HP ProtectTools

使用入门

第 1 版 2011 年 1 月

文档部件号：638391-AA1

目录

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 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（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。

笔记本计算机中可用的软件模块因机型而异。

您可以从 HP 网站预安装、预装载或下载 HP ProtectTools 软件模块。有关详细信息，请访问 http://www.hp.com。

注： 本指南中的说明假设您已经安装了合适的 HP ProtectTools 软件模块。

HP ProtectTools 功能

下表详细说明了 HP ProtectTools 模块的主要功能。

模块	重要功能
HP ProtectTools 管理控制台（供管理员使用）	• 使用“Security Manager 设置向导”设置并配置安全级别和安全登录方法。 • 配置对用户隐藏的选项。 • 配置 Device Access Manager 配置和用户访问。 • 添加和删除 HP ProtectTools 用户并使用管理员工具查看用户状态。
HP ProtectTools Security Manager（供用户使用）	• 组织、设置和更改密码。 • 配置和更改用户凭证，如 Windows 密码、指纹和智能卡。 • 配置和更改 File Sanitizer 碎化、清理以及其它设置。 • 查看 Device Access Manager 的设置。 • 配置 Computrace for HP ProtectTools。 • 配置首选项以及备份和恢复选项。
HP ProtectTools Credential Manager（Password Manager）	• 保存、组织和保护用户名与密码。 • 设置网站和程序的登录屏幕，以实现快速且安全的访问。 • 通过在 Password Manager 中输入网站用户名和密码对其进行保存。下次访问此站点时，Password Manager 会自动填写并提交信息。 • 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。
HP ProtectTools Drive Encryption（HP ProtectTools 驱动器加密，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。
File Sanitizer for HP ProtectTools	• 碎化计算机上的数字资产（机密信息，包括应用程序文件、历史的或与 Web 有关的内容，或者其它机密数据）并定期清理硬盘驱动器上的已删除资产。
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可写设备。
HP ProtectTools Privacy Manager（HP ProtectTools 隐私管理器，仅限某些机型）	• 用于获取颁发机构的证书，以供在使用 Microsoft 电子邮件和 Microsoft Office 文档时验证通信的来源、完整性和安全性。

模块	重要功能
Computrace for HP ProtectTools（单独购买）	• 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。 • 需要单独购买跟踪和追踪订阅，才能激活。
Embedded Security for HP ProtectTools（仅限某些机型）	• 使用受信任的平台模块 (TPM) 嵌入式安全保护芯片来防止非授权访问计算机上存储的用户数据和凭证。 • 允许创建个人安全驱动器 (PSD)，用以保护用户文件和文件夹信息。 • 支持使用第三方应用程序（如 Microsoft Outlook 和 Internet Explorer）来执行受保护的数字证书操作。

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。

Credential Manager for HP ProtectTools

Credential Manager（Security Manager 的一部分）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 Credential 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，Credential Manager 会自动提供凭证。如果她希望查看用户名和密码，可以对 Credential Manager 进行配置使其显示它们。

另外，Credential 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 Credential Manager for HP ProtectTools 内。完成后，这位 CPA 将 Credential 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

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。 他激活了 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。 他还可以进一步增强驱动器安全性，做法是选择用 SED（自加密驱动器）选项来加密数据。

Embedded Security for HP ProtectTools 和 Drive Encryption for HP ProtectTools 不允许访问加密数据（即使在卸下驱动器后），因为二者都绑定到原始主板。

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。

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools 用于永久性删除数据，包括 Internet 浏览器活动、临时文件、以前删除的数据或任何其它信息。可以将 File Sanitizer 配置为按用户定义的计划手动或自动运行。

示例 1： 一位律师经常处理机密的客户信息，希望确保已删除文件中的数据无法恢复。这位律师使用 File Sanitizer 来“碎化”已删除的文件，以使其几乎不可能恢复。

通常，当 Windows 删除数据时，它并不实际从硬盘驱动器中擦除数据，而是将硬盘驱动器扇区标记为可供将来使用。在数据被覆盖以前，可以使用 Internet 上提供的常见工具轻松地将其恢复。File Sanitizer 用随机数据覆盖扇区（必要时多次），从而使已删除的数据不可读、不可恢复。

示例 2： 一位研究人员希望在注销时自动碎化已删除的数据、临时文件、浏览器活动等。她使用 File Sanitizer 来安排“碎化”，因此，她可以选择要自动永久删除的常见文件或任何自定义文件。

Device Access Manager for HP ProtectTools

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。管理员还能够计划何时可以访问驱动器以及可以访问多长时间。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。Device Access Manager for HP ProtectTools 允许管理员限制和管理对硬件的访问。

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。

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools 在 Internet 电子邮件通信需要保护时使用。用户可以创建并发送仅能由授权收件人打开的电子邮件。有了 Privacy Manager，冒名者就无法泄露或截取信息。

示例 1： 一位股票经纪人希望确保自己的电子邮件仅发送到指定的客户那里，而且没有人能冒用自己的电子邮件帐号或截取邮件。这位股票经纪人将自己和客户注册到 Privacy Manager 中。Privacy Manager 向每个用户发送一个验证证书 (CA)。通过使用该工具，这位股票经纪人及其客户在进行电子邮件交换前必须进行验证。

有了 Privacy Manager for HP ProtectTools，在对收件人进行检验和验证后，发送和接受电子邮件就变得很容易。而且，还可以对邮件服务进行加密。加密过程与 Internet 上的一般信用卡购物所使用的加密过程类似。

示例 2： 一位总裁希望确保只有董事会成员可以查看他通过电子邮件发送的信息。这位总裁使用相应的选项对发送给董事们和从董事们那里接收的电子邮件进行加密。Privacy Manager 的验证证书能让这位总裁和董事们具有加密密钥的副本，因此只有他们能够解密机密的电子邮件。

Computrace for HP ProtectTools（以前叫做 LoJack Pro）

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。

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。

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 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。

Embedded Security for HP ProtectTools（仅限某些机型）

Embedded Security for HP ProtectTools 能让用户创建个人安全驱动器。通过此功能，用户可以在被访问之前处于完全隐藏状态的 PC 上创建虚拟驱动器分区。有了 Embedded Security，可以做到既隐秘地保护数据，又不对数据的其余部分进行加密。

示例 1： 一位库房经理有一台计算机，一天内会有多名工人间歇性地访问它。这位经理希望对计算机上的机密库房数据进行加密并将其隐藏起来。他希望数据足够安全，以致于即使有人盗取了硬盘驱动器，也无法解密或读取数据。这位库房经理决定激活 Embedded Security 并将机密数据移至个人安全驱动器上。他可以输入密码来访问机密数据，就像对待其它硬盘驱动器一样。当他注销或重新引导个人安全驱动器时，必须输入正确的密码才能看到或打开它。工人们永远也不会在访问这台计算机时看到机密数据。

Embedded Security 在位于主板上的硬件 TPM（受信任的计算模块）芯片内保护加密密钥。它是唯一能满足最低要求以便在有人尝试猜测解密密码时抵制密码攻击的加密工具。另外，Embedded Security 还可以对整个驱动器和电子邮件进行加密。

示例 2： 一位股票经纪人希望使用便携式驱动器将极为机密的数据传输到另一台计算机。她希望确保只有这两台计算机可以打开驱动器，即使密码被泄露也是如此。这位股票经纪人使用 Embedded Security TPM 迁移来让第二台计算机具有必需的加密密钥来解密数据。在传输过程中，即使知道密码，也只有这两台计算机可以解密数据。

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：

- 防范目标性盗窃行为
- 限制对机密数据的访问
- 防止来自内部或外部的未授权访问
- 创建强密码策略

防范目标性窃取

目标性窃取的一个例子是在机场安检处盗窃包含机密数据和客户信息的计算机。下列功能可以帮助防范目标性窃取：

- 预引导验证功能可帮助防止访问操作系统（在启用后）。请参阅以下各章：
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- 由 Embedded Security for HP ProtectTools 模块提供的个人安全驱动器功能可对机密数据进行加密，以帮助确保只有经过验证才可以访问这些数据。请参阅下面一章：
  - Embedded Security for HP ProtectTools
- Computrace 可以在计算机被盗后对计算机的位置进行跟踪。请参阅下面一章：
  - Computrace for HP ProtectTools

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 经理限制对可写设备的访问，以使机密信息无法从硬盘驱动器中打印出来或复制到可移动介质中。

防止来自内部或外部的未授权访问

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）。请参阅以下各章：
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager 帮助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。

- 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。
- File Sanitizer 通过碎化关键文件和文件夹或清理硬盘驱动器上的已删除资产（覆盖已被删除但仍可恢复的数据）来安全地删除数据。
- Privacy Manager 能让您在使用 Microsoft 电子邮件或 Microsoft Office 时获取颁发机构的证书，从而使发送和保存重要信息的过程变得很安全。

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。

其它安全保护要素

指定安全保护角色

在管理计算机安全性（尤其是对于大型企业）的方面，一项很重要的工作就是划分不同类型管理员和用户之间的责任和权限。

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，安全责任和权限可以按以下角色划分：

- 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（如 Drive Encryption 或 Embedded Security）。

  注： 通过与 HP 合作，安全管理人员可以自定义 HP ProtectTools 中的许多功能。有关详细信息，请参阅 HP 网站：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： 鼓励管理员遵循“最佳实践”限制最终用户权限以及限制用户访问。

未经授权的用户不应获得管理权限。

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。

此表也指明了那些只能由 IT 管理员设置和使用的密码。所有其它密码都可以由普通用户或管理员进行设置。

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	可用于手动登录和验证以访问各种 Security Manager 功能。
Security Manager Backup and Recovery 密码	Security Manager，由单个用户使用	保护对 Security Manager 备份和恢复文件进行的访问。
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（如果选择了智能卡令牌）。
紧急恢复令牌密码	Embedded Security，由 IT 管理员使用	保护对紧急恢复令牌（即，嵌入式安全保护芯片的备份文件）的访问。

HP ProtectTools 密码	在以下模块中设置	功能
所有者密码	Embedded Security，由 IT 管理员使用	保护系统和 TPM 芯片以使 Embedded Security 的全部所有者功能免遭非授权访问。
BIOS 管理员密码	Computer Setup，由 IT 管理员使用	保护对 Computer Setup 实用程序的访问。

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。
- 不要将您的姓名用作密码，也不要使用任何其它个人信息，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。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。

备份和恢复 HP ProtectTools 凭证

您可以使用 HP ProtectTools 的 Backup and Restore（备份和恢复）功能来选择和备份 HP ProtectTools 凭证数据和设置。

2 使用入门设置向导

Security Manager 设置向导可指导您启用适用于此计算机的所有用户的可用安全保护功能。您还可以在管理控制台的“安全保护功能”页中管理这些功能。

要通过 Security Manager 设置向导来设置安全保护功能，请执行以下操作：

1. 从 Windows 边栏上的 HP ProtectTools 桌面小工具图标中或任务栏最右侧通知区域的任务栏图标中打开 HP ProtectTools Security Manager。

HP ProtectTools 桌面小工具图标上的标志颜色指示下列情况之一：

- 红色 — HP ProtectTools 尚未设置，或者 ProtectTools 模块之一存在错误条件。
- 黄色 — 检查 Security Manager 中的“应用程序状态”页，以查看必须执行的设置更改。
- 蓝色 — HP ProtectTools 已设置，且正在正常工作。

将在小工具图标底部显示一条消息以指示下列情况之一：

- **立即设置** — 管理员必须单击小工具图标以运行 Security Manager 设置向导，以便为计算机配置验证凭证。

  设置向导是一个独立的应用程序。

- **立即注册** — 用户必须单击小工具图标以运行 Security Manager 使用入门向导，以便注册验证凭证。

  使用入门向导显示在 Security Manager 控制板中。

- **立即检查** — 单击小工具图标以在“安全应用程序状态”页中显示更多详细信息。

注： HP ProtectTools 桌面小工具图标在 Windows XP 中不可用。

– 或 –

依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。在左窗格中，单击**设置向导**。

2. 阅读“欢迎使用”屏幕内容，然后单击**下一步**。

3. 键入您的 Windows 密码以验证您的身份，然后单击**下一步**。

   如果您尚未创建 Windows 密码，系统会提示您创建它。为了保护您的 Windows 帐户免遭他人在未经授权的情况下进行访问，且为了使用 HP ProtectTools Security Manager 功能，需要 Windows 密码。

4. 在“SpareKey”页上，选择三个安全问题，输入每个问题的答案，然后单击**下一步**。

   可以在 Security Manager 控制板的 **Credential Manager** 下面的“SpareKey”页中选择不同的问题或更改答案。

注： 此 SpareKey 设置仅适用于管理用户。

5. 选中相应的复选框以启用安全保护功能，然后单击**下一步**。

   选择的功能越多，您的计算机就越安全。

注： 这些设置适用于所有用户。如果未选中任何复选框，设置向导不会提示用户注册这些凭证。

- **Windows 登录安全性** — 要求使用特定的凭证进行访问，从而保护您的 Windows 帐户。
- **Drive Encryption** — 通过对硬盘驱动器加密以使未经正确授权的人员无法读取信息，从而对您的数据进行保护。
- **Pre-Boot Security** — 在 Windows 启动之前禁止未经授权的人员进行访问，从而对您的计算机进行保护。

  注： 如果 BIOS 不支持 Pre-Boot Security，则无法使用该功能。

6. 设置向导提示您注册凭证。

   如果指纹识别器、智能卡和网络摄像头均无法使用，则会提示您输入 Windows 密码。在注册后，您可以在需要验证的时候使用注册的任何凭证来验证身份。

注： 注册的这些凭证仅适用于管理用户。

7. 在该向导的最后一页上，单击 **Finish（完成）**。

   将显示 Security Manager 控制板主页。

3 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 控制板中还提供了其它应用程序（仅限某些机型）以帮助找回丢失或被盗的计算机。

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
- 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
- 添加其它 Security Manager 应用程序

打开 HP ProtectTools 管理控制台

对于管理任务（如设置系统策略或配置软件），请按如下方法打开该控制台：

- 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。

  – 或 –

  在 Security Manager 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。

▲ 要打开 HP ProtectTools 管理控制台，请依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。

– 或 –

在 Security Manager 的左面板中，单击**管理**，然后单击**管理控制台**。

该控制台包含以下组件：

- **主页** — 用于配置以下安全保护选项：
  - **提高系统安全性**
  - **需要增强验证**
  - **管理 HP ProtectTools 用户**
  - **了解如何集中管理 HP ProtectTools**
- **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** — 提供一个可扩展的链接菜单，这些链接指向用于保护数据的 Security Manager 应用程序。
- **集中管理** — 显示用于访问其它解决方案、产品更新和消息的标签。
- **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。

  ? — 显示管理控制台软件帮助。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：

- **安全保护** — 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。

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，单击向下箭头，然后选择一个用户类别：
   - **适用于此计算机的管理员**
   - **对于非管理员用户**
3. 指定选定用户类别所需的验证凭证。
4. 选择在验证用户时是需要任意指定的凭证，还是需要所有指定的凭证。
5. 单击**应用**。

会话策略

要定义策略以控制在 Windows 会话期间访问 HP ProtectTools 应用程序所需的凭证，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，单击向下箭头，然后选择一个用户类别：
   - **适用于此计算机的管理员**
   - **对于非管理员用户**

3. 单击向下箭头，然后选择选定用户类别所需的验证凭证：

   - **需要使用指定的凭证之一**

     注： 清除所有凭证的复选框与选择**不需要进行验证**具有相同的效果。

   - **需要使用所有指定的凭证**
   - **不需要进行验证** — 选择此选项会清除窗口中的所有凭证。

4. 单击**应用**。

设置

1. 选中或清除复选框以启用或禁用以下设置：

   允许 One Step Logon — 如果在 BIOS 或加密磁盘级别执行验证，则允许此计算机的用户跳过 Windows 登录。

2. 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指定可用的设置。

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. 选中或清除复选框以允许或禁止使用 SpareKey 验证进行 Windows 登录。
2. 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。
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** — 移动滑块以调整指纹识别器在扫描指纹时使用的灵敏度。

  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** — 选择下列选项之一，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。

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** — 将计算机配置为在取下智能卡时自动锁定。

  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 Protect Tools。 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它数据。
  - **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 或任何其它应用程序。

注： 无法使用智能卡不支持的功能。

▲ 单击**应用**。

脸部

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. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 单击**凭证**，然后单击**脸**。
3. 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。
4. 单击**高级**，然后配置其它安全保护功能。 有关详细信息，请参阅第 35 页的高级用户设置。
5. 单击**应用**。

配置应用程序

您可以使用“设置”自定义当前安装的 HP ProtectTools Security Manager 应用程序的行为。

要编辑应用程序设置，请执行以下操作：

1. 在管理控制台的左面板中，单击**应用程序**下面的**设置**。
2. 选中或清除特定设置旁边的复选框以启用或禁用该设置。
3. 单击**应用**。

“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。

“应用程序”标签

在 Security Manager 中添加新应用程序后，此处显示的设置可能会发生变化。默认显示的最低设置如下所示：

- **应用程序状态** — 允许为所有应用程序显示状态。
- **Password Manager** — 为所有计算机用户启用 Password Manager。
- **Privacy Manager** — 为所有计算机用户启用 Privacy Manager。
- **启用“集中管理”链接** — 允许此计算机的所有用户通过单击**集中管理**，在 HP ProtectTools Security Manager 中添加应用程序。

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。

集中管理

可以通过其它应用程序在 Security Manager 中添加新的管理工具。该计算机的管理员可以在“设置”页中禁用此功能。“集中管理”页上有两个标签：

- **业务解决方案** — 如果有可用的 Internet 连接，则可以访问 DigitalPersona 网站 (http://www.digitalpersona.com/) 以检查新的应用程序。
- **更新和消息**
  - 要获取有关新应用程序和更新的信息，请选中**通知我新的应用程序和更新**复选框。
  - 要为自动更新设置一个时间表，请选择天数。
  - 要检查更新，请单击**立即检查**。

4 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

可以使用以下任一方法打开 Security Manager：

- 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools Security Manager**。
- 双击任务栏最右侧的通知区域中的 **HP ProtectTools** 图标。
- 右击 **HP ProtectTools** 图标，然后单击**打开 HP ProtectTools Security Manager**。
- 单击 **HP ProtectTools** 桌面小工具图标。
- 按 ctrl+Windows 徽标键+h 组合热键以打开 **Security Manager 快速链接**菜单。

  有关更改组合热键的信息，请参阅第 31 页的设置。

使用 Security Manager 控制板

Security Manager 控制板是一个中心位置，可以在其中方便地访问 Security Manager 功能、应用程序和设置。

▲ 要打开 Security Manager 控制板，请依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools Security Manager**。

控制板将显示以下组件：

- **ID 卡** — 显示 Windows 用户名和所选图片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。
  - **状态** — 检查 HP ProtectTools 安全应用程序状态。

注： 下面的列表没有显示计算机上未安装的应用程序。

- **我的登录** — 使用 Password Manager、Credential Manager、密码、SpareKey、智能卡、脸部以及指纹管理验证凭证。
- **我的数据** — 使用 Drive Encryption 和 File Sanitizer 管理数据的安全。
- **我的计算机** — 使用 Device Access Manager 管理计算机的安全。
- **我的通信** — 使用 Privacy Manager 管理通信的安全。
- **管理** — 使管理员可以访问以下选项：
  - **管理控制台** — 使管理员可以管理安全和用户。
  - **集中管理** — 使管理员可以访问其它解决方案、产品更新和消息。
- **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 软件帮助。该图标位于窗口右上角，在最小化和最大化图标旁边。

安全应用程序状态

可以在以下两个位置查看安装的安全应用程序的状态：

- **HP ProtectTools 桌面小工具**

  HP ProtectTools 小工具图标顶部的标志颜色可能会发生变化，以反映安装的安全应用程序的总体安全状态。

  - **红色** — 警告
  - **黄色** — 注意：未配置
  - **蓝色** — 良好

  将在小工具图标底部显示一条消息以指示下列情况之一：

  - **立即设置** — 管理员必须单击小工具图标以运行 Security Manager 设置向导，以便为计算机配置验证凭证。

    设置向导是一个独立的应用程序。

  - **立即注册** — 用户必须单击小工具图标以运行 Security Manager 使用入门向导，以便注册验证凭证。

    使用入门向导显示在 Security Manager 控制板中。

  - **立即检查** — 单击小工具图标以在“安全应用程序状态”页中显示更多详细信息。

- **安全应用程序状态页** — 单击 Security Manager 控制板上的**状态**以显示安装的安全应用程序的总体状态以及每个应用程序的具体状态。

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，您可以使用 Windows 密码、指纹或智能卡进行验证以启动和登录到网站和程序。
- **Credential Manager** — 提供一种轻松更改 Windows 密码、注册指纹或设置智能卡的方法。

管理员可通过以下方法添加更多应用程序：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。您可以使用该程序创建不必写下或记住的增强密码，然后使用指纹、智能卡或 Windows 密码方便快捷地进行登录。

Password Manager 提供了以下选项：

- 在**管理**标签中添加、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，并自动生成复杂的增强密码以供新网站使用。

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，则会在该图标上显示一个加号。

▲ 单击 **Password Manager** 以显示一个上下文菜单，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 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 软件帮助。

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（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** — 用于在登录中添加帐户。
- **打开 Password Manager** — 启动 Password Manager。
- **帮助** — 显示 Security Manager 软件帮助。

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。可以在浏览到网站或程序后使用这些登录，也可以从**登录**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。也可以单击 **Password Manager 管理**标签中的**添加登录**以显示此对话框。某些选项取决于计算机连接的安全保护设备；例如，使用 ctrl+Windows 徽标键+h 热键，扫描指纹或插入智能卡。
   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. 要启用 VeriSign VIP 安全保护功能，请选中**我希望在此网站上使用 VIP 安全保护功能**复选框。

      仅在提供了 VeriSign 身份保护 (VIP)的网站显示此选项。如果网站支持，您还可以选择在使用通常的验证方法时自动填充 VIP 安全代码。
   e. 单击**确定**，单击要使用的验证方法（指纹、密码或脸部），然后使用所选的验证方法进行登录。

      将从 **Password Manager** 图标中删除加号，通知您已创建登录。
   f. 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。
      - 如果 Password Manager 无法检测所有登录字段，则会显示一条消息，询问您是否继续。单击**是**。
      - 将打开一个填充了登录字段的对话框。单击每个字段的图标，将其拖到相应的登录字段中，然后单击按钮以登录到网站上。

        注： 在使用手动模式输入网站的登录数据后，以后必须继续使用这种方法登录到相同网站上。

        注： 手动输入登录数据模式仅适用于 Internet Explorer 8。
      - 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. 要显示可以在其中编辑登录信息的对话框，请单击 **Password Manager** 图标上面的箭头，然后单击**编辑登录**。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。

   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。
   - 要启用 VeriSign VIP 安全保护功能，请选中**我希望在此网站上使用 VIP 安全保护功能**复选框。

     仅在提供了 VeriSign VIP 安全保护功能的网站显示此选项。如果网站支持，您还可以选择在使用通常的验证方法时自动填充 VIP 安全代码。
   - 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“登录”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**登录**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，然后填充登录数据。

在创建登录时，该登录将自动添加到 Password Manager 的**登录**菜单中。

要显示**登录**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，请单击 Security Manager 控制板中的 **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. 从 Security Manager 控制板中，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各个登录。

要管理登录，请执行以下操作：

▲ 从 Security Manager 控制板中，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 27 页的添加登录。
  - **编辑** — 编辑登录。有关详细信息，请参阅第 28 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 28 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。

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. 单击图标箭头，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 控制板，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 27 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。

2. 要禁用显示为登录屏幕添加登录的提示的选项，请选中该复选框。
3. 要访问其它 Password Manager 设置，请单击 **Password Manager**，然后单击 Security Manager 控制板上的**设置**。

VeriSign 身份保护 (VIP)

您可以创建 VeriSign VIP 访问身份标记以用于支持 VeriSign VIP 的网站。Password Manager 使用这些身份标记创建自动登录，以结合使用拖放到支持 VeriSign VIP 的网站或手动输入到指定字段中的身份标记。

您可以在 Security Manager 控制板或任何支持 VeriSign VIP 的网站上启用 VeriSign VIP 并创建身份标记。要使用身份标记，您必须在要使用的每个网站上注册该身份标记。

在注册并首次使用身份标记后，您可以选择将其附加到常规登录凭证并与其一起提交。对于不允许附加身份标记的网站，您可以拖放或手动输入身份标记信息。

要从 Security Manager 控制板中启用 VeriSign VIP 并创建 VeriSign VIP 身份标记，请执行以下操作：

1. 打开 Security Manager 控制板。有关详细信息，请参阅第 23 页的打开 Security Manager。
2. 单击 **Password Manager**，然后单击 **VIP**。
3. 单击**获取 VIP 资格**。

   将创建 VeriSign VIP 身份标记，并在 VeriSign VIP 页中显示该身份标记。现在，只要访问此页，就会显示该身份标记。

要从网站中启用 VeriSign VIP 并创建 VeriSign VIP 身份标记，请执行以下操作：

1. 只要访问支持 VeriSign VIP 的网站，Password Manager 就会向您发送提示信息。
2. 为屏幕创建登录。有关详细信息，请参阅第 27 页的添加登录。
3. 在“创建登录”对话框中，选中**我希望使用 VIP 提供额外的帐户保护**。

要为网站注册 VeriSign VIP 身份标记，请执行以下操作：

1. 手动登录到支持 VeriSign VIP 的网站，或者使用 Password Manager 登录。
2. 单击显示的 VeriSign VIP 气球，为此网站创建一个登录。
3. 在“将登录添加到 Password Manager”对话框中，选中**我希望在此网站上使用 VIP 安全保护功能**。

   仅在提供了 VeriSign VIP 安全保护功能的网站显示此选项。如果网站支持，您还可以选择在使用通常的验证方法时自动填充 VIP 安全代码。

设置

您可以指定设置以便对 HP ProtectTools Security Manager 进行个性化设置：

1. **提示为登录屏幕添加登录** — 只要检测到网站或程序登录屏幕，就会显示带有加号的 **Password Manager** 图标，表明您可以将此屏幕的登录添加到密码库中。要禁用此功能，请在“图标设置”对话框中清除**提示为登录屏幕添加登录**旁边的复选框。
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

可以使用 Security Manager 凭证验证您是否为所声称的那个人。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
- 智能卡
- 脸

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. 从 Security Manager 控制板中，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）。

在使用入门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**下一步**。

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

在设置 SpareKey 后，您可以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

如果计算机内置或连接了指纹识别器，在使用入门向导中进行初始设置时，HP ProtectTools Security Manager 将提示您设置或“注册”指纹。也可以在 Security Manager 控制板的 **Credential Manager** 下面的“指纹”页中注册指纹。

1. 将显示双手的轮廓。已注册的手指以绿色突出显示。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. 在选择要注册的手指后，系统将提示您扫描该手指，直至成功注册其指纹。将使用绿色在轮廓上突出显示注册的手指。
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“使用入门”过程注册指纹时，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。

设置智能卡

必须先由管理员初始化并注册智能卡，然后才能使用智能卡进行验证。

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 ActivIdentity 软件。

1. 将智能卡插入读卡器中。
2. 依次单击**开始**、**所有程序**和 **ActivClient PIN 初始化工具**。
3. 输入并确认 PIN。
4. 单击**下一步**。

   智能卡软件会提供一个解锁密钥。大多数智能卡都会在 PIN 输错 5 次后进行自我锁定。密钥可用于解锁智能卡。
5. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
6. 依次单击**凭证**、**智能卡**。
7. 单击**管理**标签。
8. 确保**设置智能卡**处于选中状态。
9. 输入您的 PIN，单击**应用**，然后按照屏幕上的说明进行操作。
10. 智能卡成功初始化后，您将需要注册智能卡。

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. 在**集中管理**下，单击**设置向导**。
2. 在“欢迎使用”页中，单击**下一步**，然后输入您的 Windows 密码。
3. 在“SpareKey”页中，单击**跳过 SpareKey 设置**（除非您希望更新 SpareKey 信息）。
4. 在“启用安全保护功能”页中，单击**下一步**。
5. 在“选择您的凭证”页中，确保**设置智能卡**处于选中状态，然后单击**下一步**。
6. 在“智能卡”页中，输入您的 PIN，然后单击**下一步**。
7. 单击**完成**。

用户还可以在 Security Manager 中注册智能卡。有关详细信息，请参阅 Security Manager for HP ProtectTools 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** — 将计算机配置为在取下智能卡时自动锁定。

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 Protect Tools。 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它数据。
  - **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 或任何其它应用程序。

注： 无法使用智能卡不支持的功能。

▲ 单击**应用**。

为脸部登录注册图谱

如果计算机内置或连接了网络摄像头，在使用入门向导中进行初始设置时，HP ProtectTools Security Manager 将提示您设置或“注册”图谱。也可以在 Security Manager 控制板的 **Credential Manager** 下面的脸部登录页中注册图谱。

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。

要从使用入门向导中注册图谱，请执行以下操作：

1. 在向导的“脸”页中，单击**高级**，然后配置其它安全保护功能。有关详细信息，请参阅第 35 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. 如果未选择任何其它安全保护选项，则会提示您选择一个额外的安全保护选项。 按照屏幕上的说明进行操作，然后单击**下一步**。 有关详细信息，请参阅第 35 页的高级用户设置。
5. 单击**摄像头**图标，然后按照屏幕上的说明注册图谱。

   按照屏幕上的说明进行操作，在采集图谱时，请务必看着您的图像。

6. 单击**下一步**。
7. 单击**完成**。

也可以从 Security Manager 控制板中注册图谱：

1. 打开 Security Manager 控制板。有关详细信息，请参阅第 23 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**，然后配置其它安全保护功能。有关详细信息，请参阅第 35 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. 如果未选择任何其它安全保护选项，则会提示您选择一个额外的安全保护选项。 按照屏幕上的说明进行操作，然后单击**下一步**。 有关详细信息，请参阅第 35 页的高级用户设置。
7. 单击**摄像头**图标，然后按照屏幕上的说明注册图谱。

   按照屏幕上的说明进行操作，在采集图谱时，请务必看着您的图像。

有关详细信息，请单击脸部登录页右上角的蓝色 **?** 图标以访问 Face Recognition 软件帮助。

高级用户设置

如果未选择其它安全保护选项，则还会在“额外的安全保护”页中显示这些选项。

1. 打开 Security Manager 控制板。有关详细信息，请参阅第 23 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**以配置以下安全选项：

   a. **安全保护**标签 — 选择以下选项之一：

   - **不提供额外的安全保护** — 如果不希望为脸部登录提供额外的安全保护，请选择此选项。
   - **使用 PIN 提供额外的安全保护** — 选择此选项，要求脸部登录使用用户特定的 PIN。
     - 单击**创建 PIN**。
     - 输入 Windows 密码。
     - 输入新的 PIN，然后重新输入新 PIN 以进行确认。

       在创建 PIN 后，您可以从下列选项中进行选择：**更改**、**重置**或**删除 PIN**。
   - **使用 Bluetooth 提供额外的安全保护** — 选择此选项，将支持 Bluetooth 的手机与 Face Recognition 进行配对。在 Windows 登录期间，在验证您的脸部后，Face

Recognition 还会验证是否有配对的 Bluetooth 手机。如果有支持 Bluetooth 的配对手机，则允许您登录到 Windows。

- 确保在计算机和手机上都启用了 Bluetooth。

  如果没有支持 Bluetooth 的手机，则会提示您启用配对的 Bluetooth 手机并重新启动登录过程。30 秒后，Face Recognition 登录窗口将暂停。要启动登录过程，请单击**摄像头**图标。如果没有支持 Bluetooth 的手机，您可以使用普通 Windows 密码进行登录。

- 单击**添加**。

- 在显示 Bluetooth 设备时，选择该设备，然后单击**下一步**。

单击**确定**。

b. **其它设置**标签 — 选中复选框以启用下面的一个或多个选项，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组图像以提高以后脸部登录的成功几率。
- **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。

单击**确定**。

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。

您可以更改图片以及显示您的名称的方式。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 控制板。有关详细信息，请参阅第 23 页的打开 Security Manager。
2. 单击控制板左上角的 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**。

要更改显示的图片，请执行以下操作：

1. 打开 Security Manager 控制板。有关详细信息，请参阅第 23 页的打开 Security Manager。
2. 单击控制板左上角的 ID 卡。
3. 单击**选择图片**，单击一个图像，然后单击**保存**。

设置首选项

您可以对 HP ProtectTools Security Manager 设置进行个性化设置。从 Security Manager 控制板中，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 将提供声音反馈，它针对特定程序事件播放不同的声音。可通过 Windows 控制面板中的**声音**标签为这些事件指定新的声音，或者清除此选项以禁用声音反馈。
  - **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： 此功能仅备份数据。

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 控制板。有关详细信息，请参阅第 23 页的打开 Security Manager。
2. 在控制板的左面板中，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 控制板。有关详细信息，请参阅第 23 页的打开 Security Manager。
2. 在控制板的左面板中，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**。

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

Drive Encryption for HP ProtectTools 模块通过加密笔记本计算机的硬盘驱动器提供全面的数据保护。在激活 Drive Encryption 后，您必须在 Windows® 操作系统启动之前显示的 Drive Encryption 登录屏幕上登录。

通过使用 HP ProtectTools Security Manager 设置向导，Windows 管理员可以激活 Drive Encryption、备份加密密钥、选择或取消选择驱动器。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 TPM 保护的密码
  - 使用软件加密来加密或解密各个驱动器或分区
  - 使用硬件加密来加密或解密各个自加密驱动器
  - 通过禁用睡眠或待机以确保始终需要 Drive Encryption 预引导验证，来进一步添加安全保护

注： 只能加密内置 SATA 和外置 eSATA 硬盘驱动器。

- 创建备份密钥
- 恢复 Drive Encryption 密钥
- 使用密码、已注册指纹或智能卡 PIN 来启用 Drive Encryption 预引导验证

打开 Drive Encryption

管理员可以从 HP ProtectTools 管理控制台中访问 Drive Encryption。

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

常规任务

为标准硬盘驱动器激活 Drive Encryption

标准硬盘驱动器是使用软件加密进行加密的。执行以下步骤可激活 Drive Encryption：

1. 使用 HP ProtectTools Security Manager 设置向导激活 Drive Encryption。
2. 按照屏幕上的说明执行操作，直到显示**启用安全保护功能**页，然后继续执行下面的步骤 4。

– 或 –

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击**安全保护**左侧的 **+** 图标以显示可用的选项。
3. 单击**功能**。
4. 选择 **Drive Encryption** 复选框，然后单击**下一步**。

注： 如果没有为加密选择任何硬盘驱动器，系统就会激活 Drive Encryption 预引导验证，但不会对驱动器进行加密。

5. 在**要加密的驱动器**下，选择要加密的硬盘驱动器旁的复选框，然后单击**下一步**。
6. 要备份加密密钥，请将存储设备插入相应的插槽。

注： 要保存加密密钥，您必须使用具有 FAT32 格式的 USB 存储设备。软盘、USB 内存条、安全数字 (SD) 存储卡或 MMC 可以用于备份。

7. 在**备份 Drive Encryption 密钥**下，选择用于保存加密密钥的存储设备旁的复选框。
8. 单击**下一步**。

注： 计算机将会重新启动。

Drive Encryption 已经激活。驱动器的加密可能需要数小时，具体取决于驱动器的大小。

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

为自加密驱动器激活 Drive Encryption

如果自加密驱动器符合受信任的计算组针对自加密驱动器管理的 OPAL 规范，就可以使用软件加密或硬件加密来对其进行加密。执行以下步骤可为自加密驱动器激活 Drive Encryption：

1. 使用 HP ProtectTools Security Manager 设置向导激活 Drive Encryption。
2. 按照屏幕上的说明执行操作，直到显示**启用安全保护功能**页，然后继续执行以下“软件加密”或“硬件加密”下面的步骤 4。

注： 如果您的计算机没有自加密驱动器能够符合受信任的计算组针对自加密驱动器管理的 OPAL 规范，硬件加密选项就会不可用，默认情况下会使用软件加密。

如果自加密驱动器和标准硬盘驱动器混合在一起，硬件加密选项就会不可用，默认情况下会使用软件加密。

– 或 –

软件加密

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击**安全保护**左侧的 **+** 图标以显示可用的选项。
3. 单击**功能**。
4. 选择 **Drive Encryption** 复选框，然后单击**下一步**。
5. 在**要加密的驱动器**下，选择要加密的硬盘驱动器旁的复选框，然后单击**下一步**。
6. 要备份加密密钥，请将存储设备插入相应的插槽。

注： 要保存加密密钥，您必须使用具有 FAT32 格式的 USB 存储设备。软盘、USB 内存条、安全数字 (SD) 存储卡或 MMC 可以用于备份。

7. 在**备份 Drive Encryption 密钥**下，选择用于保存加密密钥的存储设备旁的复选框。
8. 单击**应用**。

注： 计算机将会重新启动。

Drive Encryption 已经激活。驱动器的加密可能需要数小时，具体取决于驱动器的大小。

硬件加密

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击**安全保护**左侧的 **+** 图标以显示可用的选项。
3. 单击**功能**。
4. 选择 **Drive Encryption** 复选框，然后单击**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，驱动器复选框会自动被选中，但不会灰掉。

只有选择了至少一个驱动器，**下一步**按钮才会可用。

5. 确保屏幕底部的**使用硬件驱动器加密**复选框处于选中状态。
6. 在**要加密的驱动器**下，选择要加密的硬盘驱动器旁的复选框，然后单击**下一步**。
7. 要备份加密密钥，请将存储设备插入相应的插槽。

注： 要保存加密密钥，您必须使用具有 FAT32 格式的 USB 存储设备。软盘、USB 内存条、安全数字 (SD) 存储卡或 MMC 可以用于备份。

8. 在**备份 Drive Encryption 密钥**下，选择用于保存加密密钥的存储设备旁的复选框。
9. 单击**应用**。

注： 计算机将需要重新启动。

Drive Encryption 已经激活。驱动器的加密可能需要数分钟。

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

停用 Drive Encryption

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

▲ 按照屏幕上的说明执行操作，直到显示**启用安全保护功能**页，然后继续执行下面的步骤 4。

– 或 –

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击**安全保护**左侧的 **+** 图标以显示可用的选项。
3. 单击**功能**。
4. 清除 **Drive Encryption** 复选框，然后单击**下一步**。

   Drive Encryption 停用便会开始。

注： 如果使用了软件加密，解密便会开始。这可能需要数小时，具体取决于驱动器的大小。解密完成后，Drive Encryption 便被停用。

如果使用了硬件加密，驱动器便会立即被解密，这可能需要数分钟，然后 Drive Encryption 便被停用。

驱动器被停用后，计算机将需要重新启动。

在激活 Drive Encryption 后登录

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

注： 如果是硬件加密，请确保计算机已关闭。如果计算机未关闭并重新启动，便不会显示 Drive Encryption 预引导验证屏幕。

注： 当从睡眠或待机状态醒来后，不会针对软件或硬件加密显示 Drive Encryption 预引导验证，除非它已被禁用。

当从休眠状态醒来后，会显示 Drive Encryption 预引导验证。

注： 如果 Windows 管理员在 HP ProtectTools Security Manager 中启用了预引导安全保护，您就可以在计算机开启后立即登录到计算机，而不是在显示 Drive Encryption 登录屏幕时登录。

1. 单击您的用户名，然后输入 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：

智能卡

- ActivIdentity 64K V2C 智能卡
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

PCMCIA 读卡器

- Express Card 54 SCR3340 内置读卡器
- SCR 201
- SCR 243（也是 HP 品牌）
- ActivCard
- Omnikey 4040
- Cisco

USB 读卡器

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP 智能卡终端

2. 单击**确定**。

注： 如果您使用恢复密钥在 Drive Encryption 登录屏幕中登录，系统就会在 Windows 登录屏幕中提示您用密码、智能卡 PIN 或已注册手指进行验证。

通过加密硬盘驱动器来保护数据

强烈建议您使用 HP ProtectTools Security Manager 设置向导来加密硬盘驱动器以保护数据：

1. 在左窗格中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。
2. 单击**设置**。
3. 对于软件加密的驱动器，选择要加密的驱动器分区。

注： 这也适用于混合驱动器的情况，即一个或多个标准驱动器与一个或多个自加密驱动器混合在一起。

– 或 –

▲ 对于硬件加密的驱动器，选择要加密的驱动器。必须选择至少一个驱动器。

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. 打开 HP ProtectTools Security Manager。
2. 在**我的数据**下，单击 **Drive Encryption**。

   如果是软件加密，会在**驱动器状态**下面显示下列状态代码之一：

   - 已启用
   - 已禁用
   - 未加密
   - 已加密
   - 正在加密
   - 正在解密

   如果是硬件加密，会在**驱动器状态**下面显示下列状态代码：

   - Encrypted（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。

高级任务

管理 Drive Encryption（管理员任务）

管理员可以使用“Drive Encryption”下的“设置”页来查看和更改 Drive Encryption 的状态（已启用、不活动或硬件加密已激活），以及查看计算机上所有硬盘驱动器的加密状态。

注： 硬件加密是无法在“设置”页上更改的。

- 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”，则说明 Drive Encryption 已被激活并配置。驱动器处于下列状态之一：

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

加密或解密各个驱动器（仅限软件加密）

管理员可以使用“设置”页来加密计算机上的一个或多个硬盘驱动器或者解密已经加密的驱动器。

1. 打开 HP ProtectTools 管理控制台。
2. 在左窗格中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。
3. 单击**设置**。
4. 在**加密状态**下，选中或清除每个要加密或解密的硬盘驱动器旁的复选框，然后单击**应用**。

注： 在加密或解密驱动器时，进度条会显示完成当前会话过程的剩余时间。

如果在加密过程中计算机关闭或启动睡眠/待机或休眠模式，然后重新启动，进度条上的剩余时间就会重置为从头开始，但实际加密会从上次停止的位置继续。进度条（以百分比形式显示）以及剩余时间会改变得更快以反映以前的进度。

注： 不支持动态分区。如果某个分区显示为可用，但选择它后无法加密，该分区就是动态的。动态分区起因于为在磁盘管理中创建新分区而缩小某个分区。

如果某个分区将要转变为动态分区，会显示警告消息。

备份和恢复（管理员任务）

激活 Drive Encryption 后，管理员可以使用“加密密钥备份”页将加密密钥备份到可移动介质中以及执行恢复。

备份加密密钥

管理员可以将加密驱动器的加密密钥备份到可移动存储设备上。

⚠ **注意：** 请一定将含有备份密钥的存储设备放在安全的地方，因为如果您忘记了密码、丢失了智能卡或未注册手指，该设备就是唯一能让您访问硬盘的途径了。

1. 打开 HP ProtectTools 管理控制台。
2. 在左窗格中，单击 **Drive Encryption** 左侧的 **+** 图标以显示可用的选项。
3. 单击**加密密钥备份**。
4. 插入将用于备份加密密钥的存储设备。
5. 在**驱动器**下，选中要用于备份加密密钥的设备所对应的复选框。
6. 单击**备份密钥**。
7. 阅读此页中显示的信息，然后单击**下一步**。加密密钥便会保存到您选择的存储设备上。

恢复加密密钥

管理员可以从可移动存储设备中恢复其中已经保存的加密密钥。

1. 打开笔记本计算机。
2. 插入包含备份密钥的可移动存储设备。
3. 在 Drive Encryption for HP ProtectTools 登录对话框打开后，单击**选项**。
4. 单击**恢复**。
5. 选择包含备份密钥的文件或单击**浏览**以搜索此文件，然后单击**下一步**。
6. 确认对话框打开时，请单击**确定**。

   笔记本计算机将启动。

注： 极力建议您执行恢复操作后重置密码。

6 HP ProtectTools Privacy Manager（仅限某些机型）

通过使用 Privacy Manager for HP ProtectTools，您可以在使用电子邮件或 Microsoft® Office 文档时，使用高级安全登录（验证）方法验证通信的来源、完整性和安全性。

Privacy Manager 利用了 HP ProtectTools Security Manager 提供的安全基础结构，其中包括以下安全登录方法：

- 指纹验证
- Windows® 密码
- 智能卡
- Face Recognition

您可以在 Privacy Manager 中使用以上任何安全登录方法。

打开 Privacy Manager

要打开 Privacy Manager，请执行以下操作：

- 要访问 Microsoft Outlook 中的 Outlook 特有功能，请在**消息**标签上的**隐私**组中单击**安全发送**。
- 要访问 Microsoft Office 文档中的大多数功能，请在**主页**标签上的**隐私**组中单击**签名并加密**。
- 要访问其它功能，请访问 HP ProtectTools Security Manager 控制板。
  - 依次单击**开始**、**所有程序**、**HP**、**HP ProtectTools Security Manager** 和 **Privacy Manager**。

    – 或 –

  - 单击 **HP ProtectTools** 桌面小工具图标。

    – 或 –

  - 在任务栏最右侧的通知区域中右击 **HP ProtectTools** 图标，单击 **Privacy Manager**，然后单击**配置**。

设置步骤

管理 Privacy Manager 证书

Privacy Manager 证书使用一种称为公钥基础结构 (PKI) 的加密技术来保护数据和邮件。PKI 要求用户获取加密密钥和认证机构 (CA) 颁发的 Privacy Manager 证书。与大多数只要求定期验证的数据加密和验证软件不同，Privacy Manager 要求每次使用加密密钥对电子邮件或 Microsoft Office 文档进行签名时都进行验证。Privacy Manager 使保存和发送重要信息的过程变得非常安全可靠。

通过使用 Certificate Manager，您可以执行以下任务：

- 第 50 页的申请 Privacy Manager 证书
- 第 50 页的获取预先分配的公司 Privacy Manager 证书
- 第 52 页的设置默认 Privacy Manager 证书
- 第 51 页的导入第三方证书
- 第 52 页的查看 Privacy Manager 证书详细信息
- 第 52 页的续订 Privacy Manager 证书
- 第 52 页的设置默认 Privacy Manager 证书
- 第 52 页的删除 Privacy Manager 证书
- 第 53 页的恢复 Privacy Manager 证书
- 第 53 页的吊销 Privacy Manager 证书

申请 Privacy Manager 证书

在使用 Privacy Manager 功能之前，必须先使用有效的电子邮件地址申请并安装 Privacy Manager 证书（从 Privacy Manager 内）。该电子邮件地址必须在申请 Privacy Manager 证书时所使用的计算机上设置为 Microsoft Outlook 内的帐户。

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击**申请 Privacy Manager 证书**。
3. 在“欢迎使用”页上，阅读其中的文字，然后单击**下一步**。
4. 在“许可协议”页上，阅读许可协议。
5. 确保**选中此处以接受此许可协议中的条款**旁边的复选框处于选中状态，然后单击**下一步**。
6. 在“您的证书详细信息”页上，输入所需的信息，然后单击**下一步**。
7. 在“已接受证书申请”页上，单击**完成**。

将会在 Microsoft Outlook 中收到一封电子邮件，其中附加了 Privacy Manager 证书。

获取预先分配的公司 Privacy Manager 证书

1. 在 Outlook 中，打开收到的电子邮件，该邮件指出已为您预先分配了一个公司证书。
2. 单击**获取**。

将会在 Microsoft Outlook 中收到一封电子邮件，其中附加了 Privacy Manager 证书。

要安装证书，请参阅第 51 页的设置 Privacy Manager 证书。

设置 Privacy Manager 证书

1. 在收到附加了 Privacy Manager 证书的电子邮件时，打开这封电子邮件，然后单击邮件右下角（Outlook 2007 或 Outlook 2010）或左上角 (Outlook 2003) 的**设置**按钮。
2. 使用所选的安全登录方法进行验证。
3. 在“证书已安装”页上，单击**下一步**。
4. 在“证书备份”页上，输入备份文件的位置和名称，或者单击**浏览**以查找位置。

注意： 确保将该文件保存到硬盘驱动器以外的位置，并将其存放在安全的地方。此文件应仅供您使用，以备恢复 Privacy Manager 证书和关联密钥之需。

5. 输入并确认密码，然后单击**下一步**。
6. 使用所选的安全登录方法进行验证。
7. 如果选择开始可信联系人邀请过程，请按照屏幕上的说明进行操作，从主题第 55 页的使用 Microsoft Outlook 联系人添加可信联系人的步骤 2 开始。

   - 或 -

   如果您单击**取消**，请参阅第 53 页的管理可信联系人以了解有关以后添加可信联系人的信息。

导入第三方证书

可以通过证书导入向导，将第三方证书导入到 Privacy Manager 中。

要使用该功能，必须在 **Privacy Manager** 的“设置”页中启用 HP ProtectTools 管理控制台中的**允许使用第三方证书**设置。

1. 打开 Privacy Manager，然后单击**证书**。
2. 选择 **Certificate Manager** 标签，然后单击**导入证书**。

   如果不允许导入证书，则不会显示此按钮。
3. 选择是导入已安装在此计算机上的证书，还是导入存储为 PFX（个人信息交换/PKCS#12）文件的证书，然后单击**下一步**。
   - 要导入此计算机上安装的证书，请选择所需的证书，然后单击**下一步**。
   - 要选择 PFX 证书，请单击**浏览**，浏览到 PFX 文件的位置，然后单击**下一步**。键入 PFX 文件密码，然后单击**下一步**。
4. 在完成导入过程后，单击**下一步**。
5. 将提供用于备份导入的证书的选项。

   建议您将证书备份到计算机硬盘驱动器以外的位置。

查看 Privacy Manager 证书详细信息

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击一个 Privacy Manager 证书。
3. 单击**证书详细信息**。
4. 在查看完详细信息后，单击**确定**。

续订 Privacy Manager 证书

当 Privacy Manager 证书快要到期时，将会通知您需要续订该证书：

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击**续订证书**。
3. 按照屏幕上的说明获取新的 Privacy Manager 证书。

注： Privacy Manager 证书续订过程不会替换原来的 Privacy Manager 证书。您必须获取新的 Privacy Manager 证书，然后按照第 50 页的申请 Privacy Manager 证书中的步骤安装该证书。

对于您的公司使用 Microsoft 证书颁发机构颁发的公司证书，CA 管理员必须使用与原始证书相同的私钥续订您的证书，或者使用相同的私钥颁发新证书。

设置默认 Privacy Manager 证书

只能从 Privacy Manager 中看到 Privacy Manager 证书，即使计算机上还安装了其它证书颁发机构颁发的其它证书。

如果通过 Privacy Manager 在计算机上安装了多个 Privacy Manager 证书，则可以将其中的一个证书指定为默认证书：

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击要用作默认证书的 Privacy Manager 证书，然后单击**设为默认**。
3. 单击**确定**。

注 并不要求您使用默认 Privacy Manager 证书。您可以从各种 Privacy Manager 功能中选择要使用的任何 Privacy Manager 证书。

删除 Privacy Manager 证书

如果删除了某个 Privacy Manager 证书，则无法打开使用该证书加密的任何文件或查看使用该证书加密的任何数据。如果意外删除了某个 Privacy Manager 证书，可使用在安装该证书时创建的备份文件恢复该证书。有关详细信息，请参阅第 53 页的恢复 Privacy Manager 证书。

要删除 Privacy Manager 证书，请执行以下操作：

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击要删除的 Privacy Manager 证书，然后单击**高级**。
3. 单击**删除**。

4. 在打开确认对话框时，单击**是**。
5. 单击**关闭**，然后单击**应用**。

恢复 Privacy Manager 证书

在安装 Privacy Manager 证书期间，您需要创建该证书的备份副本。也可以从“迁移”页中创建备份副本。在将证书迁移到另一台计算机或将证书恢复到同一台计算机时，可以使用此备份副本。

1. 打开 Privacy Manager，然后单击**迁移**。
2. 单击**恢复**。
3. 在“迁移文件”页上，单击**浏览**以查找在备份过程中创建的 .dppsm 文件，然后单击**下一步**。
4. 输入在创建备份时使用的密码，然后单击**下一步**。
5. 单击**完成**。

有关详细信息，请参阅第 51 页的设置 Privacy Manager 证书或第 62 页的备份 Privacy Manager 证书和可信联系人。

吊销 Privacy Manager 证书

如果觉得 Privacy Manager 证书的安全受到威胁，您可以吊销自己的证书：

注： 不会删除吊销的 Privacy Manager 证书。仍可以使用该证书来查看加密的文件。

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击**高级**。
3. 单击要吊销的 Privacy Manager 证书，然后单击**吊销**。
4. 在打开确认对话框时，单击**是**。
5. 使用所选的安全登录方法进行验证。
6. 按照屏幕上的说明进行操作。

管理可信联系人

可信联系人是与您交换了 Privacy Manager 证书的用户，以便彼此之间安全地进行通信。

通过使用可信联系人管理器，您可以执行以下任务：

- 查看可信联系人详细信息
- 删除可信联系人
- 检查可信联系人的吊销状态（高级）

添加可信联系人

添加可信联系人的过程分为三步：

1. 向可信联系人收件人发送电子邮件邀请。
2. 可信联系人收件人回复此电子邮件。
3. 您收到可信联系人收件人的回复电子邮件，然后单击**接受**。

您可以向各个收件人发送可信联系人电子邮件邀请，也可以向 Microsoft Outlook 地址簿中的所有联系人发送邀请。

请参阅以下部分以添加可信联系人。

注： 要回复邀请电子邮件以成为可信联系人，可信联系人收件人必须在计算机上安装 Privacy Manager 或安装备用客户端。有关安装备用客户端的信息，请访问 DigitalPersona 网站：http://digitalpersona.com/privacymanager/download。

添加可信联系人

1. 打开 Privacy Manager，单击**可信联系人管理器**，然后单击**邀请联系人**。

   - 或 -

   在 Microsoft Outlook 中，单击工具栏上的**安全发送**旁边的向下箭头，然后单击**邀请联系人**。

2. 如果打开了“选择证书”对话框，请单击要使用的 Privacy Manager 证书，然后单击**确定**。
3. 在打开“可信联系人邀请”对话框时，请阅读文本，然后单击**确定**。

   将自动生成一封电子邮件。

4. 输入要添加为可信联系人的收件人的电子邮件地址。
5. 编辑文本并签上您的名字（可选）。
6. 单击**发送**。

   注： 如果您尚未获得 Privacy Manager 证书，则将显示一条消息，告知您必须具有 Privacy Manager 证书才能发送可信联系人请求。单击**确定**以启动证书申请向导。有关详细信息，请参阅第 50 页的申请 Privacy Manager 证书。

7. 使用所选的安全登录方法进行验证。

   注： 当可信联系人收件人收到电子邮件时，收件人必须打开这封电子邮件并单击电子邮件右下角的**接受**，然后在打开确认对话框时单击**确定**。

8. 当您从接受邀请成为可信联系人的收件人处收到回复电子邮件时，请单击电子邮件右下角的**接受**。

   将打开一个对话框，确认已成功将该收件人添加到可信联系人列表中。

9. 单击**确定**。

使用 Microsoft Outlook 联系人添加可信联系人

1. 打开 Privacy Manager，单击**可信联系人管理器**，然后单击**邀请联系人**。

   – 或 –

   在 Microsoft Outlook 中，单击工具栏上的**安全发送**旁边的向下箭头，然后单击**邀请我的 Outlook 联系人**。

2. 当打开“可信联系人邀请”页时，选择要添加为可信联系人的收件人的电子邮件地址，然后单击**下一步**。

3. 在打开“发送邀请”页时，单击**完成**。

   将自动生成一封电子邮件，其中列出了选定的 Microsoft Outlook 电子邮件地址。

4. 编辑文本并签上您的名字（可选）。

5. 单击**发送**。

注： 如果您尚未获得 Privacy Manager 证书，则将显示一条消息，告知您必须具有 Privacy Manager 证书才能发送可信联系人请求。单击**确定**以启动证书申请向导。有关详细信息，请参阅第 50 页的申请 Privacy Manager 证书。

6. 使用所选的安全登录方法进行验证。

注： 当可信联系人收件人收到电子邮件时，收件人必须打开这封电子邮件并单击电子邮件右下角的**接受**，然后在打开确认对话框时单击**确定**。

7. 当您从接受邀请成为可信联系人的收件人处收到回复电子邮件时，请单击电子邮件右下角的**接受**。

   将打开一个对话框，确认已成功将该收件人添加到可信联系人列表中。

8. 单击**确定**。

查看可信联系人详细信息

1. 打开 Privacy Manager，然后单击**可信联系人**。
2. 单击某个可信联系人。
3. 单击**联系人详细信息**。
4. 查看完详细信息后，单击**确定**。

删除可信联系人

1. 打开 Privacy Manager，然后单击**可信联系人**。
2. 单击要删除的可信联系人。
3. 单击**删除联系人**。
4. 在打开确认对话框时，单击**是**。

检查可信联系人的吊销状态

要查看可信联系人是否吊销了其 Privacy Manager 证书，请执行以下操作：

1. 打开 Privacy Manager，然后单击**可信联系人**。
2. 单击某个可信联系人。
3. 单击**高级**按钮。

   将打开“高级可信联系人管理”对话框。
4. 单击**检查吊销**。
5. 单击**关闭**。

常规任务

可以将 Privacy Manager 与下列 Microsoft 产品配合使用：

- Microsoft Outlook
- Microsoft Office

在 Microsoft Outlook 中使用 Privacy Manager

在安装 Privacy Manager 后，Microsoft Outlook 工具栏上将显示“隐私”按钮，每个 Microsoft Outlook 电子邮件的工具栏上将显示“安全发送”按钮。在单击**隐私**或**安全发送**旁边的向下箭头时，可以从下列选项中进行选择：

- **对邮件进行签名并发送它**（仅“安全发送”按钮）— 通过使用此选项，可以在电子邮件中添加数字签名，并在使用所选的安全登录方法进行验证后发送该邮件。
- **为可信联系人密封并发送邮件**（仅“安全发送”按钮）— 通过使用此选项，可以添加数字签名，加密电子邮件，并在使用所选的安全登录方法进行验证后发送该邮件。
- **邀请联系人** — 通过使用此选项，可以发送可信联系人邀请。有关详细信息，请参阅第 54 页的添加可信联系人。
- **邀请 Outlook 联系人** — 通过使用此选项，可以向 Microsoft Outlook 通讯簿中的所有联系人发送可信联系人邀请。有关详细信息，请参阅第 55 页的使用 Microsoft Outlook 联系人添加可信联系人。
- **打开 Privacy Manager 软件** — 通过使用“证书”、“可信联系人”和“设置”选项，可以打开 Privacy Manager 软件以添加、查看或更改当前设置。有关详细信息，请参阅第 50 页的管理 Privacy Manager 证书、第 53 页的管理可信联系人或第 57 页的为 Microsoft Outlook 配置 Privacy Manager。

为 Microsoft Outlook 配置 Privacy Manager

1. 打开 Privacy Manager，单击**设置**，然后单击**电子邮件**标签。

   - 或 -

   在主 Microsoft Outlook 工具栏上，单击**安全发送**（Outlook 2003 中为**隐私**）旁边的向下箭头，然后单击**设置**。

   - 或 -

   在 Microsoft Outlook 电子邮件工具栏上，单击**安全发送**旁边的向下箭头，然后单击**设置**。

2. 选择在发送安全电子邮件时执行的操作，然后单击**确定**。

对电子邮件进行签名并发送邮件

1. 在 Microsoft Outlook 中，单击**新建**或**回复**。
2. 键入电子邮件。
3. 单击**安全发送**（Outlook 2003 中为**隐私**）旁边的向下箭头，然后单击**签名并发送**。
4. 使用所选的安全登录方法进行验证。

对电子邮件进行密封并发送邮件

只能由从可信联系人列表中选择的人员查看经过数字签名并密封（加密）的密封电子邮件。

要密封电子邮件并将其发送给可信联系人，请执行以下操作：

1. 在 Microsoft Outlook 中，单击**新建**或**回复**。
2. 键入电子邮件。
3. 单击**安全发送**（Outlook 2003 中为**隐私**）旁边的向下箭头，然后单击**为可信联系人密封并发送**。
4. 使用所选的安全登录方法进行验证。

查看密封的电子邮件

在打开密封的电子邮件时，将在电子邮件标题中显示安全标签。安全标签提供以下信息：

- 用于验证电子邮件签名者身份的证书
- 用于验证电子邮件签名者的证书的产品

在 Microsoft Office 2007 文档中使用 Privacy Manager

在安装 Privacy Manager 证书后，将在所有 Microsoft Word、Microsoft Excel 和 Microsoft PowerPoint 文档的工具栏右侧显示“签名并加密”按钮。在单击**签名并加密**旁边的向下箭头时，您可以从下列选项中进行选择：

- **对文档进行签名** — 通过使用此选项，可以在文档中添加数字签名。
- **在签名之前添加签名行**（仅限 Microsoft Word 和 Microsoft Excel）— 默认情况下，在对 Microsoft Word 或 Microsoft Excel 文档进行签名或加密时，将会添加一个签名行。要禁用此选项，请单击**添加签名行**以删除复选标记。
- **加密文档** — 通过使用此选项，可以添加数字签名并对文档进行加密。
- **删除加密** — 通过使用此选项，可以从文档中删除加密。
- **打开 Privacy Manager 软件** — 通过使用“证书”、“可信联系人”和“设置”选项，可以打开 Privacy Manager 软件以添加、查看或更改当前设置。有关详细信息，请参阅第 50 页的管理 Privacy Manager 证书、第 53 页的管理可信联系人或第 58 页的为 Microsoft Office 配置 Privacy Manager。

为 Microsoft Office 配置 Privacy Manager

1. 打开 Privacy Manager，单击**设置**，然后单击**文档**标签。

   - 或 -

   在 Microsoft Office 文档工具栏上，单击**签名并加密**旁边的向下箭头，然后单击**设置**。
2. 选择要配置的操作，然后单击**确定**。

对 Microsoft Office 文档进行签名

1. 在 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 中，创建并保存一个文档。
2. 单击**签名并加密**旁边的向下箭头，然后单击**对文档进行签名**。

3. 使用所选的安全登录方法进行验证。
4. 在打开确认对话框时，请阅读文本，然后单击**确定**。

如果以后决定编辑文档，请执行以下步骤：

1. 单击屏幕左上角的 **Office** 按钮。
2. 单击**准备**，然后单击**标记为最终**。
3. 在打开确认对话框时，单击**是**，然后继续工作。
4. 在编辑完成后，再次对文档进行签名。

对 Microsoft Word 或 Microsoft Excel 文档进行签名时添加签名行

通过使用 Privacy Manager，您可以在对 Microsoft Word 或 Microsoft Excel 文档进行签名时添加签名行：

1. 在 Microsoft Word 或 Microsoft Excel 中，创建并保存一个文档。
2. 单击**主**菜单。
3. 单击**签名并加密**旁边的向下箭头，然后单击**在签名之前添加签名行**。

注： 在选择此选项后，“在签名之前添加签名行”旁边将显示复选标记。默认情况下，将启用此选项。

4. 单击**签名并加密**旁边的向下箭头，然后单击**对文档进行签名**。
5. 使用所选的安全登录方法进行验证。

将建议的签名者添加到 Microsoft Word 或 Microsoft Excel 文档中

可以通过指定建议的签名者，在文档中添加多个签名行。建议的签名者是由 Microsoft Word 或 Microsoft Excel 文档所有者指定在文档中添加签名行的用户。建议的签名者可以是您自己，也可以是您希望对文档进行签名的其他人。例如，如果您准备一个需要由所在部门的所有成员进行签名的文档，则可以在文档的最后一页底部包含这些用户的签名行，并提供在特定日期进行签名的说明。

要在 Microsoft Word 或 Microsoft Excel 文档中添加建议的签名者，请执行以下操作：

1. 在 Microsoft Word 或 Microsoft Excel 中，创建并保存一个文档。
2. 单击**插入**菜单。
3. 在工具栏的**文本**组中，单击**签名行**旁边的向下箭头，然后单击 **Privacy Manager 签名提供者**。

   将打开“签名设置”对话框。
4. 在**建议的签名者**下面的框中，输入建议的签名者的名字。
5. 在**签名者须知**下面的框中，为建议的该签名者输入一条消息。

注： 将显示此消息以替代职务；在对文档进行签名时，将会删除此消息或被用户职务替代。

6. 选中**在签名行中显示签名日期**复选框以显示日期。
7. 选中**在签名行中显示签名者的职务**复选框以显示职务。

注： 文档所有者为其文档指定建议的签名者。必须选中**在签名行中显示签名日期**和/或**在签名行中显示签名者的职务**复选框，建议的签名者才能在签名行中显示日期和/或职务。

8. 单击**确定**。

添加建议的签名者的签名行

当建议的签名者打开文档时，他们将会在括号中看到他们的名字，表示需要其进行签名。

要对文档进行签名，请执行以下操作：

1. 双击相应的签名行。
2. 使用所选的安全登录方法进行验证。

   将按照文档所有者指定的设置显示签名行。

加密 Microsoft Office 文档

您可以对您自己和可信联系人的 Microsoft Office 文档进行加密。在加密并关闭文档后，您和从列表中选择的可信联系人必须先进行验证，然后才能打开文档。

要加密 Microsoft Office 文档，请执行以下操作：

1. 在 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 中，创建并保存一个文档。
2. 单击**主**菜单。
3. 单击**签名并加密**旁边的向下箭头，然后单击**加密文档**。

   将打开“选择可信联系人”对话框。
4. 单击将能够打开文档并查看其内容的可信联系人的名字。

注： 要选择多个可信联系人名字，请按住 ctrl 键并单击各个名字。

5. 单击**确定**。

如果以后决定编辑文档，请按照第 60 页的从 Microsoft Office 文档中删除加密中的步骤进行操作。在删除加密后，您可以对文档进行编辑。要重新加密文档，请按照本节中的步骤进行操作。

从 Microsoft Office 文档中删除加密

从 Microsoft Office 文档中删除加密后，您和可信联系人不再需要验证即可打开文档并查看其内容。

要从 Microsoft Office 文档中删除加密，请执行以下操作：

1. 打开加密的 Microsoft Word、Microsoft Excel 或 Microsoft PowerPoint 文档。
2. 使用所选的安全登录方法进行验证。
3. 单击**主**菜单。
4. 单击**签名并加密**旁边的向下箭头，然后单击**删除加密**。

发送加密的 Microsoft Office 文档

可以将加密的 Microsoft Office 文档附加到电子邮件中，而无需对电子邮件本身进行签名或加密。为此，请创建一封电子邮件并将其与签名或加密的文档一起发送，这与发送带有附件的普通电子邮件完全相同。

但是，为了获得最佳的安全性，建议您在附加签名或加密的 Microsoft Office 文档时加密电子邮件。

要发送附加了签名和/或加密的 Microsoft Office 文档的密封电子邮件，请执行以下步骤：

1. 在 Microsoft Outlook 中，单击**新建**或**回复**。
2. 键入电子邮件。
3. 附加 Microsoft Office 文档。
4. 有关详细说明，请参阅第 58 页的对电子邮件进行密封并发送邮件。

查看签名的 Microsoft Office 文档

注： 要查看签名的 Microsoft Office 文档，您并不需要具有 Privacy Manager 证书。

在打开签名的 Microsoft Office 文档时，将在文档窗口底部的状态栏中显示数字签名图标。

1. 单击**数字签名**图标以切换显示“签名”对话框，其中显示了对文档进行签名的所有用户的名称以及每个用户的签名日期。
2. 要查看每个签名的更多详细信息，请在“签名”对话框中右击某个名称，然后选择**签名详细信息**。

查看加密的 Microsoft Office 文档

要从另一台计算机中查看加密的 Microsoft Office 文档，必须在该计算机上安装 Privacy Manager。还必须恢复用于加密该文件的 Privacy Manager 证书。

如果您的证书已丢失，则必须恢复用于加密 Microsoft Office 文档的 Privacy Manager 证书才能查看该文件。

要查看加密的 Microsoft Office 文档，可信联系人必须具有 Privacy Manager 证书，并且必须在其计算机上安装 Privacy Manager。另外，还必须由加密的 Microsoft Office 文档的所有者选择可信联系人。

高级任务

将 Privacy Manager 证书和可信联系人迁移到其它计算机上

可以安全地将 Privacy Manager 证书和可信联系人迁移到其它计算机上，或者备份数据以便妥善进行保管。为此，请以使用密码保护的文件将数据备份到网络位置或任何可移动存储设备，然后将该文件恢复到新计算机。

备份 Privacy Manager 证书和可信联系人

要以使用密码保护的文件备份 Privacy Manager 证书和可信联系人，请执行以下步骤：

1. 打开 Privacy Manager，然后单击**迁移**。
2. 单击**备份**。
3. 在“选择数据”页上，选择要包含在迁移文件中的数据类别，然后单击**下一步**。
4. 在“迁移文件”页上，输入文件名称或单击**浏览**以查找位置，然后单击**下一步**。
5. 输入并确认密码，然后单击**下一步**。

注： 将此密码存放在安全的地方，因为在恢复迁移文件时需要使用它。

6. 使用所选的安全登录方法进行验证。
7. 在“迁移文件已保存”页上，单击**完成**。

恢复 Privacy Manager 证书和可信联系人

要在迁移过程中将 Privacy Manager 证书和可信联系人恢复到另一台计算机或同一台计算机，请执行以下步骤：

1. 打开 Privacy Manager，然后单击**迁移**。
2. 单击**恢复**。
3. 在“迁移文件”页上，单击**浏览**以查找文件，然后单击**下一步**。
4. 输入在创建备份文件时使用的密码，然后单击**下一步**。
5. 在“迁移文件”页上，单击**完成**。

Privacy Manager 集中管理

您的 Privacy Manager 安装可能是管理员定制的集中安装的一部分。可能启用或禁用了下面的一项或多项功能：

- **证书使用策略** — 您可能仅限于使用 Comodo 颁发的 Privacy Manager 证书，也可能允许您使用其它证书颁发机构颁发的数字证书。
- **加密策略** — 可以在 Microsoft Office 或 Microsoft Outlook 中分别启用或禁用加密功能。

7 HP ProtectTools File Sanitizer

通过使用 File Sanitizer，您可以安全地碎化计算机上的资产（例如，个人信息或文件、历史数据或与 Web 有关的数据）以及定期清理硬盘驱动器上的已删除资产。

注： 此版本的 File Sanitizer 仅支持计算机硬盘驱动器。

碎化

碎化不同于标准 Windows® 删除操作（在 File Sanitizer 中也称为简单删除）。在使用 File Sanitizer 碎化资产时，将使用无意义的数据覆盖这些文件，从而使原始资产几乎无法恢复。Windows 简单删除可能会在硬盘驱动器上完整保留文件（或资产），或使其处于可使用取证方法进行恢复的状态。

在选择碎化配置文件（**高安全保护**、**中安全保护**或**低安全保护**）时，将自动选择要碎化的预定义资产列表和清除方法。也可以通过指定碎化周期数、要包括在碎化中的资产、在碎化前确认的资产以及从碎化中排除的资产，自定义碎化配置文件。有关详细信息，请参阅第 68 页的选择或创建碎化配置文件。

您可以设置一个自动碎化计划，或者使用任务栏最右侧的通知区域中的 **HP ProtectTools** 图标手动激活碎化。有关详细信息，请参阅第 67 页的设置碎化计划、第 72 页的手动碎化单个资产或第 72 页的手动碎化所有选定的项目。

注： 只有在将 .dll 文件移到回收站时，才能碎化这些文件并将其从系统中删除。

可用空间清理

在 Windows 中删除资产时，并不会将资产内容从硬盘驱动器中完全删除。Windows 只删除对资产的引用。资产内容仍保留在硬盘驱动器上，直至其它资产使用新信息覆盖硬盘驱动器上的相同区域。

通过进行可用空间清理，您可以安全地写入随机数据以覆盖删除的资产，从而防止用户查看已删除资产的原始内容。

注： 对于通过在 File Sanitizer 中选择**简单删除设置**删除的资产、通过移到 Windows 回收站删除的资产或手动删除的资产，可以不定期地执行可用空间清理。可用空间清理不会为碎化的资产提供额外的安全保护。

您可以设置一个自动可用空间清理计划，或者使用任务栏最右侧的通知区域中的 **HP ProtectTools** 图标手动激活可用空间清理。有关详细信息，请参阅第 67 页的设置可用空间清理计划或第 72 页的手动激活可用空间清理。

打开 File Sanitizer

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

– 或 –

▲ 双击桌面上的 **File Sanitizer** 图标。

– 或 –

▲ 在任务栏最右侧的通知区域中右击 **HP ProtectTools** 图标，单击 **File Sanitizer**，然后单击**打开 File Sanitizer**。

设置步骤

设置碎化计划

您可以选择一个预定义碎化配置文件，或者创建您自己的碎化配置文件。有关详细信息，请参阅第 68 页的选择或创建碎化配置文件。您也可以随时手动碎化资产。有关详细信息，请参阅第 71 页的使用按键序列启动碎化。

注： 计划的任务将在特定时间启动。如果在计划时间关闭了系统或处于睡眠/待机状态，File Sanitizer 不会尝试重新启动该任务。

1. 打开 File Sanitizer，然后单击**碎化**。
2. 选择一个或多个碎化选项：
   - **Windows 关机** — 在 Windows 关机时碎化所有选定的资产。

     注： 在关机时，将打开一个对话框，询问您是继续碎化选定的资产，还是跳过该过程。

     单击**是**以跳过碎化过程，或者单击**否**继续进行碎化。
   - **Web 浏览器打开** — 在打开 Web 浏览器时，碎化与 Web 有关的所有选定资产，如浏览器 URL 历史记录。
   - **Web 浏览器退出** — 在关闭 Web 浏览器时，碎化与 Web 有关的所有选定资产，如浏览器 URL 历史记录。
   - **按键序列** — 用于指定按键序列以启动碎化。有关详细信息，请参阅第 71 页的使用按键序列启动碎化。

   注： 只有在将 .dll 文件移到回收站时，才能碎化这些文件并将其从系统中删除。
3. 要计划将来碎化选定资产，请选中**激活计划程序**复选框，输入 Windows 密码，然后选择日期和时间。
4. 单击**应用**。

设置可用空间清理计划

对于通过在 File Sanitizer 中选择**简单删除设置**删除的资产、通过移到 Windows 回收站删除的资产或手动删除的资产，可以不定期地执行可用空间清理。可用空间清理不会为碎化的资产提供额外的安全保护。

注： 计划的任务将在特定时间启动。如果在计划时间关闭了系统或处于睡眠/待机状态，File Sanitizer 不会尝试重新启动该任务。

1. 打开 File Sanitizer，然后单击**清理**。
2. 要计划将来清理硬盘驱动器上的已删除资产，请选中**激活计划程序**复选框，输入 Windows 密码，然后选择日期和时间。
3. 单击**应用**。

注： 可用空间清理操作可能需要相当长的时间。虽然可用空间清理是在后台执行的，但由于提高了处理器的使用率，可能会影响计算机的性能。

选择或创建碎化配置文件

可通过选择预定义配置文件或创建您自己的配置文件，指定清除方法和选择要碎化的资产。

选择预定义碎化配置文件

在选择预定义碎化配置文件时，将会自动选择预定义的清除方法和资产列表。您也可以查看选择碎化的预定义资产列表。

1. 打开 File Sanitizer，然后单击**设置**。
2. 单击一个预定义碎化配置文件：
   - **高安全保护**
   - **中安全保护**
   - **低安全保护**
3. 要查看选择碎化的资产，请单击**查看详细信息**。
   a. **所选项目将被碎化，同时将显示一条确认消息。未选择的项目将被碎化，但不显示确认消息。** — 选中此复选框可在碎化项目之前显示确认消息，或者清除此复选框，则在碎化项目之前不显示确认消息。

   注： 即使清除资产的复选框，该资产也将被碎化。

   b. 单击**应用**。
4. 单击**应用**。

自定义碎化配置文件

在创建碎化配置文件时，可以指定碎化周期数、在碎化中包含的资产、在碎化之前进行确认的资产以及从碎化中排除的资产：

1. 打开 File Sanitizer，依次单击**设置**、**高级安全设置**和**查看详细信息**。
2. 选择碎化周期数。

注： 将为每个资产执行选定数量的碎化周期。例如，如果选择三个碎化周期，将在三个不同的时间执行遮盖数据的算法。如果选择安全性较高的碎化周期，碎化可能需要相当长的时间；不过，指定的碎化周期数越高，能够恢复数据的可能性就越小。

3. 要选择碎化的资产，请执行以下操作：
   a. 在**可用碎化选项**下，单击某个资产，然后单击**添加**。
   b. 要添加自定义资产，请单击**添加自定义选项**，然后浏览到文件或文件夹，或者键入文件或文件夹的路径。
   c. 单击**打开**，然后单击**确定**。
   d. 在**可用碎化选项**下，单击自定义资产，然后单击**添加**。

   要从可用碎化选项中删除资产，请单击该资产，然后单击**删除**。

4. **所选项目将被碎化，同时将显示一条确认消息。未选择的项目将被碎化，但不显示确认消息。**— 选中此复选框可在碎化项目之前显示确认消息，或者清除此复选框，则在碎化项目之前不显示确认消息。

注： 即使清除资产的复选框，该资产也将被碎化。

要从碎化列表中删除资产，请单击该资产，然后单击**删除**。

5. 要保护文件或文件夹以防止自动碎化，请执行以下操作：

   a. 在**不要碎化以下内容**下面，单击**添加**，然后浏览到文件或文件夹，或者键入文件或文件夹的路径。

   b. 单击**打开**，然后单击**确定**。

   要从排除列表中删除资产，请单击该资产，然后单击**删除**。

6. 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的资产删除操作，而不进行碎化。可通过指定要包括的资产、删除前确认的资产以及排除的资产，自定义简单删除配置文件。

注： 如果选择**简单删除设置**，可以不定期地对手动删除的资产或通过 Windows 回收站删除的资产执行可用空间清理。

1. 打开 File Sanitizer，依次单击**设置**、**简单删除设置**和**查看详细信息**。
2. 选择要删除的资产：

   a. 在**可用删除选项**下，单击某个资产，然后单击**添加**。

   b. 要添加自定义资产，请单击**添加自定义选项**，浏览到文件或文件夹或者键入文件或文件夹的路径，然后单击**确定**。

   c. 单击自定义资产，然后单击**添加**。

   要从可用删除选项中删除资产，请单击该资产，然后单击**删除**。

3. **所选项目将被碎化，同时将显示一条确认消息。未选择的项目将被碎化，但不显示确认消息。**— 选中此复选框可在碎化项目之前显示确认消息，或者清除此复选框，则在碎化项目之前不显示确认消息。

注： 即使清除资产的复选框，该资产也将被碎化。

要从删除列表中删除资产，请单击该资产，然后单击**删除**。

4. 要保护资产以防止自动删除，请执行以下操作：

   a. 在**不要删除以下内容**下面，单击**添加**，然后浏览到文件或文件夹，或者键入文件或文件夹的路径。

   b. 单击**打开**，然后单击**确定**。

要从排除列表中删除资产，请单击该资产，然后单击**删除**。

5. 单击**应用**。

常规任务

可以使用 File Sanitizer 来执行以下任务：

- 使用按键序列启动碎化 — 此功能可让您创建按键序列（例如，ctrl+alt+s）以启动碎化。有关详细信息，请参阅第 71 页的使用按键序列启动碎化。
- 使用 File Sanitizer 图标启动碎化 — 此功能类似于 Windows 中的拖放功能。有关详细信息，请参阅第 71 页的使用 File Sanitizer 图标。
- 手动碎化特定资产或所以选定资产 — 这些功能允许您手动碎化项目，无需等到调用定期碎化计划。有关详细信息，请参阅第 72 页的手动碎化单个资产或第 72 页的手动碎化所有选定的项目。
- 手动激活可用空间清理 — 此功能允许您手动激活可用空间清理。有关详细信息，请参阅第 72 页的手动激活可用空间清理。
- 终止碎化或可用空间清理操作 — 此功能允许您停止碎化或可用空间清理操作。有关详细信息，请参阅第 73 页的中止碎化或可用空间清理操作。
- 查看日志文件 — 此功能允许您查看碎化和可用空间清理日志文件，其中包含上次碎化或可用空间清理操作的所有错误或失败。有关详细信息，请参阅第 73 页的查看日志文件。

注： 碎化或可用空间清理操作可能需要相当长的时间。即使碎化和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。

使用按键序列启动碎化

1. 打开 File Sanitizer，然后单击**碎化**。
2. 选中**按键序列**复选框。
3. 在可用的框中输入一个字符。
4. 选择 **CTRL** 框或 **ALT** 框，然后选择 **SHIFT** 框。

   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. 在按住 shift 键和 ctrl 或 alt 键（或指定的任何组合键）的同时，按所选的字符。
2. 如果打开确认对话框，请单击**是**。

使用 File Sanitizer 图标

注意： 无法恢复碎化的资产。在选择手动碎化的项目时，一定要谨慎。

1. 浏览到要碎化的文档或文件夹。
2. 将资产拖到桌面的 **File Sanitizer** 图标上。
3. 在打开确认对话框时，单击**是**。

手动碎化单个资产

注意： 无法恢复碎化的资产。在选择手动碎化的项目时，一定要谨慎。

1. 在任务栏最右侧的通知区域中右击 **HP ProtectTools** 图标，单击 **File Sanitizer**，然后单击**碎化一个**。
2. 在打开“浏览”对话框时，浏览到要碎化的资产，然后单击**确定**。

注： 选定资产可以是单个文件或文件夹。

3. 在打开确认对话框时，单击**是**。

– 或 –

1. 右击桌面上的**文件清理工具**图标，然后单击**碎化一个**。
2. 在打开“浏览”对话框时，浏览到要碎化的资产，然后单击**确定**。
3. 在打开确认对话框时，单击**是**。

– 或 –

1. 打开 File Sanitizer，然后单击**碎化**。
2. 单击**浏览**按钮。
3. 在打开“浏览”对话框时，浏览到要碎化的资产，然后单击**确定**。
4. 在打开确认对话框时，单击**是**。

手动碎化所有选定的项目

1. 在任务栏最右侧的通知区域中右击 **HP ProtectTools** 图标，单击 **File Sanitizer**，然后单击**立即碎化**。
2. 在打开确认对话框时，单击**是**。

– 或 –

1. 右击桌面上的**文件清理工具**图标，然后单击**立即碎化**。
2. 在打开确认对话框时，单击**是**。

– 或 –

1. 打开 File Sanitizer，然后单击**碎化**。
2. 单击**立即碎化**按钮。
3. 在打开确认对话框时，单击**是**。

手动激活可用空间清理

1. 在任务栏最右侧的通知区域中右击 **HP ProtectTools** 图标，单击 **File Sanitizer**，然后单击**立即清理**。
2. 在打开确认对话框时，单击**是**。

– 或 –

1. 打开 File Sanitizer，然后单击**可用空间清理**。
2. 单击**立即清理**。
3. 在打开确认对话框时，单击**是**。

中止碎化或可用空间清理操作

在进行碎化或可用空间清理操作时，将在任务栏最右侧的通知区域中的 HP ProtectTools Security Manager 图标上方显示一条消息。该消息提供碎化或可用空间清理进度（完成的百分比）的详细信息，并提供中止该操作的选项。

▲ 要取消该操作，请单击此消息，然后单击**停止**。

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。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。

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。这两个日志文件位于硬盘驱动器上：

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

对于 64 位系统，这些日志文件位于硬盘驱动器中的以下位置：

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[用户名]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[用户名]*_DiskBleachLog.txt

8 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 84 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. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
3. 在左窗格中单击 **Device Access Manager**。

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下列类别设备的访问：

- 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
- 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 **OK（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：

1. 在 Windows 7 中，单击**开始**、单击**控制面板**，然后单击**系统和安全性**。

   - 或 -

   在 Windows Vista® 中，单击**开始**、单击**控制面板**，然后单击**系统和维护**。

   - 或 -

   在 Windows XP 中，单击**开始**、单击**控制面板**，然后单击**性能和维护**。

2. 单击**管理工具**，然后单击**服务**。
3. 选择 **HP ProtectTools Device Locking/Auditing** 服务。
4. 要启动服务，单击**开始**。

   - 或 -

   如果服务正在运行，但要停止此服务，单击**停止**。

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：

- **Device List（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**——显示所有允许或拒绝访问所选设备类别或特定设备的用户和组。
  - 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 **Device Class Configuration（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。

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。如果单击此气球，则会打开“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，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，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 83 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： 不管系统驱动器（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**。

管理这个组的成员的其它方法包括：

- 对于 Windows 7 Professional 或 Windows Vista，可以使用标准的“本地用户和组”Microsoft 管理控制台（MMC）管理单元来将这些用户添加到这个组。
- 对于 Windows 7、Windows Vista 或 Windows XP 的家庭版，从有管理员权限的帐户，在命令提示窗口中键入以下内容：

  net localgroup “Device Administrators” username /add

  在这个命令中，“username” 是您希望将其添加到这个组的用户姓名。

eSATA 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

9 失窃找回

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. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 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**立即激活**。
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**。

10 Embedded Security for HP ProtectTools（HP ProtectTools 嵌入式安全保护功能，仅限某些机型）

注： 计算机必须安装了集成的可信平台模块 (TPM) 嵌入式安全保护芯片，才能使用 Embedded Security for HP ProtectTools 模块。

Embedded Security for HP ProtectTools 可以防止他人未经授权擅自访问用户数据或凭证。此软件模块提供以下安全功能：

- 增强的 Microsoft® 加密文件系统 (EFS) 文件和文件夹加密功能
- 创建个人安全驱动器 (PSD) 以保护用户数据的功能
- 数据管理功能，例如备份和恢复密钥层次结构
- 在使用 Embedded Security 软件时，支持第三方应用程序（如 Microsoft Outlook 和 Internet Explorer）采用数字证书保护措施

TPM 嵌入式安全保护芯片增强并启用其它 HP ProtectTools Security Manager 安全保护功能。例如，Credential Manager for HP ProtectTools 可以在用户登录到 Windows 时使用嵌入式芯片作为验证要素。

设置步骤

⚠ **注意：** 为减少安全风险，强烈建议您让 IT 管理员立即初始化嵌入式安全保护芯片。如果不初始化嵌入式安全保护芯片，就可能会导致非授权用户、计算机蠕虫或病毒取得计算机的所有权并控制所有者任务，如处理紧急恢复存档和配置用户访问权限设置。

按照以下各节中的步骤启用并初始化嵌入式安全保护芯片。

在 Computer Setup 中启用嵌入式安全保护芯片

嵌入式安全保护芯片必须在快速初始化向导中或在 Computer Setup 实用程序中启用。

要在 Computer Setup 中启用嵌入式安全保护芯片，请执行以下操作：

1. 打开或重新启动笔记本计算机，当屏幕的左下角显示“f10 = ROM Based Setup”（f10 = 基于 ROM 的设置）消息时，按 f10 键以打开计算机设置实用程序。
2. 如果尚未设置管理员密码，请使用箭头键依次选择**安全保护**、**设置密码**，然后按 enter 键。
3. 在 **New password**（**新密码**）和 **Verify new password**（**验证新密码**）框中键入您的密码，然后按 f10 键。
4. 在 **Security**（**安全保护**）菜单中，使用箭头键选择 **TPM Embedded Security**（**TPM 嵌入式安全保护**），然后按 enter 键。
5. 如果设备被隐藏，请在 **Embedded Security**（**嵌入式安全保护功能**）下选择 **Available**（**可用**）。
6. 选择 **Embedded security device state**（**嵌入式安全保护设备状态**），然后将设置更改为 **Enable**（**启用**）。
7. 按 f10 键接受对嵌入式安全保护功能配置的更改。
8. 要保存首选项并退出 Computer Setup，请使用箭头键依次选择 **File**（**文件**）和 **Save Changes and Exit**（**保存更改并退出**），然后按照屏幕上的说明进行操作。

初始化嵌入式安全保护芯片

在 Embedded Security 模块的初始化过程中，您将执行以下任务：

- 为嵌入式安全保护芯片设置一个所有者密码，以防止他人未经授权擅自访问嵌入式安全保护芯片的所有所有者功能。
- 建立急救档案。该档案是一个受保护的存储区域，允许为所有用户的基本用户密钥重新进行加密。

要初始化嵌入式安全保护芯片，请执行以下操作：

1. 在任务栏最右侧的通知区域中右击 **HP ProtectTools Security Manager** 图标，然后选择 **Embedded Security Initialization（Embedded Security 初始化）**。

   随即打开 HP ProtectTools Embedded Security 初始化向导。

2. 按照屏幕上的指示进行操作。

设置基本用户帐户

在 Embedded Security 模块中设置基本用户帐户时，需要执行以下任务：

- 生成一个保护加密信息的基本用户密钥，并设置一个保护该基本用户密钥的基本用户密钥密码。
- 建立一个个人安全驱动器 (PSD)，用于存储加密文件和文件夹。

⚠ **注意：** 保护基本用户密钥密码。没有此密码将无法访问或恢复加密信息。

要建立基本用户帐户并启用用户安全保护功能，请执行以下操作：

1. 如果 Embedded Security 用户初始化向导未打开，请依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **User Settings（用户设置）**。
3. 在右窗格中的 **Embedded Security Features（嵌入式安全保护功能）**下，单击 **Configure（配置）**。

   随即打开 Embedded Security 用户初始化向导。
4. 按照屏幕上的指示进行操作。

注： 要安全地使用电子邮件，必须首先将电子邮件客户端配置为使用由嵌入式安全保护功能创建的数字证书。如果没有可用的数字证书，则必须从认证机构获取一个数字证书。有关配置电子邮件和获取数字证书的说明，请参阅电子邮件客户端软件帮助。

常规任务

在建立基本用户帐户后，您可以执行以下任务：

- 对文件和文件夹进行加密
- 发送和接收加密的电子邮件

使用个人安全驱动器

在建立 PSD 后，下次登录时系统将提示您输入基本用户密钥密码。如果正确输入了基本用户密钥密码，就可以直接通过 Windows 资源管理器访问 PSD。

对文件和文件夹进行加密

处理加密文件时，请注意以下规则：

- 只能加密 NTFS 分区上的文件和文件夹。不能加密 FAT 分区上的文件和文件夹。
- 不能加密系统文件和压缩的文件，也不能压缩加密的文件。
- 应当加密临时文件夹，因为黑客们可能会对这些内容感兴趣。
- 第一次加密文件或文件夹时，将自动建立恢复策略。在您丢失加密证书和私钥的情况下，此策略可确保您能够使用恢复代理来解密信息。

要对文件和文件夹进行加密，请执行以下操作：

1. 右击要加密的文件或文件夹。
2. 单击 **Encrypt（加密）**。
3. 单击以下选项之一：
   - **Apply changes to this folder only（更改仅应用于此文件夹）。**
   - **Apply changes to this folder, subfolders, and files（更改应用于此文件夹、其子文件夹及文件）。**
4. 单击 **OK（确定）**。

发送和接收加密的电子邮件

使用嵌入式安全保护功能，可以发送和接收加密的电子邮件，但对于不同的电子邮件客户端程序，相应的步骤可能会有所不同。有关详细信息，请参阅嵌入式安全保护功能软件帮助和电子邮件客户端程序的软件帮助。

更改基本用户密钥密码

要更改基本用户密钥密码，请执行以下操作：

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **User Settings（用户设置）**。
3. 在右窗格中的 **Basic User password（基本用户密码）**下面，单击 **Change（更改）**。
4. 键入原密码，然后设置并确认新密码。
5. 单击 **OK（确定）**。

高级任务

管理员可以在 Embedded Security 中执行以下任务：

- 备份和恢复 Embedded Security 凭证、Embedded Security 设置和个人安全驱动器
- 更改所有者密码
- 重置用户密码
- 安全地将用户安全凭证从源平台迁移到目标平台

备份和恢复

Embedded Security 模块的备份功能可以创建一个档案，其中包含出现紧急情况时要恢复的认证信息。

创建备份文件

要创建备份文件，请执行以下操作：

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Backup（备份）**。
3. 在右窗格中，单击 **Configure（配置）**。Embedded Security for HP ProtectTools 备份向导便会打开。
4. 按照屏幕上的指示进行操作。

通过备份文件恢复认证数据

要通过备份文件恢复数据，请执行以下操作：

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Backup（备份）**。
3. 在右窗格中，单击**全部恢复**。 Embedded Security for HP ProtectTools 备份向导便会打开。
4. 按照屏幕上的指示进行操作。

更改所有者密码

管理员可以更改所有者密码：

1. 依次单击**开始**、**所有程序**、**HP** 和 **HP ProtectTools 管理控制台**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Advanced（高级）**。
3. 在右窗格中的 **Owner Password（所有者密码）**下，单击 **Change（更改）**。
4. 键入原来的所有者密码，然后设置并确认新的所有者密码。
5. 单击 **OK（确定）**。

重置用户密码

管理员可以帮助用户重置忘记的密码。有关详细信息，请参阅软件帮助。

使用迁移向导迁移密钥

迁移是一种高级的管理员任务，允许管理、恢复和传输密钥及证书。

有关迁移的详细信息，请参阅嵌入式安全保护功能软件帮助。

11 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。

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，在用户输入密码时，Microsoft® Windows 不显示 IME。

例如，对于某些日语 Windows XP 安装，默认 IME 称为 Microsoft IME Standard 2002 for Japanese，它实际上转换为键盘布局 E0010411。 不过，这是一个 IME 而不是键盘布局。（Microsoft 保留了该键盘布局编码方案以用于 IME，这拓展了键盘布局的概念。）由于这不是可在 BIOS Preboot Security 或 HP Drive Encryption 密码提示的键入环境中表示的键盘布局，因此，HP ProtectTools 拒绝使用该 IME 键入的任何密码。 Microsoft IME Standard 2002 for Japanese 也不同于 Microsoft Windows Vista® 中的“通用名称”。 Windows 将某些 IME 映射到一种键盘布局。 在这些情况下，HP ProtectTools 支持该 IME，因为将使用基本键盘布局定义（十六进制代码）。

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
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

语言	Windows	BIOS	Drive Encryption
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	仅限 Windows XP，完全支持标准日语键盘布局 411。通常不支持在 Windows XP 中表示为 Microsoft Standard IME 2002 的 IME。 不过，经验测试表明，在键入简单字符时，该 IME 与键盘布局 411 几乎完全相同。 因此，在使用本地化的日语密码保护 BIOS 和 HP Drive Encryption 时，本软件将该 IME 转换为键盘布局 411。 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

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. 依次单击**开始**、**控制面板**和**区域和语言选项**。
  2. 单击**语言**标签。
  3. 单击**详细信息**按钮。
  4. 在**设置**标签上，单击**添加**按钮以添加支持的键盘（在“中文输入语言”下面添加美式键盘）。
  5. 为默认输入设置支持的键盘。
  6. 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。 第 99 页的特殊按键处理列出了不支持的字符。
  2. 再次运行 Security Manager 设置向导，然后输入新的 Windows 密码。

术语表

ATM
Automatic Technology Manager，允许网络管理员在 BIOS 级别远程管理系统。

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
驱动器加密密钥的备份副本。

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。单击 ID 卡可打开 HP ProtectTools 管理控制台。

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。

Privacy Manager 证书
这是一个数字证书，每次使用它进行加密操作（例如，对电子邮件和 Microsoft Office 文档进行签名和加密）时，它都要求进行验证。

PSD
个人安全驱动器，为机密信息提供受保护的存储区域。

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。

USB 身份标记

一种安全保护设备，用于存储有关用户的标识信息。与智能卡或生物识别读卡器一样，它用于验证是否是所有者登录计算机。

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。

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。

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
注册用户用于验证的照片。

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 内由用于登录网站或其它程序的用户名和密码（以及可能选择的其它信息）组成的对象。

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。

发送安全保护按钮
此软件按钮显示在 Microsoft Outlook 电子邮件工具栏上。单击此按钮可对 Microsoft Outlook 电子邮件进行签名和/或加密。

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。

简单删除
Windows 删除对资产的引用。资产内容仍保留在硬盘驱动器上，直至可用空间清理写入遮盖数据以覆盖它。

建议的签名者
Microsoft Word 或 Microsoft Excel 文档所有者指定在文档中添加签名行的用户。

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。

可信发件人
发送签名和/或加密的电子邮件和 Microsoft Office 文档的 Trusted Contacts（可信联系人）。

可信联系人
已接受 Trusted Contacts（可信联系人）邀请的人员。

可信联系人列表
Trusted Contacts（可信联系人）的列表。

可信联系人收件人
收到邀请而成为 Trusted Contacts（可信联系人）的人员。

可信联系人邀请
向某人发送的电子邮件，请求他成为 Trusted Contacts（可信联系人）。

可信消息
在此通信会话期间，可信发件人将向 Trusted Contacts（可信联系人）发送可信消息。

可用空间清理
安全地写入随机数据以覆盖删除的资产，从而改变已删除资产的内容。

控制台
一个中心位置，可在其中访问和管理 HP ProtectTools 管理控制台中的功能和设置。

面板
一个中心位置，可在其中访问和管理 HP ProtectTools Security Manager 中的功能和设置。

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。

迁移
此任务用于管理、恢复和传输 Privacy Manager 证书和 Trusted Contacts（可信联系人）。

签名并加密按钮
此软件按钮显示在 Microsoft Office 应用程序工具栏上。可以单击此按钮，在 Microsoft Office 文档中进行签名、加密或删除加密。

签名行
这是一个占位符，表示数字签名的可视显示形式。对文档进行签名后，将显示签名者的名字和验证方法。还可能包含签名日期和签名者职务。

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。

身份标记
请参阅*安全保护登录方法*。

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。

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。

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。

数字签名
与文件一同发送的数据，用于证实发件人身份以及文件在签署后没有任何更改。

数字证书
通过使用一对电子密钥签署数字信息，并将密钥与数字证书所有者相关联来确认个人或公司标识的电子凭证。

碎化
执行一个算法以掩盖资产中包含的数据。

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。

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。

为可信联系人密封
此任务添加数字签名，加密电子邮件，并在使用所选安全登录方法验证后发送电子邮件。

虚拟身份标记
一种安全保护功能，其工作原理非常类似于智能卡和读卡器。身份标记保存在计算机硬盘驱动器上或 Windows 注册表中。当您用虚拟身份标记登录时，系统会要求您提供用户 PIN 以完成验证。

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。

自动碎化
用户在 File Sanitizer 中设置的预定碎化。

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

Z