Dell Data Protection

Security Tools 安装指南 v1.12 版

February 2017
Rev. A01

DELL EMC

注意、小心和警告

注：“注意”表示帮助您更好地使用该产品的重要信息。

小心：“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

警告：“警告”表示可能会导致财产损失、人身伤害甚至死亡。

目录

1

简介

Dell Data Protection | Security Tools 为 Dell 计算机管理员和用户提供安全与身份保护。DDP | Security Tools 预装在所有 Dell Latitude、Optiplex、 Precision 计算机以及精选的 Dell XPS 笔记本电脑上。如需*重新安装* DDP|Security Tools，请按照本指南中的说明执行操作。有关更多支持信息，请访问 www.dell.com/support > Endpoint Security Solutions。

概览

DDP | Security Tools 是一种端到端安全解决方案，旨在提供高级身份验证支持、预引导身份验证 (PBA) 支持以及自加密驱动器管理。

DDP | Security Tools 通过密码、指纹读取器和智能卡 (涵盖“非接触式卡”和“接触式卡”) 以及自行注册、一步登录 (单点登录 [SSO]) 和一次性密码 (OTP) 为 Windows 身份验证提供多重支持。

管理员可能需要使用 DDP Security Console 的管理员设置工具配置 Security Tools 的功能 (例如启用“预引导身份验证”和身份验证策略) ，最终用户才能使用 Security Tools。但如果采用默认设置，在安装和激活 Security Tools 后管理员和用户便可立即开始使用。

DDP Security Console

DDP Security Console 是 Security Tools 的界面，用户通过此界面可根据管理员设置的策略来注册、管理凭据以及配置自恢复问题。用户可访问 Security Tools 的这些应用程序：

- “加密”工具可供用户查看计算机驱动器的加密状态。
- “注册”工具可供用户设置和管理凭据，配置自恢复问题，查看其凭据注册状态。这些权限基于管理员设置的策略。
- Password Manager 可供用户自动填写和提交登录网站、Windows 应用程序和网络资源所需的各种数据。Password Manager 还为用户提供通过此应用程序更改其登录密码的功能，确保 Password Manager 所维护的登录密码与目标资源的登录密码保持同步。

管理员设置

“管理员设置”工具用于为该计算机的所有用户配置 Security Tools，允许管理员设置身份验证策略、管理用户以及配置可用于 Windows 登录的凭据。

通过“管理员设置”工具，管理员可启用加密和预引导身份验证 (PBA)，以及配置 PBA 策略和自定义 PBA 屏幕文本。

继续了解要求。

2

要求

- DDP | Security Tools 预装在所有 Dell Latitude、Optiplex、Precision 计算机以及精选的 Dell XPS 笔记本电脑上，并且满足以下最低要求。如果您需要重新安装 DDP | Security Tools，请确保您的计算机仍满足这些要求。有关更多信息，请参阅 www.dell.com/support > Endpoint Security Solutions。
- Windows 8.1 不应安装在自加密驱动器的驱动器 1 上。此操作系统配置不受支持，因为，Windows 8.1 会创建恢复分区驱动器 0，这继而会破坏预引导身份验证。正确的做法是，在配置为驱动器 0 的驱动器上安装 Windows 8.1，或者将 Windows 8.1 作为映像还原到任何驱动器。
- DDP | Security Tools 不支持动态磁盘。
- 配备自加密驱动器的计算机不能与硬件加密加速器 (HCA) 一起使用。由于不兼容，因此会妨碍 HCA 的功能。请注意，Dell 不售卖配备有支持 HCA 模块的自加密驱动器的计算机。此不受支持的配置将是售后配置。
- DDP | Security Tools 不支持多重引导磁盘配置。
- 在客户端上安装新操作系统之前，请在 BIOS 中清除可信平台模块 (TPM)。
- SED 不需要 TPM 提供高级身份验证或加密。

驱动程序

- 受支持的 Opal 兼容 SED 要求更新的 Intel 快速存储技术驱动程序，网址为 http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

注:

鉴于 RAID 和 SED 的特性，SED 管理不支持 RAID。SED 之所以发生“RAID=On”的问题，是因为 RAID 一开始就需要访问磁盘，以便在锁定的 SED 中不可用的高扇区上读写 RAID 相关数据，不能等待用户登录后才读取此数据。在 BIOS 中将 SATA 操作由“RAID=On”更改为“AHCI”可以解决这个问题。如果操作系统未预装 AHCI 控制器驱动程序，在从“RAID=On”切换为“AHCI”时操作系统将出现蓝屏。

客户端前提条件

- Security Tools 需要完整版的 Microsoft .Net Framework 4.5（或更高版本）。Dell 出厂的所有计算机均预装有完整版的 Microsoft .Net Framework 4.5。但是，如果是在非 Dell 硬件上进行安装，或是在较旧的 Dell 硬件上升级 Security Tools，则在安装 Security Tools 之前应验证所安装的 Microsoft .Net 版本并更新版本，以避免安装/升级失败。要安装完整版的 Microsoft .Net Framework 4.5，请转至 https://www.microsoft.com/en-us/download/details.aspx?id=30653

  要验证所安装的 .Net 的版本，请在要安装的目标计算机上按照这些说明操作：http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- 您计算机上的用于验证硬件的驱动程序和固件必须为最新的。要获取 Dell 计算机的驱动程序和固件，请转至 http://www.dell.com/support/home/us/en/19/Products/?app=drivers 并选择您的计算机型号。根据验证硬件，下载以下项：
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smartcard Driver
  - Dell ControlVault

  其他硬件供应商可能需要其各自的驱动程序。

如果计算机上尚未安装此组件，安装程序将进行安装：

前提条件
• Microsoft Visual C++ 2012 Update 4 或更新的可再发行软件包 (x86/x64)

软件

Windows 操作系统

下表详细介绍了受支持的软件。

Windows 操作系统（32 位和 64 位）
• Microsoft Windows 7 SP0-SP1 - 企业版 - 专业版 **注: 在 Windows 7 上支持传统引导模式。在 Windows 7 上不支持 UEFI。**
• Microsoft Windows 8 - 企业版 - 专业版 Windows 8（消费者） **注: 在使用 Opal 兼容 SED 和 Dell 计算机型号（支持 UEFI）的情况下，Windows 8 支持 UEFI 模式。**
• Microsoft Windows 8.1 - 8.1 Update 1 - 企业版 - 专业版 **注: 在使用 Opal 兼容 SED 和 Dell 计算机型号（支持 UEFI）的情况下，Windows 8.1 支持 UEFI 模式。**
• Microsoft Windows 10 版本 1511（11 月更新/Threshold 2） ○ 教育版 ○ 企业版 ○ 专业版 **注: 在使用 Opal 兼容 SED 和 Dell 计算机型号（支持 UEFI）的情况下，Windows 10 支持 UEFI 模式。**

移动设备操作系统

以下移动操作系统支持 Security Tools 一次性密码功能。

移动设备操作系统
Android 操作系统
• 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 操作系统
• iOS 7.x • iOS 8.x
Windows Phone 操作系统

移动设备操作系统
• Windows Phone 8.1 • Windows 10 Mobile

硬件

身份验证

下表详细介绍支持的身份验证硬件。

身份验证
指纹读取器
• 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 **注: 使用外部指纹读取器时，必须下载并安装您的特定读取器所需的最新驱动程序。**
非接触式卡
• 使用指定 Dell 笔记本电脑中内置非接触式卡读卡器的非接触式卡
智能卡
• 使用 ActivIdentity 客户端的 PKCS #11 智能卡 **注: ActivIdentity 客户端未预先加载，必须单独安装。**
• 通用访问卡（CAC） **注: 使用多证书 CAC，用户在登录时可从列表中选择正确的证书。**
• CSP 卡
• B 类/SIPR Net 卡

下表详细说明支持 SIPR Net 卡的 Dell 计算机型号。

Dell 计算机型号 - B 类/SIPR Net 卡支持		
• Latitude E6440 • Latitude E6540	• Precision M2800 • Precision M4800 • Precision M6800	• Latitude 14 Rugged Extreme • Latitude 12 Rugged Extreme • Latitude 14 Rugged

Dell 计算机型号 - UEFI 支持

在运行 Microsoft Windows 8、Microsoft Windows 8.1 和 Microsoft Windows 10（具有符合条件的 Opal 兼容 SED）的精选 Dell 计算机上，身份验证功能支持 UEFI 模式。运行 Microsoft Windows 7、Microsoft Windows 8、Microsoft Windows 8.1 和 Microsoft Windows 10 的其他计算机支持传统引导模式。

下表详细说明支持 UEFI 的 Dell 计算机型号。

Dell 计算机型号 - UEFI 支持			
• 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（型号 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 微型、小型塔式机箱、小型 • Optiplex 3046 • OptiPlex 3050 一体机 • OptiPlex 3050 塔式机、小型机、微型机 • Optiplex 5040 小型塔式机箱、小型 • OptiPlex 5050 塔式机、小型机、微型机 • OptiPlex 7020 • Optiplex 7040 微型、小型塔式机箱、小型 • OptiPlex 7050 塔式机、小型机、微型机 • Optiplex 3240 一体机 • OptiPlex 5250 一体机 • Optiplex 7440 一体机 • OptiPlex 7450 一体机 • OptiPlex 9020 Micro	• Venue Pro 11（型号 5175/5179） • Venue Pro 11（型号 7139）
注: 在运行 Windows 8、Windows 8.1 和 Windows 10（具有符合条件的 Opal 兼容 SED）的这些计算机上，身份验证功能支持 UEFI 模式。运行 Windows 7、Windows 8、Windows 8.1 和 Windows 10 的其他计算机支持传统引导模式。			

注: 在受支持的 UEFI 计算机上，从主菜单中选择重新启动后，计算机将重新启动，然后显示两个可能的登录屏幕之一。所显示的登录屏幕取决于计算机平台体系结构的差异。一些型号显示 PBA 登录屏幕；其他型号显示 Windows 登录屏幕。两种登录屏幕同样安全。

注:

确保 BIOS 中的“启用传统选项 ROM”设置已禁用。

要禁用“传统选项 ROM”：

1. 重新启动计算机。
2. 在重新启动期间，反复按下 **F12** 以打开 UEFI 计算机的引导设置。
3. 按向下箭头，高亮 **BIOS 设置**选项，然后按 **Enter**。
4. 选择**设置** > **常规** > **高级引导选项**。
5. 清除**启用传统选项 ROM** 复选框并单击**应用**。

Opal 兼容 SED

有关 SED 管理支持的 Opal 兼容 SED 的最新列表，请参阅以下 KB 文章：http://www.dell.com/support/article/us/en/19/SLN296720。

国际键盘

- 下表列出了支持在 UEFI 和非 UEFI 计算机上执行预引导身份验证的国际键盘。

国际键盘支持 - UEFI
○ DE-CH - 瑞士德语

国际键盘支持 - UEFI
○ DE-FR - 瑞士法语

国际键盘支持 - 非 UEFI
○ AR - 阿拉伯语（使用拉丁字母）
○ DE-CH - 瑞士德语
○ DE-FR - 瑞士法语

语言支持

DDP | Security Tools 是一种多语言用户界面 (MUI)，兼容和支持以下语言。

注:

俄语、繁体中文或简体中文不支持 UEFI 计算机中的 PBA 本地化。

语言支持	
• EN - 英语	• KO - 韩文
• FR - 法语	• ZH-CN - 简体中文
• IT - 意大利语	• ZH-TW - 繁体/中国台湾中文
• DE - 德语	• PT-BR - 巴西葡萄牙语
• ES - 西班牙语	• PT-PT - 葡萄牙（伊比利亚）葡萄牙语
• JA - 日语	• RU - 俄语

身份验证选项

以下身份验证选项要求具备特定硬件：指纹、智能卡、非接触式卡和 B 类/ SIPR Net 卡，并在 **UEFI 计算机上进行身份验证**。一次性密码功能要求 TPM 已存在、已启用且已有归属。有关更多信息，请参阅清除所有权并激活 TPM。TPM 2.0 不支持 OTP。下表显示了在满足硬件和配置要求的情况下，Security Tools 提供的身份验证选项（按操作系统显示）。

非 UEFI										
	PBA					Windows 身份验证				
	密码	指纹	接触式智能卡	OTP	SIPR 卡	密码	指纹	智能卡	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 Update 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

非 UEFI										
	PBA					Windows 身份验证				
	密码	指纹	接触式智能卡	OTP	SIPR 卡	密码	指纹	智能卡	OTP	SIPR 卡
1. 在受支持的 Opal SED 上可用。										

UEFI										
	PBA - 在受支持的 Dell 计算机上					Windows 身份验证				
	密码	指纹	接触式智能卡	OTP	SIPR 卡	密码	指纹	智能卡	OTP	SIPR 卡
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X
2. 在搭载了受支持 OPAL SED 的受支持 UEFI 计算机上可用。										

互操作性

解除配置和卸载 Dell Data Protection | Access

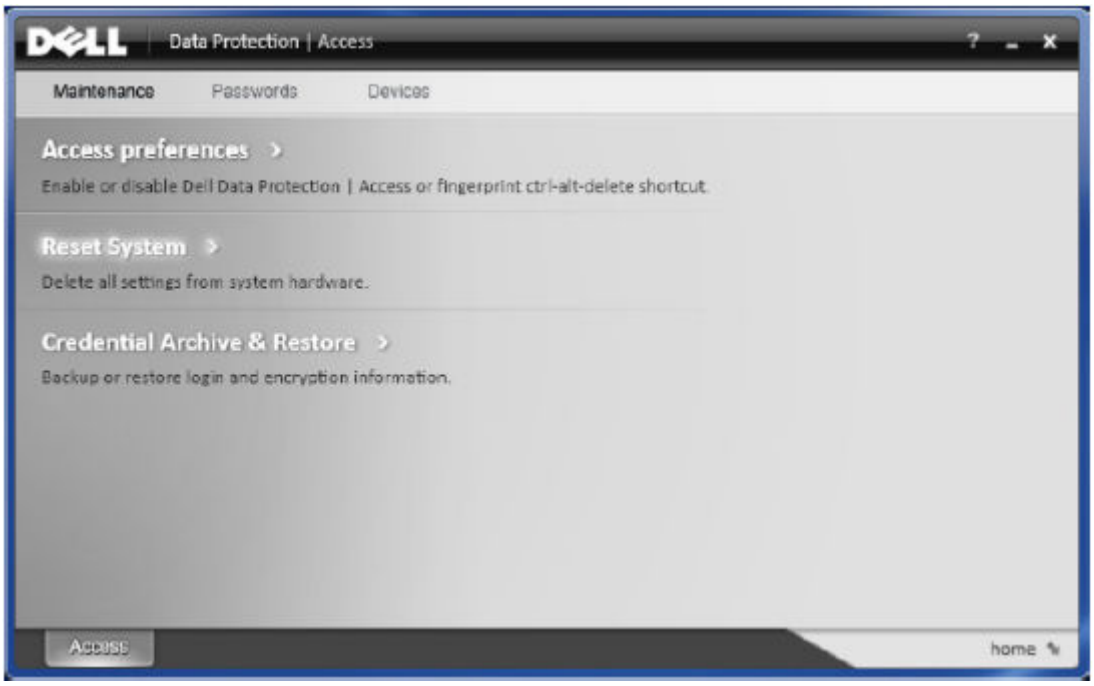
如果 DDP|A 现已安装在您的计算机上，那么在安装 Security Tools **之前**，必须解除配置由 DDP|A 管理的硬件，然后再卸载 DDP|A。如果 DDP|A 尚未使用，则可能只需卸载 DDP|A 并重新启动安装过程。

解除配置由 DDP|A 管理的硬件，包括指纹读取器、智能卡读卡器、BIOS 密码、TPM 和自加密驱动器。

注: 如果在运行 DDP|E 加密产品，请停止或暂停加密扫描。如果在运行 Microsoft BitLocker，应挂起加密策略。卸载 DDP|A 和取消挂起 Microsoft BitLocker 策略后，请按照 http://technet.microsoft.com/en-us/library/cc753140.aspx 上的说明初始化 TPM。

解除配置由 DDP|A 管理的硬件

1. 启动 DDP|A，然后单击**高级**选项卡。



2. 选择**重设系统**。这将要求您输入任意已配置凭据来验证身份。在 DDP|A 验证凭据后，DDP|A 将执行以下操作：
   - 从 Dell ControlVault 移除所有已配置凭据（如果存在）
   - 移除 Dell ControlVault 所有者密码（如果存在）
   - 从集成指纹读取器中移除所有已配置指纹（如果存在）
   - 移除所有 BIOS 密码（BIOS 系统、BIOS 管理员和 HDD 密码）
   - 清除可信平台模块
   - 移除 DDP|A 凭据提供程序

     解除配置计算机后，DDP|A 重新启动计算机以还原 Windows 默认凭据提供程序。

卸载 DDP|A

在解除配置身份验证硬件后，卸载 DDP|A。

1. 启动 DDP|A 并重设系统。

   此操作将移除 DDP|A 管理的所有凭据和密码，并清除可信平台模块 (TPM)。

2. 单击**卸载**以启动安装程序。
3. 完成卸载时，单击**是**以重新启动。

   注: 移除 DDP|A 还将解锁 SED，并移除预引导身份验证。

初始化 TPM

- 您必须是本地管理员组或同等组的成员。
- 计算机必须配备兼容的 BIOS 和 TPM。

如果使用一次性密码 (OTP) 则需要此任务。

- 请按照 http://technet.microsoft.com/en-us/library/cc753140.aspx 中的说明执行操作。

清除所有权并激活 TPM

要清除和设置 TPM 的所有权，请参阅 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2。

继续执行安装和激活。

3

安装和激活

本节详细介绍了如何在本地计算机上安装 DDP | Security Tools。要安装并激活 DDP | Security Tools，必须以管理员的身份登录计算机。

注:

在安装期间，请勿对计算机做出任何更改，包括插入或卸下外部 (USB) 驱动器。

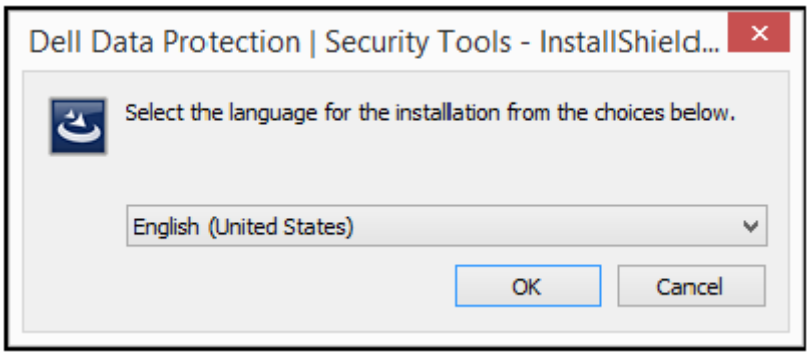
安装 DDP | Security Tools

要安装 Security Tools：

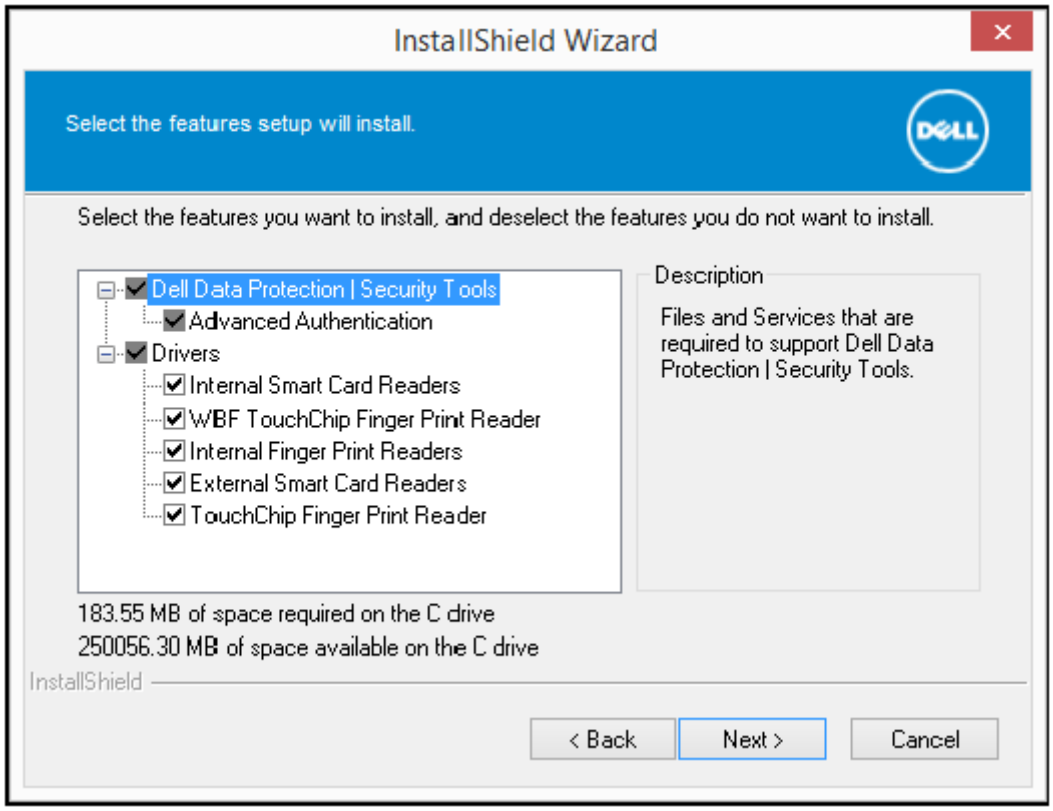
1. 找到 DDP | Security Tools 安装介质的安装文件。将其复制到本地计算机上。

   注: 安装介质可在以下位置找到：www.dell.com/support > Endpoint Security Solutions。

2. 双击该文件以启动安装程序。
3. 选择适当的语言，然后单击**确定**。



4. 显示“欢迎”屏幕时，单击**下一步**。
5. 阅读许可协议，同意其中的条款，然后单击**下一步**。
6. 单击**下一步**，在如下默认位置安装 Security Tools：`C:\Program Files\Dell\Dell Data Protection`。选择



7. 单击**安装**开始安装。
8. 完成安装后，需要重新启动计算机。选择**是**以重新启动，然后单击**完成**。

   安装完成。

激活 DDP | Security Tools

第一次运行 DDP Security Console 并且选择了“管理员设置”时，激活向导将引导您完成激活过程。

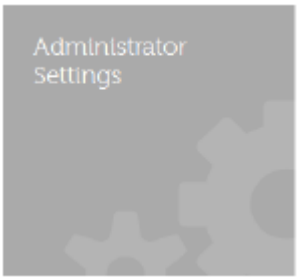
如果 DDP Security Console 尚未激活，最终用户仍可运行此工具。如果该最终用户是管理员激活 DDP | Security Tools 并自定义设置前首个使用 DDP Security Console 的人，此人将使用默认值。

要激活 Security Tools：

1. 以管理员的身份从桌面快捷方式启动 Security Tools。

注: 如果是作为普通用户登录（使用标准 Windows 帐户），必须提升 UAC 权限才能启动管理员设置工具。普通用户先要输入管理员凭据以登录此工具，然后根据提示再次输入管理员密码（即存储在管理员设置中的密码）。

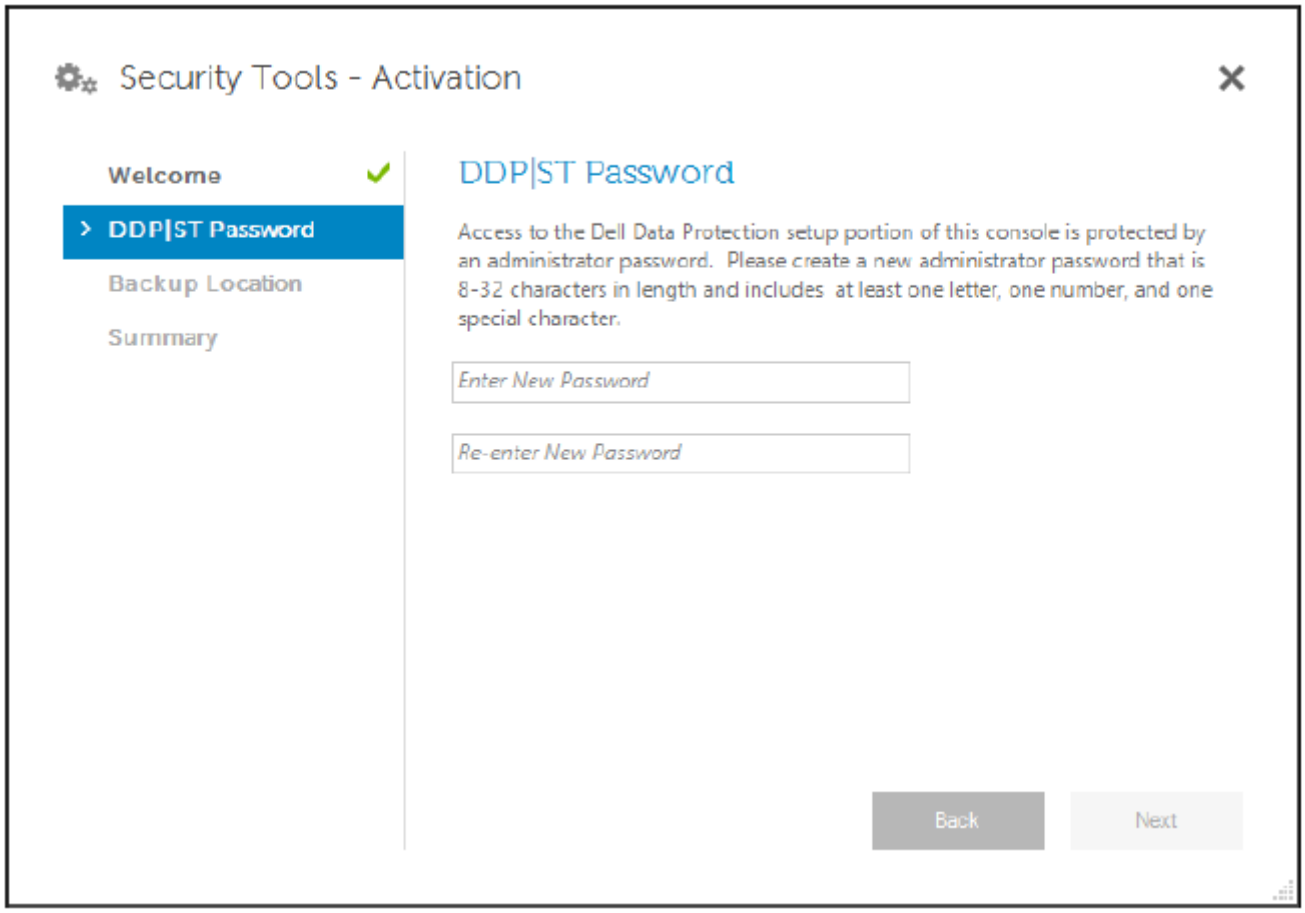
2. 单击**管理员设置**磁贴。



3. 在“欢迎”页面上，单击**下一步**。

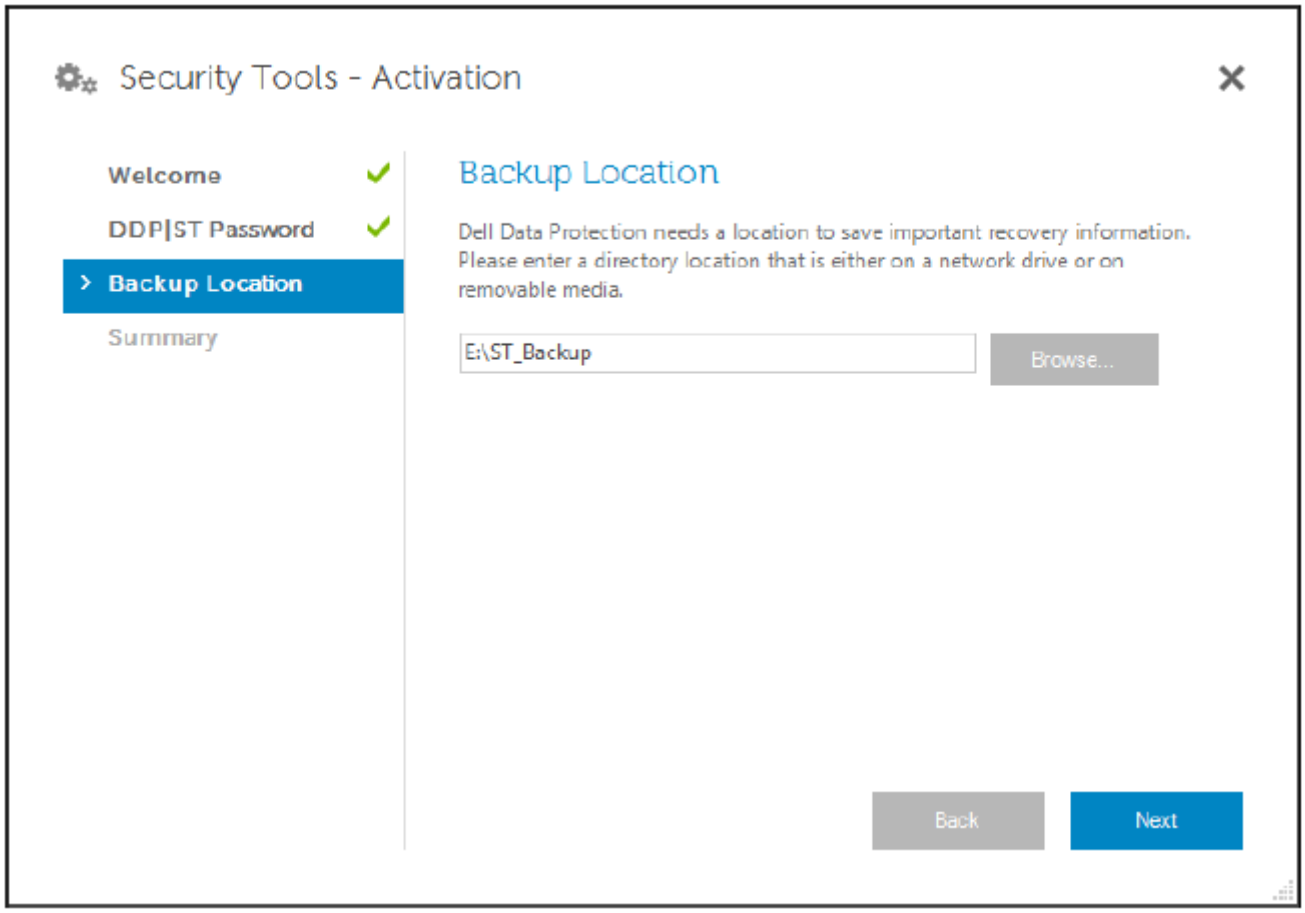
4. 创建 DDP | Security Tools 密码，然后单击**下一步**。

   必须先创建 DDP | Security Tools 管理员密码，然后才能配置 Security Tools。任何时候运行管理员设置工具均需提供此密码。密码必须为 8-32 个字符，其中至少包含一个字母、一个数字和一个特殊字符。



5. 在**备份位置**中，指定要写入备份文件的位置，然后单击**下一步**。备份文件必须保存在网络驱动器或可移动介质上。备份文件包含恢复此计算机上数据所需的密钥。Dell Support 必须要能访问此文件以帮助您恢复数据。

   恢复数据将自动备份到指定位置。如果该位置不可用（例如未插入备份 USB 驱动器），DDP | Security Tools 将提示您指定数据备份位置。要开始进行加密，需要访问恢复数据。



6. 在“摘要”页面，单击**应用。**

   Security Tools 激活完成。

   管理员和用户可立即开始使用 Security Tools 功能（基于默认设置）。

4

管理员配置任务

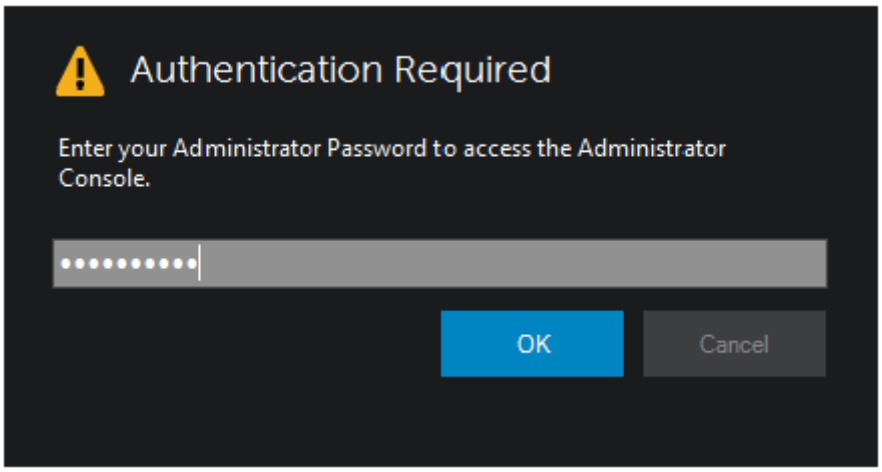
在激活 Security Tools 后，管理员和用户可在不进行其他配置的情况下，立即以默认设置使用 Security Tools。当用户使用其 Windows 密码登录到计算机时，用户将自动添加为 Security Tools 用户，但默认为不启用多重 Windows 身份验证。默认情况下也不会启用加密和预引导身份验证。

要配置 Security Tools 功能，必须在该计算机上具有管理员身份。

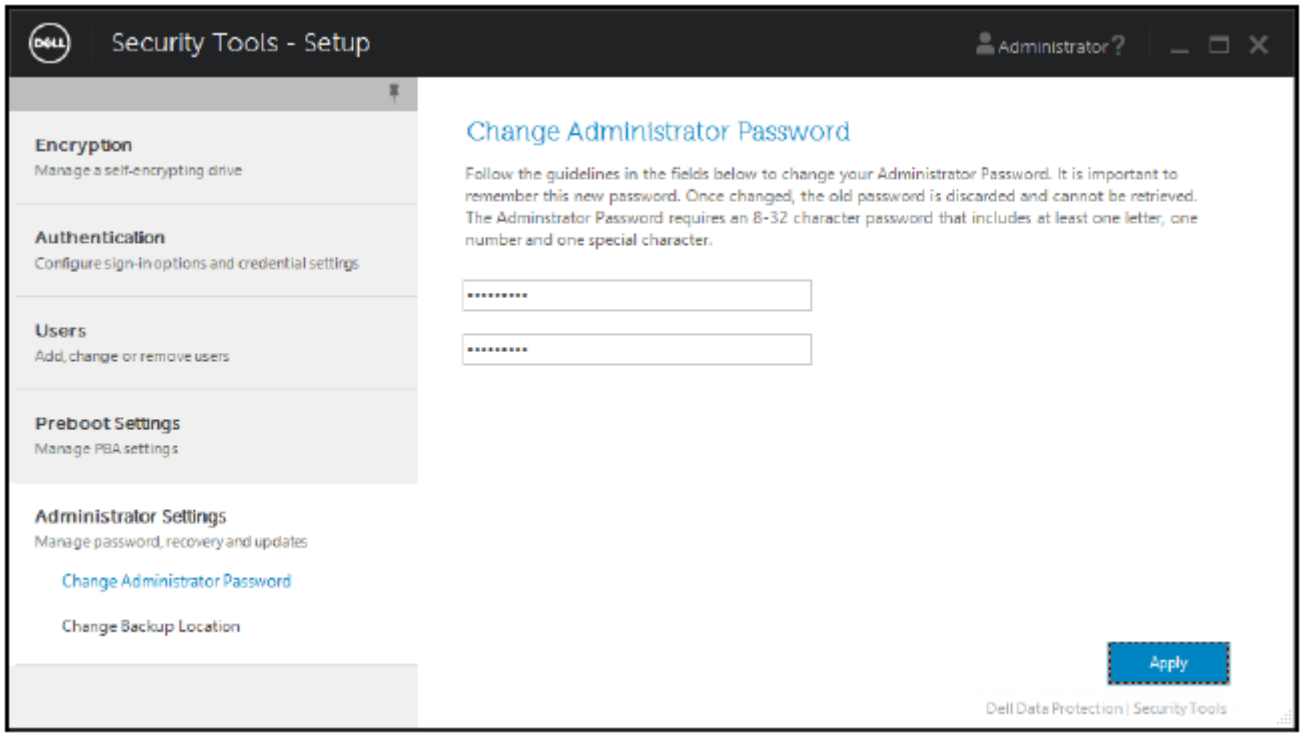
更改管理员密码和备份位置

激活 Security Tools 后，如有需要可更改管理员密码和备份位置。

1. 以管理员的身份从桌面快捷方式启动 Security Tools。
2. 单击**管理员设置**磁贴。
3. 在“身份验证”对话框中，输入激活过程中设置的管理员密码，然后单击**确定**。



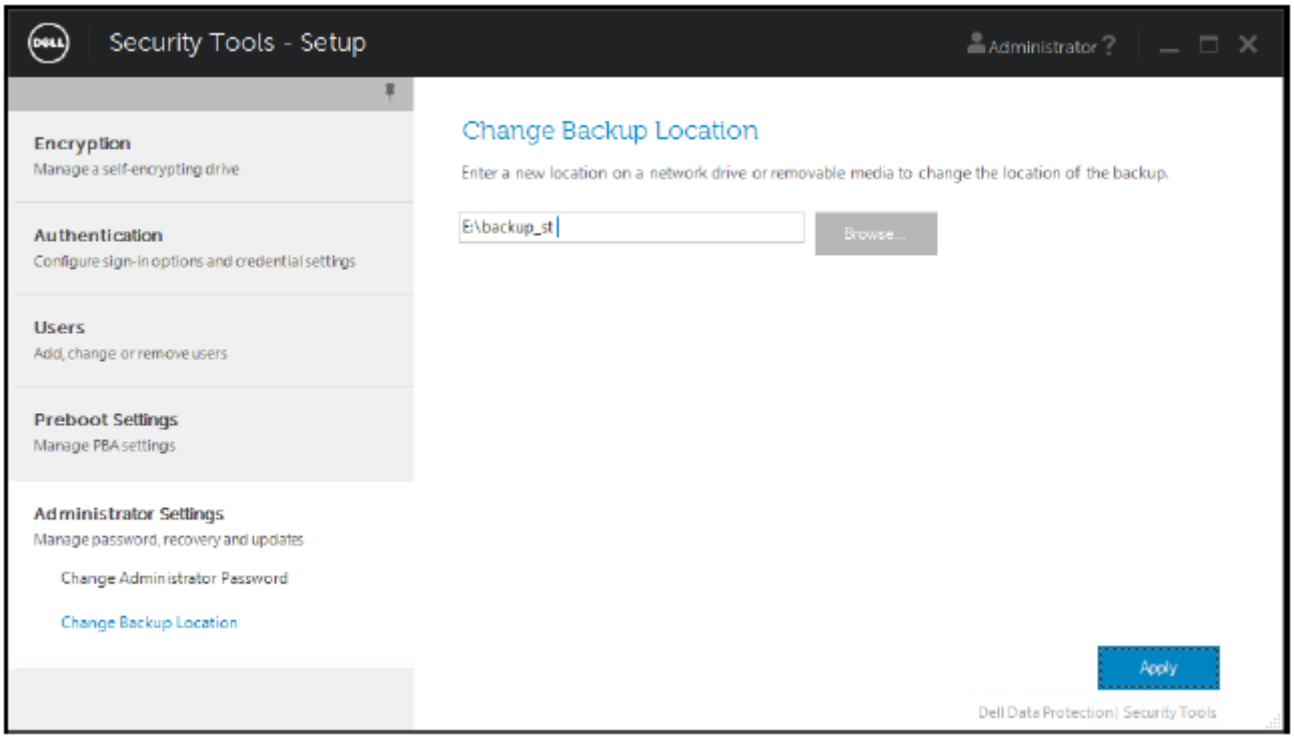
4. 单击**管理员设置**选项卡。
5. 在“更改管理员密码”页面，如果您要更改密码，请输入长度为 8 至 32 个字符的新密码，密码至少包含一个字母、一个数字和一个特殊字符。



6. 再次输入此密码进行确认，然后单击**应用**。
7. 要更改恢复密钥的存储位置，请在左侧窗格中选择**更改备份位置**。
8. 选择备份的新位置，然后单击**应用**。

   备份文件必须保存在网络驱动器或可移动介质上。备份文件包含恢复此计算机上数据所需的密钥。Dell ProSupport 必须能够访问此文件以帮助您恢复数据。

   恢复数据将自动备份到指定位置。如果该位置不可用（例如未插入备份 USB 驱动器），Security Tools 将提示您指定数据备份位置。要开始进行加密，需要访问恢复数据。



配置加密和预引导身份验证

加密和预引导身份验证 (PBA) 在配备有自加密驱动器 (SED) 的计算机上可用。加密和预引导身份验证二者均通过“加密”选项卡配置，只有计算机配备有自加密驱动器 (SED) 时“加密”选项卡方可见。启用加密或 PBA 二者之一时，另一个也随之启用。

在启用加密和 PBA 前，Dell 建议您注册并启用“恢复问题作为恢复选项”，以便在丢失密码后恢复密码。有关更多信息，请参阅配置登录选项。

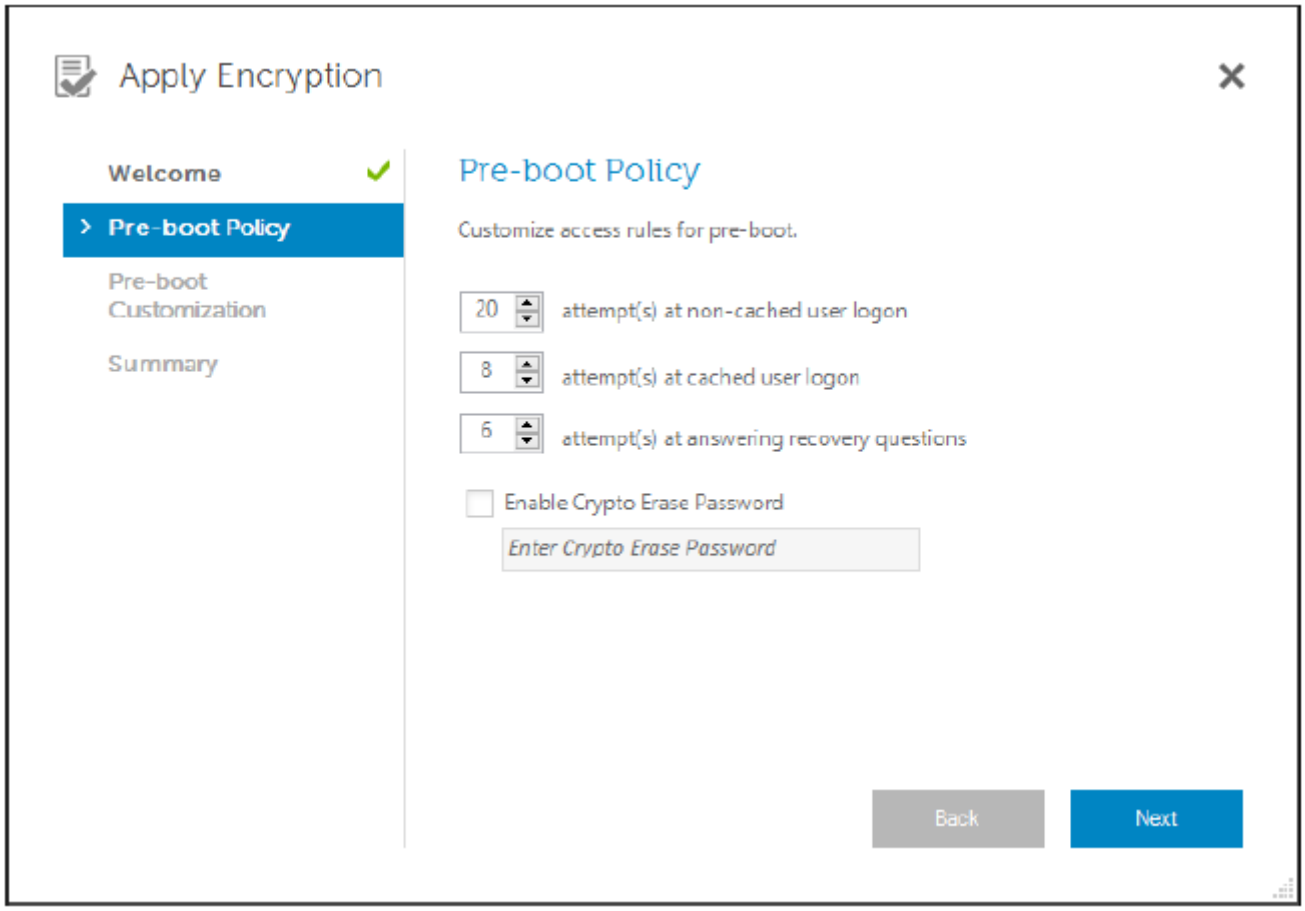
要配置加密和预引导身份验证：

1. 在 DDP Security Console 中，单击**管理员设置**磁贴。
2. 确保从该计算机可访问备份位置。

   注: 如果启用加密时显示消息“找不到备份位置”，而备份位置位于 USB 驱动器上，则表明驱动器未连接或者连接到的不是备份过程中使用的插槽。如果显示此消息，并且备份位置在网络驱动器上，表明从该计算机无法访问此网络驱动器。如果需要更改备份位置，请从管理员设置选项卡选择更改备份位置，以将位置更改为当前插槽或可访问的驱动器。重新指派位置后数秒，启用加密过程将继续。

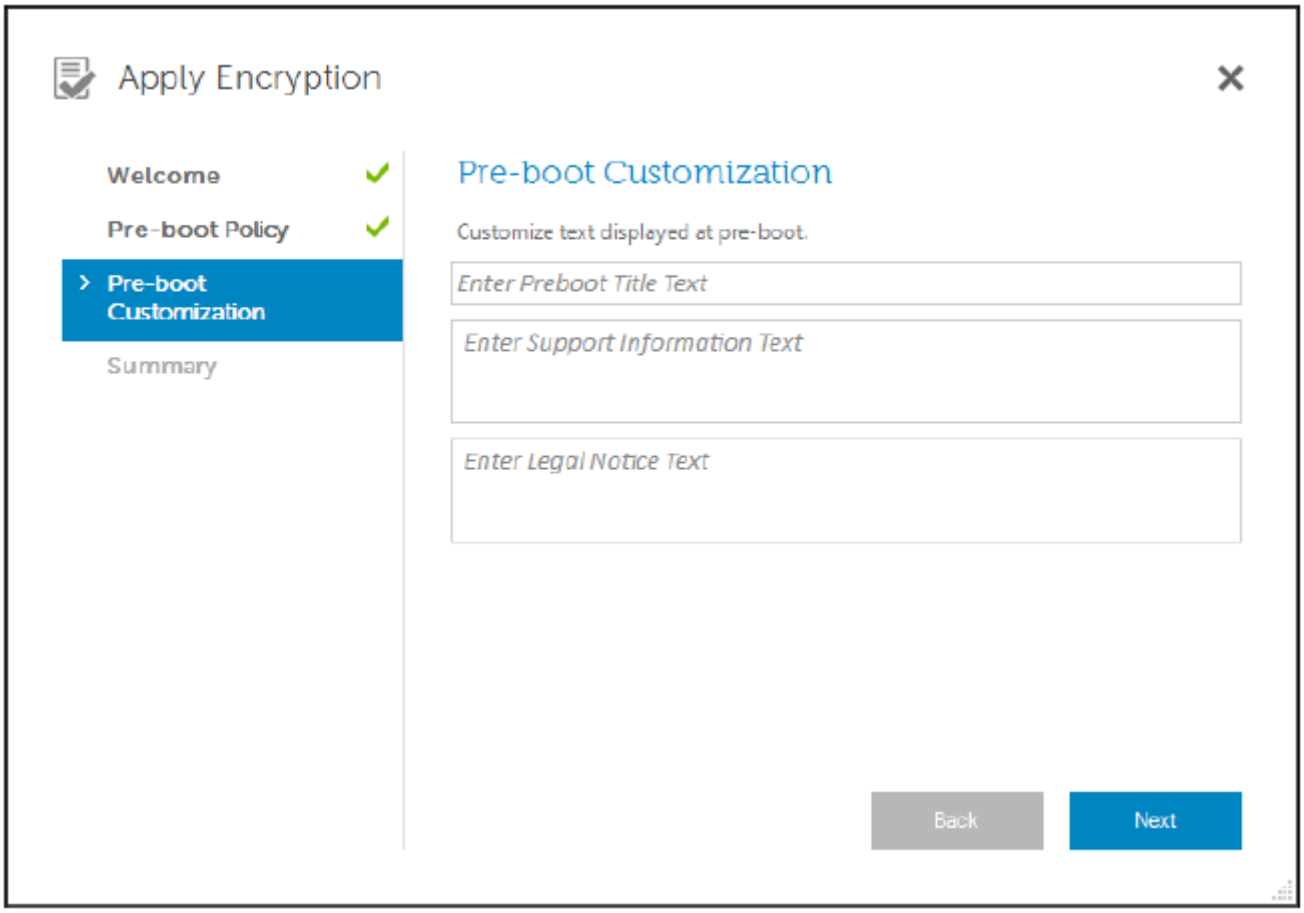
3. 单击**加密**选项卡，然后单击**加密**。
4. 在“欢迎”页面上，单击**下一步**。
5. 在“预引导策略”页面，更改或确认以下值，然后单击**下一步**。

非缓存用户尝试登录次数	未知用户（以前未登录到该计算机的用户 [尚未缓存任何凭据]）可尝试登录的次数。
缓存用户尝试登录次数	已知用户可尝试登录的次数。
回答恢复问题的尝试次数	用户可尝试输入正确答案的次数。
启用加密擦除密码	选择以启用此功能。
输入加密擦除密码	最多可包含 100 个字符的单词或代码，用作故障保护安全机制。在 PBA 身份验证过程中，如果在用户名或密码字段中输入此单词或代码，将删除所有用户的身份验证令牌并锁定该 SED。之后只有管理员才能强制解锁此设备。 如果您不想在紧急情况下设置加密擦除密码，可将此字段留空。



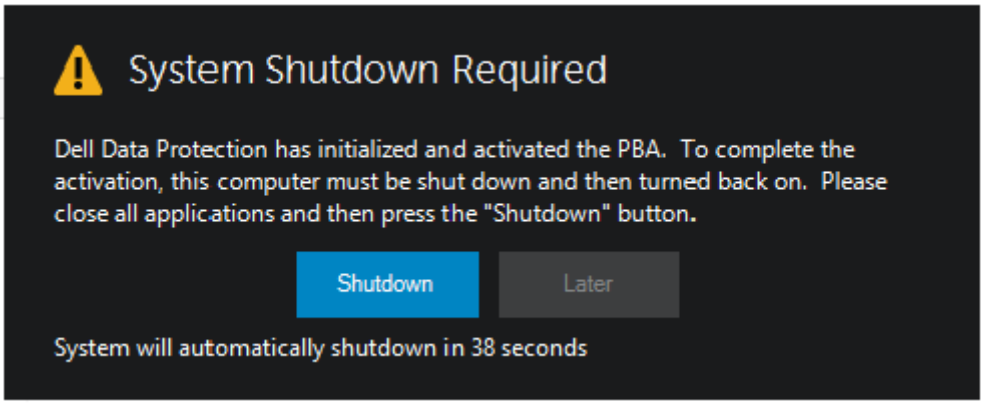
6. 在“预引导自定义”页面中，输入要在“预引导身份验证 (PBA)”屏幕上显示的自定义文本，然后单击**下一步**。

预引导标题文本	此文本显示在 PBA 屏幕顶部。如果将此字段留空，则不会显示标题。文本不换行，因此输入超过 17 个字符会导致文本被截断。
支持信息文本	此文本显示在 PBA 支持信息页面。Dell 建议您自定义消息，让其包含关于如何联系服务台或安全管理员的具体说明。如果未在此字段中输入文本，则不会为用户提供支持联系人信息。文本换行发生在单词级而非字符级。例如，如果您有一个长度超过约 50 个字符的单词，则不会换行，也不会显示滚动条，因此文本将被截断。
法律声明文本	在允许用户登录到设备之前显示的文本。例如：“单击‘确定’即表示您同意遵守可接受的计算机使用政策。”如果未在此字段中输入文本，则不会显示任何文本或“确定”/“取消”按钮。文本换行发生在单词级而非字符级。例如，如果您有一个长度超过约 50 个字符的单词，则不会换行，也不会显示滚动条，因此文本将被截断。



7. 在“摘要”页面，单击**应用**。
8. 显示提示时，单击**关机**。

   在开始加密前，需要进行一次完全关机。



9. 关机后，重新启动计算机。

   现在将由 Security Tools 管理身份验证。用户必须在“预引导身份验证”屏幕使用其 Windows 密码登录。

更改加密和预引导身份验证设置

首次启用加密并配置预引导策略和自定义后，可从“加密”选项卡执行以下操作：

- 更改预引导策略或自定义 - 单击**加密**选项卡，然后单击**更改**。
- 解密 SED，例如为了卸载 - 单击**解密**。

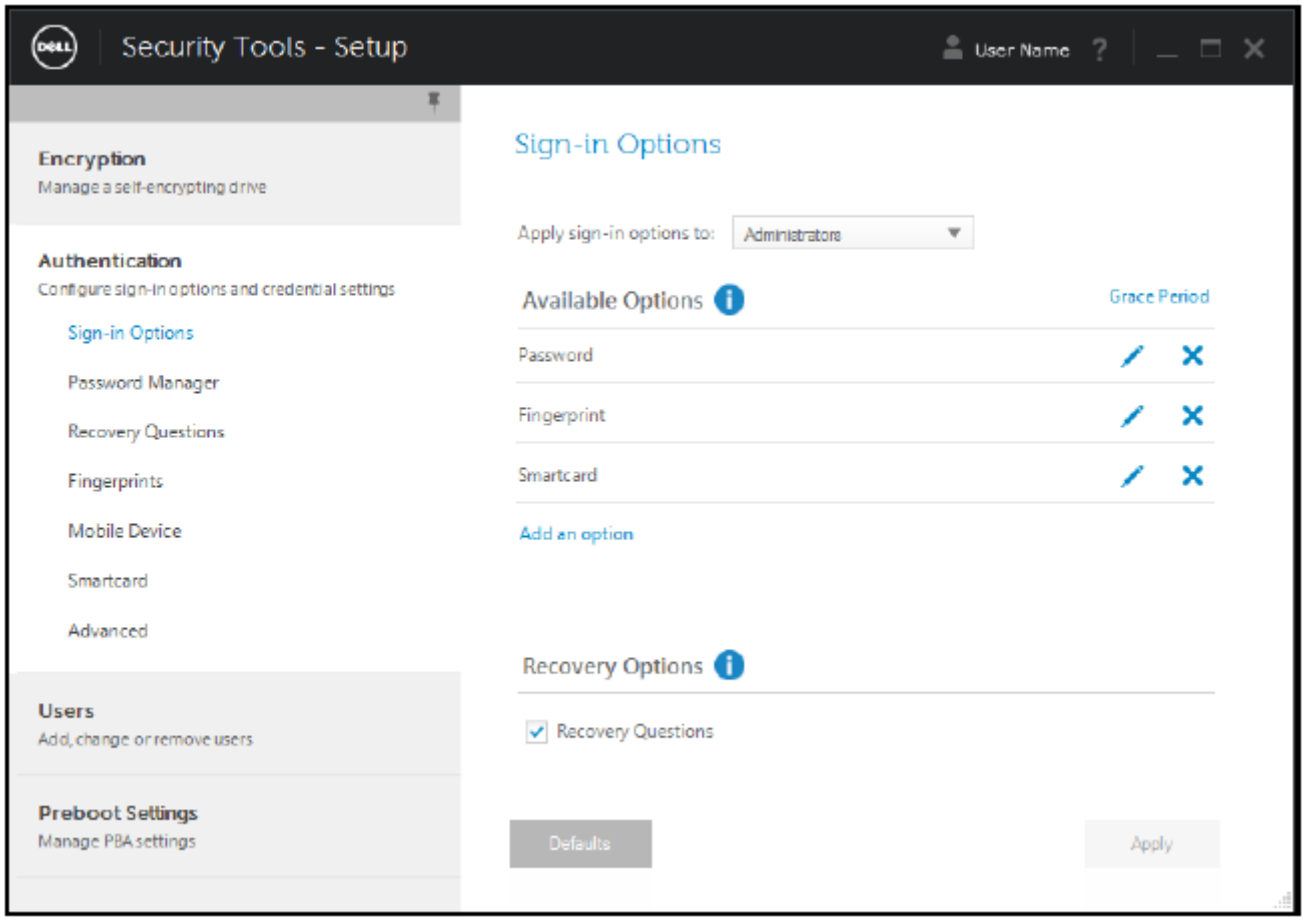
首次启用加密并配置预引导策略和自定义后，可从“预引导设置”选项卡执行以下操作：

- 更改预引导策略或自定义 - 单击**预引导设置**选项卡，然后选择**预引导自定义**或**预引导登录策略**。

有关卸载说明，请参阅卸载任务。

配置身份验证选项

管理员设置“身份验证”选项卡上的控件可用于设置用户登录选项及自定义每种选项的设置。



注: 如果 TPM 不存在、无归属或未启用，则“恢复选项”下将不会显示“一次性密码”选项。

配置登录选项

在“登录选项”页面，您可以配置登录策略。默认情况下，所有支持的凭据列示在“可用选项”中。

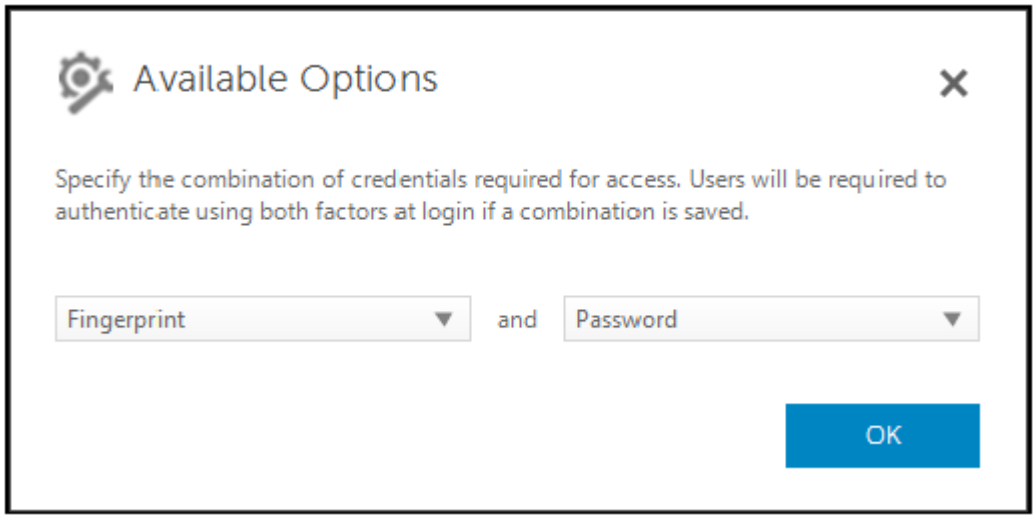
要配置登录选项：

1. 在左侧窗格中的“身份验证”下，选择**登录选项**。
2. 要选择您想设置的角色，请在**登录选项应用至**列表中选择角色：**用户**或**管理员**。您在此页面上进行的所有更改将仅应用于您选择的角色。
3. 设置身份验证的可用选项。

   默认情况下，每种身份验证方法配置为单独使用，不与其他身份验证方法结合使用。您可以按以下方式更改默认设置：

   - 要设置身份验证选项的组合，在“可用选项”下单击图标，以选择第一种身份验证方法。在“可用选项”对话框中，选择第二种身份验证方法，然后单击**确定**。

     例如，您可以要求同时将指纹和密码作为登录凭据。在对话框中，选择必须与指纹身份验证结合使用的第二种身份验证方法。



- 要允许每种身份验证方法单独使用，在“可用选项”对话框中，将第二种身份验证方法设置为**无**，然后单击**确定**。
- 要移除登录选项，在“登录选项”页面上的“可用选项”下，单击 **X** 以移除此方法。
- 要添加新的身份验证方法组合，请单击**添加选项**。

4. 为用户设置恢复问题，以在其被锁定时恢复对计算机的访问。
   - 要允许用户定义一组问题和回答以用于重新获得对计算机的访问，请选择**恢复问题**。

     要阻止使用恢复问题，请取消选择此选项。
   - 要允许用户使用移动设备恢复访问，请选择**一次性密码**。选择“一次性密码 (OTP)”作为恢复方法时，在 Windows 登录屏幕上将不会显示 OTP 作为登录选项。

     要使用 OTP 功能登录，请取消选择“恢复问题”中的选项。取消选择作为恢复方法时，只要至少有一个用户注册了 OTP，OTP 选项便将显示在 Windows 登录页面。

     注: 作为管理员，您可以控制一次性密码的用途 - 用于身份验证或用于恢复。OTP 功能可用于身份验证或用于恢复，但不能同时用于这两项用途。此配置影响该计算机的所有用户或所有管理员，具体取决于在“登录选项”字段中的选择 - 登录选项应用至。

     如果“恢复选项”下未列出“一次性密码”选项，表明您的计算机配置不支持此功能。有关更多信息，请参阅要求。
   - 如要求用户在丢失或忘记登录凭据时呼叫服务台，请取消选中“恢复选项”下的两个复选框“恢复问题”和“一次性密码”。
5. 要设置允许用户注册其身份验证凭据的时限，请选择**宽限期**。

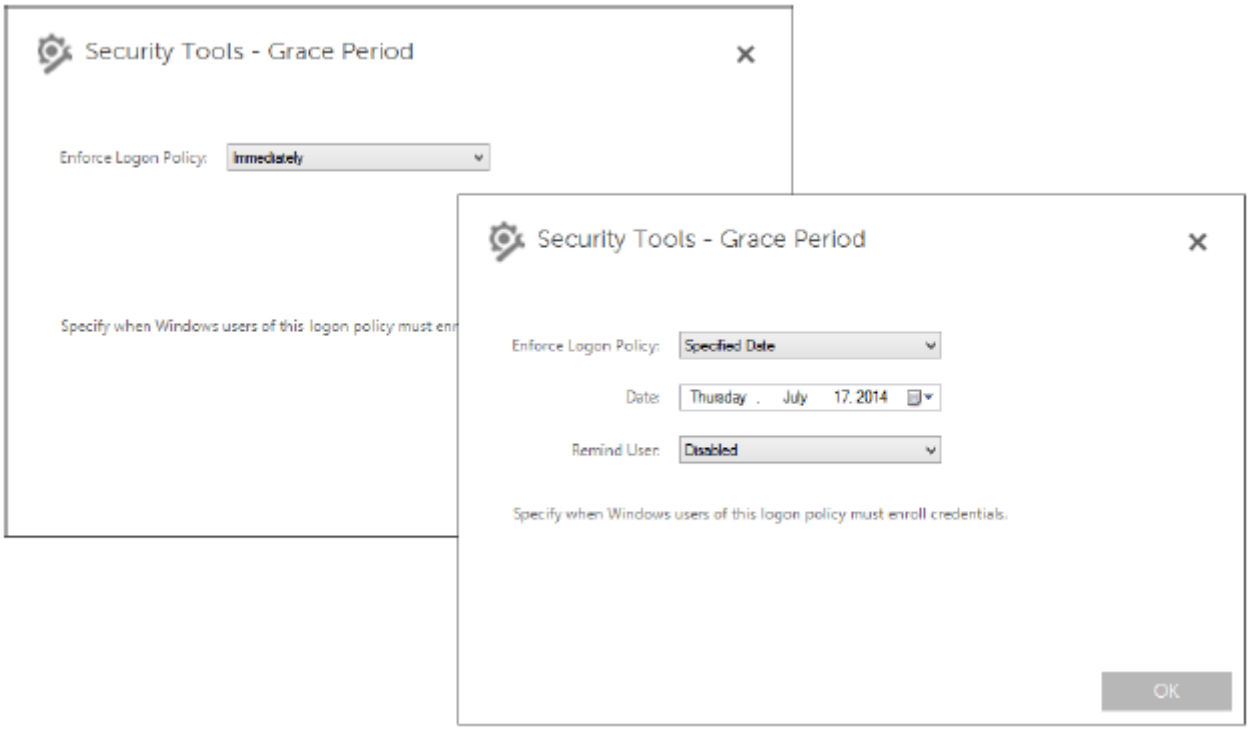
   宽限期功能可用于设置所配置的“登录选项”开始实施的日期。您可以在实施日期之前配置“登录选项”，然后设置允许用户注册的时限。默认情况下，策略将立即实施。

   要*立即*更改“登录选项实施日期”，请在“宽限期”对话框中单击下拉菜单，然后选择**指定日期**。单击日期字段右侧的向下箭头以显示日历，然后选择日历上的日期。策略的强制执行约在所选日期的凌晨 00:01 时开始。

   可以提醒用户在下次登录 Windows 时注册所需的凭据（默认设置），或者您也可以设置定期提醒。从*提醒用户*下拉列表选择提醒间隔时间。

   注:

   根据触发提醒时用户是位于 Windows 登录屏幕还是位于 Windows 会话中，向用户显示的提醒内容略有不同。提醒不会显示在“预引导身份验证”登录屏幕上。



宽限期期间的功能

在指定的宽限期内，每次登录后，当用户尚未注册更改的“登录选项”中所需的最低数量的凭据时，便会显示“附加凭据”通知。此消息的内容为：*有可用于注册的附加凭据。*

如有附加凭据可用但并不需要再提供凭据，当策略更改后，此消息只显示一次。

单击此通知可引起以下结果，具体取决于背景情况：

- 如果尚未注册任何凭据，屏幕上将显示设置向导，供管理员用户配置与计算机有关的设置，供用户注册最常用的凭据。
- 完成初始凭据注册之后，单击此通知将在 DDP 安全控制台中显示“安装向导”。

宽限期到期后的功能

在任何情况下，一旦宽限期到期，用户若不注册“登录选项”所要求的凭据，则无法登录。如果用户尝试使用不符合登录选项要求的凭据或凭据组合登录，在 Windows 登录屏幕顶部将显示设置向导。

- 如果用户成功注册所需凭据，则可登录到 Windows。
- 如果用户未成功注册所需凭据或是取消了向导，则将返回 Windows 登录屏幕。

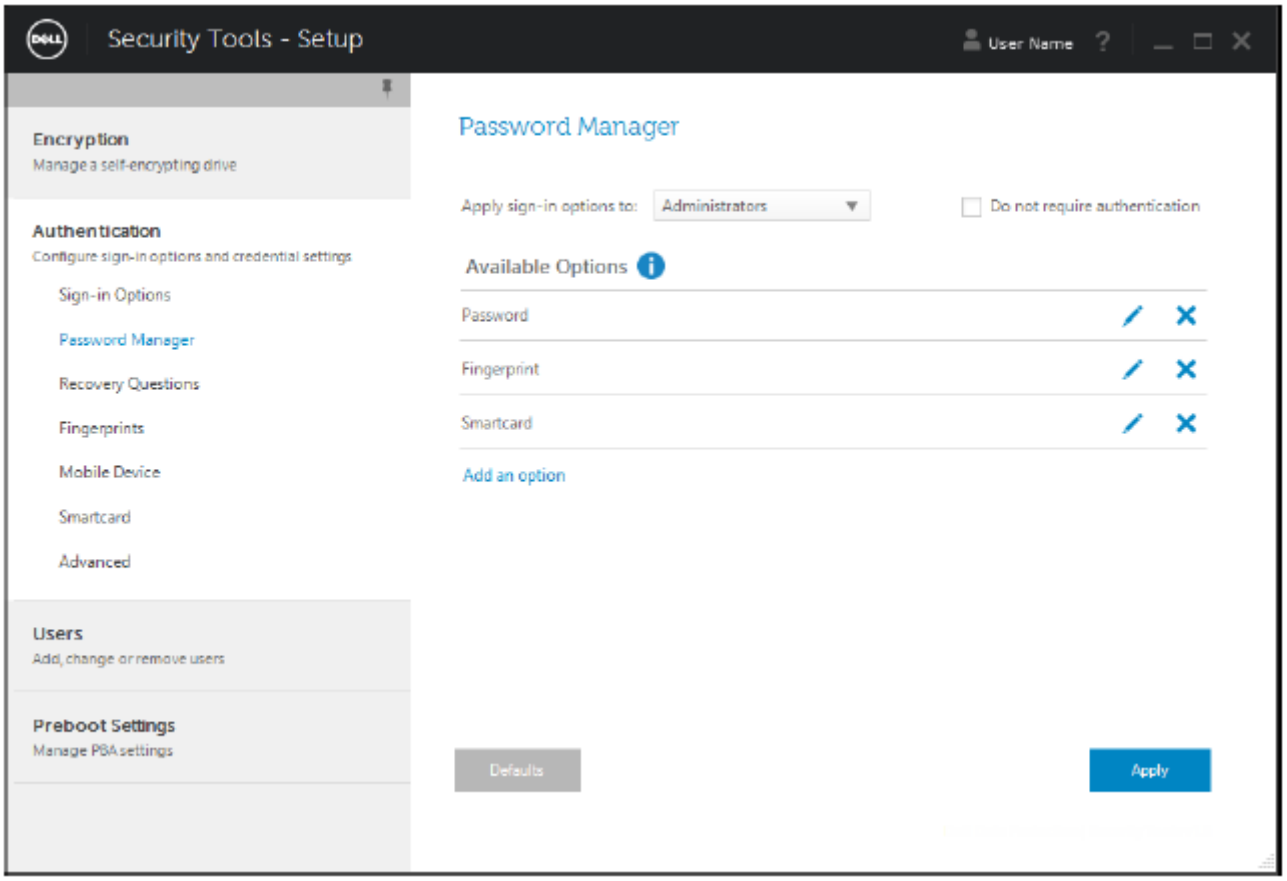
6. 要保存所选角色的设置，请单击**应用**。

配置 Password Manager 身份验证

在 Password Manager 页面中，您可以配置用户对 Password Manager 进行身份验证的方式。

要配置 Password Manager 身份验证：

1. 在左侧窗格中的“身份验证”下，选择 **Password Manager**。
2. 要选择您想设置的角色，请在**登录选项应用至**列表中选择角色：**用户**或**管理员**。您在此页面上进行的所有更改将仅应用于您选择的角色。
3. 或者选中**不要求身份验证**复选框，以允许选定的用户角色使用 Password Manager 中存储的凭据自动登录到所有软件应用程序和 Internet 网站。

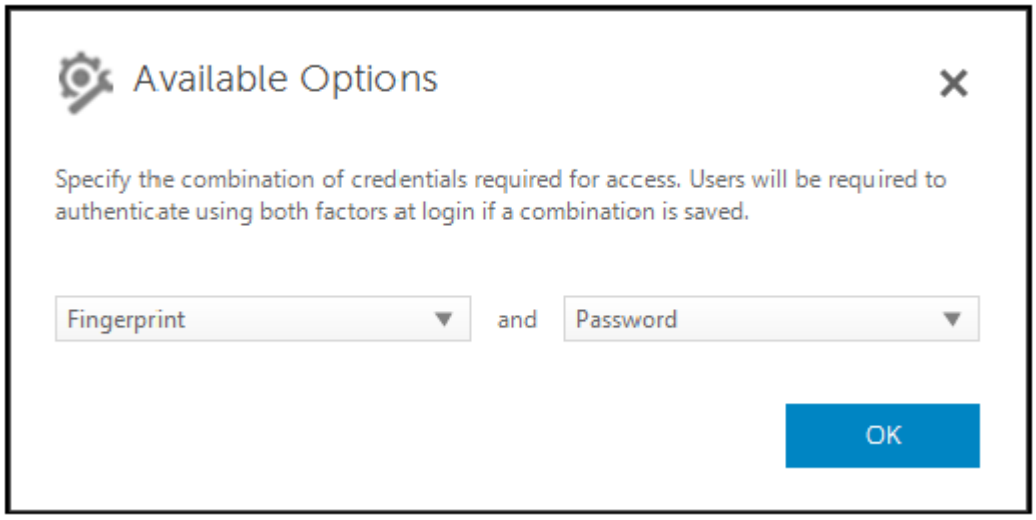


4. 设置身份验证的可用选项。

   默认情况下，每种身份验证方法配置为单独使用，不与其他身份验证方法结合使用。您可以按以下方式更改默认设置：

   - 要设置身份验证选项的组合，在“可用选项”下单击 ⁄ 图标，以选择第一种身份验证方法。在“可用选项”对话框中，选择第二种身份验证方法，然后单击**确定**。

     例如，您可以要求同时将指纹和密码作为登录凭据。在对话框中，选择必须与指纹身份验证结合使用的第二种身份验证方法。



   - 要允许每种身份验证方法单独使用，在“可用选项”对话框中，将第二种身份验证方法设置为**无**，然后单击**确定**。
   - 要移除登录选项，在“登录选项”页面上的“可用选项”下，单击 **X** 以移除此方法。
   - 要添加新的身份验证方法组合，请单击**添加选项**。

5. 要保存所选角色的设置，请单击**应用**。

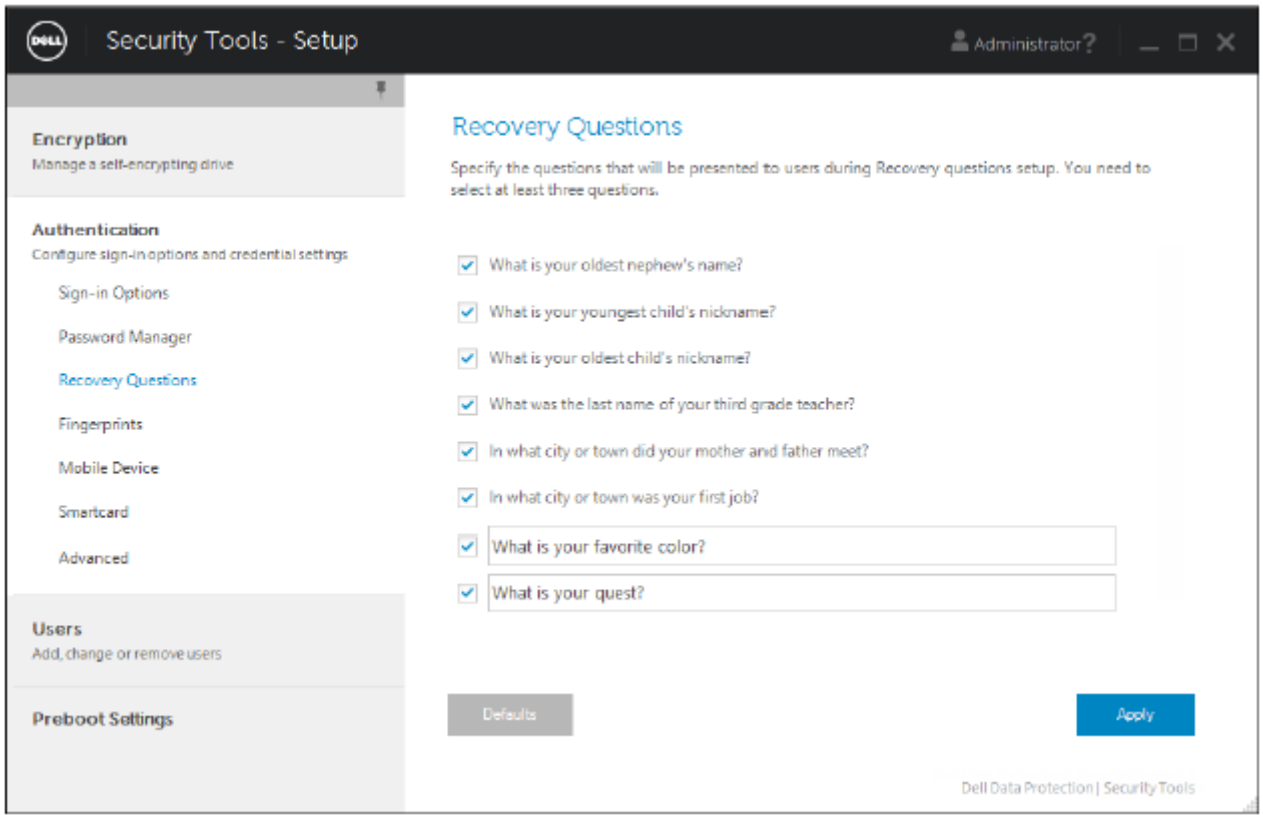
注: 选择“默认值”按钮将使设置恢复为初始值。

配置恢复问题

在“恢复问题”页面，您可以选择用户定义个人恢复问题及回答时要向其展示的问题。恢复问题能够让用户在密码过期或忘记密码时恢复对其计算机的访问。

要配置恢复问题：

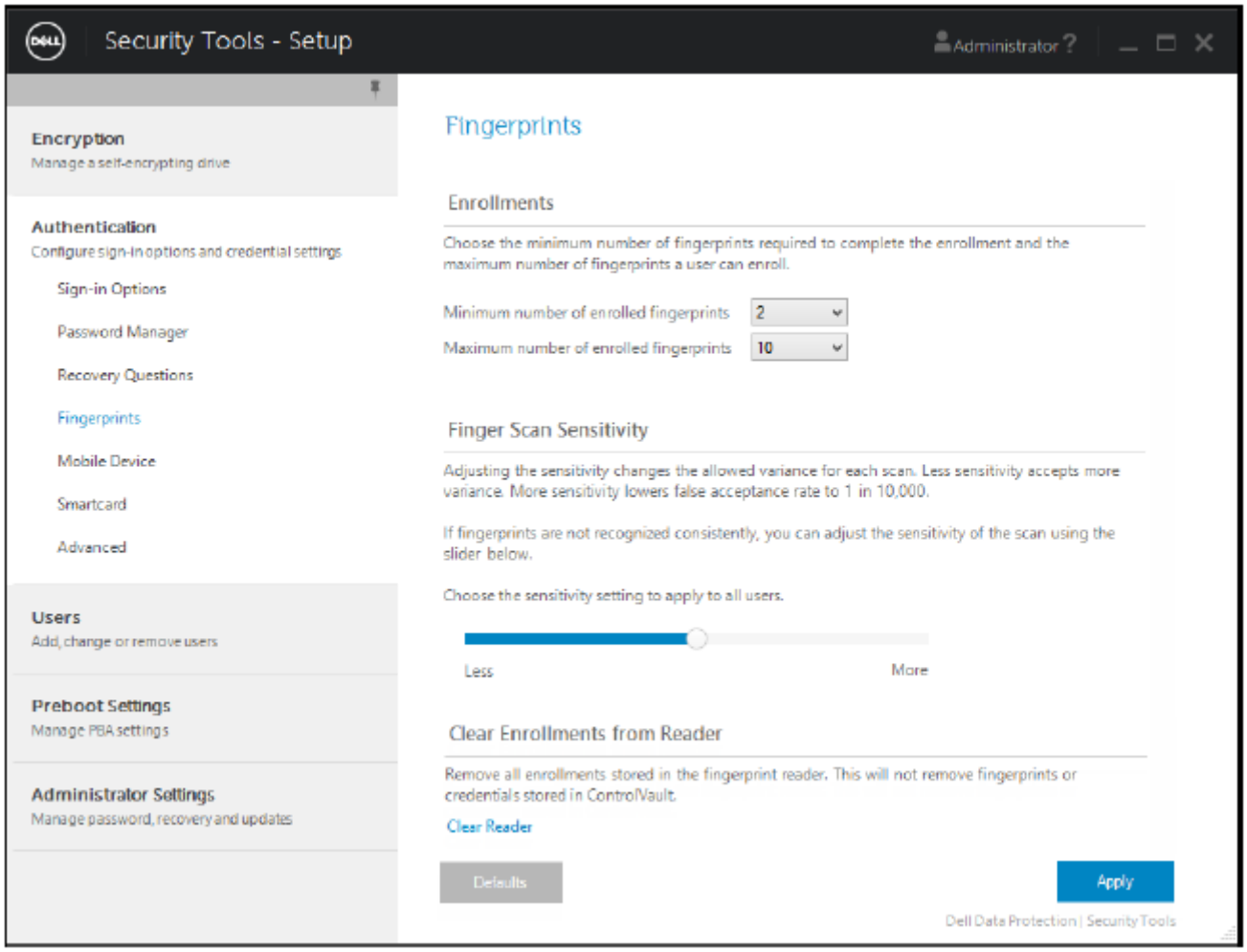
1. 在左侧窗格中的“身份验证”下，选择**恢复问题**。
2. 在“恢复问题”页面，选择至少三个预定义的恢复问题。
3. 您也可以向用户要从中选择的列表中添加多达三个自定义问题。
4. 要保存恢复问题，请单击**应用**。



配置指纹扫描身份验证

要配置指纹扫描身份验证：

1. 在左侧窗格中的**身份验证**下，选择指纹。
2. 在“注册”下，设置用户可以注册的最大和最小手指数目。



3. 设置指纹扫描灵敏度。

   灵敏度越低，容许的变化越大，接受错误扫描的可能性越高。采用最高设置时，系统可能会拒绝合格的指纹。灵敏度设置越高，容错率越低（低至万分之一）。

4. 要移除指纹读取器缓冲区中的所有指纹扫描和凭据注册，请单击**清除读取器**。此操作仅移除当前添加的数据，不会删除以前会话中存储的扫描和注册。
5. 要保存设置，请单击**应用**。

配置一次性密码身份验证

要使用一次性密码功能，用户应在其移动设备上使用 Security Tools Mobile 应用程序生成一次性密码，然后在计算机中输入此密码。此密码只能使用一次，并且只在有限的时段内有效。

为进一步增强安全性，管理员可以要求提供密码以确保此移动应用的安全。

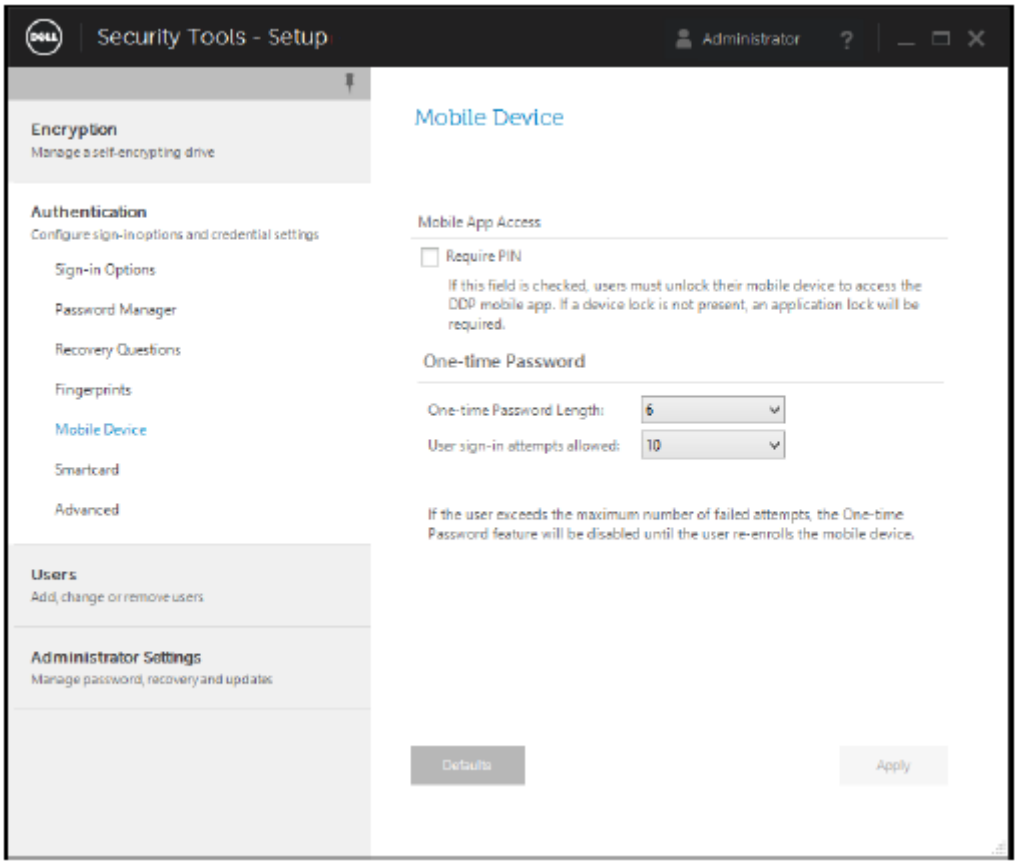
在“移动设备”页面，您可以配置设置以进一步增强移动设备和一次性密码的安全性。

要配置一次性密码身份验证：

1. 在左侧窗格中的“身份验证”下，选择**移动设备**。
2. 如要求用户输入密码以访问移动设备上的 Security Tools Mobile 应用，请选择**需要密码**。

   注: 在移动设备已向计算机注册后再启用*需要密码*策略，会导致所有移动设备被取消注册。启用此策略后，用户将需要重新注册其移动设备。

   选中**需要密码**复选框时，用户必须解锁其移动设备才能访问 Security Tools Mobile 应用。如果移动设备上未显示设备锁定，则需要提供密码。



3. 要选择一次性密码 (OTP) 的长度，请为**一次性密码长度**选择需要的密码字符数。
4. 要选择用户正确输入一次性密码的尝试次数，请为**允许用户尝试登录的次数**选择介于 **5** 至 **30** 之间的数值。

   达到最大尝试次数时，OTP 功能将被禁用，直至用户重新注册此移动设备。

   注: Dell 建议您除了设置一次性密码，至少还另外设置一种身份验证方法。

配置智能卡注册

DDP|Security Tools 支持两种智能卡：接触式卡和非接触式卡。

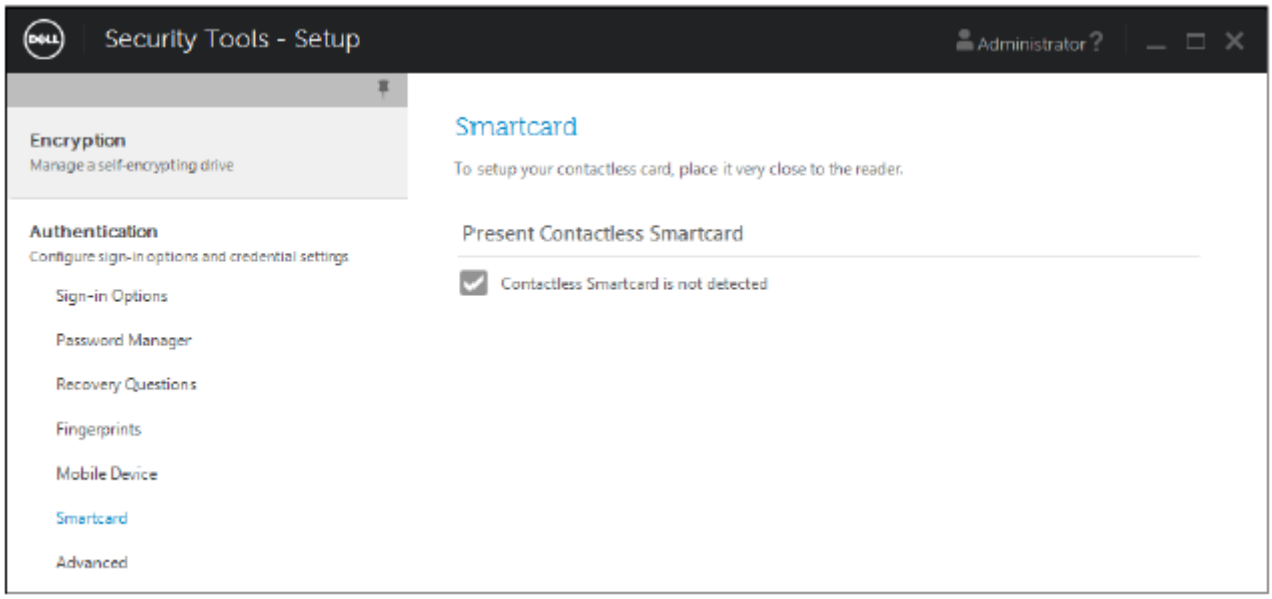
接触式卡需要使用智能卡读卡器供接触式卡插入。接触式卡只兼容域计算机。CAC 和 SIPRNet 卡均为接触式卡。鉴于这些卡的高级性，用户需要在使用卡登录后选择证书。

- 非域计算机以及使用域规范进行了配置的计算机支持非接触式卡。
- 每个用户帐户可注册一个接触式智能卡或注册多个非接触式卡。
- 预引导身份验证不支持智能卡。

注: 从注册了多个卡的帐户移除智能卡注册时，所有卡将同时取消注册。

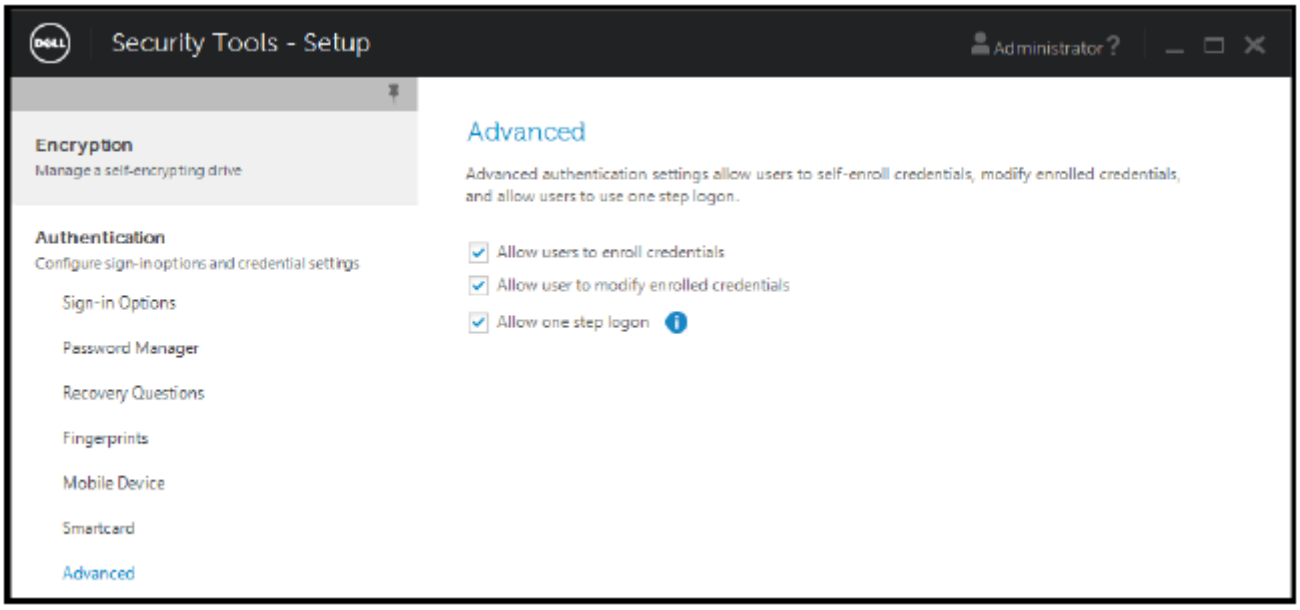
要配置智能卡注册：

在管理员设置工具的“身份验证”选项卡上，选择**智能卡**。



配置高级权限

1. 单击**高级**以修改高级最终用户选项。在*高级*下，您可以允许用户自行注册凭据（可选），或允许用户修改其注册的凭据（可选），并启用一步登录。



2. 选中或清除复选框：

   允许用户注册凭据 - 此复选框默认为选中。允许用户在没有管理员介入的情况下注册凭据。如果清除此复选框，则必须由管理员注册凭据。

   允许用户修改注册的凭据 - 此复选框默认为选中。在选中的情况下，允许用户在没有管理员介入的情况下修改或删除其注册的凭据。如果清除此复选框，普通用户将无法修改或删除凭据，必须由管理员修改或删除。

   注：要注册用户凭据，请转至管理员设置工具的*用户*页面，然后选择一个用户并单击注册。

   允许一步登录 - 一步登录即单点登录 (SSO)。此复选框默认为选中。启用此功能时，用户只能在“预引导身份验证”屏幕输入其凭据。用户将自动登录 Windows。如果清除此复选框，则用户可能需要多次登录。

   注：除非同时选择允许用户注册凭据设置，否则此选项不能选择。

3. 完成时单击**应用**。

智能卡和生物识别服务（可选）

如果您不希望 Security Tools 将智能卡和生物识别设备相关的服务更改为“自动”启动类型，可禁用服务启动功能。

在服务启动功能被禁用的情况下，Security Tools 不会尝试启动这三项服务：

- SCardSvr - 管理计算机对智能卡的读取访问。如果此服务停止，则此计算机将无法读取智能卡。如果此服务被禁用，则显式依赖此服务的所有服务将无法启动。
- SCPolicySvc - 允许将系统配置为在移除智能卡时锁定用户桌面。
- WbioSrvc - Windows 生物识别服务使客户端应用程序能够采集、比较、处理和存储生物识别数据，而不必直接访问任何生物识别硬件或样本。此服务托管在特权 SVCHOST 进程中。

禁用此功能也将取消与所需服务未运行相关的警告。

禁用自动启动服务

默认情况下，如果注册表项不存在或者其值设为 0，则此功能将启用。

1. 运行 **Regedit**。
2. 找到以下注册表项：

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

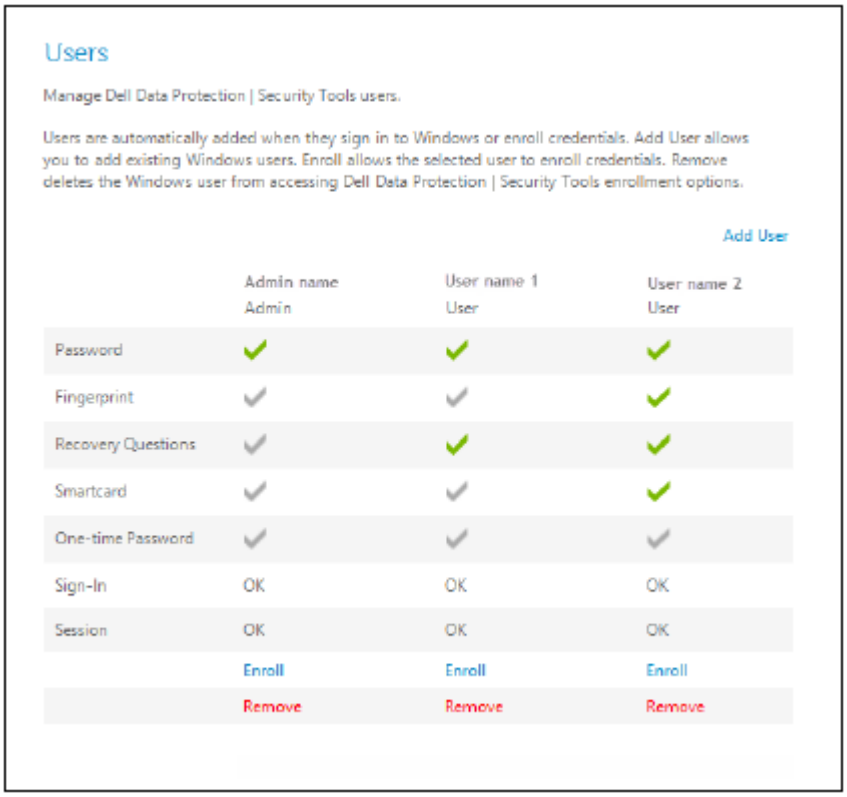
   设置为 0 将启用此功能。设置为 1 将禁用此功能。

管理用户身份验证

管理员设置“身份验证”选项卡上的控件可用于设置用户登录选项和自定义每种选项的设置。

要管理用户的身份验证：

1. 以管理员的身份单击**管理员设置**磁贴。
2. 单击**用户**选项卡，以管理用户和查看用户注册状态。从该选项卡，您可以：
   - 注册新用户
   - 添加或更改凭据
   - 移除用户凭据



注:

登录和会话显示用户的注册状态。

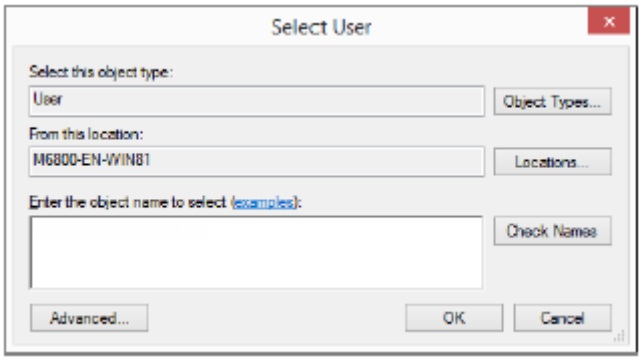
登录状态为正常，表明该用户需要登录的所有注册均已完成。会话状态为正常，表明该用户需要使用 Password Manager 的所有注册均已完成。

如果状态为否，表明该用户需要完成其他注册。要查找还需要进行哪些注册，请选择管理员设置工具，然后打开用户选项卡。灰色的复选标记框表示未完成的注册。或者单击注册磁贴，并查看状态选项卡的策略列，此列列示了需要进行的注册。

添加新用户

注: 当新 Windows 用户登录到 Windows 或注册凭据时，将自动进行添加。

1. 单击**添加用户**，开始完成现有 Windows 用户的注册过程。
2. 在*选择用户*对话框显示时，选择**对象类型。**



3. 在文本框中输入用户的对象名称，然后单击**检查名称。**
4. 完成时单击**确定。**

   注册向导随即打开。

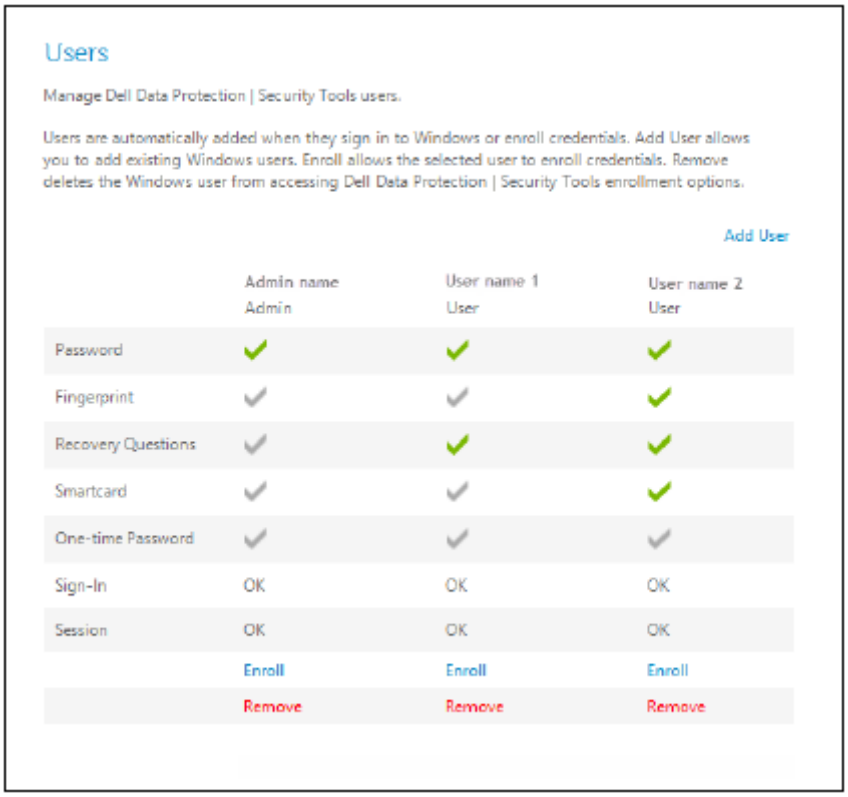
   继续按照注册或更改用户凭据中的说明执行操作。

注册或更改用户凭据

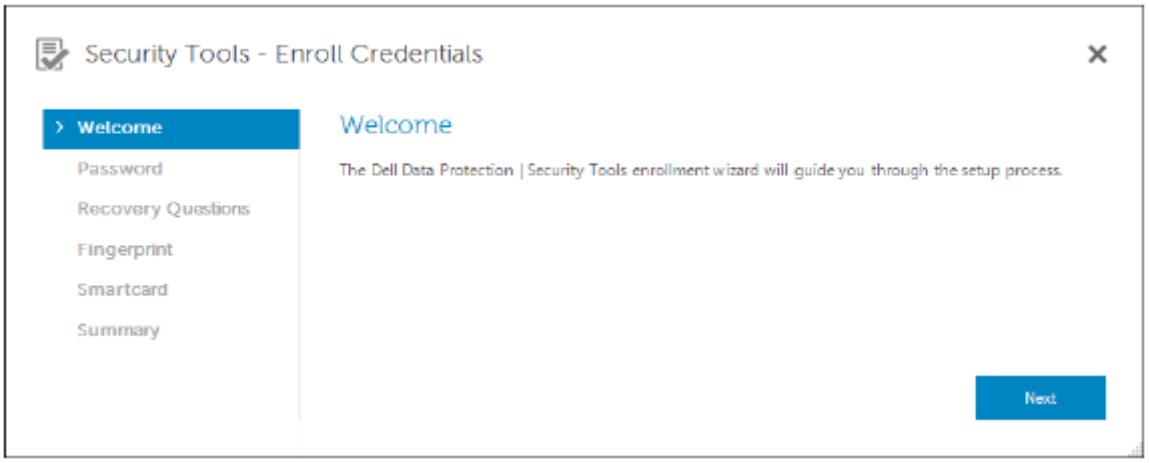
管理员可以用户名义注册或更改用户凭据，但有些注册活动要求用户亲自执行，例如回答恢复问题和扫描用户指纹。

要注册或更改用户凭据：

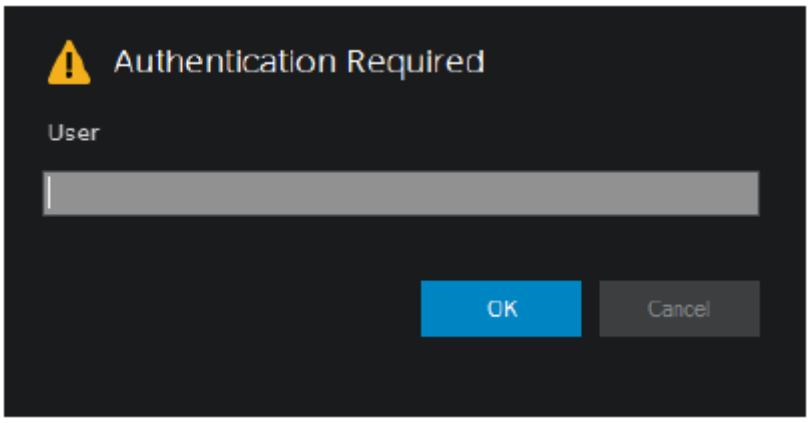
1. 在“管理员设置”中，单击**用户**选项卡。
2. 在“用户”页面中，单击**注册。**



3. 在“欢迎”页面中，单击**下一步**。



4. 在“需要身份验证”对话框中，使用用户的 Windows 密码登录，然后单击**确定**。



5. 在“密码”页面，如要更改用户的 Windows 密码，请输入新密码并进行确认，然后单击**下一步**。

   要跳过更改密码，请单击**跳过**。如果您不想注册凭据，向导将允许您跳过。要返回到一个页面，则单击**后退**。

6. 按照每个页面上的说明执行操作，并单击相应的按钮：**下一步**、**跳过**或**返回**。
7. 在“摘要”页面，确认注册的凭据，并在完成注册时单击**应用**。

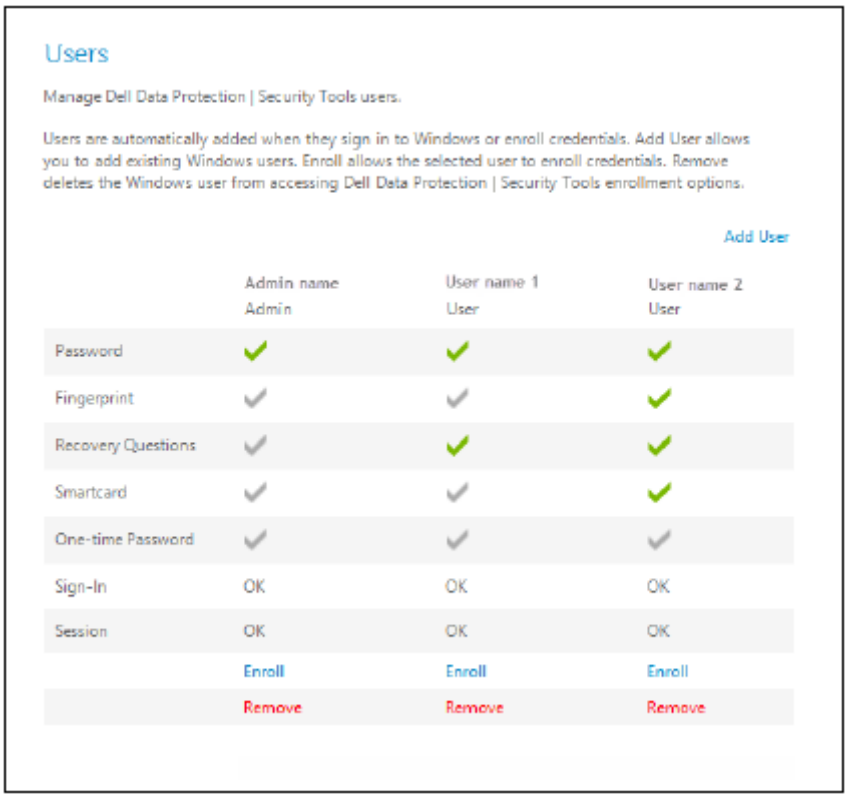
   要返回凭据注册页面进行更改，请单击**后退**直至到达您要更改的页面。

   有关注册凭据或更改凭据的详细信息，请参阅*控制台用户指南*。

移除一个已注册的凭据

1. 单击**管理员设置**磁贴。
2. 单击**用户**选项卡，查找您要更改的用户。
3. 将鼠标悬停在要移除的凭据的绿色复选标记上，它将变为 ⊗。
4. 单击 ⊗ 标记，然后单击**是**以确认删除。

   注: 如果这是用户唯一注册的凭据，则不能按这种方法移除此凭据。而且，这种方法不能移除密码。使用“移除”命令可完全移除用户对该计算机的访问。



移除用户所有已注册的凭据

1. 单击**管理员设置**磁贴。
2. 单击**用户**选项卡，查找您要移除的用户。
3. 单击**移除**。（ “移除”命令在用户设置底部显示为红色）。

   移除后，用户将不能登录此计算机，除非重新注册。

5

卸载任务

必须至少具备**本地管理员**权限，才能安装 DDP | Security Tools。

卸载 DDP | Security Tools

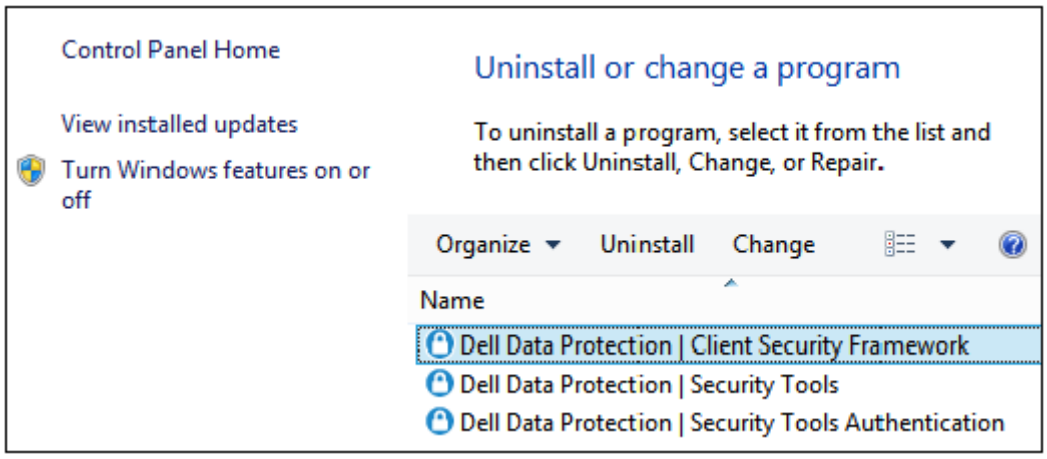
必须按此顺序卸载应用程序：

1. DDP | Client Security Framework
2. DDP | Security Tools Authentication
3. DDP | Security Tools

如果您的计算机配备有自加密驱动器，请按照以下说明进行卸载：

1. 解除配置 SED：
   a. 从管理员设置 > 单击**加密**选项卡。
   b. 单击**解密**以禁用加密。
   c. SED 取消加密后，重新启动计算机。
2. 在 Windows 控制面板中，转至**卸载程序**。

   注: 开始 > 控制面板 > 程序和功能 > 卸载程序。



3. 卸载 **Client Security Framework** 并重新启动计算机。
4. 从 Windows 控制面板卸载 **Security Tools Authentication**。

   随即将显示一条消息，提示您是否要保留用户数据。

   如果您计划要重新安装 Security Tools，请单击**是**。否则请单击**否**。

   卸载完成后，重新启动计算机。

5. 从 Windows 控制面板卸载 **Security Tools**。

   随即将显示一条消息，提示您是否要完全卸载此应用程序及其组件。

   单击**是**。

   随即将显示*卸载完成*对话框。

6. 单击**是，我想现在重新启动计算机**，然后单击**完成**。
7. 计算机将重新启动，卸载完成。

6

恢复

用户凭据过期或丢失时可使用恢复选项：

- **一次性密码 (OTP)**：用户在注册的移动设备上使用 Security Tools Mobile 应用生成 OTP，然后在 Windows 登录屏幕中输入该 OTP 以重新获取访问。此选项仅适用于用户在计算机上使用 Security Tools 注册了移动设备的情况。要使用 OTP 功能进行恢复，用户必须从未使用 OTP 登录计算机。

  注: 一次性密码 (OTP) 功能要求 TPM 已存在、已启用且已有归属。按照清除所有权并激活 TPM 中的说明执行操作。OTP 功能可用于身份验证或用于恢复，但不能同时用于这两项用途。有关详细信息，请参阅配置登录选项。
- **恢复问题**：用户正确回答一组个人问题以重新获取对该计算机的访问。此选项仅适用于管理员配置并启用了恢复问题，并且用户注册了恢复问题的情况。在“预引导身份验证”屏幕和“Windows 登录”屏幕使用此选项可重新获取对计算机的访问。

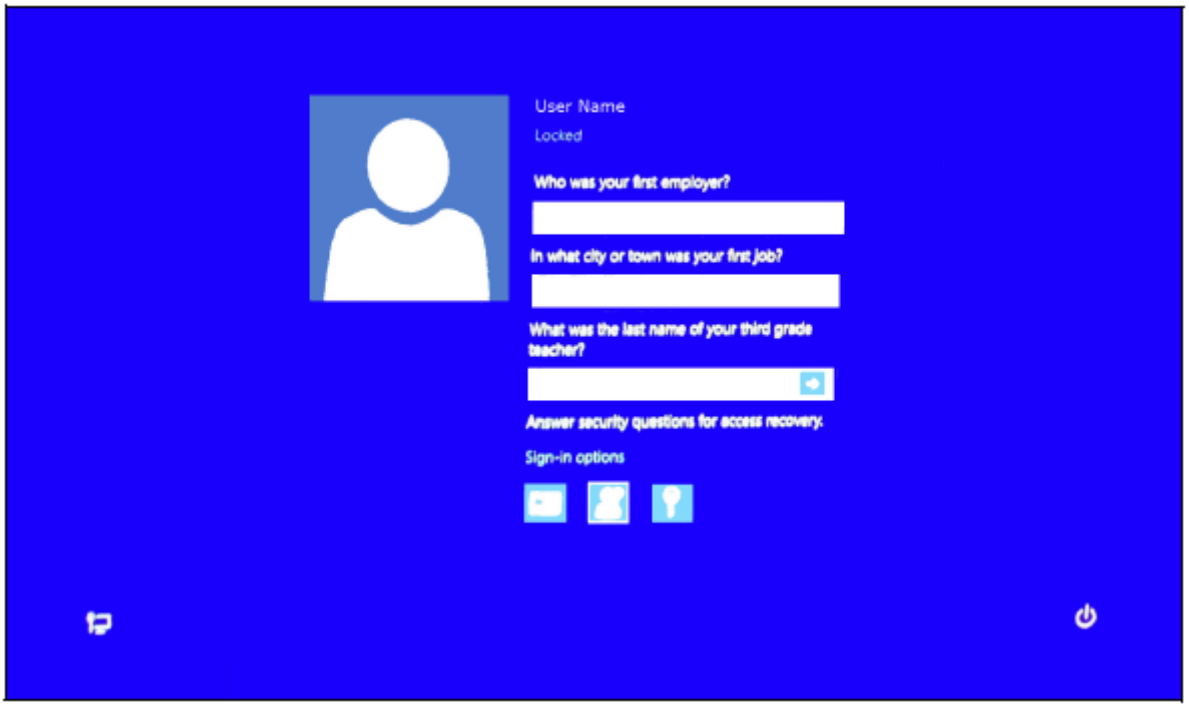
这两种恢复方法都要求您进行恢复准备，即通过注册恢复问题，或通过在计算机上使用 Security Tools 注册移动设备。

自恢复，Windows 登录恢复问题

要在 Windows 登录屏幕回答恢复问题以恢复访问：

1. 要使用恢复问题，请单击**无法访问您的帐户？**

   随即会显示您在注册过程中选择的恢复问题。



2. 输入回答，然后单击**确定。**

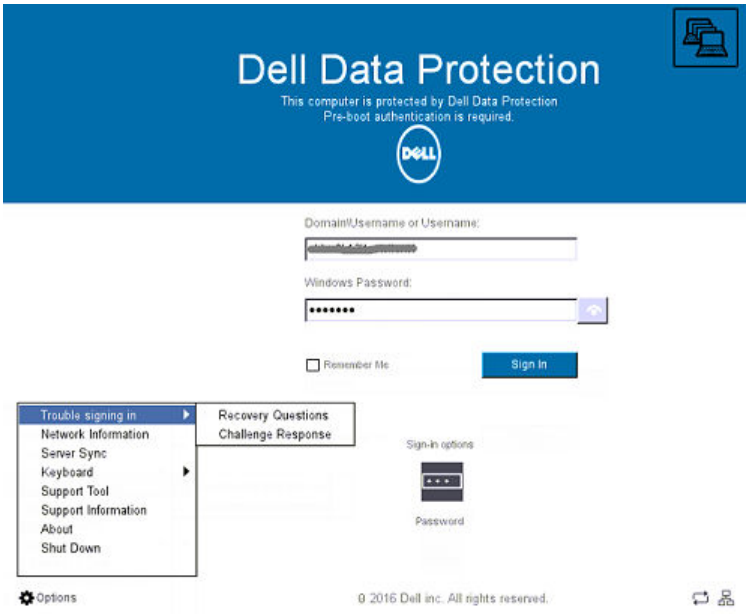
   成功输入问题的答案后，您将进入“访问恢复”模式。接下来的操作取决于已失效的凭据。

   - 如果您未能输入正确的 Windows 密码，将显示“更改密码”屏幕。
   - 如果未能识别指纹，将显示指纹注册页面，以供您重新注册指纹。

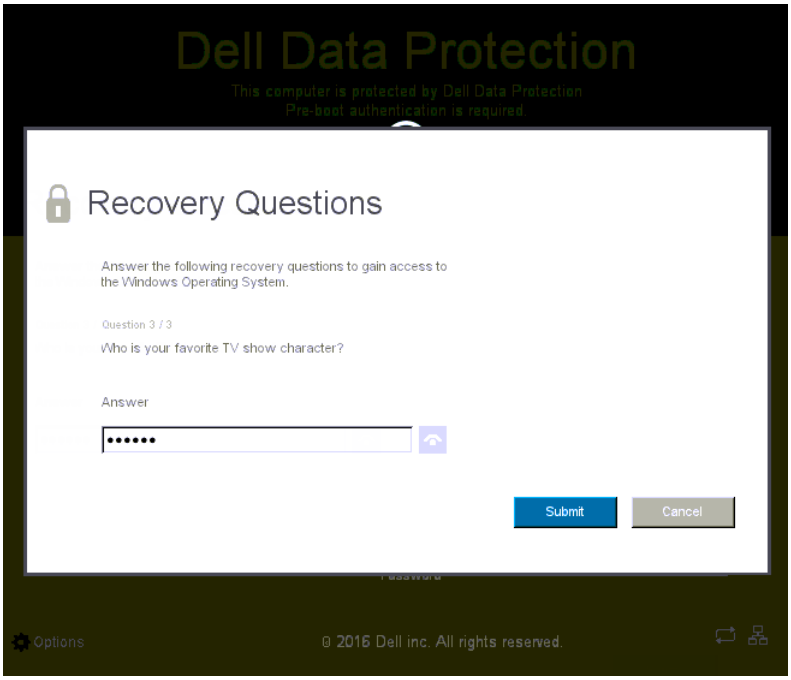
自恢复，PBA 恢复问题

要在“预引导身份验证”屏幕回答恢复问题以恢复访问：

1. 输入您的用户名。
2. 在屏幕左下方，单击**选项**>**登录时出错**。



3. 当 Q&A 对话框出现时，输入您在首次登录过程中注册“恢复问题”时提供的答案。



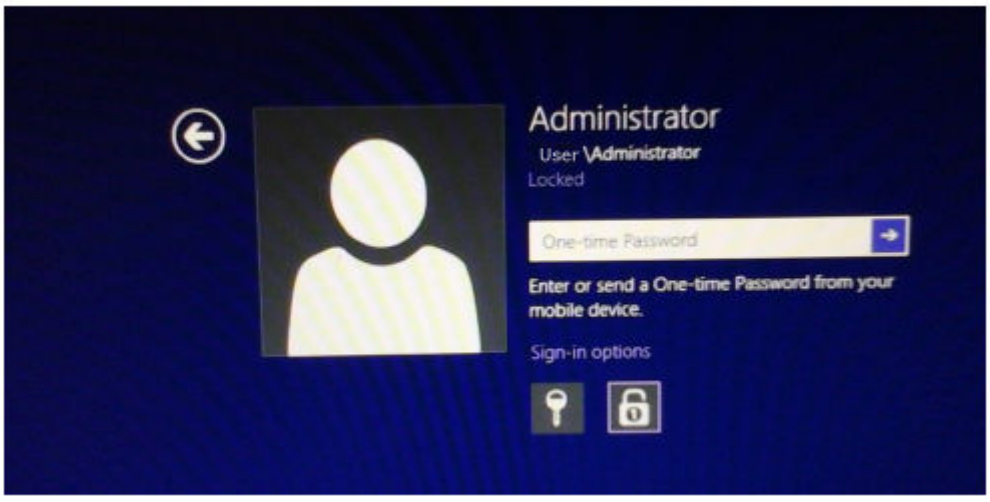
自恢复，一次性密码

此过程叙述在 Windows 密码过期、忘记 Windows 密码或超过允许的最大登录尝试次数等情况时，如何使用一次性密码 (OTP) 功能恢复对计算机的访问。一次性密码 (OTP) 选项仅适用于用户已注册了移动设备并且上次未使用 OTP 登录 Windows 的情况。

注: 一次性密码功能要求 TPM 已存在、已启用且已有归属。OTP 功能可用于 Windows 身份验证或用于恢复，但不能同时用于这两项用途。管理员可设置策略，以允许 OTP 用于恢复或身份验证的二者之一，或者禁用此功能。

要使用 OTP 恢复对计算机的访问：

1. 在 Windows 登录屏幕中，选择 OTP 图标 。



2. 在移动设备上，打开 Security Tools Mobile 应用并输入密码。
3. 选择您要访问的计算机。

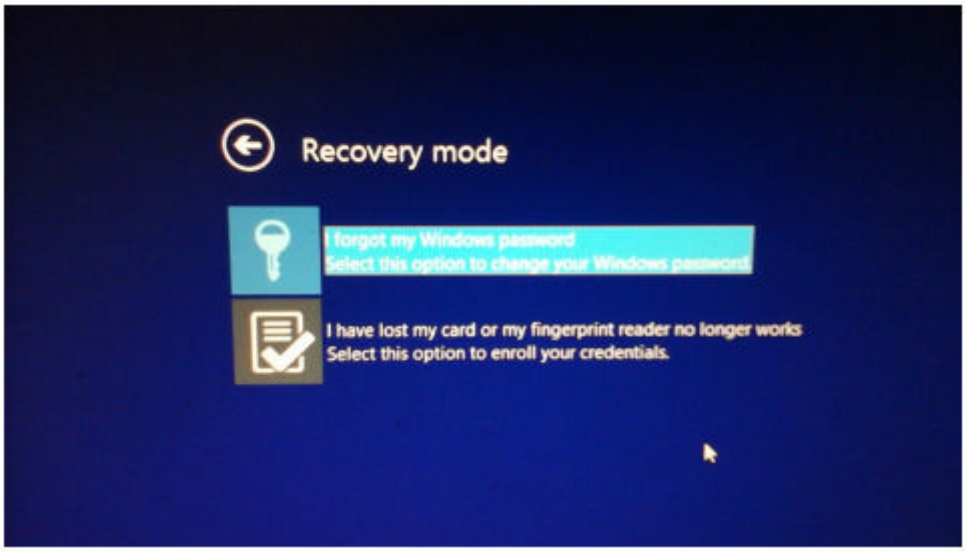
   如果移动设备上未显示计算机名称，可能发生了以下一种情况：

   - 移动设备未注册或未与您尝试访问的计算机配对。
   - 如果您有多个 Windows 用户帐户，则可能是您尝试访问的计算机上未安装 DDP | Security Tools，或者您尝试登录的用户帐户不是配对计算机和移动设备时所使用的用户帐户。
4. 点击**一次性密码**。

此时移动设备屏幕上将显示一个密码。

注: 如果需要，可单击“刷新”符号以获取新代码。刷新前两个 OTP 后，将延迟三十秒才生成另一个 OTP。计算机和移动设备必须同步，二者才能同时识别同一个密码。如尝试快速相继生成密码，将导致计算机和移动设备不同步以及 OTP 功能失效。如发生该问题，请等待三十秒以使两个设备恢复同步，然后再重试。

5. 在计算机的 Windows 登录屏幕上，键入移动设备上显示的密码并按 **Enter** 键。
6. 在计算机上的“恢复模式”屏幕中，选择**忘记了 Windows 密码**，并按照屏幕说明执行操作以重设密码。



7

词汇表

解除配置 - 解除配置操作将移除 PBA 数据库并停用 PBA。解除配置需要执行关机操作才能生效。

一次性密码 (OTP) - 一次性密码是仅可使用一次并且只在有限的时段内有效的密码。OTP 要求 TPM 已存在、已启用且已有归属。要启用 OTP，需要使用 Security Console 和 Security Tools Mobile 应用，将移动设备与计算机配对。Security Tools Mobile 应用在移动设备上生成密码，此密码用于从 Windows 登录屏幕登录到计算机。根据策略，如果 OTP 尚未用于登录该计算机，则在密码过期或忘记密码时可使用 OTP 功能恢复对该计算机的访问。OTP 功能可用于身份验证或用于恢复，但不能同时用于这两项用途。OTP 的安全性超过其他一些身份验证方法，因为所生成的密码只能使用一次并且会在短时间内过期。

预引导身份验证 (PBA) - 预引导身份验证是对 BIOS 或引导固件的扩展，在操作系统之外作为可信身份验证层，保证安全且防篡改的环境。PBA 防止读取硬盘中的任何内容（如操作系统），直至用户确认其具备正确凭据。

单点登录 (SSO) - 如果已在预启动和 Windows 登录时启用多重身份验证，SSO 可简化登录过程。如果 SSO 已启用，则仅在预引导时需要身份验证，而用户将自动登录到 Windows。如果 SSO 未启用，则可能需要执行多次身份验证。

可信平台模块(TPM)- TPM 是一块安全芯片，它有三项主要功能：安全存储、测量和证明。加密客户端将 TPM 用于其安全存储功能。TPM 还可为软件库提供加密容器。一次性密码功能也需要使用 TPM。