HP ProtectTools for Small Business Security Software 5.10 版

用户指南

HP ProtectTools for Small Business Security Software 5.10 版用户指南

HP 商用 PC

第二版： 2010 年 5 月

文档部件号：610663-AA2

关于本手册

本指南提供有关 HP ProtectTools for Small Business 安全保护软件的信息。

⚠ **警告！** 以这种方式出现的文字表示如果不按照指示操作，可能会造成人身伤害或带来生命危险。

△ **注意：** 以这种方式出现的文字表示如果不按照指示操作，可能会损坏设备或丢失信息。

注： 以这种方式出现的文字提供重要的补充信息。

目录

1 安全保护简介

HP 理解您的时间非常宝贵，您需要把精力集中在企业经营和企业发展上，而不担心用合适的安全保护软件来保护您的 PC、数据和企业。

重要的是您要考虑易于使用又能够对企业财产提供强有力保护的安全解决方案。安全保护不是“可有可无”，而是“必须！”

HP 提供的安全保护软件是安装容易，使用简单，名称是 HP ProtectTools for Small Business。

HP ProtectTools for Small Business 是提供安全保护的软件，以帮助防止他人未经允许擅自访问计算机和重要数据。各种 HP ProtectTools 软件模块提供了增强的安全保护功能。

HP ProtectTools for Small Business 提供了两个可使用的版本：HP ProtectTools Security Manager 管理控制台和 HP ProtectTools Security Manager（适用于普通用户）。管理员版本和普通用户版本均可通过**开始** > **所有程序**菜单来访问。

功能	特性
HP ProtectTools Security Manager 管理控制台	• 需要具有 Microsoft Windows 系统管理员权限才能访问 • 访问由管理员配置的模块，普通用户无法访问这些模块 • 允许进行初始安全设置，并配置适用于所有用户的选项或要求
HP ProtectTools Security Manager（适用于普通用户）	• 允许用户配置由管理员提供的选项 • 可以限制访问，并仅允许用户有限度地控制某些 HP ProtectTools 模块

HP ProtectTools 软件模块可通过预安装或预加载方式获得，也可作为可配置选件或售后选件提供给客户。有关详细信息，请访问 http://www.hp.com。

HP ProtectTools 功能

下表详细开列了 HP ProtectTools for Small Business 模块的各个重要功能：

模块	重要功能
HP ProtectTools Security Manager 管理控制台	• 管理员可以使用 Security Manager 设置向导来设置和配置安全级别和安全登录方法。 • 配置对基本用户隐藏的选项。 • 配置 Device Access Manager 配置和用户访问。 • 可以使用管理员工具来添加和删除 HP ProtectTools 用户以及查看用户状态。
HP ProtectTools Security Manager（适用于普通用户）	• 组织、设置和更改用户名和密码。 • 配置和更改用户凭证，如 Windows 密码和智能卡。 • 配置和更改 File Sanitizer 碎化、清理和设置。 • 查看 Device Access Manager 的设置。 • 配置首选项以及备份和恢复选项。
Credential Manager for HP ProtectTools（密码管理器）	• 设计用于保存、组织和保护您的用户名和密码。 • 使您能够设置网站和程序的登录屏幕，以便快速且安全地进行访问。 • 在访问各个网站时，您要保存您的用户名和密码，把它们输入“密码管理器”，以便您不必要非得再记住它们。下次当您访问这个网站时，“密码管理器”将会自动填入和提交该数据。 • 您可以创建不必写下或记住的增强密码，并使您的帐户变得更加安全。
Drive Encryption for HP ProtectTools	• 提供完善的整卷硬盘驱动器加密。 • 强制执行预引导验证，以便解密和访问硬盘驱动器上的数据。 • 帮助您遵守法律或行业要求以保护机密和敏感数据。 • 通过加密整个硬盘驱动器，防止他人未经授权擅自访问您的数据。 如果发生 PC 被盗情况，或者硬盘被人从原始系统中卸下并安装到其它系统中，并不会造成数据泄露。

模块	重要功能
File Sanitizer for HP ProtectTools	• 在 Windows 中删除数据并不是从硬驱上完全删除它们。Windows 仅删除此数据的参考。数据仍然保留在硬驱上，直到另一个文件用新的信息覆盖此硬驱上的同一个区域为止。但是，有了 File Sanitizer，您可以完全自动地擦除文档、网络浏览器的历史数据、临时文件等。 • 您可以安全地清除（或碎化）计算机上的重要文件和文件夹（个人信息或文件、历史数据、与 Web 有关的数据或其它类型数据），并定期清理（在先前删除的数据上写入）硬盘驱动器。
Device Access Manager for HP ProtectTools	• 可以用于根据配置文件控制对多媒体驱动器、USB 和其它硬件设备的访问。 • 使您能够限制用户存储重要数据的能力。 • 防止用户使用外部存储设备，如个人音响播放器，从 PC 或从网络复制数据。 • 防止用户将病毒从外部媒体引入系統。 • 使您能够有选择地按用户或用户组禁用某些设备（如 USB 钥匙、可写设备、个人音响播放器，等等）。有管理员权限的人可以登录 PC 和从 PC 复制信息，但是其他用户不能。

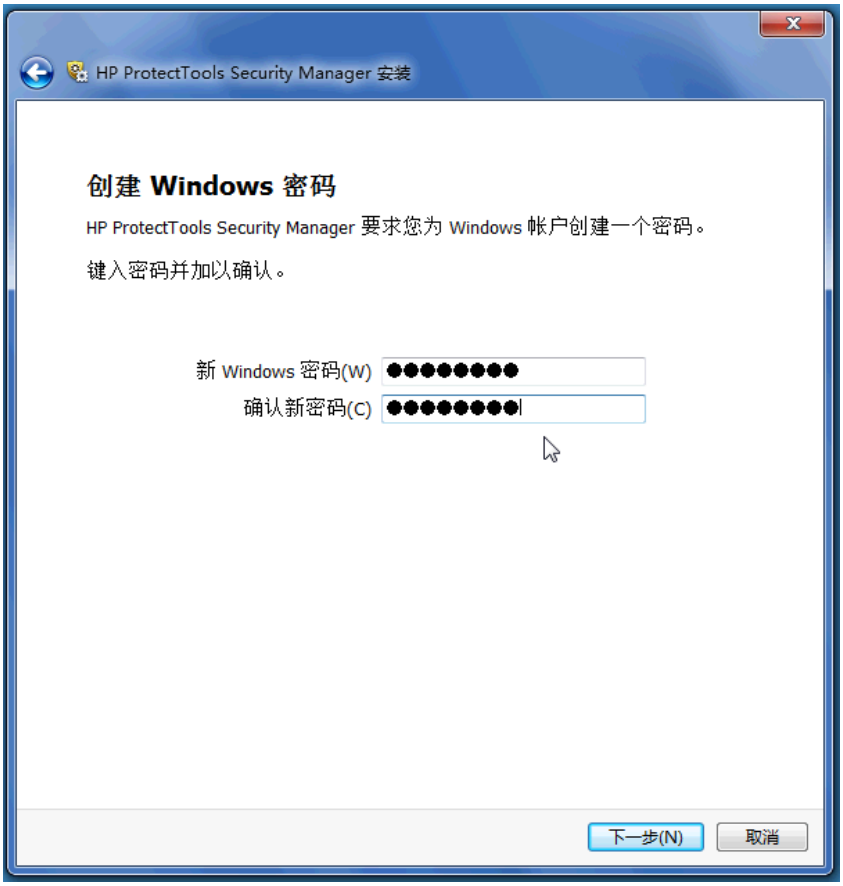
2 大多数有用选项的易于设置指南

这个“易于设置指南”设计为展示激活 HP ProtectTools for Small Business 中最常用选项的基本步骤。这个软件中有很多有用的工具和选项可用，使您能够微调您的首选项和设置您的访问控制。“易于设置指南”集中于用最少的设置努力和时间使每个模块运行起来。有关的更多信息，只需选择您感兴趣的模块，然后单击右上角的“？”或“帮助”按钮。这个按钮将自动地在当前显示的窗口中给您提供帮助信息。

使用入门

1. 从“小工具”图标、任务栏图标（金色挡板），或单击**开始** > **所有程序** > **HP**，打开 HP ProtectTools Security Manager。

2. 输入 Windows 密码，或创建一个 Windows 密码。



3. 完成设置向导。

注： 根据默认设置，HP ProtectTools Security Manager 设置为“强验证策略”。

这个设置设计用于在登录 Windows 后防止他人未经允许擅自访问计算机，因而应该在需要高度安全时使用，或在一天中用户要经常离开系统的情况下使用。如果您要更改这个设置，单击“会话策略”选项卡，然后进行您的选择。

要把 HP ProtectTools Security Manager 配置成整个会话都只使用最初的 Windows 登录，则更改以下的配置。

要使 HP ProtectTools Security Manager 在 Windows 登录期间只认证一次：

1. 单击**开始** > **所有程序** > **HP** > **HP ProtectTools 管理控制台**。
2. 在**工具**栏左边，从**安全保护**组选择**验证**。
3. 单击**会话策略**选项卡，然后从**策略**下的下拉菜单选择**不要求验证**。
4. 完成时单击**应用**按钮。

Credential Manager for HP ProtectTools（密码管理器）

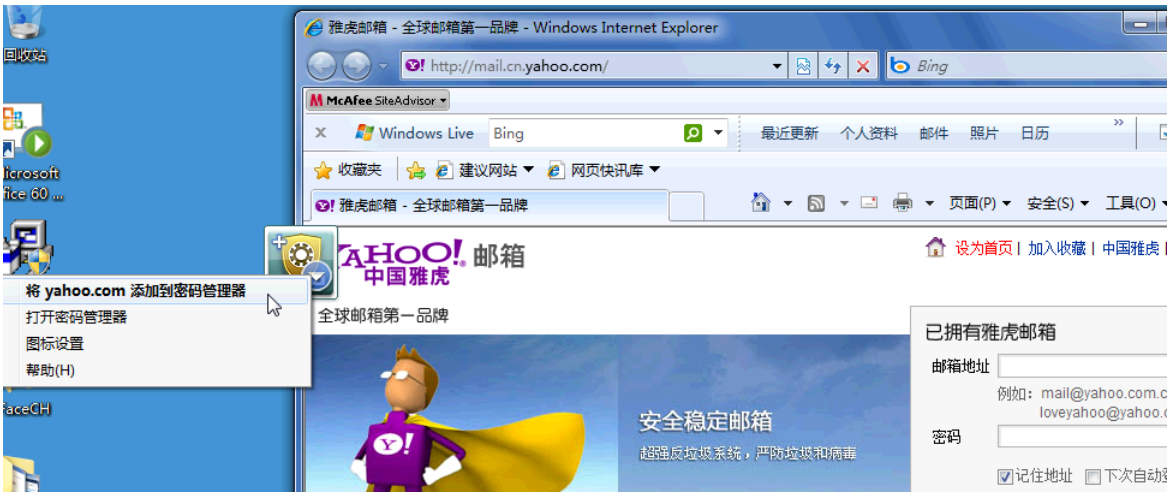
密码！我们都有很多密码，特别是如果您经常要访问网站或要使用要求登录才能使用的应用程序。对于每个应用程序和网站，通常用户或是使用相同的密码，或是很具创造性，迅速忘记了哪个密码对应于哪个应用程序。

有一个软件能够自动记住不是很重要网站的密码，或是给您能够识别哪些网站要记住和哪些网站要忽略的能力，不是很好吗？ Credential Manager for HP ProtectTools 便是答案。Credential Manager 便是给您提供那个能力的密码管理器。在您打开 PC 后，Credential Manager 将按需要给您提供密码或凭证。

当您访问任何要求凭证的应用程序或网站时，Credential Manager 将会自动地识别此网站，并且将询问您是否要该软件记住您的信息。如果您同意，则您将再也不要记住那个密码了。如果您要排除某些网站，则您可以拒绝要记住您的信息的请求。

要开始保存 Web 地址、用户名和密码：

1. 例如，浏览到您的 Web 电子信箱帐号，然后告诉 Credential Manager（单击其图标）以添加此 Web 验证。

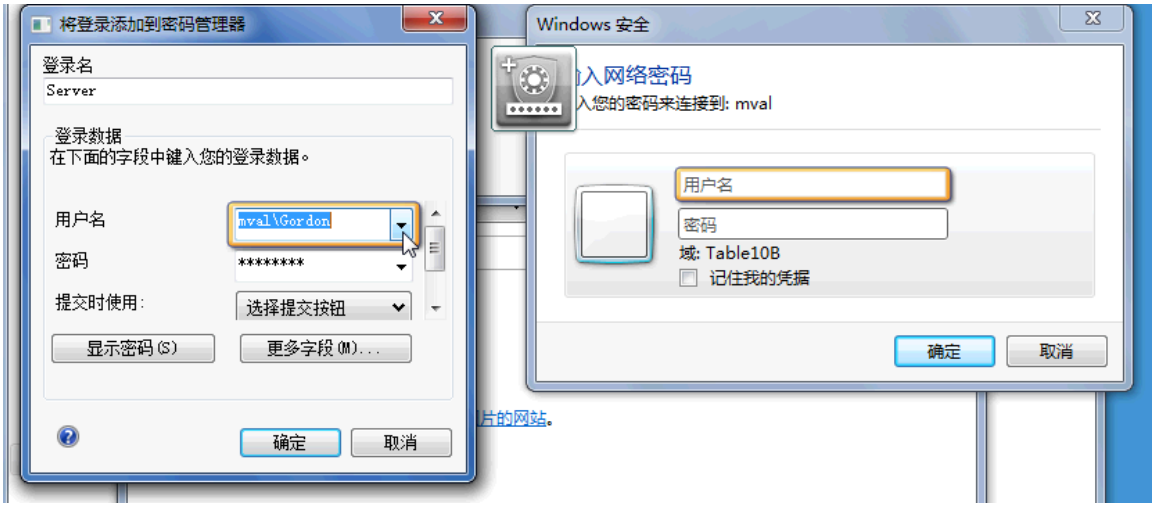


2. 命名此链接（选用），然后把用户名和密码输入 Credential Manager。

注： 网页将突出显示 Credential Manager 现在和将来常要访问的区域。

3. 完成时，单击**确定**按钮。

4. Credential Manager 还可以保存您的用户名和密码，以用于网络共享和映射网络驱动器。



查看和管理保存在 Credential Manager 中的验证

Credential Manager 的优越性是可以从中心位置查看、管理、备份和开启您的验证。Credential Manager 还支持从 Windows 开启所保存的网站。

要开启“密码管理器”，请用以下两种方法之一：

- 使用 Ctrl + Windows + H 键盘组合以开启“密码管理器”。选择**打开**将快速开启和验证保存的快捷键。

或者

- 选择“密码管理器”中的**管理**选项卡，以在可以编辑凭证的地方开启 HP ProtectTools Security Manager。

Credential Manager 的**编辑**选项将让您能够查看和修改姓名、登录名，甚至暴露密码。

HP ProtectTools for Small Business 将让所有的凭证和设置都被备份在和/或复制到另一台 PC 上。


HP ProtectTools
Security Manager
Ashley
安全应用程序
主页
Credential Manager
密码管理器
凭证
我的数据
File Sanitizer
我的计算机
Device Access Manager
查找更多
管理 »
帮助 »
高级 »
首选项 »
备份和恢复 »
关于 »
备份和恢复
HP ProtectTools 备份和恢复向导可帮助您安全地备份 HP ProtectTools 应用程序管理的数据。可以在 HP ProtectTools 保护的任何计算机上恢复该数据。
不会备份指纹数据等凭证。
请选择要执行的操作。
备份数据
恢复数据
查看备份和恢复日志

File Sanitizer for HP ProtectTools

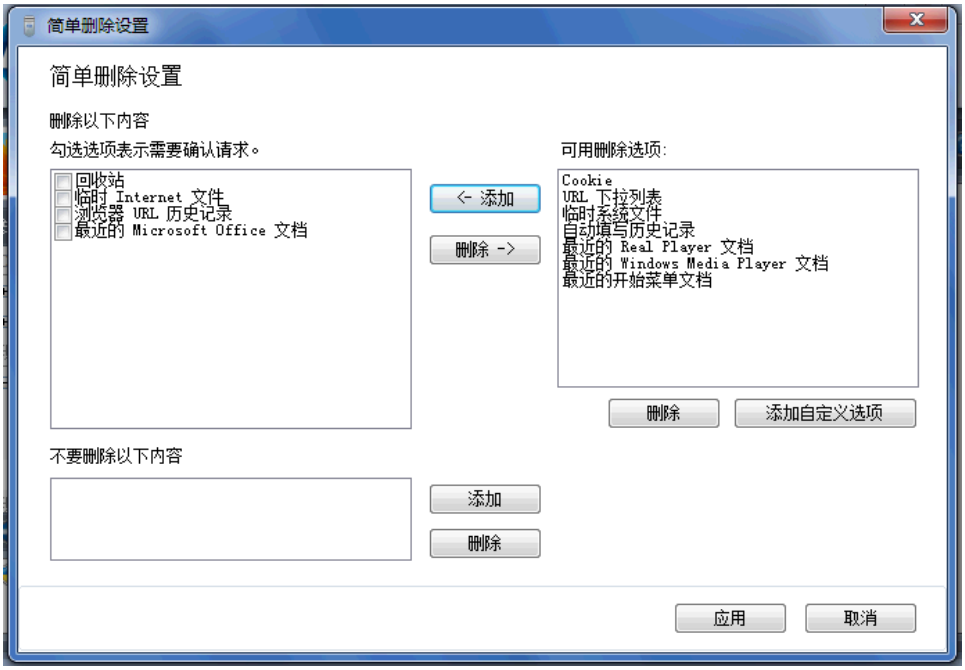
File Sanitizer 设计为让未有授权的人恢复您已删除的数据变得非常困难。您可用多个选项手动地清除，或建立定期时间表来清除包括浏览器历史数据在内的所选文件和文件夹。

下面是一些简单的配置设置。

要开始永久地清除已删除的数据，选择您不再需要的文件或文件夹。

1. 浏览到 **Security Manager** > **File Sanitizer** > **设置**。选择**简单删除设置**，然后单击**查看详细信息**按钮。

2. 在“简单删除设置”窗口的右边选择您要定期地永久删除的项目，然后单击**<-添加**按钮，以将所选的项目移到“删除”那边。



3. 从回收站开始，添加您要用碎化法清除的其他项目。

4. 在选择了您要永久清除的所有项目之后，单击**应用**。

5. 在要采取行动时，浏览到**碎化**选项，然后配置。**立即碎化**按钮将在您刚配置的“简单删除设置”窗口中立即清除所选的项目。

6. 每次“碎化”开始和完成时，都会有一个小气泡出现在任务栏。

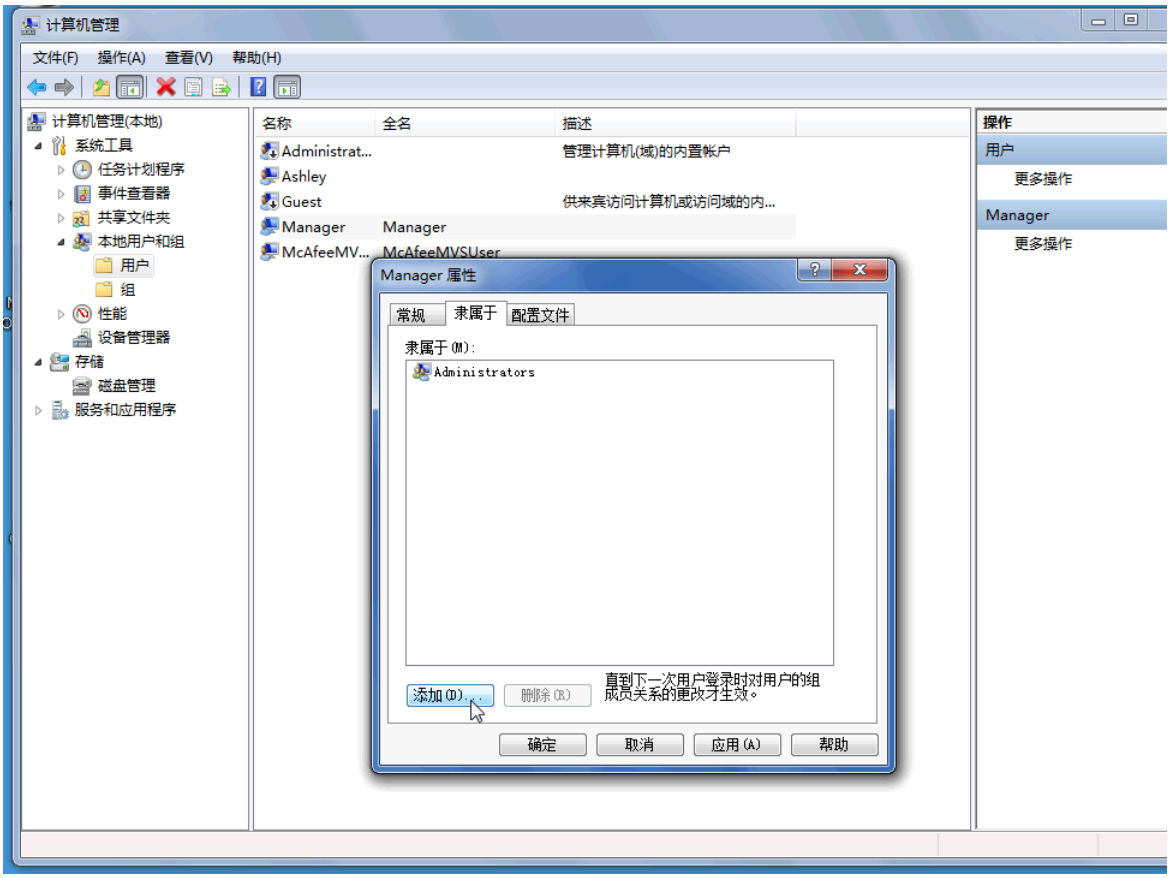
Device Access Manager for HP ProtectTools

Device Access Manager 可以用于限制使用各种内部和外部存储设备，以便您的数据将安全地保存在硬驱上而不会走出公司的门外。例如，允许用户调用您的数据，但是不让将其复制到 CD、个人音响播放器或 USB 存储设备上。下面便是进行此设置的容易方法。

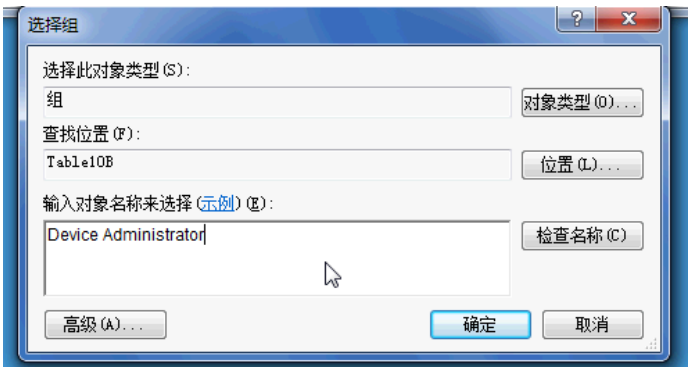
1. 单击**开始** > **所有程序** > **HP** > **管理控制台** > **Device Access Manager** > **简单配置**。
2. 选择您要限制的硬件设备，然后单击**应用**按钮以完成此过程。

3. 以下的步骤是选择谁在其他人都被锁住时将继续访问。
4. 浏览到并且选择**我的计算机**，右击并选择**管理** > **计算机管理** > **系統工具** > **本地用户和组** > **用户**。
5. 双击您要保留对锁住硬件有访问权的用户（这个样例是 Manager）。

6. 在**隶属于**选项卡下面，单击**添加**按钮，



7. 在**选择组**窗口，您可以使用**高级**选项或只键入“设备管理器”组。单击**确定**按钮，并且通过单击“确定”按钮来关闭窗口。您必须先注销，然后才能重新登录以获得此许可权。



现在，除了“设备管理器”组中包括的人员以外，所有的内部和外部存储设备，包括 CD 驱动器、USB 驱动器、个人音响播放器等等，都不会工作。

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools 软件可通过加密整个硬盘驱动器来保护您的数据。 如果您的 PC 被盗和/或硬盘驱动器被人从原始系统中卸下并安装到其它系统中，硬盘驱动器上的数据仍处于保护状态。

另外一个安全方面的好处是，Drive Encryption 要求您在系统引导之前使用您的用户名和密码正确进行验证。 此过程称为预引导验证。

为了简化这一过程，Windows 用户、域、Credential Manager for HP ProtectTools 和 HP ProtectTools Security Manager 均与 Drive Encryption 交互，以便轻松进行密码同步。

可以使用以下简单步骤激活 Drive Encryption for HP ProtectTools。

1. 单击**开始** > **所有程序** > **HP** > **HP ProtectTools 管理控制台** > **管理工具** > **设置向导**。 此时会显示下列屏幕

2. 在“欢迎使用！”屏幕上，选择**下一步**。
3. 需要提供 Windows 密码才能启动激活向导；选择**下一步**。
4. 选中 **Drive Encryption** 框，然后选择**下一步**。

5. 下面的 Drive Encryption 配置窗口将显示可以进行加密的驱动器，并要求使用 USB 闪存驱动器来存储加密恢复密钥。 如果预引导密码丢失或失效，需要使用恢复密钥来恢复数据或访问驱动器，因此请将该密钥放在安全的地方。

6. 选择**下一步**，完成该过程，然后选择**完成**。 在出现提示时，取出 USB 闪存驱动器，然后在准备就绪时重新引导系统。

7. 当系统从硬盘驱动器进行引导时，Drive Encryption 将要求您输入 Windows 密码。 请输入该密码，然后单击**确定**。

注： 在加密驱动器时，计算机的运行速度可能会下降。 在完全加密后，系统将恢复正常。 在访问驱动器上的数据时，将根据需要对该驱动器进行加密或解密。

另外请注意，Drive Encryption 验证将通过 Credential Manager Windows 登录名直接“链接”到桌面，而无需输入两次密码。

3 HP ProtectTools for Small Business 的优越性

访问 HP ProtectTools for Small Business 安全保护软件

要从 Windows 的“开始”菜单中访问 HP ProtectTools Security Manager，请执行以下操作：

▲ 在 Windows 中，依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。

要从 Windows 的“开始”菜单中访问 HP ProtectTools Security Manager 管理控制台，请执行以下操作：

▲ 在 Windows 中，依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。

实现关键的安全保护目标

HP ProtectTools 模块可以组合起来为多种安全问题提供解决方案，包括实现以下关键的安全保护目标：

- 限制访问敏感数据
- 防止来自内部或外部的未授权访问
- 创建强大可靠的密码策略

限制访问敏感数据

假设合同审计员到现场检查工作，并为其授予了计算机访问权限以检查敏感财务数据，但您不希望审计员能够打印文件或将其保存到可写设备（如 CD）中。以下功能有助于限制对数据进行的访问：

Device Access Manager for HP ProtectTools 使管理员能够限制对可写设备的访问，因此，无法打印硬盘驱动器中的敏感信息或将其复制到可移动介质中。请参阅“第 43 页的设备类别配置（高级）”。

防止来自内部或外部的未授权访问

未经授权擅自访问未受保护的商用 PC 会对重要数据（如来自金融服务机构、管理人员或研发团队的信息）以及私人信息（如病历或个人财务记录）构成非常严重的威胁。以下功能有助于防止未经授权的访问：

- 预引导验证功能（如果启用）有助于防止对操作系统进行访问。请参阅以下章节：
  - 第 32 页的 Credential Manager for HP ProtectTools（密码管理器）
  - 第 29 页的 Drive Encryption for HP ProtectTools
- Credential Manager for HP ProtectTools 有助于确保未经授权的用户无法获取密码或访问受密码保护的应用程序。请参阅下一章：
  - 第 32 页的 Credential Manager for HP ProtectTools（密码管理器）
- Device Access Manager for HP ProtectTools 使管理员能够限制对可写设备进行的访问，因此，硬盘驱动器中的敏感信息将无法复制。请参阅下一章：
  - 第 42 页的 Device Access Manager for HP ProtectTools
- 通过使用 File Sanitizer，您可以碎化重要文件和文件夹或清理硬盘驱动器（覆盖以前删除但仍存在于硬盘驱动器上的数据，以使数据更难进行恢复），从而安全地删除数据。请参阅下一章：
  - 第 36 页的 File Sanitizer for HP ProtectTools

创建强大可靠的密码策略

如果要求对很多基于 Web 的应用程序和数据库使用增强密码策略（难于修改的复杂密码），则可以使用 Credential Manager for HP ProtectTools 提供的受保护密码存储库以及非常方便的单一登录功能。请参阅下一章：

- 第 32 页的 Credential Manager for HP ProtectTools（密码管理器）

其它安全保护要素

分配安全角色

要适当的保护数据，一个重要的原则是在不同类型的管理员和用户之间划分职责和权限。

注： 对于小型企业或个人用户，这些角色可能全部由一人担任。

对于 HP ProtectTools for Small Business，安全职责和特别待遇可以分为以下角色：

- 管理员：应用和管理各个安全保护功能。也可以启用或禁用某些功能。
- 用户：使用这些安全保护功能。

管理 HP ProtectTools 密码

HP ProtectTools Security Manager 的大多数功能都是受密码保护的。下表列出了常用密码、设置密码所在的软件模块以及密码的功能。

表中说明的只是管理员设置和使用的密码。其他所有密码可以由普通用户设置。

HP ProtectTools 密码	在以下 HP ProtectTools 模块中设置	功能
“密码管理器”登录密码	密码管理器	此密码提供 2 个选项： • 在登录到 Windows 后，可以在单独的登录中使用该密码来访问“密码管理器”。 • 可以使用该密码替代 Windows 登录过程，以便同时访问 Windows 和“密码管理器”。
计算机设置实用程序密码 注： 也称为 BIOS 管理员密码、F10 设置实用程序密码或安全设置实用程序密码	BIOS，由管理员设置	防止他人未经授权擅自访问计算机设置实用程序。
开机密码	BIOS	在计算机开启、重新启动或从休眠模式恢复时，防止他人未经授权擅自对计算机内容进行访问。
Windows 登录密码	Windows 控制面板	可以用作手动登录。

创建安全的密码

创建密码时，您首先必须遵循程序设置的所有密码规范。不过，一般来说，应遵守下列准则以便创建安全可靠的密码，降低密码被破解的几率：

- 使用的密码要多于 6 个字符（最好超过 8 个字符）。
- 密码要包含大小写字母。
- 尽可能混合使用字母数字字符并包含特殊字符和标点符号。
- 用特殊字符或数字代替关键字词中的字母。例如，可以使用数字 1 代替字母 I 或 L。
- 混合使用两种或更多种语言的字词。
- 将数字或特殊字符置于单词或短语的中间，如“Mary2-2Cat45”。
- 不要使用可在字典中查到的词作为密码。
- 不要使用姓名或其它个人信息（如生日、宠物名称或母亲的姓氏）作为密码，即使反过来拼写也不可以。
- 定期更改密码。您可以只递增地更改几个字符。
- 如果您写下了密码，请不要将其存放在距离计算机很近的显眼位置。
- 不要在计算机上的文件（如电子邮件）中保存密码。
- 不要与他人共享帐户或将密码告诉别人。

备份凭证和设置

将 HP ProtectTools Security Manager 中的备份和恢复工具作为一个中心位置，您可以从中备份和恢复安装的 HP ProtectTools 模块中的安全凭证。

4 HP ProtectTools Security Manager 管理控制台

关于 HP ProtectTools 管理控制台

对 HP ProtectTools Security Manager 的管理是通过管理控制台实现的。

通过使用该控制台，本地管理员可以执行以下任务：

- 启用或禁用安全保护功能
- 管理计算机用户
- 调整设备特定的参数
- 配置 Security Manager 应用程序
- 添加其它 Security Manager 应用程序

使用管理控制台

Security Manager 管理控制台提供了一个中心位置来管理 HP ProtectTools Security Manager。

要打开该控制台，请执行以下操作：

- 选择**开始** > **所有程序** > **HP ProtectTools 管理控制台**，或者
- 单击 Security Manager 控制台左下角的**管理**链接。

管理控制台包含两个窗格：左窗格和右窗格。左窗格包含一些管理工具。右窗格包含用于配置这些工具的工作区域。

管理控制台左窗格包含以下内容：

- **主页** - 可以轻松访问常用任务，其中包括启用安全保护功能、指定安全凭证以及管理用户。
- **系统** - 管理系统范围的安全保护功能、用户以及验证设备（如智能卡读卡器）的配置。
- **应用程序** - 包含用于配置 Security Manager 及其应用程序行为的工具。
- **数据** - 提供一些备份和恢复加密密钥的工具。
- **计算机** - 提供一些高级安全选项，以便有选择性地禁用各种可能危及 PC 安全的设备，并为各种用户和组设置访问权限。

- **管理工具** - 打开默认浏览器以访问某个网页，您可以在其中查找其它管理应用程序和工具以扩展 Security Manager 的功能，以及在发布新应用程序和更新时及时得到通知。
- **链接** - 提供以下内容：
  - **设置向导** - 启动设置向导，它可指导您完成 Security Manager 的初始配置过程。
  - **帮助** - 打开帮助文件，其中提供了有关 Security Manager 及其应用程序的信息。
  - **关于** - 显示有关 Security Manager 的信息，其中包括版本号和版权声明。

设置向导入门指南

对 HP ProtectTools Security Manager 进行管理要求具有管理权限。

HP ProtectTools Security Manager 设置向导可指导您完成设置各种安全保护功能。不过，也可以通过 HP ProtectTools Security Manager 控制台使用很多其它功能。可通过该控制台（从 Windows 的“开始”菜单或者管理控制台中的链接可以打开）配置向导中提供的相同设置以及其它安全保护功能。这些设置适用于此计算机以及共享此计算机的所有用户。

第一次登录到 Windows 时，将会提示您设置 HP ProtectTools Security Manager。请单击**确定**以启动 Security Manager 设置向导，该向导将指导您完成配置该程序的基本步骤。

注： 也可以通过单击管理控制台左窗格底部的**安全向导**来启动安全向导。

按照设置向导屏幕上的说明进行操作，直至完成设置。

如果未完成此向导，它将会自动启动，直至您单击**不再显示此向导**。

要使用 HP ProtectTools Security Manager 应用程序，请从**开始**菜单中启动 HP ProtectTools Security Manager，或者右击任务栏通知区域（系统任务栏）中的 **Security Manager** 图标。共享此计算机的所有用户均可使用 Security Manager 控制台及其应用程序。

配置系统

可以从管理控制台左侧的**工具**菜单中访问**系统**应用程序组。

通过使用该组中包含的应用程序，您可以配置和管理此计算机及其用户和设备的策略和设置。

“系统”组中包含以下应用程序：

- **安全性** - 管理安全保护功能、验证策略和其它设置，以控制在登录到计算机或 HP ProtectTools 应用程序时用户如何进行身份验证。
- **用户** - 设置、管理和注册此计算机的用户。
- **设备** - 管理计算机内置或连接的安全保护设备的设置。

启用安全保护功能

此处启用的安全保护功能适用于此计算机的所有用户。

1. 在管理控制台左窗格中，展开**安全性**，然后单击**功能**。
2. 要启用安全保护功能，请单击 **Windows 登录安全性**和/或 **Drive Encryption** 旁边的相应复选框。
   - **Windows 登录安全性** - 要求使用特定凭证进行访问以保护 Windows 帐户。
   - **Drive Encryption** - 加密硬盘驱动器以保护数据，使未经正确授权的人员无法读取信息。
3. 单击**下一步**按钮。
4. 单击**应用**按钮。

定义 Security Manager 验证策略

此计算机的 Security Manager 验证策略是在两个标签（“登录”和“会话”）中定义的，用于指定在用户会话期间访问计算机和 HP ProtectTools 应用程序时验证每类用户所需的凭证。

“登录”标签

要指定访问计算机和登录到 Windows 所需的凭证，请执行以下操作：

1. 在管理控制台左窗格中，展开**安全性**，然后单击**验证**。
2. 在**登录**标签中，从下拉列表中选择一个用户类别。
3. 在**策略**部分中，单击列出的凭证旁边的复选框以指定选定用户类别所需的验证凭证。您必须至少指定一个凭证。
4. 在**策略**部分的下拉列表中，选择在验证用户时是需要任意（只有一个）指定的凭证，还是需要所有指定的凭证。
5. 单击**应用**按钮。

“会话”标签

要定义策略以控制在 Windows 会话期间登录到 HP ProtectTools 应用程序验证用户身份所需的凭证，请执行以下操作：

1. 在管理控制台左窗格中，展开**安全性**，然后单击**验证**。
2. 在**会话**标签中，选择一个用户类别。
3. 在**策略**部分中，单击列出的凭证旁边的复选框以指定选定用户类别所需的验证凭证。您必须至少指定一个凭证。
4. 在**策略**部分的下拉列表中，选择在验证用户时是需要任意（只有一个）指定的凭证，还是需要所有指定的凭证。
5. 单击**应用**按钮。

定义设置

您可以指定允许使用哪些高级安全设置。要编辑这些设置，请执行以下操作：

1. 在管理控制台左窗格中，展开**安全性**，然后单击**设置**。
2. 单击相应的复选框以启用或禁用特定设置。
3. 单击**应用**按钮以保存更改。

注： 如果在 BIOS 级执行验证，则**允许一步登录**设置允许此计算机的用户跳过 Windows 登录。

管理用户

在“用户”应用程序中，Windows 管理员可以管理此计算机的用户以及影响这些用户的策略。要在管理控制台中访问“用户”应用程序，请单击**用户**。

将列出 HP ProtectTools 用户，并根据通过 Security Manager 设置的验证策略以及满足这些策略要求所需的凭证对其进行验证。

要查看应用于特定用户的策略，请从列表中选择该用户，然后单击**查看策略**按钮。

要在用户注册凭证时监管用户，请从列表中选择该用户，然后单击**注册**按钮。

添加用户

此过程将用户添加到登录列表中。在添加某个用户之前，该用户必须已在计算机上拥有一个 Windows 用户帐户，而且该用户必须在以下过程中到场提供该密码。

要将用户添加到用户列表中，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在管理控制台的左窗格中，单击**用户**。
3. 单击**添加**按钮。将打开**选择用户**对话框。
4. 单击**高级**按钮，然后单击**立即查找**按钮以搜索要添加的用户。
5. 单击要添加到列表中的用户，然后单击**确定**。
6. 在**选择用户**对话框中，单击**确定**。
7. 键入选定帐户的 Windows 密码，然后单击**完成**。

注： 您必须使用现有 Windows 帐户，并准确键入该帐户的名称。不能使用此对话框来修改或添加 Windows 用户帐户。

删除用户

注： 此过程不会删除 Windows 用户帐户。它仅从 Security Manager 中删除该帐户。要彻底删除用户，您必须从 Security Manager 和 Windows 中同时删除用户。

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在管理控制台的左窗格中，单击**用户**。

3. 单击要删除的帐户的用户名，然后单击**删除**。

4. 在确认对话框中单击**是**。

检查用户状态

管理控制台的“用户”部分显示每个用户的当前状态：

- **绿色复选标记** - 表示用户已配置了必需的安全登录方法。
- **红色 X** - 表示用户未配置必需的安全登录方法，在尝试登录时将会锁定计算机。用户必须运行设置向导以配置必需的登录方法。
- **空白** - 表示安全登录方法不是必需的。

配置应用程序设置

“设置”窗口包含用于配置 Security Manager 及其应用程序行为的工具。要修改这些设置，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在管理控制台的左窗格中，单击**设置**。
3. 在**常规**标签中，选择 HP ProtectTools Security Manager 常规设置，然后单击**应用**按钮。
4. 在**应用程序**标签中，选择要启用或禁用的应用程序，然后单击**应用**按钮。

注： 在重新启动计算机后，启用或禁用应用程序的操作才会生效。

加密驱动器

通过使用 Drive Encryption for HP ProtectTools，您可以加密计算机的硬盘驱动器；即使将硬盘驱动器从计算机中取下或将其送到数据恢复服务机构，任何人也无法在未经授权的情况下擅自读取或访问驱动器。

要启用或禁用 Drive Encryption，请在管理控制台中单击“设置向导”。

△ **注意：** 务必将加密密钥备份到 USB 闪存驱动器上，并将该设备存放在安全的地方。 如果忘记了密码，则只能通过该设备访问硬盘驱动器。

有关使用 Drive Encryption for HP ProtectTools 的详细信息，请参阅第 29 页的 Drive Encryption for HP ProtectTools。

管理设备访问

Device Access Manager for HP ProtectTools 提供了一些高级安全保护选项，以便有选择性地禁用各种可能危及 PC 安全的设备。有关使用 Device Access Manager for HP ProtectTools 的详细信息，请参阅第 42 页的 Device Access Manager for HP ProtectTools。

5 关于 HP ProtectTools Security Manager

通过使用 HP ProtectTools Security Manager，您可以大大提高计算机的安全性。通过使用 Security Manager 应用程序，您可以执行以下任务：

- 管理登录和密码
- 轻松更改 Windows 密码
- 设置验证凭证（包括智能卡）
- 碎化或清理硬盘驱动器
- 查看驱动器加密状态
- 查看设备访问设置
- 备份和恢复 Security Manager 数据

管理密码

Credential Manager for HP ProtectTools（密码管理器）可以创建和管理登录；使您能够通过验证注册凭证，开启和登录到网站和程序。

有关管理密码的详细信息，请参阅第 32 页的 Credential Manager for HP ProtectTools（密码管理器）。

设置凭证

可以使用 Security Manager 凭证证明您就是所声称的那个人。此计算机的管理员可以设置在登录到 Windows 帐户、网站或程序时用于证明您身份的凭证。

可用的凭证可能因计算机内置或连接的安全保护设备而有所不同。每个支持的凭证在“凭证”组中具有一个条目。

更改 Windows 密码

与通过 Windows 控制面板更改 Windows 密码相比，通过 Security Manager 更改密码更加简便快捷。

要更改 Windows 密码，请执行以下操作：

1. 在 HP ProtectTools Security Manager 左窗格中，单击**凭证**。
2. 单击 **Windows 密码**。
3. 在**当前 Windows 密码**框中键入当前密码。
4. 在**新 Windows 密码**和**确认新密码**框中键入新密码。
5. 单击**更改**。

碎化或清理文件

File Sanitizer for HP ProtectTools 使用无意义的数据覆盖文件以将其删除。此过程称为“碎化”，可使删除的文件变得很难恢复，从而大大提高了信息安全性。File Sanitizer 可以使用称为“清理”的过程进一步提高信息安全性，即覆盖硬盘驱动器上以前使用的空间。操作系统或其它常用文件恢复软件无法恢复使用 File Sanitizer 删除的文件。

有关使用 File Sanitizer for HP ProtectTools 的详细信息，请参阅第 36 页的 File Sanitizer for HP ProtectTools。

查看驱动器加密状态

Drive Encryption 是 Windows 管理员在管理控制台中进行设置的。用户可以在 Security Manager 中查看其加密状态。

要查看驱动器加密状态，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击**加密状态**。“加密状态”页将显示驱动器加密是处于活动状态还是非活动状态，以及哪些驱动器已加密或未加密。

查看设备访问

设备访问是 Windows 管理员在管理控制台中设置的。用户可以在 Security Manager 中查看其设备访问设置。

要查看设备访问设置，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，展开 **Device Access Manager**。
3. 要查看被拒绝访问的设备，请单击**简单配置**。将拒绝旁边带有复选标记的设备进行访问。
4. 要查看被拒绝访问的用户或组，请单击**设备类别配置**。
5. 单击某个设备以查看拒绝或允许哪些用户或组访问该设备。

添加应用程序

可以通过其它应用程序为该程序添加新功能。

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击**查找更多**。

> **注：** 如果没有**查找更多**链接，则说明计算机管理员已将其禁用。

3. 在**添加应用程序**标签中，浏览查找其它应用程序。
4. 在**更新和消息**标签中，您可以单击**通知我新的应用程序和更新**复选框并设置检查更新的天数以及时了解发布的新应用程序和更新，也可以单击**立即检查**按钮立即检查更新。

设置首选项

在“首选项”页中，您可以选中**在任务栏中显示图标**复选框，以便在任务栏通知区域（系统任务栏）中显示 Security Manager 图标。

要访问“首选项”页，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击**高级**，然后单击**首选项**。
3. 选中或取消选中**在任务栏中显示图标**复选框，然后单击**应用**。

备份和恢复

最好定期备份 Security Manager 数据。备份频率取决于数据更改的频率。例如，如果您每天定期添加新登录，则可能需要每天备份一次数据。

也可以使用备份从一台计算机迁移到另一台计算机，这有时也称为导入和导出。但要记住，此功能仅备份数据。

如果将备份文件恢复到另一台计算机，或者在重新安装操作系统后将其恢复到同一计算机，系统必须已安装了 HP ProtectTools Security Manager，然后才能从备份文件恢复数据。

备份数据

在备份数据时，登录和凭证信息将保存到使用输入的密码保护的加密文件中。

要备份数据，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击**高级**，然后单击**备份和恢复**。
3. 单击**备份数据**。
4. 选择要包含在备份中的模块。在大多数情况下，您希望选择所有模块。单击**下一步**。
5. 输入密码以验证您的身份，然后单击箭头按钮。
6. 输入存储文件的路径和名称。默认情况下，该文件将保存到“我的文档”文件夹中。单击**浏览**可指定不同的位置。单击**下一步**。

7. 输入并确认密码以保护该文件。
8. 单击**完成**。

恢复数据

可以从以前通过 Security Manager 备份和恢复功能创建的受密码保护的加密文件恢复数据。

要恢复数据，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击**高级**，然后单击**备份和恢复**。
3. 单击**恢复数据**。
4. 输入存储文件的路径和名称，或者单击**浏览**，然后选择该文件。
5. 输入用于保护该文件的密码，然后单击**下一步**。
6. 选择要恢复数据的模块。在大多数情况下，将选择列出的所有模块。单击**下一步**。
7. 单击**完成**。

更改 Windows 用户名和图片

Windows 用户名和图片显示在 Security Manager 左上角。

要更改用户名和/或图片，请执行以下操作：

1. 单击包含用户名和图片的 Security Manager 左上角。
2. 要更改用户名，请在 **Windows 用户名**框中键入名称。
3. 要更改图片，请单击**选择图片**按钮，然后浏览以选择一个图片。
4. 单击**保存**按钮以保存更改。

6 Drive Encryption for HP ProtectTools

注： 只有某些机型提供了 Drive Encryption for HP ProtectTools。

如今，个人或公司电脑失窃的现象屡见不鲜，导致公司重要信息受到严重的安全威胁。如果对您计算机硬盘驱动器上的所有数据进行加密，那么即使从计算机上移除您的驱动器或将其送至数据恢复服务中心，任何人也不可能在未经您授权的情况下读取或访问其中的数据。

Drive Encryption for HP ProtectTools 软件通过加密硬盘驱动器来提供全面的数据保护。 在激活 Drive Encryption 后，您必须在 Windows 启动之前显示的 Drive Encryption 登录屏幕上进行登录。

在同一 Windows 会话期间，Drive Encryption 无法防止未经授权的访问。 在引导 PC 并输入您的用户名和密码后，硬盘驱动器上的数据仍处于加密状态，但任何系统用户均可进行访问。 在离开您的计算机时，请务必使用密码保护 Windows 会话。

注： 只能通过 HP ProtectTools 管理控制台中的设置向导来启用 Drive Encryption for HP ProtectTools。

注： 如果在使用 AMD 处理器的系统上配置了 RAID，则 64 位操作系统不支持 Drive Encryption。

注： Drive Encryption 不支持字典攻击防护功能。

Drive Encryption：

- 可将内部硬盘驱动器上的所有数据加密
- 可让您方便地访问密码并进行预引导验证
- 支持 Microsoft Windows XP、Windows Vista 和 Windows 7

可以在 Drive Encryption for HP ProtectTools 中执行各种任务：

- 管理 Drive Encryption
  - 加密或解密各个驱动器
- 备份和恢复
  - 创建备份密钥
  - 执行恢复操作

△ **注意：** 务必将加密密钥备份到 USB 闪存驱动器上，并将该设备存放在安全的地方。 如果忘记了密码，则只能通过该设备访问硬盘驱动器。

注意： 如果决定卸载 Drive Encryption 模块或使用备份和恢复解决方案，则必须先解密所有加密的驱动器。 否则，将无法访问加密驱动器上的数据。 无法通过重新安装 Drive Encryption 模块来访问加密的驱动器。

设置步骤

打开 Drive Encryption

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 单击 **Drive Encryption**。

常规任务

激活 Drive Encryption

可以使用 HP ProtectTools 管理控制台设置向导来激活 Drive Encryption。

停用 Drive Encryption

可以使用 HP ProtectTools 管理控制台设置向导来停用 Drive Encryption。

在激活 Drive Encryption 后登录

在激活 Drive Encryption 并注册了用户帐户之后，每次打开计算机时，您必须在 Drive Encryption 登录屏幕上登录：

注： 如果 Windows 管理员在 HP ProtectTools 管理控制台中启用了预引导安全功能，则会在打开计算机后立即登录到计算机上，而不是在 Drive Encryption 登录屏幕上进行登录。

注： 如果使用恢复密钥在 Drive Encryption 登录屏幕上登录，系统还会提示您在 Windows 登录屏幕上选择 Windows 用户名并键入密码。

高级任务

管理 Drive Encryption（管理员任务）

在 Drive Encryption 窗口中，Windows 管理员可以查看和更改 Drive Encryption 的状态（“活动”或“非活动”），以及查看计算机上的所有硬盘驱动器的加密状态。

加密或解密各个驱动器

1. 在管理控制台左窗格中，展开 **Drive Encryption**，然后单击**加密管理**。
2. 单击**更改加密**按钮。
3. 在“更改加密”对话框中，选中或取消选中您要加密或解密的每个硬盘驱动器旁边的复选框，然后单击**确定**。

注： 在加密或解密驱动器时，进度栏会显示完成当前会话过程所需的剩余时间。如果在加密过程中，计算机关机或进入了睡眠或休眠模式，然后再重新启动，则显示的剩余时间会重置为起始值，但实际上加密会从上次停止的位置继续。剩余时间和进度的显示信息会变化得更快，以反映之前的进度。

备份和恢复（管理员任务）

在“Drive Encryption：备份和恢复”窗口中，Windows 管理员可以备份和恢复加密密钥。

创建备份密钥

△ **注意：** 如果忘记了密码，只能通过包含备份密钥的存储设备访问硬盘驱动器，因此，请确保将该设备放在安全的地方。

1. 在管理控制台左窗格中，展开 **Drive Encryption**，然后单击**备份和恢复**。
2. 单击**备份密钥**按钮。
3. 在“选择备份磁盘”页面上，单击要用来备份加密密钥的设备的名称，然后单击**下一步**。
4. 阅读下一页显示的信息，然后单击**下一步**。

   加密密钥随即保存在您选择的存储设备上。
5. 确认对话框打开时，请单击**确定**。

注： 有关管理和执行恢复的信息，请参阅 Drive Encryption for HP ProtectTools 帮助文件。

7 Credential Manager for HP ProtectTools（密码管理器）

在使用“密码管理器”时，可以更方便安全地登录到 Windows、网站和程序。

通过使用“密码管理器”，您可以设置网站和程序的登录屏幕，以便快速且安全地进行访问。首先，“密码管理器”了解您的登录以及在每个登录屏幕的输入框中键入的特定数据。其次，当您位于登录屏幕后，“密码管理器”将在验证您的身份后自动填充并提交该数据。

要更快地进行访问，您可以直接使用可配置的组合热键（默认为 Ctrl+Windows+H）来显示登录菜单。在该菜单上，只需选择一个登录，“密码管理器”便会启动网站或程序，导航到登录屏幕并自动进行登录。

为证明您的身份，您将使用 HP ProtectTools for Small Business 凭证，如 Windows 密码。这意味着，您将使用相同凭证登录到设置的所有登录屏幕。因此，您可以创建不必写下或记住的增强密码，并使您的帐户变得更加安全。

通过使用 “密码管理器”，您可以快速查看任何密码是否存在安全风险，并且可以自动生成增强的复杂密码以供新网站使用。

借助于“密码管理器”，您还可以随时查看登录和密码，并对其进行编辑。也可以通过“密码管理器”图标来使用很多“密码管理器”功能；只要设置的程序登录屏幕或任何网站登录屏幕具有焦点，就会显示该图标。单击该图标将显示一个上下文菜单，您可以在其中选择以下选项。

对于尚未创建登录的网页或程序：

将在上下文菜单中显示以下选项。

- 将 [somedomain.com] 添加到“密码管理器” - 用于为当前登录屏幕添加登录。
- 打开“密码管理器” - 在“密码管理器”页上启动 Security Manager。
- “密码管理器”图标设置 - 用于指定显示“密码管理器”图标的条件。
- 帮助 - 显示“密码管理器”应用程序的联机帮助。

对于已创建登录的网页或程序：

将在上下文菜单中显示以下选项。

- 填充登录数据 - 在登录字段中填充登录数据，然后提交该页面（如果在创建登录或上次编辑登录时指定了提交）。
- 编辑登录 - 用于编辑此网站的登录数据。
- 添加登录 - 用于为相同网站或程序添加其它登录。

- 打开“密码管理器”- 在“密码管理器”页上启动 Security Manager 控制板。
- 帮助 - 显示“密码管理器”应用程序的联机帮助。

添加登录

要添加登录，请执行以下操作：

1. 打开网站或程序的登录屏幕。
2. 单击“密码管理器”图标上面的箭头，然后选择以下选项之一，具体取决于登录屏幕是用于网站还是程序。
   - 对于网站，请选择**将 [domain name] 添加到“密码管理器”**。
   - 对于程序，请选择**将此登录屏幕添加到“密码管理器”**。
3. 输入登录数据。屏幕上的登录字段及其对话框上的相应字段是使用加粗橙色边框标识的。可以使用其它选项来显示此对话框，例如，从“密码管理器”的**管理**标签中选择“添加登录”。某些选项取决于连接到计算机的安全保护设备，例如，使用 Ctrl-H 热键或插入智能卡。
   - 单击登录字段右侧的箭头，以使用某个预先设置了格式的选项填充该字段。
   - （可选）单击**选择其它字段**，将屏幕上的其它字段添加到登录中。
   - 如果要填充登录字段，但不提交这些字段，请取消选中**提交登录数据**。
   - 如果要查看此登录的密码，请单击**显示密码**。
4. 单击**确定**。将从“密码管理器”图标中删除加号，通知您已创建了登录。

现在，每次访问该网站或启动该程序时，将显示“密码管理器”图标，表明您可以使用注册的凭证进行登录。

编辑登录

要编辑登录，请执行以下操作：

1. 打开网站或程序的登录屏幕。
2. 单击“密码管理器”图标上面的箭头，然后选择**编辑登录**，以显示可以在其中编辑登录信息的对话框。屏幕上的登录字段及其对话框上的相应字段是使用加粗橙色边框标识的。
3. 编辑登录信息。
   - 单击登录字段右侧的箭头，以使用某个预先设置了格式的选项填充该字段。
   - （可选）单击**选择其它字段**，将屏幕上的其它字段添加到登录中。
   - 如果要填充登录字段，但不提交这些字段，请取消选中**提交帐户数据**。
   - 如果要查看此登录的密码，请单击“显示密码”。
4. 单击**确定**。

使用“登录”菜单

“密码管理器”提供了一种方便快捷的方法来启动已创建登录的网站和程序。只需在“密码管理器”的“登录”菜单或**管理**标签中双击某个程序或网站登录，即可启动其登录屏幕并填充登录数据。默认情况下，还会立即向网站提交该信息，但您可以选择不提交该信息，即，在最初设置或编辑登录时取消选中**提交帐户数据**。

在创建登录时，该登录将自动添加到“密码管理器”的“登录”菜单中。

要显示“登录”菜单，请按“密码管理器”组合热键。默认为 Ctrl-H，但您可以从 **密码管理器** > **设置**中更改组合热键。

将登录划分到不同类别中

可以使用类别有条理地划分登录。您可以轻松创建一个或多个类别，并将登录拖放到所需的类别中。

要添加类别，请执行以下操作：

1. 在 Security Manager 左窗格中，选择 **密码管理器**。
2. 选择**管理**标签，然后单击**添加类别**。
3. 输入该类别的名称。
4. 单击**确定**。

要将登录添加到类别中，请执行以下操作：

1. 将鼠标指针放在所需的登录上。
2. 按住鼠标左键。
3. 将登录拖到类别列表中。在将鼠标移到类别上时，将会突出显示这些类别。
4. 在突出显示所需的类别时，松开鼠标按钮。

不会将登录移到该类别中，而只是将其复制到选定类别中。这意味着，您可以将相同登录添加到多个类别中。并且，可以始终通过单击**全部**来查看所有登录。

管理登录

通过使用“密码管理器”，您可以从一个中心位置轻松且直观地管理登录信息（用户名、密码和多个登录帐户）。

将在**管理**标签中列出您的登录。只要为同一网站创建了多个登录，就会在登录列表中该网站名称下面以缩进方式列出每个登录。

要管理登录，请执行以下操作：

在 Security Manager 左窗格中，选择 **密码管理器**，然后单击**管理**标签。

- 添加登录 - 单击**添加登录**，然后按照屏幕上的说明进行操作。
- 编辑登录 - 选择一个登录并单击**编辑**，然后根据需要更改登录数据。
- 删除登录 - 选择一个登录，然后单击**删除**。

要为网站或程序添加其它登录，请执行以下操作：

1. 启动网站或程序的登录屏幕。
2. 单击“密码管理器”图标以显示其快捷菜单。
3. 选择**添加其它登录**，然后按照屏幕上的说明进行操作。

评估密码强度

使用增强密码登录到网站和程序是保护您的身份的一个重要方面。

“密码管理器”通过即时且自动地分析用于登录到网站和程序的每个密码的强度，使监视和提高安全性的过程变得轻轻松松。您可以在“密码管理器”的**密码强度**标签中检查登录使用的密码强度。

“密码管理器”图标设置

“密码管理器”尝试识别网站和程序的登录屏幕。在发现尚未创建登录的登录屏幕时，“密码管理器”将显示带加号 (+) 的“密码管理器”图标，提示您为该屏幕添加登录。

可以配置以下设置：

- 始终提示 - 选择此选项，以使“密码管理器”在显示的登录屏幕尚未设置登录时始终提示您添加登录。
- 不提示此屏幕 - 选择此选项，以使“密码管理器”不再提示您为该特定登录屏幕添加登录。
- 从不提示 - 选择此选项，以确保“密码管理器”从不提示尚未设置的登录屏幕。

8 File Sanitizer for HP ProtectTools

利用 File Sanitizer 这一工具，您可以安全地清除计算机上的重要文件和文件夹（个人信息或文件、历史数据、与 Web 有关的数据或其它类型数据），并定期清理硬盘驱动器。

注： File Sanitizer 当前只能在硬盘驱动器上运行。

关于碎化

在 Windows 中删除文件及/或文件夹并不是从硬驱上完全删除它们。Windows 仅删除其参考。内容仍然保留在硬驱上，直到另一个文件用新的信息覆盖此硬驱上的同一个区域为止。

碎化不同于标准 Windows 删除操作（在 File Sanitizer 中也称为简单删除），因为在碎化数据时，实际上是不可能恢复那个数据的。

在您选择碎化配置文件（高安全保护、中安全保护或低安全保护）时，预定义的文件及/或文件夹列表和清除方法是为碎化自动选择的。您还可以定制碎化配置文件，使您能够指定一系列的碎化周期操作，包括用于碎化的文件、碎化前要确认的文件和要排除在碎化以外的文件。

您可以设置自动碎化计划表，还可以在任何时候您想要时手动地碎化文件及/或文件夹。

关于可用空间清理

空闲空间清理使您能够在删除的文件上安全地随机写入数据，防止用户查看已经删除文件的原来内容。

注： 空闲空间清理用于采用 Windows 回收站或手动删除文件时所删除的那些文件。空闲空间清理对碎化的文件不提供额外的安全保护。

您可以设置一个自动的可用空间清理计划，也可以使用任务栏最右侧通知区域中的 HP ProtectTools 图标手动激活可用空间清理。

设置步骤

打开 File Sanitizer

要打开 File Sanitizer，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools Security Manager**。
2. 在 Security Manager 左窗格中，单击 **File Sanitizer**。

   - 或 -

- 双击 **File Sanitizer** 图标。

  - 或 -

- 右击任务栏最右侧的通知区域中的 HP ProtectTools 图标，突出显示 **File Sanitizer**，然后单击**打开 File Sanitizer**。

设置可用空间清理计划

要设置可用空间清理计划，请执行以下操作：

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**清理**。
2. 选中**激活计划程序**复选框，输入 Windows 密码，然后输入清理硬盘驱动器的日期和时间。
3. 单击**保存**图标。

注： 可用空间清理操作可能需要很长时间。即使可用空间清理是在后台执行的，但由于增加了处理器的使用率，计算机的运行速度也可能会变慢。

设置碎化计划

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**碎化**。
2. 选择一个碎化选项：

   - **Windows 关机** — 选择这个选项以在 Windows 关机时碎化所选的所有文件。

     注： 如果选择该选项，在关机时将显示一个对话框，询问您是否要继续碎化选定的文件，还是要跳过该步骤。请单击“是”跳过碎化步骤，或单击“否”继续进行碎化。必须快速选择“是”或“否”选项，因为 Windows 将关闭该软件以准备关机，并生成一个错误。如果选择“否”继续进行碎化，Windows 可能会生成一个错误屏幕，指示 File Sanitizer 没有响应。请让 File Sanitizer 完成碎化，然后再次启动关机操作。

   - **Web 浏览器打开** — 选择这个选项以在打开 Web 浏览器时，碎化所选的所有与 Web 有关的文件，如浏览器 URL 历史数据。
   - **Web 浏览器退出** — 选择这个选项以在关闭 Web 浏览器时，碎化所选的所有与 Web 有关的文件，如浏览器 URL 历史数据。
   - **按键序列** — 选择此选项可使用按键序列启动碎化。
   - **计划程序** — 选择“激活计划程序”复选框，输入您的 Windows 密码，然后输入要碎化所选文件的日期和时间。
3. 单击**保存**图标。

选择或创建碎化配置文件

您可以通过选择预定义的配置文件或创建您自己的配置文件来指定清除的方法和选择要碎化的文件及/或文件夹。

选择预定义碎化配置文件

在您选择预定义的碎化配置文件（高安全保护、中安全保护或低安全保护）时，预定义的碎化方法及文件列表是自动选择的。您可以单击“查看详细信息”按钮以查看为碎化而选择的预定义文件列表。

要选择预定义碎化配置文件，请执行以下操作：

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**设置**。
2. 单击一个预定义碎化配置文件。
3. 单击**查看详细信息**以查看为碎化而选择的文件列表。
4. 在**碎化以下内容**下面，选择在碎化之前您要确认的每个文件旁边的复选框。
5. 单击**应用**。

自定义高级安全碎化配置文件

在您创建碎化配置文件时，您可以指定碎化周期数，包括用于碎化的文件、碎化前要确认的文件和要排除在碎化以外的文件：

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，单击**设置**，选择**高级安全设置**，然后单击**查看详细信息**。
2. 指定碎化周期数。

注： 对每个文件都要执行所选的一系列碎化周期操作。例如，如果您选择 3 个碎化周期，则清除数据的方式是在 3 个不同的时间执行。如果您选择高安全保护碎化周期，则碎化可能要用相当长的时间；但是，您指定的碎化周期数越大，计算机便越安全。

3. 选择要碎化的资产：
   a. 在**可用碎化选项**下，单击一个文件，然后单击**添加**。
   b. 要添加自定义文件，请单击**添加自定义选项**，输入或浏览到所需文件名或文件夹名，然后单击**确定**。单击自定义文件，然后单击**添加**。

注： 要从可用的碎化选项删除文件，单击一个文件，然后单击**删除**。

4. 在**碎化以下内容**下面，选择在碎化之前您要确认的每个文件旁边的复选框。

注： 要从碎化列表删除文件，单击此文件，然后单击**删除**。

5. 在**不要碎化以下内容**下面，单击**添加**以选择要从碎化中排除的特定文件。
6. 在配置完碎化配置文件后，单击**应用**。

自定义简单删除配置文件

简单删除配置文件执行标准文件删除而不进行碎化操作。在您定制简单删除配置文件时，您可以指定要简单删除的文件、在执行简单删除前要确认的文件和要从简单删除排除在外的文件。

注： 如果使用简单删除选项，强烈建议您定期运行可用空间清理。

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，单击**设置**，选择**简单删除设置**，然后单击**查看详细信息**。
2. 选择要删除的文件：
   a. 在**可用删除选项**下，单击一个文件，然后单击**添加**。
   b. 要添加自定义文件，请单击**添加自定义选项**，输入或浏览到所需文件名或文件夹名，然后单击**确定**。单击自定义文件，然后单击**添加**。

   注： 要从可用的删除选项删除文件，单击此文件，然后单击**删除**。
3. 在**删除以下内容**下面，选择在删除之前您要确认的每个文件旁边的复选框。

注： 要从删除列表删除文件，单击此文件，然后单击**删除**。

4. 在**不要删除以下内容**下面，单击**添加**以选择要从碎化中排除的特定文件。
5. 在配置完简单删除配置文件后，单击**应用**。

常规任务

使用按键序列启动碎化

要指定按键序列，请执行以下步骤：

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**碎化**。
2. 选中**按键序列**复选框。
3. 在显示的框中输入一个字符，然后选中 **CTRL**、**ALT** 或 **SHIFT** 框，或者将这三个框全部选中。

   例如，要使用 S 键和 Ctrl+Shift 启动自动碎化，请在框中输入 S，然后选择 **CTRL** 和 **SHIFT** 选项。

注： 确保选择的按键序列不同于已配置的其它按键序列。

要使用按键序列启动碎化，请执行以下操作：

1. 在按下所选字符的同时，按住 Ctrl、Alt 或 Shift 键（或指定的任何组合键）。
2. 如果打开确认对话框，请单击**是**。

使用 File Sanitizer 图标

△ **注意：** 碎化的文件不能恢复。仔细考虑您选择要手动碎化的各个项目。

1. 导航到要碎化的文档或文件夹。
2. 将文件拖到桌面上的 File Sanitizer 图标上。
3. 在确认对话框打开时，单击**是**。

手动碎化一个资产

△ **注意：** 碎化的文件不能恢复。仔细考虑您选择要手动碎化的各个项目。

1. 右击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标，突出显示 **File Sanitizer**，然后单击**碎化一个**。
2. 在“浏览”对话框打开时，浏览到要碎化的文件，然后单击**打开**。

注： 选择的文件可以是单个文件或文件夹。

3. 在确认对话框打开时，单击**是**。

– 或 –

1. 右击桌面上的 **File Sanitizer** 图标，然后单击**碎化一个**。
2. 在“浏览”对话框打开时，浏览到要碎化的文件，然后单击**确定**。
3. 在确认对话框打开时，单击**是**。

– 或 –

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**碎化**。
2. 单击**浏览**按钮。
3. 在“浏览”对话框打开时，浏览到要碎化的文件，然后单击**打开**。
4. 在确认对话框打开时，单击**是**。

手动碎化所有选定的项目

1. 右击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标，突出显示 **File Sanitizer**，然后单击**立即碎化**。
2. 在确认对话框打开时，单击**是**。

– 或 –

1. 右击桌面上的 **File Sanitizer** 图标，然后单击**立即碎化**。
2. 在确认对话框打开时，单击**是**。

手动激活可用空间清理

1. 右击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标，突出显示 **File Sanitizer**，然后单击**立即清理**。
2. 屏幕上将显示一个通知泡，确认已开始清理操作。

– 或 –

1. 在 Security Manager 左窗格中，展开 **File Sanitizer**，然后单击**清理**。
2. 单击**立即清理**。
3. 屏幕上将显示一个通知泡，确认已开始清理操作。

终止碎化或可用空间清理操作

当碎化或可用空间清理操作正在进行时，将在通知区域中的 HP ProtectTools Security Manager 图标上方显示一条消息。该消息提供有关碎化或可用空间清理过程的详细信息（完成的百分比），并为您提供终止该操作的选项。

要终止该操作，请执行以下操作：

▲ 单击该消息，然后单击**停止**以取消该操作。

查看日志文件

每次执行碎化或可用空间清理操作时，都会生成任何错误或故障的日志文件。系统将始终根据最新的碎化或可用空间清理操作更新这些日志文件。

注： 成功碎化或清理的文件不会显示在日志文件中。

系统将为碎化操作创建一个日志文件，而为可用空间清理操作创建另一个日志文件。这两个日志文件都位于硬盘驱动器上：

- C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

此安全保护工具仅供管理员使用。Device Access Manager for HP ProtectTools 具有以下安全保护功能，可防止他人未经授权擅自访问连接到您的计算机系统的设备：

- 为每个用户创建设备配置文件以定义设备访问权限
- 可以根据组成员资格授予或拒绝设备访问权限

注： Device Access Manager 使用 Windows 本地用户和群组来管理访问。Windows 家庭版不支持本地用户和群组，因此 Device Access Manager 不能正常工作。不过，如果使用 DOS 命令进行用户设置，则 Device Access Manager 可以在 Microsoft Windows Vista 家庭版中使用。有关说明，请参阅 Device Access Manager 帮助文件。

启动后台服务

要应用设备配置文件，HP ProtectTools Device Locking/Auditing 后台服务必须正在运行。第一次尝试应用设备配置文件时，HP ProtectTools 管理控制台将打开一个对话框，询问您是否要启动该后台服务。请单击**是**以启动该后台服务，并将其设置为在每次系统引导时自动启动。

简单配置

Device Access Manager 在初始化时会建立一个名为“设备管理员”的新用户组，以便以管理员身份访问或使用设备。对于您控制的设备，可以通过 Device Access Manager 的“简单配置”将您想要为其赋予管理员访问权限的用户放入该用户组中。

您可以使用此功能来拒绝对下类设备的访问：

- 所有非设备管理员用户的 USB 设备
- 所有非设备管理员用户的所有可移动介质（软盘、个人音乐播放器、手写笔驱动器等）
- 所有非设备管理员用户的所有 DVD/CD-ROM 驱动器
- 所有非设备管理员用户的所有串行和并行端口

要拒绝访问所有非设备管理员用户的某类设备，请执行以下操作：

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击 **Device Access Manager**，然后单击**简单配置**。
3. 在右窗格中，选中表示要拒绝访问的设备的复选框。

4. 单击**保存**图标。

注： 如果后台服务未运行，则它立即尝试启动。单击**是**允许它启动。

5. 单击**确定**。

设备类别配置（高级）

还有更多选项可用来授予或者拒绝特定用户或用户组对多个设备类型的访问。

添加用户或组

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**设备类别配置**。
3. 在设备列表中，单击要配置的设备类别。
4. 单击**添加**。随即打开**选择用户或组**对话框。
5. 单击**高级**，然后单击**立即查找**以查找要添加的用户或组。
6. 单击要添加到有效用户和组列表中的用户或组，然后单击**确定**。
7. 单击**确定**。

删除用户或组

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**设备类别配置**。
3. 在设备列表中，单击要配置的设备类别。
4. 单击要删除的用户或组，然后单击**删除**。

拒绝或允许用户或组进行访问

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**设备类别配置**。
3. 在设备列表中，单击要配置的设备类别。
4. 在**用户/组**中，单击要拒绝其访问的用户或组。
5. 单击要拒绝其访问的用户或组旁边的**拒绝**。
6. 单击**保存**图标，然后单击**确定**。

用户访问设置（高级）

在“用户访问设置”中，管理员可以指定允许哪些用户和组使用“简单配置”和“设备类别配置”视图。

要查看“简单配置”和“设备类别配置”信息，必须为用户或组授予**查看（只读）配置设置**访问权限。

要更改“简单配置”和“设备类别配置”信息，必须为用户或组授予**更改配置设置**访问权限。

要在“简单配置”和“设备类别配置”视图中修改设置，必须为用户或组授予**完全用户管理员权限**访问权限。

添加用户或组

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**用户访问设置**。
3. 单击**添加**。将打开**选择用户或组**对话框。
4. 单击**高级**，然后单击**立即查找**以搜索要添加的用户或组。
5. 单击要添加到可用用户和组列表中的用户或组，然后单击**确定**。
6. 单击**确定**。
7. 单击**保存**图标。

删除用户或组

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**用户访问设置**。
3. 单击要删除的用户或组，然后单击**删除**。
4. 单击**保存**图标。

允许或拒绝权限

1. 依次单击**开始**、**所有程序**和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，展开 **Device Access Manager**，然后单击**用户访问设置**。
3. 在**组或用户名**框中，选择一个用户或组名称。
4. 在**权限**框中，选中相应权限的**允许**或**拒绝**复选框。
5. 单击**保存**图标。

术语表

Windows 管理员。
拥有完全权限、可以修改权限以及管理其他用户的用户。

Windows 用户帐户。
有权登录到网络或个人计算机的用户的配置文件。

安全登录方法。
用于登录到计算机的方法。

按键序列。
这是一组特定键组合，按下时会启动自动碎化 - 例如，Ctrl+Alt+S。

重新引导。
重新启动计算机的过程。

管理员。
请参见 Windows 管理员。

简单删除。
安全地删除敏感信息，包括文件、历史数据或与网络有关的内容，或其他保密数据。

开机验证。
在计算机开启时要求某些验证方式的安全特征，如密码。

可用空间清理。
在硬盘驱动器中安全地写入随机数据以覆盖删除的文件，从而改变已删除文件的内容，使数据恢复变得更加困难。

凭证。
在验证过程中，用户证明有资格承担特定任务的方法，如用户名和密码。

清理
请参见**可用空间清理**。

手动碎化。
立即碎化某个资产或选定资产，这可跳过自动碎化计划。

碎化配置文件。
指定的清除方法和资产列表。

碎化周期。
对每个资产执行碎化算法的次数。选择的碎化周期数越高，计算机就会越安全。

碎化。
执行一个算法以掩盖资产中包含的数据。

网络帐户。
本地计算机、工作组或域中的 Windows 用户或管理员帐户。

验证。
验证用户是否有权执行任务的过程，如访问计算机、修改特定程序的设置或查看安全数据。

域。
构成网络并共用同一目录数据库的一组计算机。域具有唯一的名称，并且每个域都具有一组通用的规则和程序。

资产。
位于硬盘驱动器上的数据组件，其中包括个人信息或文件、历史数据或与 Web 有关的数据等等。

自动技术管理器 (ATM)。
允许网络管理员在 BIOS 级别远程管理系统。

自动碎化。
用户在 File Sanitizer for HP ProtectTools 中设置的预定碎化。

索引

J

K

M

P

S

W

X

Y