pre-Windows
  登录屏幕中输入正确的用户名和密码，驱动器将不会启动。启用驱动器锁定功能之前，计算机上的任何用户都可以访问驱动器上的数据。
- 即使作为辅助驱动器插入其他计算机，驱动器仍然处于安全状态；需经过身份验证才可访问其上的数据。

驱动器一经设置，Self-Encrypting Drive
窗口即会显示该驱动器，以及可供用户更改驱动器密码的链接。驱动器管理员还可以通过此窗口添加或删除驱动器用户。 已设置的外部驱动器会在此窗口中显示，用户可对其解除锁定。

注意： 要锁定外部辅助驱动器，必须断开其与计算机的连接并关闭电源。

驱动器管理员可以管理**高级>设备**中的驱动器设置。更多详细信息，请参阅 设备管理 - Self-Encrypting Drive。

驱动器设置

用户可以利用 Self-Encrypting Drive
设置向导设置驱动器。以下概念很重要，请在设置驱动器时谨记。

驱动器管理员
具有系统管理员权限、并设置了驱动器访问权限和管理员密码的第一个用户将成为驱动器管理员；管理员是唯一能够更改驱动器访问权限的用户。要确保将第一个用户设置为驱动器管理员，必须选中“我理解”复选框以继续此步骤。

驱动器管理员密码
该向导将提示用户创建驱动器管理员密码并再次输入以便确认。用户必须先输入 Windows
密码验证身份，然后才可创建“驱动器管理员”密码。当前 Windows
用户必须拥有管理员权限才可创建密码。

备份驱动器凭证
键入一个位置，或单击**浏览**按钮选择一个位置，以保存驱动器管理员凭证的备份。

重要**!**

- 强烈建议您对这些凭证进行备份，并将备份保存到除主硬盘驱动器以外的其它驱动器上（如可移动介质）。否则，如果您失去对驱动器的访问权限，您将无法访问这些备份。
- 驱动器设置一经完成，任何用户都在 Windows 加载之前先输入正确的用户名和密码（或指纹），才能在系统下一次启动时进入系统。

添加驱动器用户

驱动器管理员可以将其他有效的 Windows 用户添加至驱动器。将用户添加至驱动器时，管理员可以要求用户首次登录时重置密码。在驱动器解锁之前，系统会要求用户在 pre-Windows 认证屏幕上重置密码。

高级设置

- *Single Sign On* - 默认情况下，为认证驱动器而在 pre-Windows 中输入的 Self-Encrypting Drive 密码也将用于自动登录 Windows（这就称为 "Single Sign On"）。要禁用此功能，请在配置驱动器设置时，选中“我想在 Windows 启动时再次登录”复选框。
- *指纹登录* - 在支持此功能的平台上，您可以指定使用指纹（而非密码）认证 self-encrypting drive。
- *“睡眠”/“待机” (S3) 支持*（如果平台支持） - 如果启用此功能，您的 self-encrypting drive 可以安全地进入“睡眠”/“待机”模式（也称为 S3 模式）；当其从“睡眠”/“待机”模式恢复至正常工作模式时，需要进行 pre-Windows 认证。

注意：

- 启用 S3 支持后，驱动器加密密码受任何可能已存在的 BIOS 密码的限制。有关系统任何可能存在的特定 BIOS 密码限制的详细信息，请咨询系统硬件制造商。
- 并非所有 self-encrypting drive 都支持 S3 模式。在驱动器设置过程中，系统将提示您驱动器是否支持“睡眠”/“待机”模式。对于不支持此模式的驱动器，如果启用“休眠”模式（强烈建议在您的计算机上启用“休眠”模式），则 Windows 的 S3 请求会自动变为休眠请求。
- 设置 Single Sign On (SSO) 选项之后首次登录时，进程会在 Windows 登录提示出现时暂停。此时您需要输入 Windows 认证表单。表单内容将被安全存储，以备将来登录 Windows 时使用。系统下次启动时，SSO 会自动让您登录到 Windows。更改用户的 Windows 认证（密码、指纹、Smartcard PIN）也需要遵循相同的程序。 如果计算机 在一个域中，而该域要求登录 Windows 时按 ctrl+alt+del，则需要遵从此要求。

小心！如果要卸载 **Dell Data Protection | Access** 应用程序，必须先禁用 self-encrypting drive 数据保护功能并解除对驱动器的锁定。

Self-Encrypting Drive 用户功能

Self-encrypting drive
管理员可以对驱动器安全和用户进行全方位管理。非驱动器管理员的驱动器用户则只能执行以下任务：

- 更改自己的驱动器密码
- 解除对驱动器的锁定

这些任务可以通过 **Dell Data Protection | Access** 中的 **Self-Encrypting Drive** 选项卡访问。

更改密码
注册用户可利用此功能创建新的驱动器认证密码。用户必须先输入 Self-Encrypting Drive 的当前密码，然后才可设置新密码。

注意：

- 如果启用了 Windows 密码长度和复杂性策略，则此应用程序会实施这些策略。如果未启用 Windows 密码策略，则 Self-Encrypting Drive 密码的最大长度为 32 个字符。请注意，如果没有启用 S3 （“睡眠”/“待机”），则密码的最大长度为 127 个字符。
- 用户的 Self-Encrypting Drive 密码与 Windows 密码没有关联。 除非启用“Windows 密码同步”功能，否则当用户的 Windows 密码更改或重置时，不会影响到该用户的 Self-Encrypting Drive 密码。有关详细信息，请参阅设备： Self-Encrypting Drive。
- 某些非英语键盘设有一套不能在 self-encrypting drive 密码中使用的限制字符。如果 Windows 密码含有限制字符，在启用 Windows 密码同步的情况下，同步过程将失败，并会显示错误消息。

驱动器解锁：
注册用户可以利用驱动器解锁功能对锁定的驱动器进行解锁。如果启用了驱动器锁定功能，一旦关闭计算机电源，驱动器即进入锁定状态。系统重新接通电源后，用户必须在 pre-Windows 认证屏幕上输入密码对驱动器进行认证。

注意：

- 如果当前在计算机上激活了多个 self-encrypting drive 用户帐户，则可能无法进入省电模式（即“睡眠”/“待机”或“休眠”）。
- 在以下语言的应用程序本地化版本中，会使用 "User 1" 和 "User 2" 来替代 pre-Windows 认证屏幕中的驱动器用户名：中文、日文、韩文以及俄文。

高级选项

拥有管理员权限的用户可以使用 **Dell Data Protection | Access** 中的高级选项，管理下述应用：

维护
密码
设备

注意： 只有拥有管理员权限的用户可对“高级”选项进行修改。普通用户只能查看这些设置。

维护

管理员可通过维护窗口设置 Windows
登录首选项、重置系统以重新部署，以及归档或恢复存储于系统安全硬件中的用户凭证。有关详细信息，请参阅下列主题：

访问首选项
重置系统
凭证归档**& 恢复**

访问首选项

管理员可以从“访问首选项”窗口指定系统上所有用户的 Windows 登录首选项。

启用 Dell 安全登录
您可以通过“按 Ctrl-Alt-Del 替换标准 Windows 屏幕”选项，使用除 Windows 密码之外的其他认证因子访问 Windows。您可以将指纹添加为第二种认证因子，从而使 Windows 登录过程更加安全。此外，也可以添加包括 martcard 或 TPM 证书在内的其他认证因子登录 Windows。

注意：

- 启用 Dell 安全登录会影响系统上的所有用户。
- 建议用户登记完指纹或 smartcard 后，再启用此选项。
- 启用安全登录后，您在首次登录时，系统将提示您根据标准策略向 Windows 提供认证信息。下次启动时您需要使用新的认证因子进行登录认证。

禁用 Dell 安全登录
选择此项将禁用登录 Windows 的所有 **Dell Data Protection | Access** 功能。选定后，您需遵从先前的标准 Windows 登录策略。

注意：

- 尝试登录时，如果看到有关 Windows 安全登录的错误消息，请先禁用 Dell 安全登录选项，然后重新启用。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

重置系统

“重置系统”功能可用于清除平台上所有安全硬件的用户数据；例如，可重新部署计算机。此选项将清除系统中除 Windows 用户密码之外的所有密码以及硬件设备（如 ControlVault、TPM 和指纹读取器）中保存的数据。对于 self-encrypting drive，此功能将同时禁用数据保护，让您可以访问驱动器数据。

您必须先确认了解正在进行的系统重置操作，才能单击**下一步**。要重置系统，您需要输入每个安全设备的密码（如果已设置）：

- TPM 所有者
- ControlVault 管理员
- BIOS 管理员
- BIOS 系统 (pre-Windows)
- 硬盘 (BIOS)
- Self-Encrypting Drive 管理员

注意： 对于 self-encrypting drive，只要求输入硬盘管理员密码，而无需所有的硬盘用户密码。

重要！恢复系统重置时所清除数据的唯一途径是从之前保存的档案中恢复。如果您未创建档案，则无法恢复清除的数据。对于 self-encrypting drive，只会删除设置数据；驱动器上的个人数据不会删除。

凭证归档和恢复

使用凭证归档和恢复功能，可以备份和恢复存储在 ControlVault 与 Trusted Platform Module (TPM)
中的所有用户凭证（登录和加密信息）。重置计算机或由于硬盘错误要恢复数据时，需要使用这些数据，所以一定要对这些数据进行备份。这样就可以轻松将所有凭证从已保存的归档文件中恢复到新的计算机中。

您可以选择为系统上的单个或所有用户凭证进行归档或恢复。

用户凭证包含在 pre-Windows 中使用的数据，如存储在 TPM 中的已登记指纹、smartcard 数据和密钥。TPM 会根据安全应用程序的请求创建密钥，例如，生成数字证书会在 TPM 中创建密钥。

注意： 要确定 **Dell Data Protection | Access** 是否能归档 TPM 密钥，请查阅安全应用程序文档。 通常，支持使用 "Wave TCG-Enabled CSP" 生成密钥的应用程序。

归档凭证

要归档凭证，须执行以下操作：

- 指定归档凭证的对象是您自己，还是系统上的所有用户。
- 输入系统 (pre-Windows) 密码、ControlVault 管理员密码和 TPM 所有者密码，向安全硬件提供认证。
- 创建凭证备份密码。
- 使用**浏览**按钮指定档案位置。 档案位置必须是可移动的介质，如 USB 闪存驱动器或者网络驱动器，以防硬盘驱动器出现故障。

重要注意事项：

- 请记录档案位置，因为用户在恢复凭证信息时将会需要这些信息。
- 请记录凭证备份密码以确保数据可以恢复。因为此密码无法恢复，所以必须做好记录。
- 如果不知道 TPM 所有者密码，请联系系统管理员，或参考计算机的 TPM 设置说明。

恢复凭证

要恢复凭证，须执行以下操作：

- 指定恢复凭证的对象是您自己，还是系统上的所有用户。
- 浏览到档案位置，然后选择档案文件。
- 输入设置归档时创建的凭证备份密码。
- 输入系统 (pre-Windows) 密码、ControlVault 管理员密码和 TPM 所有者密码，向安全硬件提供认证。

注意：

- 如果收到错误消息提示凭证恢复失败，并且您已多次尝试恢复但仍然无法完成，请尝试恢复其它档案文件。如果仍然失败，请创建新的凭证档案，并尝试从该档案恢复数据。
- 如果收到错误消息提示无法恢复 TPM 密钥，请创建凭证档案，然后清除 BIOS 中的 TPM 。要清除 TPM，请重启您的计算机，在开始备份时按 **F2** 键进入 BIOS 设置并导航至安全 >TPM 安全。然后重新建立 TPM 所有权并再次尝试恢复凭证。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

密码管理

通过密码管理窗口，管理员能够创建或更改系统中的所有安全密码：

- 系统（也称 Pre-Windows）*
- 管理员*
- 硬盘*
- ControlVault
- TPM 所有者
- TPM Master
- TPM Password Vault
- Self-Encrypting Drive

注意：

- 密码管理窗口将只显示适用于当前平台配置的密码；该窗口随着系统配置和状态的变化而变化。
- 右上角带有 * 符号的密码为 BIOS 密码，可以通过 BIOS 系统进行更改。
- 如果 BIOS 管理员拒绝更改密码，则无法创建或更改 BIOS 级密码。
- 如单击 self-encrypting drive 的**设置**链接，将启动 Self-Encrypting Drive 设置向导；如单击**管理**，用户可以更改一个或多个 Self-Encrypting Drive 密码。
- 如单击 TPM Password Vault 的**管理**链接，系统将显示一个窗口，您可在其中查看或更改 TPM 密钥的保护密码。创建要求密码的 TPM 密钥时，密码将随机生成并存放于 vault。必须先创建 TPM 主密码，然后才可管理 TPM Password Vault。

Windows 密码 复杂性规则

Dell Data Protection | Access 可确保下列密码符合计算机的 Windows 密码复杂性规则：

- TPM 所有者密码

要定义计算机的 Windows 密码复杂性规则，请遵循以下步骤：

1. 进入“控制面板”。
2. 双击“管理工具”。
3. 双击“本地安全策略”。
4. 展开“帐户策略”并选择“密码规则”。

设备

管理员可使用“设备”窗口管理安装在其系统上的所有安全设备，并且可以查看每台设备的状态和其他详细信息，比如固件的版本。单击**显示**可查看每台设备的设备信息，单击**隐藏**可折叠此部分。管理员可管理以下几种设备，具体取决于平台包含哪些设备：

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive
认证设备信息

Trusted Platform Module (TPM)

必须启用 TPM 安全芯片并建立 TPM 所有权，才可使用 **Dell Data Protection | Access** 和 TPM 提供的高级安全功能。

只有当系统检测到 TPM 时，才会在**设备管理**中显示 Trusted Platform Module 窗口。

TPM 管理
系统管理员可以利用这些功能管理 TPM。

状态
显示 TPM 状态：*激活*或*未激活*。“激活”状态表明已在 BIOS 中启用 TPM 并可以对其进行设置（即，可以获取所有权）。如果 TPM 未激活（启用），则不能对 TPM 进行管理，也不能访问其安全功能。

如果系统检测到 TPM，但其未被激活（启用），则可以在此窗口中单击**激活**链接启用它，而无需进入系统 BIOS。使用此功能启用 TPM 后，必须重新启动计算机。重启过程中，有时会显示提示信息，要求您接受更改。

注意： 可能不是所有平台都支持从此应用程序启用（激活） TPM 。如果不支持，则必须在系统 BIOS 中启用 TPM。要执行此操作，请在 Windows 加载之前按 **F2** 键进入 BIOS 设置，然后导航至安全 > TPM 安全并激活 TPM。

您也可以在此处单击**取消激活**链接以*取消激活* TPM ；取消激活 TPM 后，其高级安全功能将不可用。但是，取消激活 TPM 不会更改任何 TPM 设置，也不会删除或更改任何存储在其中的信息或密钥。

所有
显示所有权（即“所有”） 状态，并可让您建立或更改 TPM 所有者。必须先建立 TPM 所有权，用户才可使用其安全功能。建立所有权之前，必须先启用（激活）TPM。

建立所有权的过程中，具备管理员权限的用户需 创建 TPM 所有者密码。 此密码一经定义，TPM 的所有权即已建立，TPM 可供使用。

注意： TPM 所有者密码必须符合系统的 Windows 密码复杂性规则。

重要！切勿丢失或忘记 TPM 所有者密码，因为只有通过此密码才可访问 **Dell Data Protection | Access** 中 的 TPM 高级安全功能。

已锁定
显示 TPM 状态：*已锁定*或*已解锁*。“锁定”是 TPM 的安全功能；当输入错误 TPM 所有者的次数达到指定数量后，TPM 将进入锁定状态。TPM 所有者可以在此处对 TPM 进行解锁；解锁需要输入 TPM 所有者密码。

注意：

- 如果收到错误消息提示无法建立 TPM 所有者，请清除系统 BIOS 中的 TPM 并尝试再次建立所有者。要清除 TPM，请重启计算机，开始备份时按 **F2** 键进入 BIOS 设置；然后导航至安全 TPM> 安全。

- 如果收到错误消息提示无法更改 TPM 所有者密码，请归档 TPM 数据（凭证档案），然后清除 BIOS 中的 TPM，重新建立 TPM 所有者并恢复 TPM 数据（恢复凭证）。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

Dell ControlVault

Dell ControlVault (CV) 是一种基于硬件的安全存储方案，用来存放 pre-Windows 登录过程中所使用的用户凭证（比如用户密码或已登记的指纹数据）。只有当系统检测到 ControlVault 时，才会在**设备管理**中显示 ControlVault 窗口。

ControlVault 管理

系统管理员可使用以下功能对系统的 controlVault 进行管理。

状态

显示 ControlVault 的状态：*激活*或*未激活*。如果状态显示为未激活，则表示您的系统未提供 controlVault 存储功能。请查阅 Dell 系统文档，确定系统是否配有 ControlVault。

密码

指示是否已设置 ControlVault 管理员密码；并允许您进行设置或更改（如果已设置）。只有系统管理员才可以设置或更改密码。设置 ControlVault 管理员密码后，才可执行以下操作：

- 归档或恢复凭证。
- 清除用户数据（所有用户）。

注意： 如果未设置 ControlVault 管理员密码，当管理员尝试执行归档或恢复操作时，系统将会提示创建管理员密码。

登记用户

指示用户是否登记了目前存储在 ControlVault 中的登录凭证（如密码、指纹或 smartcard 数据）。

清除用户数据

某些情况下，可能需要清除 ControlVault 中的数据；例如用户使用或登记 pre-Windows 凭证进行认证遇到困难时。在此窗口中，您可以清除单个用户或所有用户存储在 ControlVault 中的全部数据。

必须先输入 ControlVault 管理员密码，才能清除平台上的所有用户数据。如果登记了任何 pre-Windows 凭证，那么系统还将提示您输入系统 (pre-Windows) 密码。清除所有用户数据时，ControlVault 管理员密码和系统密码将重置。请注意，这是清除 ControlVault 管理员密码的唯一途径。

注意： 清除所有用户数据后，系统将提示您重新启动计算机。为了使系统正常运作，请务必重启计算机。

清除单个用户的凭证时无需设置 ControlVault 管理员密码。当您单击**清除用户数据**时，系统会提示您选择要清除 ControlVault 凭证的用户。选定用户后，系统将提示您输入系统密码（前提是 pre-Windows 凭证已登记）。

注意：

- 如果收到错误消息提示无法创建 ControlVault 管理员密码，则应执行以下操作：归档凭证；清除 ControlVault 中的所有用户数据；重新启动计算机；重新尝试创建密码。

- 如果收到错误消息提示无法从 ControlVault
  清除单个用户的凭证，则应执行以下操作：归档凭证；尝试清除所有用户数据；然后重新尝试清除单个用户数据。
- 如果收到错误消息提示无法从 ControlVault
  清除所有用户的凭证，则应考虑**重置系**统。**重要！** 重置系统之前，请查看重置系统帮助主题，因为此操作可清除所有 用户安全数据。
- 如果收到错误消息提示 ControlVault 和 TPM 数据无法备份，请在系统 BIOS 中禁用 TPM 。请按以下步骤执行：重启计算机；开始备份时按 **F2** 键进入 BIOS 设置；导航至安全>TPM 安全；然后重新启用 TPM 并再次尝试归档 ControlVault 数据。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

Self-Encrypting Drive：高级

Dell Protection | Access在 self-encrypting drive
硬件内嵌入了数据加密功能，可管理驱动器基于硬件的安全功能。此管理功能可确保启用驱动器锁定功能后，只有授权用户才能访问加密数据。

只有在系统配置有一个或多个 self-encrypting drive (SED) 时，**设备管理**的 Self-Encrypting Drive 窗口才会显示。

重要！ 驱动器一经设置，即会“启用”Self-encrypting drive 的数据保护和驱动器锁定功能。

设备管理
驱动器管理员可以利用这些功能管理驱动器安全设置。对驱动器安全设置所作的更改在驱动器关闭后即会生效。

数据保护
显示 self-encrypting drive
的数据保护状态：*启用*或*禁用*。“启用”状态表明驱动器安全已设置，但只有打开驱动器*锁定*后，用户才能在 pre-Windows 上对驱动器进行认证以便访问。

您可以在此处禁用 Self-encrypting drive 数据保护功能。禁用后，Self-encrypting drive 的所有高级安全功能将关闭，仅具备普通驱动器的功能。禁用数据保护也会删除所有安全设置，包括驱动器管理员和驱动器用户凭证。但是，此功能不会更改或删除驱动器上的任何用户数据。

锁定
显示 Self-encrypting drive 的状态：*启用*或*禁用*。有关锁定驱动器的操作信息，请参阅 Self-Encrypting Drive 主题。

必要时，您可以在此处暂时禁用驱动器的锁定功能。不建议禁用此功能。因为一旦禁用，访问驱动器就不需要凭证，因此所有平台上的用户都可以访问驱动器数据。禁用驱动器锁定功能不会删除任何安全设置，包括驱动器管理员和驱动器用户凭证，以及驱动器上的任何用户数据。

小心！如果要卸载 **Dell Data Protection | Access** 应用程序，必须先禁用 Self-encrypting drive 数据保护功能并解除对驱动器的锁定。

驱动器管理员

显示当前的驱动器管理员。驱动器管理员可以在此处将其他用户更改为驱动器管理员。新管理员必须是系统上具备管理员权限的有效 Windows 用户。系统只能有一个驱动器管理员。

驱动器用户

显示驱动器的注册用户以及当前注册的用户数量。可支持的最大用户数取决于 Self-encrypting drive（Seagate 驱动器支持 4 个用户，Samsung 驱动器支持 24 个用户）。

Windows 密码同步
Windows 密码同步 (WPS) 功能可自动将用户的 Windows 密码设置为 Self-Encrypting Drive 的密码。此功能并非针对驱动器管理员而提供，仅适用于驱动器用户。每隔一段特定时间（比如每

90 天）就必须更改一次密码的企业可以采用 WPS 功能；启用此选项后，如果用户的 Windows 密码更改，其 Self-encrypting drive 密码也会自动更新。

注意：启用 Windows 密码同步 (WPS) 功能后，用户的 Self-Encrypting Drive 密码不能直接更改；须先更改 Windows 密码让驱动器密码自动更新。

记住最后一个用户名
启用此选项后，默认会在 pre-Windows 认证屏幕的**用户名**字段中显示最后输入的用户名。

用户名选择
启用此选项后，用户可以查看 pre-Windows 认证屏幕**用户名**字段中的所有驱动器用户名。

加密删除
此选项可“清除” self-encrypting drive 上的所有数据。 但是并不能真正地删除数据，而只是删除用于加密数据的密钥，从而使数据不可用。加密删除后，驱动器上的数据将无法恢复，self-encrypting drive 数据保护会禁用，驱动器可重新部署。

注意：

- 如果遇到与 self-encrypting drive 管理功能相关的错误，请彻底关闭计算机（非重启），然后再重新开机。
- 有关特定错误消息的更多详细信息，请访问 wave.com/support/Dell。

认证设备信息

在**设备管理**的“认证设备信息”窗口中，显示了与系统连接的所有认证设备（如指纹读取器、传统或 contactless smartcard 读取器）的信息和状态。

技术支持

Dell Data Protection | Access 软件的技术支持可从 http://www.wave.com/support.dell.com 获得。

Wave TCG-Enabled CSP

Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) 随 **Dell Data Protection | Access** 应用程序一起提供，在需要 CSP 时可随时使用。它可以从应用程序直接调用，也可从已安装的 CSP 列表中选择。 在可能的情况下，选择 "Wave TCG-Enabled CSP" 以确保 TPM 生成密钥，并且密钥及其密码由 **Dell Data Protection | Access** 管理。

Wave Systems TCG-enabled CSP 使得应用程序能够直接通过 MSCAPI 利用兼容 TCG 平台上的可用功能。 这种 TCG 增强型 MSCAPI CSP 模块为 TPM 提供非对称的密钥功能，并充分利用 TPM 提供的加强安全性，而不受 Trusted Software Stack (TSS) 提供商的不同需求的影响。

注意：如果由 Wave TCG-enabled CSP 生成的 TPM 密钥需要密码、且用户已经创建了 TPM 主密码，则单个密钥密码将随机生成并存储于 TPM Password Vault 中。