HP ProtectTools

使用入门

第 1 版：2012 年 8 月

文档部件号：702113-AA1

目录

1 安全保护简介 1

HP ProtectTools 功能 1

HP ProtectTools 安全保护产品的说明和常用示例 2

Password Manager 2

Drive Encryption for HP ProtectTools（仅限某些机型） 3

Device Access Manager for HP ProtectTools（仅限某些机型） 3

Computrace for HP ProtectTools（以前成为 LoJack Pro，需单独购买） 3

实现关键安全保护目标 4

防止有针对性的盗窃 4

限制对机密数据的访问 4

防止从内部或外部位置进行非授权访问 5

创建强密码策略 5

更多安全保护元素 5

分配安全保护角色 5

管理 HP ProtectTools 密码 5

创建安全密码 6

备份凭证和设置 6

2 入门 7

HP Client Security 设置向导 7

HP ProtectTools Security Manager 设置向导 8

HP Client Security 控制板 8

3 针对小型企业的简易设置指南 9

入门 9

Password Manager 9

在 Password Manager 中查看和管理保存的验证 10

Device Access Manager for HP ProtectTools 11

Drive Encryption for HP ProtectTools 11

4 HP ProtectTools Security Manager 管理控制台 13

入门 13

HP Client Security 设置向导 13

HP ProtectTools Security Manager 设置向导 14

HP Client Security 控制板 14
打开 HP ProtectTools 管理控制台 15
使用管理控制台 15
配置系统 15
为计算机设置验证 16
登录策略 16
会话策略 16
设置 17
管理用户 17
凭证 17
SpareKey 17
指纹 18
脸 18
智能卡 18
初始化智能卡 18
注册智能卡 19
配置智能卡 19
非接触卡 20
接近卡 20
Bluetooth 20
PIN 20
应用程序 20
“常规”标签 21
“应用程序”标签 21
数据 21
计算机 21

5 HP ProtectTools Security Manager 22

打开 Security Manager 22
使用 Security Manager 用户控制台 22
个人 ID 卡 23
我的登录 23
Password Manager 23
对于尚未创建登录的网页或程序 24
对于已创建登录的网页或程序 24
添加登录 24
编辑登录 25
使用“Password Manager 快速链接”菜单 26
将登录划分到不同类别中 26

管理登录 26
评估密码强度 27
Password Manager 图标设置 27
设置 28
Credential Manager 28
更改 Windows 密码 28
设置 SpareKey 28
注册指纹 29
为脸部登录注册图谱 29
验证 30
黑暗模式 30
学习 30
删除图谱 31
高级用户设置 31
设置智能卡 31
初始化智能卡 31
注册智能卡 31
更改智能卡 PIN 32
非接触卡 32
接近卡 32
Bluetooth 32
PIN 32
管理 33
高级 33
设置首选项 33
备份和恢复数据 33

6 Drive Encryption for HP ProtectTools（仅限某些机型） 35

打开 Drive Encryption 35
常规任务 36
针对标准硬盘驱动器激活 Drive Encryption 36
针对自我加密驱动器激活 Drive Encryption 36
停用 Drive Encryption 37
在激活 Drive Encryption 后登录 38
通过加密硬盘驱动器来保护数据 38
高级任务 39
管理 Drive Encryption（管理员任务） 39
使用含 TPM 的增强安全（仅限某些机型） 39
加密或解密个别驱动器分区（仅软件加密） 39

备份和恢复（管理员任务） 40
备份加密密钥 40
使用备份密钥恢复访问激活的计算机 40
执行 HP SpareKey 恢复 41
显示加密状态 41

7 HP ProtectTools Device Access Manager（仅限某些机型） 43
打开 Device Access Manager 43
设置步骤 43
配置设备访问权限 43
简单配置 44
启动后台服务 44
设备类别配置 45
拒绝用户或组的访问 46
允许用户或组的访问 46
允许组中的一个用户访问某类设备 46
允许组中的一个用户访问特定设备 47
删除用户或组的设置 47
重置配置 47
JITA 配置 48
为用户或组创建 JITA 48
创建用户或组的可延长 JITA 49
禁用用户或组的 JITA 49
高级设置 49
设备管理员组 50
eSATA 设备支持 50
无管理的设备类别 50

8 失窃找回（仅限某些机型） 52

9 本地化的密码例外情况 53
在拒绝密码时该怎么办 53
Preboot Security 或 HP Drive Encryption 级别不支持 Windows IME 53
使用支持的其它键盘布局更改密码 53
特殊按键处理 54

术语表 56

索引 59

1 安全保护简介

HP ProtectTools Security Manager 软件提供的安全保护功能有助于防止他人未经授权擅自访问计算机、网络和重要的数据。

应用程序	功能
HP ProtectTools Security Manager 管理控制台(供管理员使用)	• 需要有 Microsoft Windows® 管理员权限，才能访问。 • 提供由管理员配置，对用户不可用的模块的访问权限。 • 允许初始安全设置并为所有用户配置选项或要求。
HP ProtectTools Security Manager 用户控制台（供用户使用）	• 允许用户配置由管理员提供的选项。 • 允许管理员为用户提供对某些 HP ProtectTools 模块的有限控制。

可用于您的计算机的软件模块可能因您的型号而异。

HP ProtectTools 软件模块可以是预安装的、预装载的或者可从 HP 网站下载。有关详细信息，请转到 http://www.hp.com。

注： 本指南中的说明假设您已安装了适用的 HP ProtectTools 软件模块。

HP ProtectTools 功能

下表详述了 HP ProtectTools 模块的关键功能。

模块	关键功能
HP ProtectTools Security Manager 管理控制台	管理员可以执行以下功能： • 使用 Security Manager 设置向导设置和配置安全保护级别和安全保护登录方法。 • 配置对用户隐藏的选项。 • 激活 Drive Encryption 并配置用户访问。 • 配置 Device Access Manager 策略和用户访问。 • 使用管理员工具添加和删除 HP ProtectTools 用户以及查看用户状态。
HP ProtectTools Security Manager 用户控制台	一般用户可以执行以下功能： • 查看加密状态和 Device Access Manager 的设置。 • 激活 Computrace for HP ProtectTools。 • 配置首选项以及备份和恢复选项。

模块	关键功能
Credential Manager	一般用户可以执行以下功能： • 更改用户名和密码。 • 配置和更改用户凭证，如 Windows 密码、指纹、脸部图像、智能卡、感应卡或无触点卡。
Password Manager	一般用户可以执行以下功能： • 组织和设置用户名和密码。 • 创建更强的密码以提高帐户安全性。Password Manager 自动填充并提交信息。 • 通过单一登录功能简化登录过程，以便自动记住并应用用户凭证。
Drive Encryption for HP ProtectTools（仅限某些机型）	• 提供完全的整卷硬盘驱动器加密。 • 强制进行预引导验证，以便解密并访问数据。 • 提供用于激活自加密驱动器的选项（仅限某些机型）。
Device Access Manager for HP ProtectTools（仅限某些机型）	• 允许 IT 经理根据用户配置文件来控制对设备的访问。 • 防止非授权用户使用外部存储介质删除数据或从外部介质中将病毒引入系统。 • 允许管理员禁止特定个人或用户组访问通信设备。
失窃找回（Computrace for HP ProtectTools，单独购买）	• 需要单独购买跟踪和追踪订阅，才能激活。 • 提供安全的资产跟踪。 • 监控用户活动以及硬件和软件更改。 • 即使硬盘驱动器被重新格式化或被更换，仍可保持活动状态。

HP ProtectTools 安全保护产品的说明和常用示例

大部分 HP ProtectTools 安全保护产品都既有用户验证（通常是密码），又有管理备份来获取访问权限。后者可以在密码丢失、不可用或已忘记，或者公司安全保护需要访问权限时使用。

注： 某些 HP ProtectTools 安全保护产品专用于限制对数据的访问。如果数据十分重要，以致于用户宁愿丢失信息也不愿泄露数据，就应该对数据进行加密。建议将所有数据都备份到安全的位置。

Password Manager

Password Manager 存储用户名和密码，可以用于：

- 保存用于 Internet 访问或电子邮件的登录名和密码。
- 自动将用户登录到网站或电子邮件。
- 管理和组织验证。
- 选择一个 Web 或网络资产并直接访问链接。
- 在必要时查看名称和密码。

示例 1： 大型制造商的采购代理通过 Internet 完成大部分公司交易。另外，她还经常访问多个需要登录信息的流行网站。她强烈意识到安全的重要性，因此不在每个帐户上使用相同的密码。这位采购代理已决定使用 Password Manager 来匹配具有不同用户名和密码的 Web 链接。当她转到某个网站进行

登录时，Password Manager 会自动提供凭证。如果她希望查看用户名和密码，可以对 Password Manager 进行配置使其显示它们。

另外，Password Manager 还可以用于管理和组织验证。该工具将允许用户选择一个 Web 或网络资产并直接访问链接。而且，用户还可以在必要时查看用户名和密码。

示例 2： 工作勤奋的 CPA 得到了升职，现在将管理整个财务部门。该团队必须登录到大量客户 Web 帐户，而每个帐户都使用不同的登录信息。这些登录信息需要与其他员工共享，因此，机密性就成了问题。该 CPA 决定将所有 Web 链接、公司用户名和密码都组织到 Password Manager 内。完成后，这位 CPA 将 Password Manager 部署到员工，以使他们能够在 Web 帐户上工作，但永不知道所使用的登录凭证。

Drive Encryption for HP ProtectTools（仅限某些机型）

Drive Encryption 用于限制对整个计算机硬盘驱动器或辅助驱动器上的数据的访问。另外，Drive Encryption 还可以管理自加密驱动器。

示例 1： 一位医生希望确保只有他自己可以访问其计算机硬盘驱动器上的任何数据。他激活 Drive Encryption，这就需要在 Windows 登录前进行预引导验证。进行设置后，在操作系统启动前，没有密码就不能访问硬盘驱动器。他还可以通过选择使用自加密驱动器选项加密数据，来进一步增强驱动器安全性。

Drive Encryption for HP ProtectTools 不允许访问加密数据（即使在卸下驱动器后），因为它们都绑定到原始主板。

示例 2： 一位医院管理员希望确保只有医生和授权人员可以访问本地计算机上的任何数据，而且不共享个人密码。IT 部门添加了管理员、医生以及所有授权人员并使他们成为 Drive Encryption 用户。现在，只有授权人员可以使用个人用户名和密码来引导计算机或域。

Device Access Manager for HP ProtectTools（仅限某些机型）

Device Access Manager for HP ProtectTools 允许管理员限制和管理对硬件的访问。Device Access Manager for HP ProtectTools 可以用于阻止非授权访问 USB 闪存驱动器，以免将数据复制到那里。另外，它还可以限制对 CD/DVD 驱动器的访问、USB 设备的控制、网络连接等。示例情况是：外部供应商需要访问公司计算机，但不应该能够将数据复制到 USB 驱动器。

示例 1： 一位医疗供应公司经理经常在公司信息中处理个人医疗记录。员工们需要访问该数据，但绝对不能让 USB 驱动器或任何其它外部存储介质移动计算机中的数据。网络是安全的，但计算机有 CD 刻录机和 USB 端口，可能会导致数据被复制或被盗。这位经理使用 Device Access Manager 来禁用 USB 端口和 CD 刻录机，使其无法被使用。即使阻止了 USB 端口，鼠标和键盘仍继续起作用。

示例 2： 一家保险公司不希望员工从家中安装或加载个人软件或数据。某些员工需要访问所有计算机上的 USB 端口。其 IT 经理使用 Device Access Manager 来允许某些员工进行访问，而禁止其他员工进行外部访问。

Computrace for HP ProtectTools（以前成为 LoJack Pro，需单独购买）

Computrace for HP ProtectTools（单独购买）是一项能让用户在计算机被盗时通过访问 Internet 来跟踪被盗计算机位置的服务。Computrace for HP ProtectTools 还可以帮助远程管理和定位计算机，以及监控计算机使用情况和应用程序。

示例 1： 一位校长让 IT 部门对学校里的所有计算机进行跟踪。在对计算机进行盘点后，IT 管理员将所有计算机都注册到 Computrace 中，以便在万一被盗时能够对它们进行追踪。最近，学校发现有几台计算机不见了，因此，IT 管理员向有关当局和 Computrace 官员报了警。这些计算机被有关当局找到并归还给学校。

示例 2： 一家房地产公司需要管理和更新世界各地的计算机。他们使用 Computrace 来监控和更新计算机，而不必为每台计算机配备一名 IT 人员。

实现关键安全保护目标

HP ProtectTools 的各个模块可以彼此协作，为许多安全保护问题提供解决方案，包括以下关键安全保护目标：

- 防止有针对性的盗窃
- 限制对机密数据的访问
- 防止从内部或外部位置进行非授权访问
- 创建强密码策略

防止有针对性的盗窃

例如，一台含有机密数据和客户信息的计算机在机场安检口被盗就属于有针对性的盗窃。以下功能可帮助防止有针对性的盗窃：

- 预引导验证功能可帮助防止访问操作系统（在启用后）。
  - Security Manager for HP ProtectTools—请参阅第 22 页的 HP ProtectTools Security Manager。
  - Drive Encryption for HP ProtectTools—请参阅第 35 页的 Drive Encryption for HP ProtectTools（仅限某些机型）。
- 加密可帮助确保数据无法被访问，即使硬盘驱动器被卸下并装入一个不受保护的系统。
- Computrace 可以在计算机被盗后对计算机的位置进行跟踪。
  - Computrace for HP ProtectTools—请参阅第 52 页的失窃找回（仅限某些机型）。

限制对机密数据的访问

假设一位合同审核员在单位工作，可以访问计算机以审查机密的财务数据；您不希望这位审核员能够打印文件或将文件保存到可写设备（如 CD）中。以下功能可帮助限制对数据的访问：

- Device Access Manager for HP ProtectTools 能让 IT 经理限制对通信设备的访问，以使机密信息无法从硬盘驱动器中复制出来。请参阅第 45 页的设备类别配置。

防止从内部或外部位置进行非授权访问

不受保护的业务计算机一旦遭到非授权访问，极有可能会对公司网络资源（如财务服务、主管人员或研发团队发出的信息）以及私人信息（如患者记录或个人财务记录）造成危险。以下功能可帮助防止非授权访问：

- 预引导验证功能可帮助防止访问操作系统（在启用后）。
  - Security Manager for HP ProtectTools—请参阅第 22 页的 HP ProtectTools Security Manager。
  - Drive Encryption for HP ProtectTools—请参阅第 35 页的 Drive Encryption for HP ProtectTools（仅限某些机型）。
- Security Manager 可帮助确保非授权用户无法获得密码或访问受密码保护的应用程序。请参阅第 22 页的 HP ProtectTools Security Manager。
- Device Access Manager for HP ProtectTools 能让 IT 经理限制对可写设备的访问，以使机密信息无法从硬盘驱动器中复制出来。请参阅第 43 页的 HP ProtectTools Device Access Manager（仅限某些机型）。

创建强密码策略

如果公司实施一项政策，要求对大量基于 Web 的应用程序和数据库使用强密码策略，Security Manager 便可提供受保护的密码存储库和单一登录功能。请参阅第 22 页的 HP ProtectTools Security Manager。

更多安全保护元素

分配安全保护角色

在管理计算机安全保护方面（特别是对于大型组织），一个重要做法是将责任和权利分给多种类型的管理员和用户。

注： 在小型组织中或对于个人使用，这些角色可以由同一个人拥有。

对于 HP ProtectTools，安全保护责任和权限可以分成以下角色：

- 安全管理人员—定义公司或网络的安全保护级别，确定要部署的安全保护功能，例如 Drive Encryption。

  注： HP ProtectTools 中的许多功能可以由安全管理人员与 HP 合作自定义。有关详细信息，请转到 http://www.hp.com。
- IT 管理员—应用和管理由安全管理人员定义的安全保护功能。另外，还可以启用和禁用某些功能。例如，如果安全管理人员已决定部署智能卡，IT 管理员就可以启用密码和智能卡模式。
- 用户—使用安全保护功能。例如，如果安全管理人员和 IT 管理员已经为系统启用智能卡，用户就可以设置智能卡 PIN 并使用该卡进行验证。

注意： 鼓励管理员按照“最佳方法”来限制最终用户权限和用户访问。

不应向非授权的用户授予管理权限。

管理 HP ProtectTools 密码

大多数 HP ProtectTools Security Manager 功能受密码保护。下表列出常用密码、设有密码的软件模块，以及密码功能。

仅由 IT 管理员设置和使用的密码也显示在此表中。所有其它密码可以由一般用户或管理员设置。

HP ProtectTools 密码	在以下模块中设置	功能
Windows 登录密码	Windows 控制面板或 HP ProtectTools Security Manager	可以用于手动登录以及访问多种 Security Manager 功能所需的验证。
Security Manager Backup and Recovery 密码	Security Manager，单个用户	保护对 Security Manager Backup and Recovery 文件的访问。
智能卡 PIN	Credential Manager	可以用作多重验证。 可以用作 Windows 验证。 对 Drive Encryption 的用户进行验证（如果选择了智能卡）。

创建安全密码

当创建密码时，必须先遵循程序所设置的任何规范。但通常情况下，考虑以下准则可帮助您创建强密码并减少密码泄露的可能性：

- 使用多于 6 个字符（最好是多于 8 个字符）的密码。
- 在密码中混用大小写。
- 如果可能，混用字母数字字符并包括特殊字符和标点符号。
- 用特殊字符或数字替换关键字中的字母。例如，可以使用数字 1 表示字母 I 或 L。
- 组合 2 种或更多种语言的单词。
- 在词或短语中间以数字或特殊字符分隔，例如 “Mary2-2Cat45”。
- 不要将字典中出现的词语用作密码。
- 不要将您的姓名用作密码，也不要使用任何其他个人信息，如出生日期、宠物名字或母亲的娘家姓，即使是倒着拼写也不行。
- 定期更改密码。可以仅更改几个递增的字符。
- 如果记下密码，则不要将其存放在极为靠近计算机的通常能够看到的位置。
- 不要将密码保存在计算机上的文件中，如电子邮件。
- 不要分享帐户，也不要将密码告诉任何人。

备份凭证和设置

可以按以下方式备份凭证：

- 使用 Drive Encryption for HP ProtectTools 选择并备份 HP ProtectTools 凭证。
- 将 HP ProtectTools Security Manager 中的 Backup and Recovery 工具用作中央位置，以便您从某些已安装的 HP ProtectTools 模块中备份和恢复安全保护凭证。

2 入门

要配置 HP ProtectTools 的设置，请使用 HP Client Security 设置向导或 HP ProtectTools Security Manager 设置向导。

在完成 HP Client Security 设置向导后，HP Client Security 控制板上将显示应用程序状态。

HP Client Security 设置向导

注： HP ProtectTools 管理需要具有管理权限。

HP Client Security 设置向导可指导您完成设置最常用 Security Manager 功能的过程。如果此前尚未完成 HP Client Security 设置向导，您可以按照以下方法之一来启动 HP Client Security 设置向导：

▲ 在“启动”屏幕中单击或点击 **HP Client Security** 应用程序。

– 或 –

在 Windows 桌面上单击或点击 **HP ProtectTools** 小工具。

页面按照以下顺序显示：

1. **Windows 密码**—输入 Windows 密码。

   这样将使用强验证来保护您的 Windows 帐户。

2. **SpareKey**—要注册 SpareKey 选项，请选择三个安全问题。

3. **注册指纹**—如果安装了指纹识别器和相关的驱动程序，则您可以注册指纹。您必须选择并注册至少两个指纹。

4. **Drive Encryption**—如果安装了 Drive Encryption for HP ProtectTools，则您可以在主驱动器上激活加密：

   - 传统硬盘驱动器软件加密
   - 硬件加密（如果检测到自加密驱动器）。

   在启用加密之前，您必须通过以下一种或多种方法保存加密密钥：

   注： 如果此时取消向导，您将无法激活 Windows 和 Drive Encryption 验证。

   - **可移动介质**，例如 FAT 32 格式的 USB 闪存驱动器。
     - 如果在显示 Drive Encryption 页面之前检测到单个可移动设备，则默认选定该选项。
     - 如果检测到两个或更多的可移动设备，请选择显示的某个驱动器。
   - **SkyDrive**—如果检测到 Internet 连接，则可以使用该选项。

     需要使用 Windows® Live ID。输入 ID 和密码，或者注册一个 ID。

5. “完成”页面将显示成功通知，系统将提示您重新启动以激活 Drive Encryption。

HP ProtectTools Security Manager 设置向导

注： HP ProtectTools 管理需要具有管理权限。

HP ProtectTools Security Manager 设置向导将指导您完成设置 Security Manager 的功能。除了此向导中提供的设置以外，管理员还可以通过管理控制台来配置很多其它安全保护功能。这些设置适用于计算机以及共享计算机的所有用户。

要启动 HP ProtectTools Security Manager 设置向导，请执行以下操作：

▲ 单击管理控制台左面板中的**设置向导**，然后按照屏幕上的说明进行操作，直至完成设置。

管理域可以通过 HP ProtectTools Security Manager 用户控制台来启动管理控制台。有关详细信息，请参阅第 13 页的 HP ProtectTools Security Manager 管理控制台。

共享此计算机的所有用户均可使用 Security Manager 及其应用程序。

HP Client Security 控制板

如果此前已经完成 HP Client Security 设置向导，要打开 HP Client Security，请执行以下操作：

▲ 在“开始”屏幕中键入 hp，然后选择 **HP Client Security**。

控制板显示每个应用程序的功能以及相关状态的快速概览。

▲ 单击或点击应用程序行可以显示选定应用程序的更多信息：

- **立即配置**按钮表明应用程序尚未配置。单击或点击该按钮可以打开应用程序页面，以便配置该应用程序。
- **设置**按钮表明应用程序的状态良好。单击或点击该按钮可以访问应用程序的设置。
- 启动**用户控制台**以进行用户配置。
- 启动**管理控制台**以进行需要管理员权限的配置。
- 在启动用户控制台或管理控制台后，**状态控制板**将保持打开，一旦配置了设置并关闭控制台，状态将刷新。

3 针对小型企业的简易设置指南

本章专门用于演示激活 HP ProtectTools for Small Business 内的最常见和最有用选项的基本步骤。此软件中提供了许多工具和选项，能让您细调首选项和设置访问控制。此简易设置指南将侧重于让每个模块以最少设置工作量和时间运行。有关更多信息，仅需选择您感兴趣的模块，然后单击右上角的 **？** 或“帮助”按钮。此按钮将自动提供信息以帮助您了解当前显示的窗口。

入门

1. 在 Windows 桌面上双击任务栏最右侧通知区域中的 **HP ProtectTools** 图标以打开 HP ProtectTools Security Manager。
2. 输入 Windows 密码，或创建 Windows 密码。
3. 完成此设置向导。

注： 默认情况下，HP ProtectTools Security Manager 设置为强验证策略。

此设置专门用于防止在登录到 Windows 时进行非授权访问，应该在需要很高安全性时或用户经常整天不在系统旁时使用。如果您想更改此设置，请单击“会话策略”选项卡，然后进行选择。

要让 HP ProtectTools Security Manager 仅在 Windows 登录过程中进行一次验证，请按照下列过程执行操作。

1. 在 Windows 桌面上双击任务栏最右侧通知区域中的 **HP ProtectTools** 图标以打开 HP ProtectTools Security Manager。
2. 在左窗格中单击**管理**，然后单击**管理控制台**。
3. 在左窗格的**系统**下，从**安全性**组中选择**验证**。
4. 单击**会话策略**标签，然后选择会话的登录组合要求。要撤销这些选择，请单击**恢复默认值**。
5. 完成后，单击**应用**按钮。

Password Manager

密码！我们都在使用很多的密码，－特别是在需要定期访问网站或使用需要登录的应用程序的情况下。普通用户要么在所有的应用程序和网站中都使用相同的密码，要么使用具有创造性的密码但很快就忘记哪个应用程序应使用哪个密码。

Password Manager 可以自动记忆您的密码，或者让您能够辨别需要记住和忽略哪些站点。在登录计算机后，Password Manager 将向您提供加入的应用程序或网站的密码或凭证。

当您访问任何需要凭证的应用程序或网站时，Password Manager 将自动识别该网站，并询问您是否希望此软件记住您的信息。如果您希望排除某些网站，则可以拒绝请求。

要开始保存 Web 位置、用户名和密码，请执行以下操作：

1. 例如，导航至加入的网站或应用程序，然后单击网页左上角的 Password Manager 图标以添加 Web 验证。
2. 命名该链接（可选）并在 Password Manager 中输入用户名和密码。

注： Password Manager 将立即使用且针对后续访问突出显示的区域。

3. 完成后，单击**确定**按钮。
4. Password Manager 还可以为网络共享或映射网络驱动器保存您的用户名和密码。

在 Password Manager 中查看和管理保存的验证

Password Manager 能让您从中央位置查看、管理、备份和启动验证。Password Manager 还支持从 Windows 启动已保存的网站。

要打开 Password Manager，请使用以下两种方法之一：

- 使用 ctrl+Windows 徽标键+h 的键盘组合打开 Password Manager，然后单击**打开**启动并验证已保存的快捷键。

  - 或 -

- 在 Password Manager 中选择**管理**标签以打开 HP ProtectTools Security Manager，然后编辑凭据。

Password Manager’ 的**编辑**选项可用于查看和修改姓名、登录名甚至显示密码。

HP ProtectTools for Small Business 可以将所有凭证和设置备份和/或复制到另一台计算机。

Device Access Manager for HP ProtectTools

Device Access Manager 可以用于限制多种内部和外部存储设备的使用以使数据在硬盘上一直受到保护而且不离开您的企业。例如，允许用户访问您的数据，但阻止用户将数据复制到光盘、个人音乐播放器或 USB 存储设备。下面是进行此设置的简便方法。

1. 在 Windows 桌面上双击任务栏最右侧通知区域中的 **HP ProtectTools** 图标以打开 HP ProtectTools Security Manager 用户控制台。
2. 在 HP ProtectTools Security Manager 的左面板中，单击**管理**，然后单击**管理控制台**。
3. 单击 **Device Access Manager**，然后单击**设备类别配置**。
4. 下一步骤是选择谁将继续有权访问而其他任何人都将被阻止。
5. 选择要限制的硬件设备，然后单击**应用**按钮完成此过程。
6. 选择**添加**，单击**高级**，然后单击**立即查找**。
7. 选择所需的用户，然后单击**确定 > 确定 > 应用**。

   您的选择将显示在**用户/组**框中。
8. 选择用户将使用的**设备类别**，然后选择**允许**或**拒绝**，最后单击**应用**。

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools 用于通过加密整个硬盘驱动器来保护数据。即使计算机被盗和/或硬盘驱动器从原来的计算机上卸下并放入另外的计算机中，硬盘驱动器上的数据仍将受到保护。

另一个安全性优势在于 Drive Encryption 会在启动操作系统之前要求您使用用户名和密码进行正确的验证。该过程被称为预引导验证。

为了让您感到简便，多个软件模块自动同步密码，包括 Windows 用户帐户、域、Drive Encryption for HP ProtectTools、Password Manager 和 HP ProtectTools Security Manager。

使用以下简单步骤激活 Drive Encryption for HP ProtectTools：

1. 在 Windows 桌面上双击任务栏最右侧通知区域中的 **HP ProtectTools** 图标以打开 HP ProtectTools Security Manager。
2. 在左窗格中单击**管理**，然后单击**管理控制台**。
3. 在左窗格中，单击**设置向导**。
4. 在欢迎屏幕中选择**下一步**。
5. 输入 Windows 密码以启动激活向导，然后单击**下一步**。
6. 跳过 SpareKey（如果不需要它）。
7. 选中 **Drive Encryption** 框，然后单击**下一步**。
8. 选中要加密的驱动器，然后单击**下一步**。
9. Drive Encryption 配置窗口要求使用 USB 闪存驱动器或其他外部设备来存储加密恢复密钥。请确保恢复密钥的安全，因为如果预引导密码丢失或失败，它可以用于恢复数据或访问驱动器。

10. 单击**下一步**，完成此过程，然后单击**完成**。卸下 USB 闪存驱动器，然后在就绪后重新引导计算机。

11. 系统启动后，Drive Encryption 将要求您提供 Windows 密码。请输入密码，然后单击**确定**。

注： 在驱动器加密过程中，计算机运行速度可能会变慢。一旦完全加密，性能将恢复正常。在存取驱动器上的数据时，它们将根据管理员的要求进行加密或解密。

Drive Encryption 验证将通过 Windows 登录直接“链接”至 Windows 桌面，这样您便不需要重复输入密码。

4 HP ProtectTools Security Manager 管理控制台

HP ProtectTools Security Manager 软件提供的安全保护功能有助于防止他人未经授权擅自访问计算机、网络和重要的数据。HP ProtectTools Security Manager 管理是通过管理控制台功能提供的。

Security Manager 用户控制台中还提供了其它应用程序以帮助找回丢失或被盗的计算机（仅限某些机型）。

通过使用该管理控制台，本地管理员可以执行以下任务：

- 启用或禁用安全保护功能
- 指定验证所需的凭证
- 管理计算机用户
- 调整设备特定的参数
- 配置安装的 Security Manager 应用程序

入门

要配置 HP ProtectTools 的设置，请使用 HP Client Security 设置向导或 HP ProtectTools Security Manager 设置向导。

在完成 HP Client Security 设置向导后，HP Client Security 控制板上将显示应用程序状态。

HP Client Security 设置向导

注： HP ProtectTools 管理需要具有管理权限。

HP Client Security 设置向导可指导您完成设置最常用 Security Manager 功能的过程。如果此前尚未完成 HP Client Security 设置向导，您可以按照以下方法之一来启动 HP Client Security 设置向导：

▲ 在“启动”屏幕中单击或点击 **HP Client Security** 应用程序。

- 或 -

在 Windows 桌面上单击或点击 **HP ProtectTools** 小工具。

页面按照以下顺序显示：

1. **Windows 密码**—输入 Windows 密码。

   这样将使用强验证来保护您的 Windows 帐户。

2. **SpareKey**—要注册 SpareKey 选项，请选择三个安全问题。

3. **注册指纹**—如果安装了指纹识别器和相关的驱动程序，则您可以注册指纹。您必须选择并注册至少两个指纹。

4. **Drive Encryption**—如果安装了 Drive Encryption for HP ProtectTools，则您可以在主驱动器上激活加密：

   - 传统硬盘驱动器软件加密
   - 硬件加密（如果检测到自加密驱动器）。

   在启用加密之前，您必须通过以下一种或多种方法保存加密密钥：

   注： 如果此时取消向导，您将无法激活 Windows 和 Drive Encryption 验证。

   - **可移动介质**，例如 FAT 32 格式的 USB 闪存驱动器。
     - 如果在显示 Drive Encryption 页面之前检测到单个可移动设备，则默认选定该选项。
     - 如果检测到两个或更多的可移动设备，请选择显示的某个驱动器。
   - **SkyDrive**—如果检测到 Internet 连接，则可以使用该选项。

     需要使用 Windows® Live ID。输入 ID 和密码，或者注册一个 ID。

5. “完成”页面将显示成功通知，系统将提示您重新启动以激活 Drive Encryption。

HP ProtectTools Security Manager 设置向导

注： HP ProtectTools 管理需要具有管理权限。

HP ProtectTools Security Manager 设置向导将指导您完成设置 Security Manager 的功能。除了此向导中提供的设置以外，管理员还可以通过管理控制台来配置很多其它安全保护功能。这些设置适用于计算机以及共享计算机的所有用户。

要启动 HP ProtectTools Security Manager 设置向导，请执行以下操作：

▲ 单击管理控制台左面板中的**设置向导**，然后按照屏幕上的说明进行操作，直至完成设置。

管理域可以通过 HP ProtectTools Security Manager 用户控制台来启动管理控制台。有关详细信息，请参阅第 13 页的 HP ProtectTools Security Manager 管理控制台。

共享此计算机的所有用户均可使用 Security Manager 及其应用程序。

HP Client Security 控制板

如果此前已经完成 HP Client Security 设置向导，要打开 HP Client Security，请执行以下操作：

▲ 在“开始”屏幕中键入 hp，然后选择 **HP Client Security**。

控制板显示每个应用程序的功能以及相关状态的快速概览。

▲ 单击或点击应用程序行可以显示选定应用程序的更多信息：

- **立即配置**按钮表明应用程序尚未配置。单击或点击该按钮可以打开应用程序页面，以便配置该应用程序。
- **设置**按钮表明应用程序的状态良好。单击或点击该按钮可以访问应用程序的设置。
- 启动**用户控制台**以进行用户配置。
- 启动**管理控制台**以进行需要管理员权限的配置。
- 在启动用户控制台或管理控制台后，**状态控制板**将保持打开，一旦配置了设置并关闭控制台，状态将刷新。

打开 HP ProtectTools 管理控制台

使用 HP ProtectTools 管理控制台可以执行管理任务，例如设置系统策略或配置软件。通过打开 HP ProtectTools Security Manager 可以访问管理控制台：

1. 在 Windows 桌面上双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。

   - 或 -

   在**控制面板**中选择**系统和安全**，然后选择 **HP ProtectTools Security Manager**。

2. 在 Security Manager 用户控制台的左面板中，单击**管理**，然后单击**管理控制台**。

使用管理控制台

HP ProtectTools 管理控制台是管理 HP ProtectTools Security Manager 功能和应用程序的重要区域。

1. 在 Windows 桌面上双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。

   - 或 -

   在**控制面板**中选择**系统和安全**，然后选择 **HP ProtectTools Security Manager**。

2. 在 Security Manager 用户控制台的左面板中，单击**管理**，然后单击**管理控制台**。

管理控制台在左面板中的“主页”下方显示以下选择：

- **系统**—用于为用户和设备配置以下安全保护功能和验证。
  - **安全保护**
  - **用户**
  - **凭证**
- **应用程序**—用于配置 HP ProtectTools Security Manager 和 Security Manager 应用程序的设置。
- **数据**—用于配置 Drive Encryption 的设置（仅限某些机型）。
- **计算机**—用于配置 Device Access Manager 的设置。
- **设置向导**—指导您完成设置 HP ProtectTools Security Manager 的过程。
- **关于**—显示有关 HP ProtectTools Security Manager 的信息，如版本号和版权声明。
- **主区域**—显示应用程序特定的屏幕。

  ?—显示管理控制台帮助。该图标位于窗口右上角，在最小化和最大化图标旁边。

配置系统

可以从 HP ProtectTools 管理控制台左侧的菜单面板中访问**系统**组。您可以使用该组中的应用程序来管理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**—管理功能、验证和设置，以控制用户与计算机进行交互的方式。
- **用户**—设置、管理和注册此计算机的用户。
- **凭证**—管理计算机内置或连接的安全保护设备的设置以及配置这些设置。

为计算机设置验证

在“验证”应用程序中，您可以设置控制计算机访问的策略。可以指定在登录到 Windows 或在用户会话期间登录到网站和程序时验证每类用户所需的凭证。

要在计算机上设置验证，请执行以下操作：

1. 在管理控制台的左面板中，单击**安全保护**，然后单击**验证**。
2. 要配置登录验证，请单击**登录策略**标签，进行相应的更改，然后单击**应用**。
3. 要配置会话验证，请单击**会话策略**标签，进行相应的更改，然后单击**应用**。

登录策略

要定义策略以控制在登录到 Windows 时验证用户所需的凭证，请执行以下操作：

1. 在管理控制台的左面板中，单击**安全保护**，然后单击**验证**。
2. 在**登录策略**标签上选择用户类别，例如“管理员”或“标准用户”。
3. 单击验证凭证以显示编辑对话框。
4. 如果要求使用两个验证凭证的组合，请单击向下箭头以选择每个凭证，然后单击**确定**。
5. 要删除凭证，请单击 **X**，或右击该凭证，然后单击**删除**。
6. 在配置对话框上单击**是**。
7. 要确认用户能否登录，请单击**检查 HP ProtectTools 是否可以登录**。
8. 要恢复原始设置，请单击**恢复默认值**。
9. 单击**应用**。

会话策略

要定义策略以控制在 Windows 会话期间执行验证所需的凭证，请执行以下操作：

1. 在管理控制台的左面板中，单击**安全保护**，然后单击**验证**。
2. 在**会话策略**标签上选择用户类别，例如“管理员”或“标准用户”。
3. 单击验证凭证以显示编辑对话框。
4. 如果要求使用两个验证凭证的组合，请单击向下箭头以选择每个凭证，然后单击**确定**。
5. 要删除凭证，请单击 **X**，或右击该凭证，然后单击**删除**。
6. 在配置对话框上单击**是**。
7. 要确认用户能否登录，请单击**检查 HP ProtectTools 是否可以登录**。
8. 要恢复原始设置，请单击**恢复默认值**。
9. 单击**应用**。

设置

如果已在 BIOS 级别或 Drive Encryption 级别执行了验证，则要允许该计算机的用户跳过 Windows 登录，请执行以下操作：

1. 在管理控制台的左面板中，单击**安全保护**，然后单击**设置**。
2. **允许 One Step Logon**—选中该复选框以启用 One Step Logon，或清除该复选框以将其禁用。
3. 单击**应用**。

管理用户

在“用户”应用程序中，您可以监视和管理此计算机的 HP ProtectTools 用户。

将列出所有 HP ProtectTools 用户并根据通过 Security Manager 设置的策略对其进行验证，而不考虑这些用户是否已注册了使其符合这些策略要求的相应凭证。

要管理用户，请从以下设置中进行选择：

- 要添加其他用户，请单击**添加**。
- 要删除用户，请单击该用户，然后单击**删除**。
- 要为用户设置其它凭证，请单击该用户，然后单击**注册**。
- 要查看特定用户的策略，请选择该用户，然后在下面的窗口中查看策略。

凭证

在“凭证”应用程序中，您可以为 HP ProtectTools Security Manager 识别的任何内置或连接的安全保护设备配置可用的设置。

SpareKey

您可以配置是否允许使用 SpareKey 验证进行 Windows 登录，以及管理在用户的 SpareKey 注册期间向用户提出的安全保护问题。

1. 选择在 SpareKey 注册期间向用户提出的安全保护问题。

   您最多可以指定三个自定义问题，也可以允许用户键入他们自己的密码。

2. 要允许 Windows 登录使用 SpareKey 恢复，请选中该复选框。
3. 单击**应用**。

指纹

如果计算机安装或连接了指纹识别器，“指纹”页将显示以下标签：

- **注册**—选择允许用户注册的最小和最大指纹数。

  也可以从指纹识别器中清除所有数据。

  注意： 如果从指纹识别器中清除所有数据，则会清除所有用户（包括管理员）的所有指纹数据。如果登录策略只要求使用指纹，则会禁止所有用户登录到此计算机。

- **灵敏度**—移动滑块以调整在扫描指纹时指纹识别器使用的灵敏度。

  如果始终无法识别您的指纹，则可能需要选择较低的灵敏度设置。较高的设置可提高对指纹扫描变化的灵敏度，因而会降低发生误接受的可能性。**中到高**设置可以很好地兼顾安全性和简便性问题。

- **高级**—选择以下选项之一，配置指纹识别器以节省电能和改进可视反馈：
  - **已优化**—在需要时，将激活指纹识别器。首次使用指纹识别器时，您可能会感到略有延迟。
  - **节省电能**—指纹识别器响应略慢一些，但此设置需要的电能较少。
  - **完全功耗**—指纹识别器始终处于就绪状态，但此设置需要的电能最多。

脸

如果计算机安装或连接了网络摄像头，而且安装了 Face Recognition 程序，则管理员可以为 Face Recognition 设置安全级别，以便在易用性和破坏计算机安全性的难度之间实现平衡。

1. 单击**凭证**，然后单击**脸**。
2. 要提高简便性，请单击滑块以将其向左移动；要提高准确性，请单击滑块以将其向右移动。
   - **方便**—在极少数情况下，要使注册用户更方便地进行访问，请单击滑块以将其移到**方便**位置。
   - **平衡**—如果您的计算机中包含敏感信息，或者其他人可能在您的计算机所在的区域中未经授权擅自进行登录，要很好地兼顾安全性和实用性，请单击滑块以将其移到**平衡**位置。
   - **精确**—要在注册的图谱或当前光线条件低于正常水平时使用户更难进行访问，以及尽可能少地出现误接受的情况，请单击滑块以将其移到**精确**位置。
3. 要将设置恢复为原始值，请单击**恢复默认值**。
4. 单击**应用**。

智能卡

必须先由管理员初始化智能卡，然后才能使用智能卡进行验证。Windows 中支持大多数 CSP 和 PKCS11 标准智能卡。

初始化智能卡

HP ProtectTools Security Manager 可以支持许多不同的智能卡。用作 PIN 号码的字符数和字符类型可能会有所不同。智能卡生产商应提供工具来安装安全证书和管理 PIN，以供 HP ProtectTools 在其安全算法中使用。

注： 必须安装智能卡中间件。

1. 获取并安装所用智能卡的中间件（如 ActivIdentity 智能卡的中间件为 ActivClient 6.x）。
2. 将智能卡插入读卡器。

3. 初始化（格式化）智能卡。

   a. 启动智能卡初始化工具，也可在将智能卡插入读卡器时显示此工具。

   b. 按照屏幕上的说明设置 PIN。

   c. 记下解锁代码供将来参考。

4. 创建密钥对和安全证书。

   a. 启动 **HP ProtectTools 管理控制台**。

   b. 依次单击**凭证**、**智能卡**、**管理**标签。

   c. 确保选中**初始化智能卡**。

   d. 输入您的 PIN，单击**应用**，然后按照屏幕上的说明进行操作。

      成功地初始化智能卡之后，需要注册智能卡。

注册智能卡

初始化智能卡后，管理员可以在 HP ProtectTools 管理控制台中将智能卡注册为一种验证方法：

1. 单击**设置向导**。
2. 在**欢迎使用**屏幕中，单击**下一步**。
3. 输入您的 Windows 密码，然后单击**下一步**。
4. 在 **SpareKey** 页中，单击**跳过 SpareKey 设置**（除非要更新 SpareKey 信息），然后单击**下一步**。
5. 在**启用安全保护功能**页中，单击**下一步**。
6. 在**选择您的凭证**页中，确保选中**智能卡**，然后单击**下一步**。
7. 在**智能卡**页中，输入您的 PIN，然后单击**下一步**。
8. 单击**完成**。

用户还可以在 Security Manager 用户控制台中注册智能卡。有关详细信息，请单击“智能卡”页右上角的蓝色 **?** 图标以参阅 HP ProtectTools Security Manager 软件帮助。

配置智能卡

如果计算机安装或连接了智能卡，“智能卡”页将显示两个标签：

- **设置**—选中**取出智能卡时锁定计算机**复选框以将计算机配置为在取出智能卡时自动锁定，然后单击**应用**。

  注： 只有在将智能卡用作登录 Windows 的验证凭证时，计算机才会锁定。取下未用作登录 Windows 的智能卡并不会锁定计算机。

- **管理**—从以下选项中进行选择：

  - **初始化智能卡**—准备智能卡以用于 HP ProtectTools。如果以前在 HP ProtectTools 外部初始化了智能卡（包含不对称密钥对和关联的证书），则无需重新对其进行初始化，除非需要针对特定证书进行初始化。

  - **更改智能卡 PIN**—用于更改与智能卡一起使用的 PIN。

- **仅清除 HP ProtectTools 数据**—仅清除卡初始化期间创建的 HP ProtectTools 证书。不会清除卡上的任何其他数据。
- **清除智能卡上的所有数据**—清除指定智能卡上的所有数据。该卡不能再用于 HP ProtectTools 或任何其他应用程序。

注： 无法使用智能卡或关联的中间件不支持的功能。

▲ 单击**应用**。

非接触卡

非接触卡是一张包含计算机芯片的小塑料卡。如果计算机连接了非接触卡读卡器、已安装制造商提供的相关驱动程序并且已选择非接触卡作为验证凭证，则可使用非接触卡进行验证。HP ProtectTools 支持以下几种类型的非接触卡：

- 非接触 HID iCLASS 存储卡
- 非接触 MiFare Classic 1k、4k 和微型存储卡

▲ 要设置非接触卡，请将其放在距读卡器很近的地方，按照屏幕上的说明进行操作，然后单击**应用**。

接近卡

接近卡是一张包含计算机芯片的小塑料卡。如果计算机连接了接近卡读卡器、已安装制造商提供的相关驱动程序并且已选择接近卡作为验证凭证，则可将接近卡与其它凭证配合使用以提供额外的安全保护。

▲ 要设置接近卡，请将其放在距读卡器很近的地方，然后单击**应用**。

Bluetooth

如果计算机配备了 Bluetooth® 功能、已选择 Bluetooth 作为验证凭证并且已有 Bluetooth 手机与计算机配对，则可将该 Bluetooth 手机与其它凭证配合使用以提供额外的安全保护。指定 Bluetooth 设置：

▲ 要允许无提示验证，请选中该复选框，然后单击**应用**。

PIN

如果已选择 PIN 作为验证凭证，则可将 PIN 与其它凭证配合使用以提供额外的安全保护。指定 PIN 设置：

1. 单击向上或向下箭头以选择最小 PIN 长度。

   允许的最大位数为 8。

2. 单击**应用**。

应用程序

管理控制台左面板中“应用程序”下的“设置”页中含有两个标签，从中可自定义当前安装的 HP ProtectTools Security Manager 应用程序的行为。

▲ 在管理控制台的左面板中，单击**应用程序**下面的**设置**。

“常规”标签

常规标签上提供了以下设置：

- **不要为管理员自动启动设置向导**—选择此选项可防止在登录后自动打开该向导。
- **不要为用户自动启动入门向导**—选择此选项可防止在登录后自动打开用户设置。

1. 选中或清除特定设置旁边的复选框以启用或禁用该设置。
2. 单击**应用**。

“应用程序”标签

管理员可启用或禁用以下应用程序：

- **状态**—选中该复选框以启用所有应用程序，或清除该复选框以禁用所有应用程序。
- **Password Manager**—为所有计算机用户启用 Password Manager。

1. 选中或清除特定设置旁边的复选框以启用或禁用该设置。
2. 单击**应用**。

要将所有应用程序恢复为出厂设置，请单击**恢复默认设置**按钮。

数据

在管理控制台左面板的“数据”部分中，可配置以下应用程序的设置：

- **Drive Encryption**—配置设置和显示驱动器状态。有关详细信息，请单击“Drive Encryption”页右上角的蓝色 **?** 图标以参阅 Drive Encryption 软件帮助。

计算机

在管理控制台左面板的“计算机”部分中，可配置 Device Access Manager 应用程序的设置：

- 简单配置
- 设备类别配置
- 及时验证 (JITA) 配置
- 高级设置

有关详细信息，请单击“Device Access Manager”页右上角的蓝色 **?** 图标以参阅 Device Access Manager 软件帮助。

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager 可让您显著提高计算机的安全性。

可以使用预装的 Security Manager 应用程序以及可从网站直接下载的其它应用程序来执行以下操作：

- 管理登录和密码。
- 轻松更改 Windows® 操作系统密码。
- 设置程序首选项。
- 使用指纹提供额外的安全性和简便性。
- 为验证注册一个或多个图谱。
- 为验证设置智能卡。
- 备份和恢复程序数据。
- 添加更多应用程序。

打开 Security Manager

您可以使用以下某种方法打开 Security Manager：

▲ 在 Windows 桌面上双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。

- 或 -

在**控制面板**中选择**系统和安全**，然后选择 **HP ProtectTools Security Manager**。

使用 Security Manager 用户控制台

Security Manager 用户控制台是一个中心位置，可以在其中方便地访问 Security Manager 功能、应用程序和设置。用户控制台将显示以下组件：

- **ID 卡**—显示 Windows 用户名和图标以标识登录的用户帐户。
- **安全应用程序**—显示一个可扩展的链接菜单，用于配置以下类别的安全保护功能：
  - **主页**—管理密码，设置验证凭证或检查安全应用程序状态。
  - **失窃找回**—Computrace for HP ProtectTools（单独购买）
- **我的登录**—使用 Password Manager 和 Credential Manager 管理验证凭证。
- **我的数据**—使用 Drive Encryption 管理数据的安全。

注： 如果未安装应用程序，则不会显示该项。

- **我的计算机**—使用 Device Access Manager 管理计算机的安全。

注： 如果未安装应用程序，则不会显示该项。

- **管理**—使管理员可访问**管理控制台**以管理安全性和用户。

- **高级**—显示用于访问其它功能的命令，其中包括：
  - **首选项**—用于对 Security Manager 设置进行个性化设置。
  - **备份和恢复**—用于备份或恢复数据。
  - **关于**—显示有关 HP ProtectTools Security Manager 的信息，如版本号和版权声明。
- **主区域**—显示应用程序特定的屏幕。
- **?**—显示 Security Manager 用户控制台帮助。该图标位于窗口右上角，在最小化和最大化图标旁边。

个人 ID 卡

您的 ID 卡将您唯一地标识为此 Windows 帐户的所有者，其中显示了您的名称和所选的图片。将在 Security Manager 页面左上角的醒目位置显示该卡。

您可以更改名称的显示方式。默认情况下，将显示在 Windows 设置期间选择的完整 Windows 用户名和图片。

要更改显示的名称，请执行以下操作：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 单击用户控制台左上角的 ID 卡。
3. 单击显示此帐户的 Windows 用户名的框，键入新的名称，然后单击**保存**。

我的登录

该组中包含的应用程序可帮助您管理数字身份的各个方面。

- **Password Manager**—创建和管理快速链接，通过这些链接可使用 Windows 密码、指纹、脸部、智能卡、接近卡、非接触卡、Bluetooth 手机或 PIN 进行验证以启动和登录网站和程序。
- **Credential Manager**—提供一种方法，可方便地更改 Windows 密码、注册指纹、注册脸部或设置智能卡、非接触卡、接近卡、Bluetooth 手机或 PIN。

管理员可访问有关可用的其它安全应用程序的信息，具体方法为单击**管理**，然后单击控制板左下角的**集中管理**。

Password Manager

在使用 Password Manager 时，可以更方便、更安全地登录到 Windows、网站和应用程序。可使用该程序创建强密码（不必写下或记住），然后使用指纹、脸部、智能卡、接近卡、非接触卡、PIN 或 Windows 密码方便快捷地进行登录。

Password Manager 提供了以下选项：

“管理”标签

- 添加、编辑或删除登录。
- 使用快速链接启动默认浏览器并登录到任何网站或程序（在设置后）。
- 通过拖放操作，将快速链接划分到不同类别中。
- 快速查看任何密码是否存在安全风险。

“密码强度”标签

- 检查用于网站和应用程序的个别密码的强度以及总体密码强度。
- 以红色、黄色或绿色状态指示器表示密码强度。

Password Manager 图标显示在网页或应用程序登录屏幕左上角。如果还没有为该网站或应用程序创建登录，则在该图标上显示一个加号。

▲ 单击 **Password Manager** 图标以显示一个上下文菜单，从中可选择以下选项：

- 将 [somedomain.com] 添加到 Password Manager
- 打开 Password Manager
- 图标设置
- 帮助

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 Password Manager**—用于为当前登录屏幕添加登录。
- **打开 Password Manager**—启动 Password Manager。
- **图标设置**—用于指定显示 **Password Manager** 图标的条件。
- **帮助**—显示 Security Manager 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：

- **填写登录数据**—显示“验证您的身份”页。如果验证成功，您的登录数据将自动输入登录字段，然后提交该页（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**—用于将帐户添加到 Password Manager。
- **打开 Password Manager**—启动 Password Manager。
- **帮助**—显示 Security Manager 帮助。

注： 此计算机的管理员可能已将 Security Manager 设置为在验证身份时需要多个凭证。

添加登录

可通过输入一次登录信息，轻松为网站或程序添加登录。此后，Password Manager 将自动为您输入该信息。可在浏览到网站或程序后使用这些登录，也可从 **Password Manager 快速链接**菜单中单击某个登录，让 Password Manager 打开网站或程序并进行登录。

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 **Password Manager** 图标上面的箭头，然后单击以下按钮之一，具体取决于登录屏幕是用于网站还是程序：
   - 对于网站，请单击**将 [domain name] 添加到 Password Manager**。
   - 对于程序，请单击**将此登录屏幕添加到 Password Manager**。
3. 输入您的登录数据。屏幕上的登录字段以及对话框中的相应字段是使用加粗橙色边框标识的。通过单击 **Password Manager 管理**标签中的**添加登录**、使用 ctrl+Windows 徽标键+h 热键或扫描手指，也可显示此对话框。
   a. 要使用某个预先设置了格式的选项填充登录字段，请单击该字段右侧的箭头。
   b. 要查看此登录的密码，请单击**显示密码**。
   c. 要填充登录字段但不提交，请清除**自动提交登录数据**复选框。
   d. 单击**确定**以选择要使用的验证方法（指纹、脸部、智能卡、接近卡、非接触卡、Bluetooth 手机、PIN 或密码），然后用所选验证方法进行登录。

      将从 **Password Manager** 图标中删除加号，通知您已创建登录。
   e. 如果 Password Manager 未检测登录字段，请单击**更多字段**。
      - 选中登录所需的每个字段的复选框，或消除登录不需要的任何字段的复选框。
      - 单击**关闭**。

每次访问该网站或打开该程序时，都会在网站或应用程序登录屏幕左上角显示 **Password Manager** 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，请执行以下步骤：

1. 打开网站或程序的登录屏幕。
2. 要显示可从中编辑登录信息的对话框，请单击 **Password Manager** 图标上的箭头，然后单击**编辑登录**。屏幕上的登录字段以及对话框中的相应字段是使用加粗橙色边框标识的。

   也可以通过单击 **Password Manager 管理**标签中的**编辑所需的登录**来显示此对话框。
3. 编辑登录信息。
   - 要选择具有预设格式选项的**用户名**登录字段，请单击字段右侧的向下箭头。
   - 要选择具有预设格式选项的**密码**登录字段，请单击字段右侧的向下箭头。
   - 要将屏幕上的其它字段添加到登录中，请单击**更多字段**。
   - 要查看此登录的密码，请单击**显示密码**。
   - 要填充登录字段但不提交，请清除**自动提交登录数据**复选框。
4. 单击**确定**。

使用“Password Manager 快速链接”菜单

Password Manager 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。在 **Password Manager 快速链接**菜单或 Password Manager 的**管理**标签中双击某个程序或网站登录以打开登录屏幕，然后填写登录数据。

创建登录后，会自动将该登录添加到 Password Manager 的**快速链接**菜单。

要显示**快速链接**菜单，请执行以下操作：

1. 按 **Password Manager** 组合热键（ctrl+Windows 徽标键+h 是出厂设置）。要更改组合热键，请双击 Security Manager 用户控制台中的 **Password Manager**，然后单击**设置**。
2. 扫描指纹（在内置或连接了指纹识别器的计算机上）或输入 Windows 密码。

将登录划分到不同类别中

创建一个或多个类别，以便分门别类地划分登录。然后，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 用户控制台中，单击 **Password Manager**。
2. 单击**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。在将鼠标指针移到类别上时，将会突出显示该类别。
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。您可以将相同登录添加到多个类别中，并通过单击**全部**显示所有登录。

管理登录

通过使用 Password Manager，可以从一个中心位置轻松管理用户名、密码和多个登录帐户的登录信息。

管理标签中列出了您的登录。如果为同一网站创建了多个登录，则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 用户控制台中，单击 **Password Manager**，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。
- **您的登录**—单击一个现有登录，选择以下选项之一，然后按照屏幕上的说明进行操作：
  - **打开**—打开具有现有登录的网站或程序。
  - **添加**—添加登录。有关详细信息，请参阅第 24 页的添加登录。

- **编辑**—编辑登录。有关详细信息，请参阅第 25 页的编辑登录。
- **删除**—删除具有现有登录的网站或程序。

- **添加类别**—单击**添加类别**，然后按照屏幕上的说明进行操作。有关详细信息，请参阅第 26 页的将登录划分到不同类别中。

要为网站或程序添加其它登录，请执行以下操作：

1. 打开网站或程序的登录屏幕。
2. 单击 **Password Manager** 图标以显示其上下文菜单。
3. 单击**添加登录**，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。

Password Manager 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。

在**密码强度**标签上，红色、黄色或绿色状态指示器表示用于网站和应用程序的个别密码的强度以及总体密码强度。

Password Manager 图标设置

Password Manager 尝试标识网站和程序的登录屏幕。在检测到尚未创建登录的登录屏幕时，Password Manager 将显示带有加号的 **Password Manager** 图标，以提示您为该屏幕添加登录。

1. 单击图标，然后单击**图标设置**以自定义 Password Manager 如何处理可能的登录网站。

   - **提示为登录屏幕添加登录**—单击此选项，让 Password Manager 在显示的登录屏幕尚未设置登录时提示您添加登录。
   - **排除此屏幕**—选中此复选框，以使 Password Manager 不再提示您为该登录屏幕添加登录。

     要为以前排除的屏幕添加登录，请执行以下操作：

     - 在显示以前排除的网站登录或程序页时，打开 Security Manager 用户控制台，然后单击 **Password Manager**。
     - 单击**添加登录**。

       将打开“添加登录”对话框，并在**当前屏幕**字段中列出网站登录屏幕或程序。
     - 单击**继续**。

       将显示“将登录添加到 Password Manager”屏幕。
     - 按照屏幕上的说明进行操作。有关详细信息，请参阅第 24 页的添加登录。
     - 只要打开该网站登录或程序屏幕，就会显示 **Password Manager** 图标。

     不提示为登录屏幕添加登录—选中该单选按钮。
2. 要访问其它 Password Manager 设置，请双击 **Password Manager**，然后单击 Security Manager 用户控制台上的**设置**。

设置

可指定用于对 Password Manager 进行个性化的设置：

1. **提示为登录屏幕添加登录**—检测到网站或程序登录屏幕时，**Password Manager** 图标上即显示一个加号，表示可将此屏幕的登录添加到**登录**菜单。要禁用此功能，请清除**提示为登录屏幕添加登录**旁的复选框。
2. **使用 ctrl+win+h 打开 Password Manager**—打开 **Password Manager 快速链接**菜单的默认热键是 ctrl+Windows 徽标键+h。要更改该热键，请单击此选项并输入新的组合键。组合键可能包含下面的一个或多个键：ctrl、alt 或 shift 以及任何字母或数字键。
3. 单击**应用**以保存更改。

Credential Manager

您可以使用 Security Manager 凭证来验证您的身份。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的身份的凭证。

可用的凭证可能因此计算机内置或连接的安全保护设备而有所不同。在单击**我的登录**下面的 **Credential Manager** 时，将显示支持的凭证、要求和当前状态，可能包括以下内容：

- 密码
- SpareKey
- 指纹
- 脸
- 智能卡
- 非接触卡
- 接近卡
- Bluetooth
- PIN

要注册或更改凭证，请单击该链接，然后按照屏幕上的说明进行操作。

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，请执行以下步骤：

1. 在 Security Manager 用户控制台中，单击 **Credential Manager**，然后单击**密码**。
2. 在**当前 Windows 密码**文本框中输入当前密码。
3. 在**新 Windows 密码**文本框中键入新密码，然后在**确认新密码**文本框中再次键入该密码。
4. 单击**更改**，将当前密码立即更改为输入的新密码。

设置 SpareKey

通过使用 SpareKey，您可以回答管理员以前定义的列表中的三个安全问题以访问计算机（在支持的平台上）。

在 HP ProtectTools Security Manager 设置向导中进行初始设置时，HP ProtectTools Security Manager 将提示您设置个人 SpareKey。

要设置 SpareKey，请执行以下操作：

1. 在向导的 SpareKey 页中，选择三个安全问题，然后输入每个问题的答案。
2. 单击**创建**。

可以在 **Credential Manager** 下面的 SpareKey 页中选择不同的问题或更改答案。

设置 SpareKey 后，可从预引导登录屏幕或 Windows 欢迎屏幕中使用 SpareKey 访问计算机。

注册指纹

如果管理员在**选择您的凭证**屏幕上选择了“指纹”，并且计算机内置或连接了指纹识别器，则 HP ProtectTools Security Manager 设置向导将指导您完成设置（即“注册”）指纹的过程：您也可以在 Security Manager 用户控制台的 **Credential Manager** 下面的“指纹”页面中注册指纹。

1. 在向导的“指纹”页上，将显示两只手的轮廓。已注册的手指将突出显示。单击轮廓上的一根手指。

注： 要删除以前注册的指纹，请单击该手指。

2. 系统将提示您扫描该手指，直至成功注册其指纹。注册的手指将在轮廓上突出显示。
3. 您必须至少注册两根手指；最好是食指或中指。对于其它手指，请重复步骤 1 和 2。
4. 单击**下一步**，然后按照屏幕上的说明进行操作。

注意： 在通过向导注册指纹时，在单击**下一步**后才会保存指纹信息。如果计算机处于不活动状态一段时间或关闭了该程序，则**不会**保存所做的更改。

为脸部登录注册图谱

如果选择了脸部登录，并且计算机内置或连接了网络摄像头，则 HP ProtectTools Security Manager 设置向导将提示您注册图谱。您也可以在 Security Manager 用户控制台的 **Credential Manager** 下面的“脸部登录”页面中注册图谱。

要使用脸部登录，您必须注册一个或多个图谱。在成功注册后，如果因以下一项或多项条件改变而造成登录困难，则还可以注册新的图谱：

- 在上次注册后，您的脸部发生了较大变化。
- 光线条件与以前的任何注册都差别较大。
- 在上次注册期间，您戴或没有戴眼镜。

注： 如果您在注册图谱时遇到问题，请尽量朝摄像头靠近一些。

要通过 HP ProtectTools Security Manager 设置向导注册图谱，请执行以下操作：

1. 在向导的“脸部登录”页中，单击**高级**，然后配置其它选项。有关详细信息，请参阅第 31 页的高级用户设置。
2. 单击**确定**。
3. 单击**开始**或**注册新的图谱**（如果以前注册了图谱）。
4. 在注册图谱过程中，可通过单击**播放视频**来观看演示。

   如果这是首次注册，则将显示一个对话框，询问是否要观看演示视频。单击**是**或**否**。

5. 在光线较暗的情况下，软件可自动提高屏幕亮度，或者，要更改背景光，请单击**灯泡**图标。
6. 单击**摄像头**图标，然后按照屏幕上的说明注册图谱。

注： 在采集图谱时，请务必看着您的图像，相应地转动头部。

7. 单击**下一步**。

您也可以在 Security Manager 用户控制台中注册图谱：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在**我的登录**下面，单击 **Credential Manager**，然后单击**脸**。
3. 单击**高级**以配置其它选项。有关详细信息，请参阅第 31 页的高级用户设置。
4. 单击**确定**。
5. 单击**开始**或**注册新的图谱**（如果以前注册了图谱）。
6. 如果系统提示您输入 Windows 密码，请输入它，然后单击**下一步**。
7. 在注册图谱过程中，可通过单击**播放视频**来观看演示。

   如果这是首次注册，则将显示一个对话框，询问是否要观看演示视频。单击**是**或**否**。
8. 在光线较暗的情况下，软件可自动提高屏幕亮度，或者，要更改背景光，请单击**灯泡**图标。
9. 单击**摄像头**图标，然后按照屏幕上的说明注册图谱。

注： 在采集图谱时，请务必看着您的图像，相应地转动头部。

有关详细信息，请单击“脸部注册”页右上角的蓝色 **?** 图标以参阅 Face Recognition 软件帮助。

验证

在注册一个或多个图谱后，可以在登录到计算机或开始新的 Windows 会话时使用您的脸部进行验证。

1. 在验证屏幕启动后摄像头检测您的脸部时，您有 5 秒钟的时间来启动登录过程。如果您的脸部成功通过验证，您便可以访问计算机了。
2. 如果脸部登录超时，Face Recognition 就会暂停。单击**相机**图标可恢复验证过程。

注： 如果光线不足，您无法使用 Face Recognition 登录，则可以使用 Windows 密码登录到计算机。

3. 登录到计算机后，如果 Face Recognition 要求您添加更多图谱来增强您在以后的登录会话中的登录能力，请单击**是**。

黑暗模式

如果在脸部登录过程中光线过暗，脸部登录屏幕的背景色就会自动切换为白色屏幕，以便为脸部提供更好的照明效果。

要手动切换脸部登录屏幕的背景色，请单击**灯泡**图标。

学习

如果脸部登录失败，但您成功输入了密码，系统就可能会提示您保存一组图像以提高以后脸部登录的成功几率。

删除图谱

要删除当前注册的图谱，请执行以下操作：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在**我的登录**下，单击 **Credential Manager**，然后单击**脸部**。
3. 单击要删除的图谱，然后单击**回收站**图标。
4. 在确认对话框中单击**确定**。

高级用户设置

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在**我的登录**下面，单击 **Credential Manager**，然后单击**脸**。
3. 单击**高级**以配置以下选项：

   其它设置标签—选中该复选框以启用以下一个或多个选项，或者清除复选框以禁用某个选项。这些设置仅适用于当前用户。

   - **在发生脸部识别事件时播放声音**—在脸部登录成功或失败时播放声音。
   - **在登录失败时提示更新图谱**—如果脸部登录失败，但成功输入了密码，则可能会提示您保存一系列采集的图像以提高未来脸部登录成功的可能性。
   - **在登录失败时提示注册新的图谱**—如果脸部登录失败，但成功输入了密码，则可能会提示您注册新的图谱以提高以后脸部登录的成功几率。
4. 要将设置恢复为原始值，请单击**恢复默认值**。
5. 单击**确定**。

设置智能卡

如果计算机内置或连接了智能卡读卡器，并且管理员已启用智能卡作为验证凭证并执行了 HP ProtectTools 管理控制台软件帮助中所述的步骤，则 HP ProtectTools Security Manager 设置向导将提示您插入并设置智能卡。您也可以在 Security Manager 用户控制台的 **Credential Manager** 下面的“智能卡”页中设置智能卡。

注： 管理员必须先初始化智能卡，然后才能使用。

初始化智能卡

HP ProtectTools Security Manager 可以支持许多不同的智能卡。用作 PIN 号码的字符数和字符类型可能会有所不同。智能卡制造商应提供相应工具以安装安全证书和管理 PIN，以供 HP ProtectTools 在安全算法中使用。

管理员可使用制造商’的软件和 HP ProtectTools 管理控制台初始化智能卡。有关详细信息，请参阅 HP ProtectTools 管理控制台软件帮助。

注册智能卡

初始化智能卡后，用户可以在 Security Manager 中对其进行注册：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 依次单击 **Credential Manager**、**智能卡**。

3. 确保选中**设置**。
4. 输入您的 Windows 密码和 PIN，然后单击**保存**。

另外，管理员还可以在 HP ProtectTools 管理控制台中注册智能卡。有关详细信息，请参阅 HP ProtectTools 管理控制台软件帮助。

更改智能卡 PIN

要更改智能卡 PIN，请执行以下操作：

1. 插入已经格式化和初始化的智能卡。
2. 选择**更改智能卡 PIN**。
3. 输入旧 PIN，然后输入并确认新 PIN。

非接触卡

非接触卡是一张包含计算机芯片的小塑料卡。如果计算机连接了非接触卡读卡器、管理员已安装了制造商提供的相关驱动程序并且管理员已启用非接触卡作为验证凭证，则可使用非接触卡作为验证凭证。HP ProtectTools 支持以下几种类型的非接触卡：

- 非接触 HID iCLASS 存储卡
- 非接触 MiFare Classic 1k、4k 和微型存储卡

▲ 要设置非接触卡，请将其放在距读卡器很近的地方，按照屏幕上的说明进行操作，然后单击**应用**。

接近卡

接近卡是一张包含计算机芯片的小塑料卡。如果计算机连接了接近卡读卡器、管理员已安装了制造商提供的相关驱动程序并且管理员已启用接近卡作为验证凭证，则可将接近卡与其它凭证配合使用以提供额外的安全保护。

▲ 要设置接近卡，请将其放在距读卡器很近的地方，按照屏幕上的说明进行操作，然后单击**应用**。

Bluetooth

如果管理员已启用 Bluetooth 作为验证凭证，则可设置 Bluetooth 手机与其它凭证配合使用以提供额外的安全保护。

注： 仅支持 Bluetooth 手机设备。

1. 确保在计算机上启用了 Bluetooth 功能，并确保将 Bluetooth 手机设置为发现模式。要连接手机，可能需要在 Bluetooth 设备上键入一个自动生成的代码。根据 Bluetooth 设备的配置设置，可能需要在计算机与手机之间比较配对代码。
2. 要注册手机，请选择该手机，然后单击**注册**。
3. 在确认对话框中单击**确定**。

PIN

如果管理员已启用 PIN 作为验证凭证，则可设置 PIN 与其它凭证配合使用以提供额外的安全保护。

▲ 要设置新 PIN，请输入该 PIN，然后再次输入以进行确认。

管理

管理员可以通过单击**管理**，然后选择 HP ProtectTools Security Manager 用户控制台左下角面板中的**管理控制台**来访问“管理控制台”和“集中管理”。

有关详细信息，请参阅 HP ProtectTools 管理控制台软件帮助。

高级

您可以通过单击用户控制台左下角的**高级**来访问以下选项：

- **首选项**—用于对 Security Manager 设置进行个性化设置。
- **备份和恢复**—用于备份和恢复 Security Manager 数据。
- **关于**—显示有关 Security Manager 的版本信息。

设置首选项

您可以对 HP ProtectTools Security Manager 设置进行个性化设置。在 Security Manager 用户控制台中，单击**高级**，然后单击**首选项**。将在以下两个标签中显示可用的设置：**常规**和**指纹**。

“常规”标签

外观—在任务栏通知区域中显示图标

- 要允许在任务栏中显示图标，请选中此复选框。
- 要禁止在任务栏中显示图标，请清除此复选框。

“指纹”标签

注： 只有在计算机上安装了指纹识别器和正确的驱动程序时，才会显示**指纹**标签。

- **快速操作**—可以使用快速操作选择在扫描指纹时按住指定键所执行的 Security Manager 任务。

  要为列出的某个键指定快速操作，请单击一个**（键）+ 指纹**选项，然后从菜单中选择某个可用任务。

- **指纹扫描反馈**—仅在指纹识别器可用时显示。可以使用此设置调整在扫描指纹时出现的反馈。
  - **启用声音反馈**—在扫描指纹后，Security Manager 给出一个声音反馈，对各种特定的程序事件播放不同的声音。可通过 Windows 控制面板中“声音”设置中的**声音**标签向这些事件分配新的声音，也可通过清除此选项禁用声音反馈。
  - **显示扫描质量反馈**

    要显示所有扫描，而无论质量好坏，请选中此复选框。

    要仅显示高质量的扫描，请清除此复选框。

备份和恢复数据

建议您定期备份 Security Manager 数据。备份频率取决于数据更改的频率。例如，如果您每天都添加新登录，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，这也称为导入和导出。

注： 此功能仅备份 Password Manager 和 Face Recognition 信息。Drive Encryption 具有单独的备份方法。不备份 Device Access Manager 和指纹验证信息。

接收备份数据的任何计算机上必须安装 HP ProtectTools Security Manager，然后才能从备份文件中恢复数据。

要备份数据，请执行以下操作：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在用户控制台的左面板中，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。大多数情况下，您将选择所有模块。
5. 验证您的身份。
6. 输入存储文件的名称。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。
7. 输入密码以保护该文件。
8. 单击**完成**。

要恢复数据，请执行以下操作：

1. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在用户控制台的左面板中，单击**高级**，然后单击**备份和恢复**。
3. 单击**恢复数据**。
4. 选择以前创建的存储文件。在提供的字段中输入路径，或者单击**浏览**。
5. 输入用于保护该文件的密码。
6. 选择要恢复数据的模块。大多数情况下，您将选择列出的所有模块。
7. 验证 Windows 密码。
8. 单击**完成**。

6 Drive Encryption for HP ProtectTools（仅限某些机型）

Drive Encryption for HP ProtectTools 通过加密计算机的数据，提供全面的数据保护。激活 Drive Encryption 后，必须在 Drive Encryption 登录屏幕（在 Windows 操作系统启动之前显示）® 上进行登录。

通过 HP ProtectTools Security Manager（HP Client Security 设置向导、高级设置向导或管理控制台），Windows 管理员可激活 Drive Encryption、备份加密密钥以及选择或取消选择要加密的驱动器或分区。有关详细信息，请参阅 HP ProtectTools Security Manager 软件帮助。

可以使用 Drive Encryption 执行以下任务：

- 选择 Drive Encryption 设置：
  - 激活受 TPM 保护的密码
  - 使用软件加密方式加密或解密各个驱动器或分区
  - 使用硬件加密方式加密或解密各个自我加密驱动器
  - 通过禁用睡眠或待机来确保始终要求 Drive Encryption 预引导验证，从而进一步增加了安全性

注： 只能加密内置 SATA 硬盘驱动器和外置 eSATA 硬盘驱动器。

- 创建备份密钥
- 使用备份密钥和 HP SpareKey 恢复访问加密的计算机
- 使用密码、已注册指纹或选定智能卡的 PIN 来启用 Drive Encryption 预引导验证

打开 Drive Encryption

管理员可通过打开 HP ProtectTools Security Manager 用户控制台来访问 Drive Encryption。

1. 在 Windows 桌面上双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。

   - 或 -

   在**控制面板**中选择**系统和安全**，然后选择 **HP ProtectTools Security Manager**。

2. 在 HP ProtectTools Security Manager 用户控制台的左面板中，选择**管理**，然后选择**管理控制台**。
3. 在 HP ProtectTools 管理控制台的左面板中选择 **Drive Encryption**。

常规任务

针对标准硬盘驱动器激活 Drive Encryption

标准硬盘驱动器使用软件加密方式加密。要激活 Drive Encryption，请执行以下步骤：

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击**设置向导**。
3. 选择 **Drive Encryption** 复选框，然后单击**下一步**。
4. 要备份加密密钥，请连接外部设备以记录该密钥。如果其他方法失败，则必须使用该密钥来访问数据。
5. 在 **Back up Drive Encryption keys（备份 Drive Encryption 密钥）**下，选中将要保存加密密钥的存储设备旁的复选框。
6. 单击 **Next（下一步）**。

注： 此时将提示重新启动计算机。重新启动后，显示 Drive Encryption 预引导屏幕，其中要求在 Windows 启动之前进行验证。

Drive Encryption 已经激活。加密所选的驱动器分区可能需要几小时时间，具体取决于分区的数量和大小。

有关详细信息，请参阅 HP ProtectTools Security Manager 软件帮助。

针对自我加密驱动器激活 Drive Encryption

可以使用软件或硬件加密方式对符合可信计算组 OPAL 规范的自我加密驱动器进行加密（该规范用于管理自我加密驱动器）。按照下列步骤针对自我加密驱动器激活 Drive Encryption：

注： 仅在计算机内所有驱动器均为自加密驱动器，并且符合可信计算组有关自加密驱动器管理的 OPAL 规范时，才能使用硬件加密。这种情况下，有**使用硬件驱动器加密**选项，并可使用硬件或软件加密。

如果混合使用自加密驱动器和标准硬盘驱动器，则无**使用硬件驱动器加密**选项，并且只能使用软件加密。有关详细信息，请参阅第 36 页的针对标准硬盘驱动器激活 Drive Encryption。

▲ 使用 HP ProtectTools Security Manager 设置向导可激活 Drive Encryption。

– 或 –

软件加密

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击**设置向导**。
3. 选中 **Drive Encryption** 复选框，然后单击 **Next（下一步）**。

注： 如果屏幕底部有**使用硬件驱动器加密**选项，则清除该复选框。

4. 在 **Drives to be encrypted（要加密的驱动器）**下，选中要加密的硬盘驱动器旁的复选框，然后单击 **Next（下一步）**。
5. 要备份加密密钥，请将存储设备插入相应的插槽。

6. 在 **Back up Drive Encryption keys（备份 Drive Encryption 密钥）**下，选中将要保存加密密钥的存储设备旁的复选框。
7. 单击 **Apply（应用）**。

注： 计算机将重新启动。

Drive Encryption 已被激活。根据驱动器的大小，可能需要数小时来加密驱动器。

硬件加密

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击**设置向导**。
3. 选中 **Drive Encryption** 复选框，然后单击 **Next（下一步）**。
4. 如果屏幕底部有**使用硬件驱动器加密**复选框，则确保将其选中。

   如果清除了该复选框或无该复选框，则应用软件加密。有关详细信息，请参阅第 36 页的针对标准硬盘驱动器激活 Drive Encryption。
5. 在 **Drives to be encrypted（要加密的驱动器）**下，选中要加密的硬盘驱动器旁的复选框，然后单击 **Next（下一步）**。

注： 如果只显示一个驱动器，驱动器复选框就会自动被选中并灰掉。

如果显示多个驱动器，则还将自动选择并灰显磁盘 0，但提供选择其它硬盘驱动器进行硬件加密的选项。

只有选择了至少一个驱动器，**下一步**按钮才会可用。

6. 要备份加密密钥，请将存储设备插入相应的插槽。
7. 在 **Back up Drive Encryption keys（备份 Drive Encryption 密钥）**下，选中将要保存加密密钥的存储设备旁的复选框。
8. 单击 **Apply（应用）**。

注： 此时将提示重新启动计算机。并将显示 Drive Encryption 预引导，其中要求在 Windows 启动之前进行身份验证。

Drive Encryption 已被激活。驱动器的加密过程可能需要几分钟的时间。

有关详细信息，请参阅 HP ProtectTools Security Manager 软件帮助。

停用 Drive Encryption

管理员可使用 HP ProtectTools Security Manager 设置向导停用 Drive Encryption。有关详细信息，请参阅 HP ProtectTools Security Manager 软件帮助。

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击**设置向导**。
3. 清除 **Drive Encryption** 复选框，然后单击 **Next（下一步）**。

   开始停用 Drive Encryption。

注： 如果使用了软件加密，解密便会开始。这可能需要几小时时间，具体取决于所加密的硬盘驱动器分区的大小。解密完成后，Drive Encryption 便被停用。

如果使用了硬件加密，则立即解密驱动器，并在几分钟后停用 Drive Encryption。

停用 Drive Encryption 后，如果为硬件加密，则提示关闭计算机，如果为软件加密，则提示重新启动计算机。

在激活 Drive Encryption 后登录

如果在激活 Drive Encryption 并注册您的帐户后打开计算机，则必须在 Drive Encryption 登录屏幕中登录：

注： 无论软件加密还是硬件加密，从睡眠或待机唤醒时均不显示 Drive Encryption 预引导验证。硬件加密提供**禁用睡眠模式以提高安全性**选项，这样可防止在启用睡眠或待机后发生此现象。

对于软件或硬件加密，从休眠唤醒时均显示 Drive Encryption 预引导验证。

注： 如果 Windows 管理员在 HP ProtectTools Security Manager 中启用了 BIOS Pre-boot Security 并且启用了一步登录（默认情况下），则在 BIOS 预引导时进行验证后可立即登录计算机，而无需在 Drive Encryption 登录屏幕上重新验证。

单用户登录：

- 在**登录**页面上，输入 Windows 密码、智能卡 PIN、SpareKey、脸部或者扫描经过注册的手指。

多用户登录：

1. 在**选择要登录的用户**页面上，从下拉列表中选择要登录的用户，然后单击**下一步**。
2. 在**登录**页面上，输入 Windows 密码或智能卡 PIN，或者扫描经过注册的手指。

注： 下列智能卡受到支持：

支持的智能卡

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

注： 如果使用恢复密钥在 Drive Encryption 登录屏幕上登录，则 Windows 登录时需要额外的凭证才能访问用户帐户。

通过加密硬盘驱动器来保护数据

强烈建议使用 HP ProtectTools Security Manager 设置向导通过加密硬盘驱动器来保护数据。激活后，可按以下这些步骤加密所添加的任何硬盘驱动器或所创建的任何分区：

1. 在左面板中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。
2. 单击 **Settings（设置）**。
3. 对于使用软件加密的驱动器，选择要加密的驱动器分区。

注： 这也适用于使用混合驱动器的情况，即存在一个或多个标准硬盘驱动器和一个或多个自我加密驱动器。

– 或 –

▲ 对于硬件加密的驱动器，选择其它要加密的驱动器。

高级任务

管理 Drive Encryption（管理员任务）

管理员可使用“Drive Encryption”下的“设置”页查看和更改 Drive Encryption 的状态（已启用、已禁用或硬件加密已激活）以及查看计算机上所有硬盘驱动器的加密状态。

注： 在 Drive Encryption 的“设置”页上只能选择或取消选择其它硬盘驱动器进行硬件加密。

- 如果状态为“已禁用”，则说明 Drive Encryption 未被 Windows 管理员激活，未保护硬盘驱动器。使用 HP ProtectTools Security Manager 设置向导可激活 Drive Encryption。
- 如果状态为“已启用”，则表示已激活和配置 Drive Encryption。驱动器处于以下任一状态：

软件加密

- 未加密
- 已加密
- 正在加密
- 正在解密

硬件加密

- 已加密
- 未加密（对于其它驱动器）

使用含 TPM 的增强安全（仅限某些机型）

如果激活了可信平台模块 (TPM) 并选择了含 TPM 功能的 Drive Encryption 增强安全，则 Drive Encryption 密码将受 TPM 安全保护芯片的保护。如果取下硬盘驱动器将其装入另一台计算机，则会拒绝访问该驱动器。

注意： 无法与 Windows TPM.msc 共享 TPM 所有权。

注： 由于密码受到 TPM 安全保护芯片的保护，因此，如果将硬盘驱动器移到另一台计算机上，将无法访问上面的数据，除非将 TPM 设置也迁移到该计算机上。

注： 必须在 BIOS 设置中启用 TPM 选项。

加密或解密个别驱动器分区（仅软件加密）

管理员可使用 Drive Encryption 的“设置”页加密计算机上的一个或多个硬盘驱动器分区或解密任何已加密的驱动器分区。

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。

3. 单击 **Settings（设置）**。
4. 在 **Drive Status（驱动器状态）**下，选中或清除每个希望加密或解密的硬盘驱动器旁的复选框，然后单击 **Apply（应用）**。

注： 加密或解密分区时，有一个进度条会显示加密分区的百分比和完成此过程所需的剩余时间。

注： 不支持动态分区。如果某分区显示为可用，但是选择之后无法加密，则表示该分区为动态分区。动态分区是在“磁盘管理”中减小某分区以新建分区时出现的。

将分区转换为动态分区时会出现警告。

备份和恢复（管理员任务）

激活 Drive Encryption 后，管理员可使用“加密密钥备份”页将加密密钥备份到可移动介质中，并进行恢复。

备份加密密钥

管理员可以将已加密驱动器的加密密钥备份到可移动存储设备上。

注意： 务必将含有备份密钥的存储设备放置在安全地点，因为如果忘记密码、丢失智能卡或未注册手指，则只能通过此设备访问计算机。存放地点也应受到保护，因为通过存储设备可访问 Windows。

注： 要保存加密密钥，必须使用 FAT32 或 FAT16 格式的 USB 存储设备。可使用 USB 闪存盘、安全数字 (SD) 存储卡或多媒体卡 (MMC) 进行备份。

1. 启动 **HP ProtectTools 管理控制台**。有关详细信息，请参阅第 15 页的打开 HP ProtectTools 管理控制台。
2. 在左面板中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。
3. 单击**备份加密密钥**。
4. 插入正在使用的存储设备，以备份加密密钥。

   注： 要保存加密密钥，您必须使用 FAT32 格式的 USB 存储设备。可使用 USB 闪存盘、安全数字 (SD) 存储卡或多媒体卡 (MMC) 进行备份。某些情况下可能要使用 SkyDrive。
5. 在 **Drive（驱动器）**下，选中要备份加密密钥的设备旁的复选框。
6. 单击**备份密钥**。
7. 阅读随后显示的页上的信息，然后单击**确定**。加密密钥便会保存到您选择的存储设备上。

使用备份密钥恢复访问激活的计算机

管理员可使用在激活时或通过选择 Security Manager 中的**备份 Drive Encryption 密钥**选项备份到可移动存储设备的 Drive Encryption 密钥来执行恢复。

1. 插入包含备份密钥的可移动存储设备。
2. 打开笔记本计算机。
3. 在打开 Drive Encryption for HP ProtectTools 登录对话框时，单击**选项**。
4. 单击 **Recovery（恢复）**。
5. 输入包含备份密钥的文件路径或名称，然后单击**恢复**。

   - 或 -

单击**浏览**以搜索所需的备份文件，单击**确定**，然后单击**恢复**。

6. 确认对话框打开时，请单击**确定**。

   将显示 Windows 登录屏幕。

注： 如果使用恢复密钥在 Drive Encryption 登录屏幕上登录，则 Windows 登录时需要额外的凭证才能访问用户帐户。极力建议您执行恢复操作后重置密码。

执行 HP SpareKey 恢复

Drive Encryption 预引导中的 SpareKey 恢复要求正确回答安全问题后才能访问计算机。有关设置 SpareKey 恢复的详细信息，请参阅 Security Manager 软件帮助。

要在忘记密码时执行 HP SpareKey 恢复，请执行以下步骤：

1. 打开笔记本计算机。
2. 显示“Drive Encryption for HP ProtectTools”页后，导航至用户登录页面。
3. 单击 **SpareKey**。

注： 如果尚未在 Security Manager 中初始化 SpareKey，则无 **SpareKey** 按钮。

4. 键入所显示问题的正确回答，然后单击**登录**。

   将显示 Windows 登录屏幕。

注： 如果使用 SpareKey 在 Drive Encryption 登录屏幕上登录，则 Windows 登录时需要额外的凭证才能访问用户帐户。极力建议您执行恢复操作后重置密码。

显示加密状态

用户可从 HP ProtectTools Security Manager 显示加密状态。

注： 管理员可以使用 HP ProtectTools 管理控制台更改 Drive Encryption 状态。

1. 启动 **HP ProtectTools 用户控制台**。有关详细信息，请参阅第 22 页的打开 Security Manager。
2. 在**我的数据**下，单击 **Drive Encryption**。

   在软件或硬件加密的情况中，驱动器加密状态显示为以下某项：

   - 已启用
   - 已禁用

   在软件加密的情况中，每个硬盘驱动器或硬盘驱动器分区的驱动器加密状态显示为以下某项：

   - 未加密
   - 已加密
   - 正在加密
   - 正在解密

   在硬件加密的情况中，驱动器加密状态显示为以下某项：

   - 未加密
   - 已加密

如果正在加密或解密硬盘驱动器，则会以进度条显示完成百分比以及完成加密或解密的剩余时间。

7 HP ProtectTools Device Access Manager（仅限某些机型）

HP ProtectTools Device Access Manager 通过禁用数据传输设备来控制对数据的访问。

注： Device Access Manager 不控制某些人机接口/输入设备，例如鼠标、键盘、触摸屏和指纹识别器。有关详细信息，请参阅第 50 页的无管理的设备类别。

Windows® 操作系统管理员使用 HP ProtectTools Device Access Manager 来控制对系统设备的访问，并防止未经授权的访问：

- 为每位用户创建设备配置文件，以规定允许或拒绝他们可访问的设备。
- 及时验证（JITA）允许规定的用户验证他们的身份以访问在其它情况下不能访问的设备。
- 通过将管理员和受信用户添加到“设备管理员”组中，可以将他们排除在 Device Access Manager 对设备访问所施加的限制之外。这个组的成员是用“高级设置”管理的。
- 设备的访问权可以根据小组的成员资格或单个用户进行授予或拒绝。
- 对于某些设备类别（如 CD-ROM 驱动器和 DVD 驱动器），可以分别允许或拒绝读取访问权限和写入访问权限。

打开 Device Access Manager

1. 以管理员身份登录。
2. 从 **HP Client Security 控制板**启动 **HP ProtectTools Security Manager**。

   - 或 -

   在 Windows 桌面上双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。

   - 或 -

   在**控制面板**中选择**系统和安全**，然后选择 **HP ProtectTools Security Manager**。
3. 在 HP ProtectTools Security Manager 用户控制台的左面板中，单击**管理**，然后选择**管理控制台**。
4. 在管理控制台的左面板中单击 **Device Access Manager**。

只有标准用户可以使用 HP ProtectTools Security Manager 查看 HP ProtectTools Device Access Manager 策略。这个控制台提供只读视图。

设置步骤

配置设备访问权限

HP ProtectTools Device Access Manager 提供四个视图：

- **简单配置**—根据“设备管理员”组中的成员资格允许或拒绝访问某些类别的设备。
- **设备类别配置**—对特定的用户或组，允许或拒绝他们对某些设备或特定设备的访问。

- **JITA 配置**—配置及时验证（JITA），所选用户通过验证他们的身份，允许他们访问 DVD/CD-ROM 驱动器或可移动介质。
- **高级设置**—配置 Device Access Manager 将不限制访问的驱动器字母表，例如 C 或系统驱动器。从这个视图也可以管理“设备管理员”组中的成员。

简单配置

管理员可以用**简单配置**视图授权或拒绝所有非 - 设备管理员对以下类别设备的访问：

- 所有可移动介质（软盘、USB 闪存驱动器等）
- 所有 DVD/CD-ROM 驱动器
- 所有串行和并行端口
- 所有 Bluetooth 设备

注： 如果将 Bluetooth 设备用作验证凭证，则不应在 Device Access Manager 策略中限制 Bluetooth 设备访问权限。

- 所有调制解调器设备
- 所有 PCMCIA/ExpressCard 设备
- 所有 1394 设备

要允许或拒绝所有非设备管理员访问某个类别的设备，请按照下列步骤操作：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**简单配置**。
2. 要拒绝访问，请在右窗格中选中设备类别或特定设备的复选框。清除此复选框可允许对该设备类别或特定设备进行访问。

   如果复选框显示为灰色，则表示已经从**设备类别配置**视图中更改了影响访问模式的值。要重置为工厂设置，单击**设备类别配置**视图中的**重置**。
3. 单击**应用**。

注： 如果后台服务没在运行，则会打开一个对话框，询问您是否要启动该服务。单击**是**。

4. 单击**确定**。

启动后台服务

当首次定义和应用一个新的策略时，HP ProtectTools Device Locking/Auditing 后台服务会自动启动，并且将它设置为在每次系统启动时它都会自动启动。

注： 必须定义设备配置文件才能显示后台服务提示。

管理员也可以启动或停止该服务。

停止 Device Locking/Auditing 服务并不会停止设备锁定。两个组件会强制执行设备锁定：

- Device Locking/Auditing 服务
- DAMDrv.sys 驱动程序

启动该服务将启动设备驱动程序，但停止该服务不会停止驱动程序。

要确定后台服务是否正在运行，请打开命令提示窗口，然后键入 `sc query flcdlock`.

要确定设备驱动程序是否正在运行，请打开命令提示窗口，然后键入 `sc query damdrv`.

设备类别配置

管理员可以查看和修改允许或拒绝访问某些类别设备或特定设备的用户或组的列表。

设备类别配置视图有以下几部分：

- **设备列表**—显示所有类别的设备和系统中安装的设备或系统中以前可能安装的设备。
  - 保护是通常采用的一种设备类别。所选用户或组将可以访问该设备类别中的任何设备。
  - 保护也可以应用于特定设备。
- **用户列表**—显示被允许或拒绝访问所选设备类别或特定设备的所有用户和组。
  - 可以为特定用户或用户所属的组创建“用户列表”条目。
  - 如果 User List（用户列表）中的用户或组条目不可用，则表明该设置是从 Device List（设备列表）的设备类别或从 Class 文件夹继承来的。
  - 对于某些设备类别（如 DVD 和 CD-ROM），可以通过将读取访问权限和写入访问权限分开来允许或拒绝，实施更精细的控制。

    对于其它的设备和类别，可以继承读取和写入访问权限。例如，读取访问权可以从更高的类别继承，但是可以针对具体的某个用户或组拒绝其写入访问权。

    注： 如果**读取**复选框被清除了，则访问控制条目对设备的读取访问权限没有作用，但也不会拒绝读取访问。

    注： “用户列表”中不能加入管理员组。应改用“设备管理员”组。

    例 1—如果拒绝用户或组对某个设备或某类设备进行写入访问：

    只能授权同一用户、同一组或同一组中的成员写入访问或读取兼写入访问设备层次结构中位于该设备下层的设备。

    例 2—如果允许用户或组对某个设备或某类设备进行写入访问：

    只能拒绝同一用户、同一组或同一组中的成员写入访问或读取兼写入访问同一设备或设备层次结构中位于该设备下层的设备。

    例 3—如果允许用户或组对某个设备或某类设备进行读取访问：

    只能拒绝同一用户、同一组或同一组中的成员读取访问或读取兼写入访问同一设备或设备层次结构中位于该设备下层的设备。

    例 4—如果拒绝用户或组对某个设备或某类设备进行读取访问：

    只能授权同一用户、同一组或同一组中的成员访问或读取兼写入访问设备层次结构中位于该设备下层的设备。

    例 5—如果允许用户或组对某个设备或某类设备进行读取兼写入访问：

    只能拒绝同一用户、同一组或同一组中的成员写入访问或读取兼写入访问同一设备或设备层次结构中位于该设备下层的设备。

    例 6—如果拒绝用户或组对某个设备或某类设备进行读取兼写入访问：

    只能授权同一用户、同一组或同一组中的成员读取访问或读取兼写入访问设备层次结构中处于该设备下层的设备。

拒绝用户或组的访问

要禁止某个用户或组访问一台设备或某类设备：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 在设备列表中，单击您要配置的设备类别。
   - **设备类别**
   - **所有设备**
   - **单台设备**
3. 在**用户/组**下，单击要拒绝其访问的用户或组，然后单击**拒绝**。
4. 单击**应用**。

注： 当在同一设备级别为用户设置了拒绝和允许设置时，拒绝访问将优先于允许访问。

允许用户或组的访问

要授权用户或组访问一台设备或某类设备：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 在设备列表中，单击以下任一一项：
   - **设备类别**
   - **所有设备**
   - **单台设备**
3. 单击 **Add（添加）**。

   此时将打开 **Select Users or Groups（选择用户或组）**对话框。
4. 单击 **Advanced（高级）**，然后单击 **Find Now（立即查找）**以搜索要添加的用户或组。
5. 单击需要添加到可用用户和组列表中的用户或组，然后单击 **OK（确定）**。
6. 再次单击 **OK（确定）**。
7. 单击**允许**以授予此用户访问权限。
8. 单击**应用**。

允许组中的一个用户访问某类设备

要允许用户访问某类设备，但拒绝该用户所在组中的所有其他成员进行访问：

1. 在 **HP ProtectTools 管理控制台**的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 在设备列表中，单击您要配置的设备类别。
   - **设备类别**
   - **所有设备**
   - **单台设备**

3. 在 **User/Groups（用户/组）**下，选择要拒绝其访问的组，然后单击 **Deny（拒绝）**。
4. 浏览到所要求的类别下面的文件夹，然后添加特定的用户。
5. 单击 **Allow（允许）**以授予此用户访问权限。
6. 单击**应用**。

允许组中的一个用户访问特定设备

管理员可以允许某个用户访问一台特定的设备，但拒绝该用户所在组中的所有其他成员访问此类别中的所有设备：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 在设备列表中，单击您要配置的设备类别，然后浏览到此类别下的文件夹。
3. 在 **User/Groups（用户/组）**下，单击要授予其访问权的组旁边的 **Allow（允许）**。
4. 单击要拒绝其访问的组旁边的 **Deny（拒绝）**。
5. 浏览到设备列表中允许用户访问的特定设备。
6. 单击**添加**。

   此时将打开**选择用户或组**对话框。
7. 单击 **Advanced（高级）**，然后单击 **Find Now（立即查找）**以搜索要添加的用户或组。
8. 单击要允许其访问的用户，然后单击 **OK（确定）**。
9. 单击 **Allow（允许）**以授予此用户访问权限。
10. 单击**应用**。

删除用户或组的设置

要删除用户或组对某个设备或某类设备的访问权限，请按照下列步骤操作：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 在设备列表中，单击您要配置的设备类别。
   - **设备类别**
   - **所有设备**
   - **单台设备**
3. 在 **User/Groups（用户/组）**下，单击您要删除的用户或组，然后单击 **Remove（删除）**。
4. 单击**应用**。

重置配置

注意： 重置配置将弃置所有已做的设备配置更改，并且会将所有设置恢复到出厂设置值。

注： 未对“高级设置”页进行重置。

要将配置设置重置为出厂值：

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击**设备类别配置**。
2. 单击**重置**。
3. 单击**是**以确认请求。
4. 单击**应用**。

JITA 配置

JITA 配置允许管理员查看和修改允许使用及时验证 (JITA) 来访问设备的用户或组的列表。

JITA 授权的用户将能够访问在**设备类别配置**或**简单配置**视图中创建策略已经限制的设备。

- **模式**—“简单配置”策略配置为拒绝所有非设备管理员访问 DVD/CD-ROM 驱动器。
- **结果**—试图访问 DVD/CD-ROM 驱动器的 JITA 授权用户与 JITA 未授权按的用户都收到了相同的“拒绝访问”信息。然后显示一个气球提示信息，问用户是否要采用 JITA 访问。如果单击那个气球，则会显示验证用户对话框。当用户成功输入凭证后，则可以访问 DVD/CD-ROM 驱动器。

授权的 JITA 时间可以是设好的分钟数或 0 分钟。0 分钟的 JITA 时间将不会过期。从验证后到他们注销系统前，用户都可以访问设备。

如果配置了允许延长，则 JITA 时间也可以延长。在这种情况下，JITA 时间大约要过期前 1 分钟，用户可以单击提示来延长他们的访问时间而不需要重新验证。

无论用户得到的是有限或无限的 JITA 时间，一旦用户注销系统或另一个用户登录，JITA 时间立即失效。该用户下次再登录并试图访问启用了 JITA 的设备时，都会显示输入凭证的提示。

JITA 可用于以下的设备类别：

- DVD/CD-ROM 驱动器
- 可移动介质

为用户或组创建 JITA

管理员可以允许用户或组使用及时验证来访问设备。

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击 **JITA 配置**。
2. 从设备’的下拉菜单中，选择**可移动介质**或 **DVD/CD-ROM 驱动器**。
3. 单击 **+** 以将用户或组添加到 JITA 配置。
4. 选择**已启用**复选框。
5. 将 JITA 时间设为所要求的时间。
6. 单击**应用**。

用户必须注销然后再登录才能应用新的 JITA 设置。

创建用户或组的可延长 JITA

管理员可以允许用户或组使用及时验证来访问设备，使用户在访问过期前可以延长访问时间。

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击 **JITA 配置**。
2. 从设备’的下拉菜单中，选择**可移动介质**或 **DVD/CD-ROM 驱动器**。
3. 单击 **+** 以将用户或组添加到 JITA 配置。
4. 选择**已启用**复选框。
5. 将 JITA 时间设为所要求的时间。
6. 选择**可延长**复选框。
7. 单击**应用**。

用户必须注销然后再登录才能应用新的 JITA 设置。

禁用用户或组的 JITA

管理员可以禁用用户或组采用及时验证法来访问设备。

1. 在 HP ProtectTools 管理控制台的左窗格中，单击 **Device Access Manager**，然后单击 **JITA 配置**。
2. 从设备’的下拉菜单中，选择**可移动介质**或 **DVD/CD-ROM 驱动器**。
3. 选择您要禁用其 JITA 的用户或组。
4. 清除**已启用**复选框。
5. 单击**应用**。

当那个用户登录并试图访问该设备时，访问将被拒绝。

高级设置

高级设置提供以下功能：

- 管理“设备管理员”组
- 管理 Device Access Manager 从不拒绝访问的驱动器字母。

“设备管理员”组用于将受信用户（根据设备访问权受信）排除在 Device Access Manager 策略所施加的限制之外。受信用户通常包括系统管理员。有关详细信息，请参阅第 50 页的设备管理员组。

高级设置视图还让管理员能够配置 Device Access Manager 不限制任何用户访问的驱动器字母表。

注： 在配置驱动器字母表时，Device Access Manager 后台服务必须正在运行。

要开始这些服务：

1. 应用“简单配置”策略，如拒绝所有非设备管理员访问可移动介质。

   - 或 -

   打开有管理员权限的命令提示窗口，然后键入：

   ```
   sc start flcdlock
   ```

   按 enter 键。

2. 在服务开始后，可以编辑驱动器列表。输入您不想要 Device Access Manager 控制的设备的驱动器字母表。

   显示的驱动器字母代表实际的硬盘或分区。

注： 不管系統驱动器（通常是 C）是否在这个列表之中，都不会拒绝任何用户对它的访问。

设备管理员组

安装 Device Access Manager 后，即会创建“设备管理员”组。

“设备管理员”组用于将受信用户（根据设备访问权受信）排除在 Device Access Manager 策略所施加的限制之外。受信用户通常包括系统管理员。

注： 将用户添加到“设备管理员”组并不会自动允许该用户访问设备。在**设备类别配置**视图中，如果拒绝一个用户组访问一台设备，则必须授予“设备管理员”组访问权限，以便该组的成员有访问这台设备的权限。但是，**简单配置**视图可以用来拒绝不是该“设备管理员”组的成员的所有用户对设备类别的访问。

要将用户添加到此“设备管理员”组：

1. 在**高级设置**视图中，单击 **+**。
2. 输入受信用户的姓名。
3. 单击**确定**。
4. 单击**应用**。

eSATA 设备支持

为了要 Device Access Manager 控制 eSATA 设备，必须配置以下条目：

1. 在系統开启时，驱动器必须已经连接了。
2. 使用**高级设置**视图，确保 eSATA 驱动器字母不在 Device Access Manager 将不拒绝访问的驱动器列表中。如果列出了 eSATA 驱动器字母，则删除此驱动器字母，然后单击**应用**。
3. 通过使用**简单配置**视图或**设备类别配置**视图，用“可移动介质”设备类别可以控制此设备。

无管理的设备类别

HP ProtectTools Device Access Manager 并不管理以下设备类别：

- 输入/输出设备
  - 生物
  - 鼠标
  - 键盘

- 打印机
- 即插即用（PnP）打印机
- 打印机升级
- 红外人体学接口设备
- 智能卡读卡器
- 多串口
- 磁盘驱动器
- 软盘控制器（FDC）
- 硬盘控制器（HDC）
- 人体学接口设备（HID）类别

- 电源
  - 电池
  - 高级电源管理（APM）支持
- 其它
  - 计算机
  - 解码器
  - 显示器
  - 处理器
  - 系统
  - 未知
  - 卷
  - 大量快照
  - 安全设备
  - 安全加速器
  - Intel® 统一显示驱动程序
  - 介质驱动程序
  - 中变换器
  - 多功能
  - Legacard
  - 网络客户
  - 网络服务
  - 网络 Trans
  - SCSI 适配器

8 失窃找回（仅限某些机型）

通过 Computrace for HP ProtectTools（单独购买），您可以远程监控、管理和跟踪您的计算机。

在激活 Computrace for HP ProtectTools 后，可从 Absolute Software 客户服务中心对其进行配置。在客户服务中心，管理员可以配置 Computrace for HP ProtectTools 让其监控或管理计算机。如果系统被放错地方或被盗，客户服务中心可以帮助当地有关当局找到并恢复计算机。在对 Computrace 进行配置后可以让其继续发挥作用，即使硬盘驱动器被擦除或更换也没有问题。

要激活 Computrace for HP ProtectTools，请执行以下操作：

1. 连接到 Internet。
2. 打开 Security Manager 用户控制台。有关详细信息，请参阅第 22 页的打开 Security Manager。
3. 在 Security Manager 的左面板中，单击**失窃恢复**。
4. 要启动 Computrace 激活向导，请单击**开始**。
5. 输入联系信息和信用卡支付信息，或者输入售前产品密钥。

激活向导会安全地在 Absolute Software 客户服务中心网站上处理事务并设置您的用户帐户。完成后，您会收到一封确认电子邮件，其中包含您的客户服务中心帐户信息。

如果您以前运行了 Computrace 激活向导，而且已经有了客户服务中心用户帐户，就可以与 HP 客户代表联系以购买更多许可证。

要登录到客户服务中心，请执行以下操作：

1. 转到 https://cc.absolute.com/。
2. 在**登录 ID** 和**密码**字段中，输入您在确认电子邮件中收到的凭证，然后单击**登录**。

通过使用客户服务中心，您可以：

- 监控计算机。
- 保护远程数据。
- 报告 Computrace 保护的任何计算机失窃。

▲ 有关 Computrace for HP ProtectTools 的详细信息，请单击**更多信息**。

9 本地化的密码例外情况

在 Preboot Security 和 HP Drive Encryption 级别，仅提供有限的密码本地化支持，如以下几节中所述。

在拒绝密码时该怎么办

可能会由于以下原因拒绝密码：

- 用户使用不支持的 IME。这是双字节语言（韩语、日语和中文）的一个常见问题。要解决该问题，请执行以下操作：
  1. 通过**控制面板**来添加支持的键盘布局（在“中文输入语言”下添加美式/英语键盘）。
  2. 为默认输入设置支持的键盘。
  3. 重新启动 HP ProtectTools，然后再次输入密码。
- 用户使用不支持的字符。要解决该问题，请执行以下操作：
  1. 更改 Windows 密码，以使其仅使用支持的字符。有关不支持的字符的详细信息，请参阅 HP ProtectTools 管理控制台软件帮助。
  2. 再次运行 HP ProtectTools Security Manager 设置向导，然后输入新的 Windows 密码。

Preboot Security 或 HP Drive Encryption 级别不支持 Windows IME

在 Windows 中，用户可以选择一种 IME（输入法编辑器）以使用标准西方键盘输入复杂字符和符号，如日语或中文字符。

Preboot Security 或 HP Drive Encryption 级别不支持 IME。无法在 Preboot Security 或 HP Drive Encryption 登录屏幕中使用 IME 输入 Windows 密码，这样做可能会导致发生锁定。在某些情况下，当用户输入密码时，Microsoft® Windows 不显示 IME。

解决办法是切换到以下支持的键盘布局之一，这些布局将转换为键盘布局 00000411：

- Microsoft IME for Japanese
- 日语键盘布局
- Office 2007 IME for Japanese—如果 Microsoft 或第三方使用术语 IME 或输入法编辑器，输入法实际上可能不是 IME。这可能会产生混淆，但本软件读取的是十六进制代码表示形式。因此，如果 IME 映射到支持的键盘布局，则 HP ProtectTools 可以支持该配置。

⚠ **警告！** 如果部署了 HP ProtectTools，则会拒绝使用 Windows IME 输入的密码。

使用支持的其它键盘布局更改密码

如果最初使用某种键盘布局（如美国英语 (409)）设置密码，然后用户使用另一种支持的键盘布局（如拉丁美洲语 (080A)）更改密码，并且用户使用的字符（例如 ē）在 BIOS 中存在，而在 HP Drive Encryption 中不存在，则可以在后者中更改密码，而无法在前者中更改密码。

注： 管理员可通过以下方法解决该问题：使用 HP ProtectTools 的“管理用户”功能从 HP ProtectTools 中删除该用户，在操作系统中选择所需的键盘布局，然后针对同一用户再次运行 Security Manager 设置向导。BIOS 将存储所需的键盘布局，并在 BIOS 中正确设置可使用该键盘布局键入的密码。

另一个潜在问题是，使用可生成相同字符的不同键盘布局。例如，美国国际键盘布局 (20409) 和拉丁美洲语键盘布局 (080A) 均可生成字符 é，但可能需要使用不同的按键序列。如果密码最初是使用拉丁美洲语键盘布局设置的，则在 BIOS 中设置拉丁美洲语键盘布局，即使随后使用美国国际键盘布局更改了密码。

特殊按键处理

- 中文、斯洛伐克语、加拿大法语和捷克语

  如果用户选择上述键盘布局之一，然后输入密码（如 abcdef），则必须在 BIOS Preboot Security 和 HP Drive Encryption 中按 shift 键（表示小写）以及 shift 和 caps lock 键（表示大写）时输入相同的密码。数字密码必须使用数字小键盘进行输入。

- 韩语

  如果用户选择支持的韩语键盘布局，然后输入密码，则必须在 BIOS Preboot Security 和 HP Drive Encryption 中按右 alt 键（表示小写）以及右 alt 和 caps lock 键（表示大写）时输入相同的密码。

- 下表列出了不支持的字符：

语言	Windows	BIOS	Drive Encryption
阿拉伯语	ﻷ、ﻹ 和 ﻵ 键生成两个字符。	ﻷ、ﻹ 和 ﻵ 键生成一个字符。	ﻷ、ﻹ 和 ﻵ 键生成一个字符。
加拿大法语	在 Windows 中，使用 caps lock 输入的 ç、è、à 和 é 是 Ç、È、À 和 É。	在 BIOS Preboot Security 中，使用 caps lock 输入的 ç、è、à 和 é 是 ç、è、à 和 é。	在 HP Drive Encryption 中，使用 caps lock 输入的 ç、è、à 和 é 是 ç、è、à 和 é。
西班牙语	不支持 40a。由于本软件将其转换为 c0a，它仍可正常工作。不过，由于键盘布局之间的细微差别，建议西班牙语用户将其 Windows 键盘布局更改为 1040a（西班牙语变体）或 080a（拉丁美洲语）。	不适用	不适用
美国国际	◦ 拒绝最上面一排的 ¡、¤、‘、’、¥ 和 × 键。 ◦ 拒绝第二排的 å、® 和 Þ 键。 ◦ 拒绝第三排的 á、ð 和 ø 键。 ◦ 拒绝最下面一排的 æ 键。	不适用	不适用

语言	Windows	BIOS	Drive Encryption
捷克语	◦ 拒绝 ğ 键。 ◦ 拒绝 į 键。 ◦ 拒绝 ų 键。 ◦ 拒绝 ė、ı 和 ż 键。 ◦ 拒绝 ģ、ķ、ļ、ņ 和 ţ 键。	不适用	不适用
斯洛文尼亚语	拒绝 ż 键。	◦ 键入时拒绝 š、ś 和 ş 键，但在使用软键盘输入时接受这些键。 ◦ ţ 失效键生成两个字符。	不适用
匈牙利语	拒绝 ż 键。	ţ 键生成两个字符。	不适用
斯洛文尼亚语	Windows 中拒绝 żŻ 键，alt 键在 BIOS 中生成一个失效键。	BIOS 中拒绝 ú、Ú、ů、Ů、ş、Ş、ś、Ś、š 和 Š 键。	不适用
日语	如果可用，Microsoft Office 2007 IME 是更好的选择。尽管 IME 名称不同，它实际上就是支持的键盘布局 411。	不适用	不适用

术语表

Drive Encryption
通过加密硬盘驱动器保护您的数据，使没有获得适当授权的用户无法读取该信息。

Drive Encryption 登录屏幕
在 Windows 启动之前显示的登录屏幕。用户必须输入其 Windows 用户名和密码或智能卡 PIN。在大多数情况下，在 Drive Encryption 登录屏幕上输入正确信息后便可直接访问 Windows，而不必在 Windows 登录屏幕上再登录一次。

DriveLock
一种安全保护功能，用于将硬盘驱动器链接到用户并要求用户在计算机启动时正确键入 DriveLock 密码。

HP SpareKey 恢复
允许通过正确回答安全问题访问您的计算机。

ID 卡
一个 Windows 桌面小工具，用于以可视方式通过用户名和所选图片识别您的桌面。

JITA
及时验证。

PIN
个人识别号。

PKI
公钥基础架构标准，定义用于创建、使用和管理证书与加密密钥的界面。

SATA 设备模式
计算机和大容量存储设备（如硬盘驱动器和光盘驱动器）之间的数据传输模式。

TXT
可信执行技术。

Windows 登录安全性
通过要求使用特定凭证进行访问，保护您的 Windows 帐户。

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。

安全保护登录方法
用于登录笔记本计算机的方法。

备份
使用备份功能可将重要程序信息的副本保存到该程序以外的位置。然后可以在以后的时间使用该副本将这些信息恢复到同一计算机或其它计算机上。

标识
HP ProtectTools Security Manager 中的一组凭证和设置，其处理方式类似于特定用户的帐户或配置文件。

重新引导
重新启动计算机的过程。

场景
用于验证的注册用户图像。

单一登录
一种功能，用于存储验证信息以及允许您使用 Security Manager 来访问需要密码验证的 Internet 和 Windows 应用程序。

登录
Security Manager 中的对象，它包含可用于登录到网站或其它程序的用户名和密码（还可能包含其它选定信息）。

吊销密码
此密码是在用户请求数字证书时创建的。当用户要吊销其数字证书时，需要输入此密码。这可确保只有该用户能够吊销此证书。

管理控制台
一个中心位置，管理员可以从中访问和管理 HP ProtectTools 中的功能和设置。

管理员
请参阅 *Windows 管理员*。

后台服务
即 HP ProtectTools Device Locking/Auditing 后台服务，必须运行此服务才能使设备访问控制策略得到应用。可以在“控制面板”中管理工具选项下的“服务”应用程序中查看此服务。如果未运行此服务，当应用设备访问控制策略时，HP ProtectTools Security Manager 将尝试启动此服务。

恢复
将程序信息从先前保存的备份文件复制到此程序的过程。

激活
必须完成该任务，之后才可以访问 Drive Encryption 的任何功能。可使用 HP ProtectTools Setup Wizard（HP ProtectTools 设置向导）来激活 Drive Encryption。只有管理员能够激活 Drive Encryption。激活过程包括激活软件、加密驱动器、创建用户帐户以及在可移动存储设备上创建初始备份加密密钥。

加密
在加密技术中将明文转换为密文以防止未授权收件人读取数据的过程（例如使用算法加密）。数据加密有多种类型，它们是网络安全的基础。常用的类型包括“数据加密标准”和公用密钥加密。

加密服务提供商 (CSP)
加密算法的提供商或库，可以用在定义完善的界面中，执行特定加密功能。

加密技术
加密和解密数据，以便只有特定个人可以将其解码的做法。

加密文件系统 (EFS)
一种用于加密所选文件夹内的所有文件和子文件夹的系统。

解密
一种在加密技术中用于将加密数据转换为明文的过程。

紧急恢复档案
一个受保护的存储区域，允许在不同平台所有者密钥之间对基本用户密钥进行重新加密。

开机验证
一种安全保护功能，要求在计算机开启时进行某种形式的验证，如智能卡、安全保护芯片或密码。

凭证
一种手段，用户赖以在验证过程中证明自己有资格执行特定任务。

设备访问控制策略
允许或拒绝用户访问的设备列表。

设备类别
特定类型的所有设备，例如驱动器。

生物识别
使用生理特征（例如指纹）来识别用户的验证凭证类型。

受信任的平台模块 (TPM) 嵌入式安全保护芯片
HP ProtectTools 嵌入式安全保护芯片的通称。TPM 对计算机进行验证，而不是对用户进行验证，具体做法是存储特定于主机系统的信息，如加密密钥、数字证书和密码。TPM 可最大限度地降低计算机上的信息因物理盗窃泄露或被外部黑客攻击的风险。

网络帐户
一种 Windows 用户或管理员帐户，位于本地计算机上、工作组中或域中。

验证
此过程检验用户是否被授权执行某个任务，如访问计算机、修改特定程序的设置或查看被保护的数据。

用户
Drive Encryption 中的注册用户。非管理员用户在 Drive Encryption 中的权限受限。他们只能进行注册（在管理员许可下）和登录。

域
网络中的一组计算机，彼此共享同一个目录数据库。域的名称是唯一的，每个都有一组通用规则和过程。

证书颁发机构 (CA)
一项服务，用于颁发运行公钥基础架构所需的证书。

指纹
对您的指纹图像的数字提取。Security Manager 永远不会存储您的实际指纹图像。

智能卡
一小块硬件，其大小与形状和信用卡类似，用于存储有关所有者的标识信息。用于验证是否是所有者登录到计算机。

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。

组
对某个设备类别或特定设备具有相同访问级别或拒绝访问权限的一组用户。

索引

符号/编号

“常规”标签，设置 21
“应用程序”标签，设置 21

A

安全性 5
  关键目标 4
  角色 5

B

Bluetooth 20, 32
备份
  HP ProtectTools 凭证 6
  加密密钥 40
  数据 33

C

Computrace 52
Credential Manager 28
重置 47

D

Device Access Manager for HP ProtectTools
  打开 43
  简易设置 11
Drive Encryption for HP ProtectTools 35
  简易设置 11
打开
  Device Access Manager for HP ProtectTools 43
  HP ProtectTools 管理控制台 15
  Security Manager 22
打开 Drive Encryption 35
盗窃，防止 4
灯泡图标 30
登录
  编辑 25
  管理 26
  类别 26
  添加 24
登录到笔记本计算机 38

E

eSATA 50

F

访问
  防止非授权 5
  控制 43
非接触卡 20, 32
非授权访问，防止 5

G

高级设置 49
功能，HP ProtectTools 1
关键安全保护目标 4
管理
  加密或解密驱动器分区 39
  密码 21, 23, 24
  凭证 28
  用户 17
管理控制台
  配置 15
  使用 15

H

HP Client Security 控制板 8, 14
HP ProtectTools Device Access Manager 43
HP ProtectTools Drive Encryption 39
  备份和恢复 40
  管理 Drive Encryption 39
  激活 36
  加密各个驱动器 39
  解密各个驱动器 39
  停用 36
  在激活 Drive Encryption 后登录 36
HP ProtectTools Security Manager 22
  Backup and Recovery 密码 6
HP ProtectTools Security Manager 设置向导 8, 14
HP ProtectTools 功能 1
HP ProtectTools 管理控制台 8, 13, 14
  打开 15
HP SpareKey 恢复 41
黑暗模式 30
后台服务 44
恢复
  HP ProtectTools 凭证 6
  使用备份密钥访问 40
  数据 33

I

ID 卡 23

J

JITA
  创建用户或组的可延长 49
  禁用用户或组 49
  配置 48
  为用户或组创建 48
激活
  针对标准硬盘驱动器的 Drive Encryption 36
  针对自我加密驱动器的 Drive Encryption 36
及时验证配置 48
加密
  驱动器 35
  软件 36, 37, 39, 41
  硬件 36, 37, 41
  硬盘驱动器 38
  硬盘驱动器分区 39
加密密钥
  备份 40
加密状态，显示 41
简单配置 44
接近卡 20, 32
解密
  驱动器 35
  硬盘驱动器分区 39

拒绝 46

K
控制设备访问 43
快速链接
  菜单 26

L
脸，设置 18

M
密码
  HP ProtectTools 5
  安全 6
  策略 5
  更改 28
  管理 5
  拒绝 53
  例外情况 53
  强度 27
  使用不同的键盘布局更改 53
  准则 6
目标，安全性 4

P
Password Manager 21, 23, 24
  查看和管理保存的验证 10
  简易设置 9
PIN 32
配置
  重置 47
  管理控制台 15
  简单 44
  设备访问权限 43
  设备类别 45
凭证 23
  指定 17
屏幕颜色 30

R
入门 9, 44
软件加密 36, 37, 39, 41

S
Security Manager，打开 22
SpareKey
  设置 17, 28
删除
  访问 47
设备类别
  无管理的 50
  允许用户访问 46
设备类别配置
  配置 45
设备设置
  SpareKey 17
  脸 18
  指纹 18
  智能卡 19
设备，允许用户访问 47
设置 17, 33
  高级用户 31
  添加 21, 22
  图标 27
  应用程序 21, 22
  “常规”标签 21
设置向导 8, 14
失窃找回 52
首选项，设置 33
数据
  备份 33
  恢复 33
  限制访问 4

T
TPM 39
特殊按键处理 54
停用 Drive Encryption 37
图谱
  删除 31
  注册 29

W
Windows 登录密码 6
无管理的设备类别 50

X
限制
  访问机密数据 4
  设备访问 43
向导
  HP ProtectTools Client Security 设置 7
  HP ProtectTools Security Manager 设置 7
向导，HP ProtectTools Security Manager 设置 8, 14
学习 30

Y
验证 16, 30
应用程序 20
硬件加密 36, 37, 41
用户
  拒绝访问 46
  删除 47
  允许访问 46
用户控制台设置 22
允许访问 46

Z
针对小型企业的简易设置指南 9
指定安全设置 17
指纹
  设置 18
  注册 29
智能卡 31
  PIN 6
  初始化 18, 31
  更改 PIN 32
  配置 19
  注册 19, 31
注册
  图谱 29
  指纹 29
组
  拒绝访问 46
  删除 47
  允许访问 46