HP Client Security

使用入门

第一版：2013 年 8 月

文档部件号：735339-AA1

目录

1 HP Client Security Manager 简介

HP Client Security 可用于保护数据、设备和身份，从而提高计算机的安全性。

可用于您的计算机的软件模块可能因您的型号而异。

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

注： 撰写本指南中的说明时，假定您已安装适用的 HP Client Security 软件模块。

HP Client Security 功能

下表详细说明了 HP Client Security 模块的主要功能。

模块	关键功能
HP Client Security Manager	管理员可以执行以下功能： • 在 Windows® 启动之前保护计算机 • 使用强验证来保护您的 Windows 帐户 • 管理网站和应用程序的登录名和密码 • 轻松更改 Windows 操作系统密码 • 使用指纹提供额外的安全性和简便性 • 设置用于验证的智能卡、非接触卡或接近卡 • 使用 Bluetooth 电话作为标识方法 • 设置 PIN 扩大验证选择 • 配置登录或会话策略 • 备份和恢复程序数据 • 添加更多应用程序，如 HP Drive Encryption、HP File Sanitizer、HP Trust Circles、HP Device Access Manager 和 HP Computrace 普通用户可执行以下功能： • 查看加密状态和 Device Access Manager 的设置。 • 激活 Computrace。 • 配置首选项以及备份和恢复选项。

模块	关键功能
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电子邮件和 Web 帐户的安全性。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。 • 将帐户标记为泄露，以提示您注意含有类似凭证的其它帐户。 • 从支持的浏览器中导入登录数据。
HP 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。 • 提供用于激活自加密驱动器的选项（仅限某些机型）。
HP Device Access Manager	• 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。
HP Trust Circles	• 保护文件和文档安全。 • 将文件置于用户特定的文件夹中，在信任圈中保护它们。 • 仅允许信任圈中的成员使用并分享文件。
失窃找回（Computrace，需单独购买）	• 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 Client Security 产品描述和常用示例

大多数 HP Client Security 产品都具有两种获取访问权限的方式，一种是用户身份验证（通常为密码），另一种是管理备份（在缺少密码、密码不可用或忘记密码时或者从公司安全性出发需要访问权限的任何时候使用）。

注： 某些 HP Client Security 产品的设计旨在限制对数据的访问。当数据非常重要以至于用户宁愿丢失该信息也不希望其受到危害时，应当加密数据。建议将所有数据备份在一个安全的位置。

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。

- 将帐户标记为泄露，以提示您注意含有类似凭证的其它帐户。
- 从支持的浏览器中导入登录数据。

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： 工作勤奋的员工得到了升职，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。该员工决定将所有 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。

HP 驱动器加密（仅限某些机型）

“HP 驱动器加密”用于限制对整个计算机硬盘驱动器和次驱动器上数据的访问。“驱动器加密”还可管理自加密驱动器。

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。

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。

HP Device Access Manager（仅限某些机型）

HP Device Access Manager 允许管理员限制和管理对硬件的访问。Device Access Manager 可用于阻止对可将数据复制到的 USB 闪存驱动器的未经授权的访问。它还可以限制对 CD/DVD 驱动器的访问，对 USB 设备、网络访问等的控制。举例来说，外部供应商需要访问公司计算机，但不应当能够将数据复制到 USB 驱动器上，这将是一种情况。

示例 1： 医疗用品公司的经理经常将个人医疗记录与其公司信息一起使用。员工需要访问此数据，但是不能通过 USB 驱动器或者任何其他外部存储介质将该数据从计算机上删除，这一点极为重要。网络是安全的，但是计算机具有可允许复制或窃取数据的 CD 刻录机和 USB 端口。该经理使用 Device Access Manager 禁用 USB 端口和 CD 刻录机，这样就可以限制员工对它们的使用了。即使阻止了 USB 端口，鼠标和键盘仍将继续发挥作用。

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（需单独购买）

Computrace（需单独购买）是一种服务，可用于追踪失窃笔记本计算机的位置（只要该用户访问 Internet）。Computrace 还可以帮助远程管理和查找笔记本计算机，以及监视其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 Client Security 模块可以协同工作，提供多种安全问题（包括以下重要安全目标）的解决方案：

- 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）。
  - HP Client Security — 请参阅第 11 页的 HP Client Security。
  - HP 驱动器加密 — 请参阅第 25 页的 HP 驱动器加密（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 — 请参阅第 44 页的失窃找回（仅限某些机型）。

限制对机密数据的访问

假设合同审核员正在现场办公且已被授予计算机访问权限以查看敏感财务数据。您不希望该审核员能够打印这些文件或者将其保存到可写设备，如 CD。下列功能可帮助限制对数据的访问：

- HP Device Access Manager 可让 IT 经理限制对通信设备的访问，以便无法从硬盘驱动器复制敏感信息。请参阅第 36 页的系统视图。

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）。（请参阅第 25 页的 HP 驱动器加密（仅限某些机型）。
- HP Client Security 有助于确保未经授权的用户无法取得密码或受密码保护的应用程序的访问权。请参阅第 11 页的 HP Client Security。
- HP Device Access Manager 可让 IT 经理限制对可写设备的访问，以便无法从硬盘驱动器复制敏感信息。请参阅第 35 页的 HP 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 16 页的 Password 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 Client Security，安全责任和权限可分配到以下几个角色中：

- 安全人员—定义公司或网络的安全级别，并确定要部署的安全功能，如驱动器加密。

  注： 安全人员可通过与 HP 协商来自定义 HP Client Security 中的很多功能。有关详细信息，请参阅 http://www.hp.com。

- IT 管理员 — 应用并管理由安全人员定义的安全功能。还可以启用或禁用某些功能。例如，如果安全人员已决定部署智能卡，则 IT 管理员可以启用密码和智能卡模式。
- 用户 — 使用安全功能。例如，如果安全人员和 IT 管理员已为系统启用智能卡，则用户可以设置智能卡 PIN 并将该卡用于身份验证。

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。

不应向非授权的用户授予管理权限。

管理 HP Client Security 密码

大多数 HP Client Security 功能由密码保护。下表列出了常用密码、设置密码的软件模块和密码功能。

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 Client Security 密码	在以下模块中设置	功能
Windows 登录密码	Windows 控制面板或 HP Client Security	可用于手动登录或验证对多种 HP Client Security 功能的访问。
HP Client Security Backup and Recovery 密码	HP Client Security，单个用户	保护对 HP Client Security 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。
- 在中间利用数字和特殊字符拆分单词或短语，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

您可以将 HP Client Security 中的 Backup and Recovery 工具作为一个中心位置，从中备份并储存来自已安装 HP Client Security 模块的安全凭证。

2 使用入门

要设置 HP Client Security 以便与凭证一起使用，请通过以下某种方法来启动 HP Client Security：一旦用户完成了向导，此用户就不能再次启动此向导。

1. 在“开始”或“应用”屏幕中单击或点击 **HP Client Security** 应用程序 (Windows 8)。

   - 或 -

   在 Windows 桌面上单击或点击 **HP Client Security** 应用程序 (Windows 7)。

   - 或 -

   在 Windows 桌面上双击或双点击任务栏最右侧的通知区域中的 **HP Client Security** 图标。

   - 或 -

   在 Windows 桌面上单击或点击通知区域中的 **HP Client Security** 图标，然后选择**打开 HP Client Security**。

2. HP Client Security 设置向导启动，并显示欢迎页面。

3. 阅读欢迎屏幕，键入您的 Windows 密码以验证您的身份，然后单击或点击**下一步**。

   如果尚未创建 Windows 密码，则会提示您创建一个密码。要使用 HP Client Security 功能以及防止未经授权的人员访问您的 Windows 帐户，必须设置 Windows 密码。

4. 在 HP SpareKey 页中，选择三个安全问题。输入每个问题的答案，然后单击**下一步**。也允许使用自定义问题。有关详细信息，请参阅第 12 页的 HP SpareKey —密码恢复。

5. 在指纹页面上，至少注册需要的最少指纹数，然后单击或点击**下一步**。有关详细信息，请参阅第 11 页的指纹。

6. 在 Drive Encryption 页面上，激活加密，备份加密密钥，然后单击或点击**下一步**。有关详细信息，请参阅 HP Drive Encryption 软件帮助。

   注： 这适用于用户为管理员且 HP Client Security 设置向导之前未被管理员配置过的情形。

7. 在向导的最后一页中，单击或点击**完成**。

   此页提供功能和凭证的状态。

8. HP Client Security 设置向导确保激活及时验证和 File Sanitizer 功能。有关详细信息，参阅 HP Device Access Manager 软件帮助和 HP File Sanitizer 软件帮助。

   注： 这适用于用户为管理员且 HP Client Security 设置向导之前未被管理员配置过的情形。

打开 HP Client Security

您可以使用以下某种方法打开 HP Client Security 应用程序：

注： 在可以启动 HP Client Security 应用程序之前，必须完成 HP Client Security 设置向导。

- 在“开始”或“应用”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 Client Security** 应用程序 (Windows 7)。

– 或 –

在 Windows 桌面上双击或双点击任务栏最右侧的通知区域中的 **HP Client Security** 图标。

– 或 –

在 Windows 桌面上单击或点击通知区域中的 **HP Client Security** 图标，然后选择**打开 HP Client Security**。

3 针对小型企业的简易设置指南

本章的设计旨在针对小型企业演示如何在 HP Client Security 中激活最常用选项的基本步骤。此软件中的许多工具和选项允许您微调首选项和设置访问控制。此简易设置指南的重点在于利用最少的设置工作量和时间确保每个模块的运行。有关其他信息，请选择相关模块，然后单击窗口右上角的 **?** 或“帮助”按钮。此按钮会自动显示可在当前显示的窗口中为您提供帮助的信息。

入门

1. 在 Windows 桌面上，通过双击位于任务栏最右侧的通知区域中的 **HP Client Security** 图标打开 HP Client Security。
2. 输入 Windows 密码，或创建 Windows 密码。
3. 完成 HP Client Security Setup。

要让 HP Client Security 仅在 Windows 登录过程中进行一次验证，请参阅第 22 页的安全保护功能。

Password Manager

每个人都具有相当多的密码 – 尤其是当您经常访问网站或者使用需要登录的应用程序时。正常用户或者将同一个密码用于所有应用程序，或者为不同应用程序创造出各不相同的密码，但那样不久就会忘记哪个密码用于哪个应用程序。

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。
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。

如需打开 Password Manager，请使用组合键“Ctrl+Windows 徽标键+h”打开 Password Manage，然后单击 **Log in** 以启动并验证保存的快捷方式。

“密码管理器”的**编辑**选项卡允许您查看和修改名称、登录名，甚至显示密码。

用于小型企业的 HP Client Security 允许将所有凭证和设置备份和/或复制到另一台计算机上。

HP Device Access Manager

Device Access Manager 可用于限制各种内部和外部存储设备的使用，这样即可保持硬盘驱动器上数据的安全性，不会将其泄漏到企业外部。例如，允许用户访问您的数据，但阻止其将数据复制到 CD、个人音乐播放器或 USB 内存设备上。

1. 打开 **Device Access Manager**（请参阅第 35 页的打开 Device Access Manager）。

   显示当前用户的访问状态。

2. 如需更改用户、组或设备的访问权，请单击或点击 **Change**。有关详细信息，请参阅第 36 页的系统视图。

HP 驱动器加密

“HP 驱动器加密”通过加密整个硬盘驱动器保护您的数据。如果您的 PC 失窃，和/或如果将您的硬盘驱动器从原始笔记本计算机拆除并安装在不同的笔记本计算机上，则该硬盘驱动器上的数据仍为受保护状态。

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。

为使其更加易于操作，多种软件模块会自动同步密码，包括 Windows 用户帐户、验证域、HP Drive Encryptio、Password Manager 和 HP Client Security。

若是初次使用 HP Client Security Setup 设置向导设置 HP Drive Encryption，请参阅第 7 页的使用入门。

4 HP Client Security

HP Client Security 主页面是一个中心位置，可以在其中方便地访问 HP Client Security 功能、应用程序和设置。主页面分为三个部分：

- **数据** — 可由此访问用于管理数据安全性的应用程序。
- **设备** — 可由此访问用于管理设备安全性的应用程序。
- **身份** — 注册和管理身份凭证。

将光标移动至应用程序磁贴上以显示应用程序的说明。

HP Client Security 可在页面底部提供用户和管理员设置的链接。HP Client Security 可让用户通过点击或单击**齿轮**（设置）图标访问高级设置和功能。

标识功能，应用程序和设置

HP Client Security 提供的标识功能，应用程序和设置可协助您管理数字标识的各方面事宜。在 HP Client Security 主页面上单击或点击以下一个磁贴，然后输入您的 Windows 密码：

- **指纹** — 注册和管理指纹凭证。
- **SpareKey** — 设置和管理 HP SpareKey 凭证，可在其他凭证丢失或错放时用于登录计算机。也可以用于重置遗忘的密码。
- **Windows 密码** — 方便访问以更改 Windows 密码。
- **Bluetooth 设备** — 允许您注册和管理 Bluetooth 设备。
- **卡** — 允许您注册和管理智能卡、非接触式卡和感应卡。
- **PIN** — 允许您注册和管理 PIN 凭证。
- **RSA SecurID**— 允许您注册和管理 RSA SecurID 凭证（如果相应设置到位）。
- **Password Manager** — 允许您管理在线帐户和应用程序的密码。

指纹

HP Client Security 设置向导可指导您完成设置或“注册”指纹的过程。

您也可以在指纹页面上注册或删除指纹，它可通过单击或点击 HP Client Security 主页面上的**指纹**图标访问。

1. 在指纹页面上，滑动指纹直至成功注册。

   页面上指示需要注册的指纹数。首选食指和中指。

2. 要删除以前注册的指纹，单击或点击**删除**。
3. 要注册其他指纹，单击或点击**注册其他指纹**。
4. 在离开此页之前，单击或点击**保存**。

⚠ **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，或关闭此程序，则您做的更改将**不**保存。

- 要访问指纹管理设置，单击或点击**管理设置**（需要管理权限），管理员可在其中指定注册、精确度和其他设置。
- 要访问指纹用户设置，单击或点击**用户设置**，用户可以在其中指定管理指纹识别外观和行为的设置。

指纹管理设置

管理员可以指定指纹识别器的注册、精确度和其他设置。需要管理员权限。

- 要访问指纹凭证的管理员设置，单击或点击指纹页面上的**管理设置**。

- **用户注册** — 择允许用户注册的最小和最大指纹数。
- **识别** — 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识别设置。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。

指纹用户设置

在指纹用户设置页面上，您可以指定管理指纹指标外观和行为的设置。

- 要访问指纹凭证的用户设置，单击或点击指纹页面上的**用户设置**。

- **启用声音反馈** — 默认情况下，滑动指纹后，HP Client Security 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，也可通过清除此复选框禁用声音反馈。
- **显示扫描质量反馈** — 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。

HP SpareKey —密码恢复

通过使用 SpareKey，您可以回答三个安全问题以访问计算机（在支持的平台上）。

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

要设置 HP SpareKey，请执行以下操作：

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

   可以从预定义列表中选择问题也可以写上自己的问题。

2. 单击或点击**注册**。

要删除 HP SpareKey，请执行以下操作：

- 单击或点击**删除 SpareKey**。

设置 SpareKey 后，可从开机验证登录屏幕或 Windows 欢迎屏幕中使用 SpareKey 访问计算机。

您可以在 SpareKey 页中选择不同问题或更改答案，此页可以从 HP Client Security 主页面的密码恢复磁贴上访问。

要访问 HP SpareKey 设置，单击**设置**（需要管理权限），管理员可在其中指定与 HP SpareKey 凭证相关的设置。

HP SpareKey Settings

在 HP SpareKey 设置页面上，可以指定与管理 HP SpareKey 凭证行为和使用相关的设置。

▲ 要启动 HP SpareKey 设置页面，单击或点击在 HP SpareKey 页面上的**设置**（需要管理权限）。

管理员可以选择以下设置：

- 指定在 HP SpareKey 设置过程中向每个用户显示的问题。
- 添加最多三个自定义安全问题以添加至向用户显示的列表中。
- 选择是否允许用户写自己的安全问题。
- 指定哪种验证环境（Windows 或开机验证）允许使用 HP SpareKey 进行密码恢复。

Windows 密码

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

要更改 Windows 密码：

1. 从 HP Client Security 主页面上，单击或点击 **Windows 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. 单击或点击**更改**，将当前密码立即更改为输入的新密码。

Bluetooth 设备

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，然后单击或点击**注册**。

要访问第 13 页的 Bluetooth 设备设置页面，单击**设置**（需要管理权限），管理员可在其中指定 Bluetooth 设备的设置。

Bluetooth 设备设置

管理员可以指定以下管理 Bluetooth 设备凭证的行为和使用的设置：

无声验证

- **在验证身份时自动使用连接的已注册 Bluetooth 设备** — 选择此复选框允许用户无需操作地使用 Bluetooth 凭证进行验证，或者清除复选框禁用此选项。

Bluetooth 近距感应

- **在已注册的 Bluetooth 设备移出计算机范围时锁定计算机**— 当登录时连接的蓝牙设备移出计算机范围时，选中复选框以锁定计算机，或清除复选框以禁用该选项。

注： 要利用此功能，您计算机上的 Bluetooth 模块必须支持此功能。

卡

HP Client Security 可支持各种标识卡，这是保护计算机芯片的小塑料卡。这包括智能卡、非接触式卡和感应卡。如果计算机连接了其中一种卡和相应的读卡器、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。

智能卡制造商应提供相应工具以安装安全证书和 PIN 管理，以供 HP Client Security 在安全算法中使用。用作 PIN 的字符数和字符类型可能会有所不同。管理员必须先初始化智能卡，然后才能使用。

HP Client Security 支持以下智能卡格式：

- CSP
- PKCS11

HP Client Security 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

HP Client Security 支持以下感应卡格式：

- HID 感应卡

要注册智能卡，请执行以下操作：

1. 将卡插入连接的智能卡读卡器中。
2. 卡被识别之后，输入卡的 PIN，然后单击或点击**注册**。

要更改智能卡 PIN，请执行以下操作：

1. 将卡插入连接的智能卡读卡器中。
2. 卡被识别之后，输入卡的 PIN，然后单击或点击**验证**。
3. 单击或点击**更改 PIN**，然后输入新的 PIN。

要注册非接触式卡或感应卡：

1. 将卡置于相应的读卡器上或非常靠近读卡器。
2. 卡被识别之后，单击或点击**注册**。

要删除已注册的卡，请执行以下操作：

1. 将卡插入读卡器中。
2. 仅对于智能卡，输入卡指定的 PIN，然后单击或点击**验证**。
3. 单击或点击**删除**。

卡一经注册，该卡的详细信息在**已注册卡**下方显示。卡被删除之后，则从列表上删除。

要访问感应卡、非接触式卡和智能卡设置，单击或点击**设置**（需要管理权限），管理员可以在其中指定与卡凭证相关的设置。

感应卡、非接触式卡和智能卡设置

要访问卡的设置，单击或点击列表中的卡，然后单击或点击显示的箭头。

要更改智能卡 PIN，请执行以下操作：

1. 将卡插入读卡器中
2. 输入卡指定的 PIN，然后单击或点击**继续**。
3. 输入并确认新的 PIN，然后单击或点击**继续**。

要初始化智能卡 PIN，请执行以下操作：

1. 将卡插入读卡器中
2. 输入卡指定的 PIN，然后单击或点击**继续**。
3. 输入并确认新的 PIN，然后单击或点击**继续**。
4. 单击或点击**是**确认初始化。

要清除卡数据，请执行以下操作：

1. 将卡插入读卡器中
2. 输入卡指定的 PIN（仅智能卡），然后单击或点击**继续**。
3. 单击或点击**是**确认删除。

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。

要设置新的 PIN，请执行以下操作：

▲ 输入 PIN，再次输入进行确认，然后单击或点击**应用**。

要删除 PIN，请执行以下操作：

▲ 单击或点击**删除**，然后单击或点击**是**进行确认。

要访问 PIN 设置，单击或点击**设置**（需要管理权限），管理员可以在其中指定与 PIN 凭证相关的设置。

PIN 设置

在 PIN 设置页面上，可以指定 PIN 凭证可接受的最小和最大长度。

RSA SecurID

如果管理员已经启用 RSA 作为验证凭证，且以下条件为真，您可以注册或删除 RSA SecurID 凭证。

注： 需要相应的设置。

- 用户必须已经在 RSA 服务器上创建。
- RSA SecurID 令牌已经指定给此用户，且计算机必须已经加入 RSA 服务器域。
- 计算机上安装有 SecurID 软件。
- 可连接正确配置的 RAS 服务器。

要注册 RSA SecurID 凭证，请执行以下操作：

▲ 输入 RSA SecurID 用户名和密码（RSA SecurID 令牌代码或 PIN+令牌代码，视环境而定），然后单击或点击**应用**。

注册成功时，“您的 RSA SecurID 凭证注册成功”消息显示，“删除”按钮启用。

要删除 RSA SecurID 凭证，请执行以下操作：

▲ 单击**删除**，然后在询问“确定要删除 RSA SecurID 凭证？”的弹出对话框中选择**是**。

Password Manager

在使用 Password Manager 时，可以更方便、更安全地登录到网站和应用程序。可创建强密码（不必写下或记住），然后使用指纹、智能卡、感应卡、非接触式卡、Bluetooth 电话、PIN、RSA 凭证或 Windows 密码方便快捷地进行登录。

注： 由于 Web 登录屏幕结构不断更改，Password Manager 可能无法始终支持所有网站。

Password Manager 提供了以下选项：

Password Manager 页面

- 单击或点击一个帐户以自动启动网页或应用程序并登录。
- 使用类别组织帐户。

密码强度

- 快速查看任何密码是否存在安全风险。
- 在添加登录数据时，查看网站和应用程序使用的各个秘密强度。
- 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。

▲ 单击或点击 **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 HP Client Security 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，则将您的登录数据填入登录字段，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 HP Client Security 帮助。

注： 此计算机的管理员可能已将 HP Client Security 凭证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。在浏览网站或程序之后，可使用这些登录。

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. 单击或点击 **Password Manager** 图标，然后单击或点击以下按钮之一，具体取决于登录屏幕是用于网站还是程序：
   - 对于网站，请单击或点击**将 [domain name] 添加到 Password Manager**。
   - 对于程序，请单击或点击**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。
   a. 要使用某个预先设置了格式的选项填充登录字段，请单击或点击该字段右侧的箭头。
   b. 要查看此登录的密码，请单击或点击**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. 单击或点击**确定**以选择要使用的验证方法（指纹、智能卡、感应卡、非接触式卡、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，请单击或点击**更多字段**。
      - 选中登录所需的每个字段对应的复选框，或清除登录不需要的所有字段对应的复选框。
      - 单击或点击**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，请执行以下操作：

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，请单击或点击 **Password Manager** 图标，然后单击或点击**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。

   您也可以通过单击或点击登录以显示编辑选项，然后选择**编辑**，从 Password Manager 页面内编辑帐户信息。
3. 编辑登录信息。
   - 要编辑**帐户名称**，在字段中输入新的名称。
   - 要添加或编辑**类别**名称，在**类别**字段中输入或修改名称。
   - 要选择具有预设格式选项的**用户名**登录字段，请单击或点击字段右侧的向下箭头。

     仅在从 Password Manager 图标上下文菜单的编辑命令中编辑登录时才能使用预设格式选项。
   - 要选择具有预设格式选项的**密码**登录字段，请单击或点击字段右侧的向下箭头。

     仅在从 Password Manager 图标上下文菜单的编辑命令中编辑登录时才能使用预设格式选项。
   - 要将屏幕上的其它字段添加到登录中，请单击或点击**更多字段**。
   - 要查看此登录的密码，请单击或点击**显示密码**图标。
   - 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。
   - 要将此登录标记为拥有泄露的密码，选择**此密码泄露**复选框。

     在保存更改之后，所有其他共享同样密码的登录都将标记为泄露。如果需要，您可以访问每个受影响的帐户，更改密码。
4. 单击或点击**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 HP Client Security 的 Password Manager 页面中双击或双点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：

▲ 按 **Password Manager** 热键组合（Ctrl+Windows 徽标键+h 是出厂设置）。要更改热键组合，在 HP Client Security 主页面中，单击 **Password Manager**，然后单击或点击**设置**。

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。

要将登录分配到类别中，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击 **Password Manager**。
2. 单击或点击帐户条目，然后单击或点击**编辑**。
3. 在**类别**字段，输入类别名称。
4. 单击或点击**保存**。

要从类别中移除帐户，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击 **Password Manager**。
2. 单击或点击帐户条目，然后单击或点击**编辑**。
3. 在**类别**字段，清除类别名称。
4. 单击或点击**保存**。

要重命名类别，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击 **Password Manager**。
2. 单击或点击帐户条目，然后单击或点击**编辑**。
3. 在**类别**字段，更改类别名称。
4. 单击或点击**保存**。

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。

Password Manager 页面中列出了您的登录。

要管理登录，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击 **Password Manager**。
2. 单击或点击现有登录，选择以下选项之一，然后按照屏幕上的说明进行操作：
   - **编辑** — 编辑登录。有关详细信息，请参阅第 18 页的编辑登录。
   - **登录** — 登录至选定帐户。
   - **删除** — 删除选定帐户的登录。

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. 单击或点击 **Password Manager** 图标以显示其上下文菜单。
3. 单击或点击**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。

在创建某个帐户的 Password Manager 登录过程中输入密码时，密码下方显示彩色条，指示密码的强度。颜色指示以下值：

- **红色** — 弱
- **黄色** — 一般
- **绿色** — 强

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. 单击或点击图标，然后单击或点击**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** — 单击或点击此选项，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。
   - **不提示为登录屏幕添加登录** — 选中该单选按钮。
2. 要为以前排除的屏幕添加登录，请执行以下操作：
   a. 登录至之前排除的网站。
   b. 要让 Password Manager 记住此网站的密码，单击或点击弹出对话框上的**记住**，保存密码并为屏幕创建登录。
3. 要访问其他 Password Manager 设置，单击或点击 Password Manager 图标，单击或点击**打开 Password Manager**，然后单击或点击 Password Manager 页面上的**设置**。

导入和导出登录

在 HP Password Manager 导入和导出页面上，可以将计算机上 Web 浏览器保存的登录导入。也可以从 HP Client Security 备份文件中导入数据并将数据导出到 HP Client Security 备份文件。

▲ 要启动导入和导出页面，单击或点击 Password Manager 页面上的**导入和导出**。

要从浏览器导入密码，请执行以下操作：

1. 单击或点击要从中导入密码的浏览器（仅显示安装的浏览器）。
2. 清除不希望导入密码的任何帐户的复选框。
3. 单击或点击**导入**。

可通过导入和导出页面上的相关链接（在**其他选项下方**）从 HP Client Security 备份文件导入数据或向其导出数据。

注: 此功能仅导入和导出 Password Manager 数据。有关备份和还原其它 HP Client Security 数据的信息，请参阅第 24 页的备份和还原数据。

要从 HP Client Security 备份文件导入数据，请执行以下操作：

1. 从 HP Password Manager 导入和导出页面，单击或点击**从 HP Client Security 备份文件导入数据**。
2. 验证您的身份。
3. 选择之前创建的备份文件或者在提供的字段中输入路径，然后单击或点击**浏览**。

4. 输入用来保护文件的密码，然后单击或点击**下一步**。
5. 单击或点击**还原**。

要导出数据至 HP Client Security 备份文件，请执行以下操作：

1. 从 HP Password Manager 导入和导出页面，单击或点击**从 HP Client Security 备份文件导出数据**。
2. 验证身份，然后单击或点击**下一步**。
3. 输入备份文件的名称。默认情况下，该文件将保存到“我的文档”文件夹中。要指定其他位置，单击或点击**浏览**。
4. 输入并确认用来保护文件的密码，然后单击或点击**保存**。

设置

可指定用于对 Password Manager 进行个性化的设置：

- **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。

- **使用 Ctrl+Win+h 打开 Password Manager** — 打开 **Password Manager Quick Links** 菜单的默认热键是 Ctrl+Windows 徽标键+h。

  要更改该热键，请单击或点击此选项并输入新的键组合。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。

  不能使用为 Windows 或 Windows 应用程序保留的组合。

- 要将设置恢复为出厂默认值，请单击或点击**还原默认值**。

高级设置

管理员可以通过选择 HP Client Security 主屏幕上的**齿轮**（设置）图标访问以下选项。

- **管理员策略** — 允许您配置管理员的登录和会话策略。
- **标准用户策略** — 允许您配置标准用户的登录和会话策略。
- **安全保护功能** — 允许您通过使用强验证和/或启用 Windows 启动之前验证，提高计算机的安全性。
- **用户** — 允许您管理用户及其凭证。
- **我的策略** — 允许您查看您的验证策略和注册状态。
- **备份和还原** — 用于备份或还原 HP Client Security 数据。
- **关于 HP Client Security**— 显示有关 HP Client Security 的版本信息。

管理员策略

可以为此计算机的管理员配置登录和会话策略。此处设置的登录策略管理本地管理员登录 Windows 所需的凭证。此处设置的会话策略管理本地管理员在 Windows 会话中验证身份所需的凭证。

默认情况下，在点击或单击**应用**之后，所有新的或更改的策略立即强制实施。

要添加新的策略，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**管理员策略**。
3. 单击或点击**添加新策略**。
4. 单击向下箭头为新的策略选择主要和（可选）备用凭证，然后单击或点击**添加**。
5. 单击**应用**。

要延迟实施新的或更改的策略，请执行以下操作：

1. 单击或点击**立即实施此策略**。
2. 选择**在特定日期实施此策略**。
3. 输入或使用弹出日历选择实施此策略的日期。
4. 如果需要，选择何时提醒用户新策略。
5. 单击**应用**。

标准用户策略

可以为此计算机的标准用户配置登录和会话策略。此处设置的登录策略管理标准用户登录 Windows 所需的凭证。此处设置的会话策略管理标准用户在 Windows 会话中验证身份所需的凭证。

默认情况下，在点击或单击**应用**之后，所有新的或更改的策略立即强制实施。

要添加新的策略，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**标准用户策略**。
3. 单击或点击**添加新策略**。
4. 单击向下箭头为新的策略选择主要和（可选）备用凭证，然后单击或点击**添加**。
5. 单击**应用**。

要延迟实施新的或更改的策略，请执行以下操作：

1. 单击或点击**立即实施此策略**。
2. 选择**在特定日期实施此策略**。
3. 输入或使用弹出日历选择实施此策略的日期。
4. 如果需要，选择何时提醒用户新策略。
5. 单击**应用**。

安全保护功能

可以启用 HP Client Security 安全保护功能以帮助防止他人未经授权擅自访问计算机。

要设置安全保护功能，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**安全保护功能**。

3. 选中相应的复选框以启用安全保护功能，然后单击或点击**应用**。选择的功能越多，您的计算机就越安全。

   这些设置适用于所有用户。

   - **Windows 登录安全性** — 要求使用 HP Client Security 凭证进行访问，从而保护您的 Windows 帐户。
   - **预引导安全保护（开机验证）** — 在 Windows 启动之前保护您的计算机。如果 BIOS 不支持预引导安全保护，则无法使用该功能。
   - **允许 One Step logon** — 如果之前在开机验证或 Drive Encryption 级别执行了验证，则允许跳过 Windows 登录。

4. 单击或点击**用户**，然后单击或点击用户的磁贴。

用户

可以监控和管理此计算机的 HP Client Security 用户。

要为 HP Client Security 添加另一个 Windows 用户，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**用户**。
3. 单击或点击**为 HP Client Security 添加另一个 Windows 用户**。
4. 选择希望添加的用户的名称，然后单击或点击**确定**。
5. 输入用户的 Windows 密码。

   用户页面上显示添加的用户的磁贴。

要从 HP Client Security 删除 Windows 用户，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**用户**。
3. 单击或点击希望删除的用户的名称。
4. 单击或点击**删除用户**，然后单击或点击**是**进行确认。

要显示用户的登录概要以及为其实施的会话策略，请执行以下操作：

▲ 单击或点击**用户**，然后单击或点击用户的磁贴。

我的策略

可以显示您的验证策略和注册状态。我的策略页面也提供管理员策略和标准用户策略页面的链接。

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**我的策略**。

   显示当前登录用户的登录和为其实施的会话策略。

我的策略页面也提供第 21 页的管理员策略和第 22 页的标准用户策略的链接。

备份和还原数据

建议您定期备份 HP Client Security 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。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 Client Security，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. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**管理员策略**。
3. 单击或点击**备份和还原**。
4. 单击或点击**备份**，然后验证身份。
5. 选择希望在备份中包含的模块，然后单击或点击**下一步**。
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。要指定其他位置，单击或点击**浏览**。
7. 输入并确认保护该文件的密码。
8. 单击或点击**保存**。

要还原数据，请执行以下操作：

1. 从 HP Client Security 主页面上，单击或点击**齿轮**图标。
2. 在高级设置页面上，单击或点击**管理员策略**。
3. 单击或点击**备份和还原**。
4. 选择**还原**，然后验证身份。
5. 选择以前创建的存储文件。在提供的字段中输入路径。要指定其他位置，单击或点击**浏览**。
6. 输入用来保护文件的密码，然后单击或点击**下一步**。
7. 选择要恢复数据的模块。
8. 单击或点击**还原**。

5 HP 驱动器加密（仅限某些机型）

HP Drive Encryption 通过加密计算机的数据，提供全面的数据保护。激活 Drive Encryption 后，您必须登录到 Drive Encryption 登录屏幕，该屏幕在 Windows® 操作系统启动之前显示。

通过 HP Client Security Home 屏幕，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 Client Security 软件帮助。

可以使用 Drive Encryption 执行以下任务：

- 选择 Drive Encryption 设置：
  - 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 Client Security 来访问 Drive Encryption。

1. 在“开始”屏幕上，单击或点击 **HP Client Security** 应用程序 (Windows 8)。

   - 或 -

   在 Windows 桌面上双击或双点击任务栏最右侧的通知区域中的 **HP Client Security** 图标。

2. 单击或点击 **Drive Encryption** 图标。

一般任务

针对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。执行以下步骤以加密驱动器或磁盘分区：

1. 启动 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 选择希望加密的驱动器或分区的复选框，然后单击或点击**备份密钥**。

注： 为更加安全起见，选择**禁用睡眠模式以提高安全性**复选框。禁用睡眠模式时，绝对不存在将用于解锁驱动器的凭证存储在内存中的风险。

3. 选择一个或多个备份选项，然后单击或点击**备份**。有关详细信息，请参阅第 28 页的备份加密密钥。
4. 您可以在备份加密密钥时继续工作。 请勿重新启动计算机。

注： 此时系统将提示重新启动计算机。重新启动后，将显示驱动器加密预引导屏幕，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 Client Security 软件帮助。

针对自我加密驱动器激活 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。硬件加密比软件加密快得多。但是，您不能选择要加密的磁盘分区。整个磁盘都将加密，包括任何磁盘分区。

要加密特定分区，必须使用软件加密。确保清除**仅允许硬件加密自加密驱动器(SED)**复选框。

执行以下步骤可为自加密驱动器激活 Drive Encryption：

1. 启动 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 选择希望加密的驱动器的复选框，然后单击或点击**备份密钥**。

注： 为更加安全起见，选择**禁用睡眠模式以增加安全性**复选框。禁用睡眠模式时，绝对不存在将用于解锁驱动器的凭证存储在内存中的风险。

3. 选择一个或多个备份选项，然后单击或点击**备份**。有关详细信息，请参阅第 28 页的备份加密密钥。
4. 您可以在备份加密密钥时继续工作。 请勿重新启动计算机。

注： 对于自加密驱动器，系统提示您关闭计算机。

有关详细信息，请参阅 HP Client Security 软件帮助。

停用 Drive Encryption

1. 启动 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 清除所有加密的驱动器的复选框，然后单击或点击**应用**。

   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

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： 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 Client Security 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 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，然后单击或点击**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

- 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。

加密其他硬盘驱动器

强烈建议使用 HP Drive Encryption 并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. 启动 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 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）

管理员可以使用 Drive Encryption 查看和更改计算机上所有硬盘驱动器的加密状态（未加密或加密）。

- 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）

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 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 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 在**驱动器状态**下，选中或清除每个要加密或解密的硬盘驱动器分区旁的复选框，然后单击或点击**应用**。

注： 加密或解密分区时，有一个进度条会显示已加密分区的百分比。

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。

磁盘管理

- **昵称** — 您可以为驱动器或分区命名以便于识别。
- **断开连接驱动器** — Drive Encryption 可以跟踪从计算机上移除的磁盘。从计算机上移除的产品会自动移动到断开连接列表。如果磁盘返回至系统，则会再次出现在连接列表上。
- 如果不再需要跟踪或管理断开连接的驱动器，可以将断开连接的驱动器从断开连接列表上移除。
- Drive Encryption 保持激活的状态，直至所有连接的驱动器的复选框都被清除并且断开连接列表为空。

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。

1. 启动 **Drive Encryption**。有关详细信息，请参阅第 25 页的打开 Drive Encryption。
2. 选择驱动器的复选框，然后单击或点击**备份密钥**。

3. 在**创建 HP Drive Encryption 恢复密钥**下方，选择以下一个或多个选项：

   - **可移动存储** — 选中此复选框，然后选择将保存加密密钥的存储设备。
   - **SkyDrive** — 选中此复选框。必须连接至 Internet。登录 Microsoft SkyDrive，然后单击或点击**是**。

     注： 要使用存储在 SkyDrive 上的 HP Drive Encryption 备份密钥，您必须将其从 SkyDrive 下载至可移动存储设备上，然后将此存储设备插入此计算机。

   - **TPM** （仅部分型号）— 可用来使用您的 TPM 密码恢复数据。

     注意： 如果 TPM 被清除或者计算机受损，您将无法访问备份。如果选择此方法，也应选择另一个备份方法。

4. 单击或点击**备份**。

   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 Drive Encryption 中的**备份密钥**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. HP Drive Encryption 对话框打开时，请单击或点击**恢复**。
4. 输入包含备份密钥的文件路径或名称，然后单击或点击**恢复**。
5. 确认对话框打开时，请单击或点击**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 Recovery 的详细信息，请参阅 HP Client Security 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 HP Drive Encryption 页后，导航至用户登录页面。
3. 单击 **SpareKey**。

   注： 如果尚未在 HP Client Security 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。

6 HP File Sanitizer（仅限某些机型）

通过使用 File Sanitizer，您可以安全地碎化计算机内置硬盘驱动器上的资产（例如：个人信息或文件、历史数据或与 Web 有关的数据），以及定期清理计算机的内置硬盘驱动器。

File Sanitizer 无法用于清理以下类型的驱动器：

- 固态驱动器 (SSD)，包括跨越 SSD 设备的 RAID 卷
- 通过 USB、Firewire 或 eSATA 接口连接的外部驱动器

如果试图在 SSD 上执行碎化或清理操作，则会显示一条警告消息，并且不会执行该操作。

碎化

碎化不同于标准 Windows® 删除操作。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 简单删除操作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。

您可以计划未来碎化时间，也可以通过选择 HP Client Security Home 屏幕上的 **File Sanitizer** 图标或者使用 Windows 桌面上的 **File Sanitizer** 图标手动激活碎化。有关详细信息，请参阅第 31 页的设置碎化计划、第 33 页的右击碎化或第 33 页的手动开始碎化操作。

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 中删除一项资产并不会从硬盘中完全清除资产内容。Windows 只是删除对资产的引用，或是资产在硬盘上的位置。资产内容仍然保留在硬盘上，直到另一项资产使用新信息覆盖硬盘上的相同区域。

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： 可用空间清理不会为碎化的资产提供额外的安全保护。

您可以设置未来可用空间清理时间，也可以通过选择 HP Client Security Home 屏幕上的 **File Sanitizer** 图标或者使用 Windows 桌面上的 **File Sanitizer** 图标手动激活之前碎化的资产的可用空间清理。有关详细信息，请参阅第 32 页的设置可用空间清理计划、第 34 页的手动开始可用空间清理或第 33 页的使用 File Sanitizer 图标。

打开 File Sanitizer

1. 在“开始”屏幕上，单击或点击 **HP Client Security** 应用程序 (Windows 8)。

   - 或 -

   在 Windows 桌面上双击或双点击任务栏最右侧的通知区域中的 **HP Client Security** 图标。

2. 在**数据**下方，单击或点击 **File Sanitizer**。

– 或 –

▲ 双击或双点击 Windows 桌面上的 **File Sanitizer** 图标。

– 或 –

▲ 右击或点击 Windows 桌面上的 **File Sanitizer** 图标不放，然后选择**打开 File Sanitizer**。

设置步骤

碎化— File Sanitizer 可以安全地删除或碎化特定类型的资产。

1. 在**碎化**下方，选择要碎化的每个文件类型的复选框或者清除不希望碎化的文件类型的复选框。
   - **回收站** — 碎化回收站中的所有项目。
   - **临时系统文件** — 碎化位于系统临时文件夹中的所有文件。将按以下顺序搜索下面的环境变量，并将找到的第一个路径视为系统文件夹：
     - TMP
     - TEMP
   - **临时 Internet 文件** — 碎化 Web 浏览器为提高查看速度而保存的网页、图像和媒体的副本。
   - **Cookie** — 碎化网站为保存首选项（如登录信息）而存储在计算机上的所有文件。
2. 要开始碎化，单击或点击**碎化**。

清理 — 将随机数据写入可用空间并防止恢复已经删除的项目。

▲ 要开始清理，单击或点击**清理**。

File Sanitizer 选项 — 选中该复选框以启用以下各个选项，或者清除复选框以禁用某个选项。

- **启用桌面图标** — 在 Windows 桌面上显示 File Sanitizer 图标。
- **启用右击** — 让您可以右击或点击某个资产不放，然后选择 **HP File Sanitizer – 碎化**。
- **在手动碎化之前询问 Windows 密码** — 在手动碎化某个项目之前，要求使用 Windows 密码进行验证。
- **在关闭浏览器时碎化 Cookie 和临时 Internet 文件** — 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。

设置碎化计划

您可以计划执行自动碎化的时间，也可以手动随时碎化资产。有关详细信息，请参阅第 31 页的设置步骤。

1. 打开 File Sanitizer，然后单击或点击**设置**。
2. 要计划碎化选定资产的未来时间，在**碎化计划**下方，选择**从不**、**一次**、**每日**、**每周**或**每月**，然后选择天和时间：
   a. 单击或点击小时、分钟或 AM/PM 字段。
   b. 在其他字段相同等级上，滚动直至需要的值显示。
   c. 单击或点击时间设置字段周围的白色空间。
   d. 重复每个字段，直到选定了正确的计划。

3. 列出以下四种类型资产：

   - **回收站** — 碎化回收站中的所有项目。
   - **临时系统文件** — 碎化位于系统临时文件夹中的所有文件。将按以下顺序搜索下面的环境变量，并将找到的第一个路径视为系统文件夹：
     - TMP
     - TEMP
   - **临时 Internet 文件** — 碎化 Web 浏览器为提高查看速度而保存的网页、图像和媒体的副本。
   - **Cookie** — 碎化网站为保存首选项（如登录信息）而存储在计算机上的所有文件。

   如果选中，这些资产在计划的时间碎化。

4. 要选择碎化其他自定义的资产，请执行以下操作：

   a. 在**计划的碎化列表**下方，单击或点击**添加文件夹**，然后导航至文件或文件夹。

   b. 单击或点击**打开**，然后单击或点击**确定**。

   要从计划的碎化列表中移除一个资产，清除该资产的复选框。

设置可用空间清理计划

可用空间清理不会为碎化的资产提供额外的安全保护。

1. 打开 File Sanitizer，然后单击或点击**设置**。
2. 要计划碎化清理硬盘驱动器的未来时间，在**清理计划**下方，选择**从不**、**一次**、**每日**、**每周**或**每月**，然后选择天和时间：

   a. 单击或点击小时、分钟或 AM/PM 字段。

   b. 在其他字段相同等级上，滚动直至需要的时间显示。

   c. 单击或点击时间设置字段周围的白色空间。

   d. 重复操作，直到选定了正确的计划。

注： 可用空间清理操作可能需要相当长的时间。请确保您的计算机已连接到交流电源。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。可用空间清理可在工作完毕之后或不使用计算机时执行。

保护文件以防止碎化

要保护文件或文件夹以防止碎化，请执行以下操作：

1. 打开 File Sanitizer，然后单击或点击**设置**。
2. 在**从不碎化列表**下方，单击或点击**添加文件夹**，然后导航至文件或文件夹。
3. 单击或点击**打开**，然后单击或点击**确定**。

注： 只要文件保留在列表中，它们就会受到保护。

要从排除列表中移除一个资产，清除该资产的复选框。

一般任务

使用 File Sanitizer 执行以下任务：

- **使用 File Sanitizer 图标启动碎化** — 将文件拖到 Windows 桌面上的 **File Sanitizer** 图标。有关详细信息，请参阅第 33 页的使用 File Sanitizer 图标。
- **手动碎化特定资产或所有选定资产** — 随时碎化项目，而无需等待到预先设定的碎化时间。有关详细信息，请参阅第 33 页的右击碎化或第 33 页的手动开始碎化操作。
- **手动激活可用空间清理** — 随时激活可用空间清理。有关详细信息，请参阅第 34 页的手动开始可用空间清理。
- **查看日志文件** — 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过程中出现的所有错误或故障信息。有关详细信息，请参阅第 34 页的查看日志文件。

注： 碎化或可用空间清理操作可能占用很长时间。尽管碎化或可用空间清理在后台执行，但是处理器使用率的增加还是可能影响笔记本计算机的性能。

使用 File Sanitizer 图标

注意： 无法恢复碎化的资产。仔细考虑要选定进行手动碎化的项目。

在开始手动碎化操作时，File Sanitizer 视图中的标准碎化列表被碎化（参见第 31 页的设置步骤）。

您可以使用以下某种方法开始手动碎化操作：

1. 打开 File Sanitizer（参见第 30 页的打开 File Sanitizer），然后单击或点击**碎化**。
2. 在确认对话框打开时，确保选中希望碎化的资产，然后单击或点击**确定**。

– 或 –

1. 右击或点击 Windows 桌面上的 **File Sanitizer** 图标不放，然后单击或点击**立即碎化**。
2. 在确认对话框打开时，确保选中希望碎化的资产，然后单击或点击**碎化**。

右击碎化

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。

如果已经在 File Sanitizer 视图中选择**启用右击碎化**，可以按如下方式碎化资产：

1. 转至希望碎化的文档或文件夹。
2. 右击或点击文件或文件夹不放，然后选择 **HP File Sanitizer – 碎化**。

手动开始碎化操作

注意： 无法恢复碎化的资产。仔细考虑要选定进行手动碎化的项目。

在开始手动碎化操作时，File Sanitizer 视图中的标准碎化列表被碎化（参见第 31 页的设置步骤）。

您可以使用以下某种方法开始手动碎化操作：

1. 打开 File Sanitizer（参见第 30 页的打开 File Sanitizer），然后单击或点击**碎化**。
2. 在确认对话框打开时，确保选中希望碎化的资产，然后单击或点击**确定**。

– 或 –

1. 右击或点击 Windows 桌面上的 **File Sanitizer** 图标不放，然后单击或点击**立即碎化**。
2. 在确认对话框打开时，确保选中希望碎化的资产，然后单击或点击**碎化**。

手动开始可用空间清理

在开始手动清理操作时，File Sanitizer 视图中的标准碎化列表被清理（参见第 31 页的设置步骤）。

您可以使用以下某种方法开始手动清理操作：

1. 打开 File Sanitizer（参见第 30 页的打开 File Sanitizer），然后单击或点击**清理**。
2. 确认对话框打开时，请单击或点击**确定**。

– 或 –

1. 右击或点击 Windows 桌面上的 **File Sanitizer** 图标不放，然后单击或点击**立即清理**。
2. 确认对话框打开时，请单击或点击**清理**。

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： 已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以下文件夹中：

- 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以下文件夹中：

- 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

7 HP Device Access Manager（仅限某些机型）

HP 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 37 页的无管理的设备类别。

Windows® 操作系统管理员可使用 HP Device Access Manager 控制对系统中设备的访问以及防止未经授权的访问：

- 可以为每个用户创建设备配置文件，以定义允许或拒绝他们访问的设备。
- “及时验证 (JITA)”允许预定义用户对他们自己进行身份验证，以便访问否则就会拒绝访问的设备。
- 通过将管理员和可信用户添加到“设备管理员”组，可以将他们从 Device Access Manager 对设备访问施加的限制中排除。使用“高级设置”管理此组的成员资格。
- 可以根据组成员资格或者为个别用户授予或拒绝设备访问权限。
- 针对不同设备类别，例如 CD-ROM 驱动器和 DVD 驱动器，可以分别允许或拒绝读访问权限和写访问权限。

HP Device Access Manager 在完成 HP Client Security 设置向导过程中会自动配置以下设置：

- 及时验证 (JITA) 可移动介质对管理员和用户启用。
- 设备策略允许完全访问其他设备。

打开 Device Access Manager

1. 在“开始”屏幕上，单击或点击 **HP Client Security** 应用程序 (Windows 8)。

   - 或 -

   在 Windows 桌面上双击或双点击任务栏最右侧的通知区域中的 **HP Client Security** 图标。

2. 在**设备**下方，单击或点击**设备权限**。
   - 标准用户可以查看其当前的设备访问权限（参见第 35 页的用户视图）。
   - 管理员可以通过单击或点击**更改**，然后输入管理员密码来查看和更改当前为计算机配置的设备访问权限（参见第 36 页的系统视图）。

用户视图

如果选中**设备权限**，则显示用户视图。因策略而定，标准用户和管理员可以查看其拥有的设备类别或此计算机上单个设备的访问权限。

- **当前用户** — 显示当前登录的用户的名称。
- **设备类别** — 显示设备类别。
- **访问权限** — 显示对设备类别或特定设备配置的访问权限。

- **期限** — 显示您访问 CD/DVD-ROM 驱动器或可移动磁盘驱动器的时间限制。
- **设置** — 管理员可以更改哪些驱动器拥有由 Device Access Manager 控制的访问权限。

系统视图

在系统视图上，管理员可以允许或拒绝用户组或管理员组对此计算机上设备的访问权限。

▲ 管理员可以通过单击或点击**更改**，输入管理员密码，然后从以下选项中选择，访问系统视图：

- **Device Access Manager** — 要让 HP Device Access Manager 开启或关闭 Just In Time Authentication，单击或点击 **On** 或 **Off**。
- **此计算机上的用户和组** —选择允许或拒绝访问选定的设备类别的用户组或管理员组。
- **设备类别** — 显示设备类别和系统中安装的设备或系统中以前可能安装的设备。要展开列表，单击**+**图标。显示连接至计算机的所有设备，管理员和用户组被展开以显示器成员资格。要刷新设备列表，单击圆箭头（刷新）图标。
  - 保护通常应用于设备类别。如果访问设为**允许**，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。
  - 配置及时验证（JITA），允许所选用户通过验证他们的身份，访问 DVD/CD-ROM 驱动器或可移动介质。有关详细信息，请参阅第 37 页的 JITA 配置。
  - 允许或拒绝访问其他设备类别，如可移动介质（如 USB 闪存驱动器）、串行和并行端口、Bluetooth® 设备、调制解调器设备、PCMCIA/ExpressCard 设备、1394 设备、指纹识别器和智能卡读卡器。如果指纹识别器和智能卡读卡器被拒绝，它们可被用作为验证凭证，但是不能在会话策略级别使用。

    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。
  - 如果选择组或设备类别级别的设置，系统询问是否要将设置应用于子对象：

    是 — 设置将传播。

    否 — 设置不会传播。
  - 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。

    注： “用户列表”中不能加入管理员组。
- **访问权限** — 单击或点击向下箭头，然后，选择以下其中一个访问类型以允许或拒绝访问：
  - **允许 - 完全访问**
  - **允许 - 只读**
  - **允许 - 需要 JITA** — 有关更多信息，参阅第 37 页的 JITA 配置。

    如果选择此访问类型，在**期限**下方，单击或点击向下箭头选择时间限制。
  - **拒绝**
- **期限** — 单击或点击向下箭头以选择访问 CD/DVD-ROM 驱动器或可移动磁盘驱动器的时间限制（参阅第 37 页的 JITA 配置）。

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**视图中创建策略已经限制的设备。

授权的 JITA 时间可以是设好的分钟数或无限。从验证后到他们注销系统前，无限用户都可以访问设备。

如果用户被赋予有限的 JITA 期间，在 JITA 期间过期前 1 分钟，系统询问用户是否延长访问权限。一旦用户注销系统或其他用户登录，JITA 期间就过期。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
- 可移动磁盘驱动器

为用户或组创建 JITA 策略

管理员可以允许用户或组使用及时验证 (JITA) 来访问设备。

1. 启动 **Device Access Manager**，然后单击或点击**更改**。
2. 选择用户或组，然后在**可移动磁盘驱动器**或 **DVD/CD-ROM 驱动器**的**访问权限**下方，单击或点击向下箭头，然后选择**允许 - 需要 JITA**。
3. 在**期限**下方，单击或点击向下箭头选择 JITA 访问的时期。

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 策略

管理员可以禁用用户或组采用及时验证法来访问设备。

1. 启动 **Device Access Manager**，然后单击或点击**更改**。
2. 选择用户或组，然后在**可移动磁盘驱动器**或 **DVD/CD-ROM 驱动器**的**访问权限**下方，单击或点击向下箭头，然后选择**拒绝**。

当那个用户登录并试图访问该设备时，访问将被拒绝。

设置

使用**设置**视图，管理员可以查看和更改拥有由 Device Access Manager 控制的权限的驱动器。

注： 在配置驱动器字母表时，Device Access Manager 必须启用（参阅第 36 页的系统视图）。

无管理的设备类别

HP Device Access Manager 并不管理以下设备类别：

- 输入/输出设备
  - CD-ROM
  - 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
- 红外人体学接口设备
- 鼠标
- 多串口
- 键盘
- 即插即用 (PnP) 打印机
- 打印机
- 打印机升级

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

8 HP Trust Circles

HP Trust Circles 是文件和文档安全应用程序，它将文件夹文件加密和方便的信任圈文档共享功能结合在一起。此应用程序将文件置于用户特定的文件夹中，在信任圈中保护它们。一经保护，文件只能由信任圈的成员使用和共享。如果非成员收到受保护的文件，文件保持加密状态，非成员不能访问内容。

打开 Trust Circles

1. 在“开始”屏幕中单击或点击 **HP Client Security** 应用程序。

   - 或 -

   在 Windows 桌面上，双击位于任务栏最右侧的通知区域中的 **HP Client Security** 图标。

2. 在**数据**下方，单击或点击 **Trust Circles**。

使用入门

有两种方法发送电子邮件邀请并进行回复：

- **使用 Microsoft® Outlook** — 使用 Trust Circles 和 Microsoft Outlook 自动处理任何 Trust Circle 邀请并回复其他 Trust Circle 用户。
- **使用 Gmail、Yahoo、Outlook.com 或其他电子邮件服务 (SMTP)**—输入姓名、电子邮件地址和密码时，Trust Circles 使用您的电子邮件服务向选中加入您的信任圈的成员发送电子邮件邀请。

要设置基本配置文件，请执行以下操作：

1. 输入姓名和电子邮件地址，然后单击或点击**下一步**。

   受邀加入您的信任圈的任何成员可以看到此姓名。电子邮件地址用于发送、接收或回复邀请。

2. 输入电子邮件帐户的密码，然后单击或点击**下一步**。

   系统发送测试电子邮件确保电子邮件设置正确。

   注： 计算机必须连接至网络。

3. 在 **Trust Circle 名称**字段，输入信任圈的名称，然后单击或点击**下一步**。
4. 添加成员和文件夹，然后单击或点击**下一步**。创建的信任圈带有选定的文件夹，并向选定的任何成员发送电子邮件邀请。如果，因为任何原因无法发送邀请，则显示通知。可随时通过单击**您的 Trust Circles**，然后双击或双点击信任圈，从 Trust Circle 视图中再次邀请成员。有关详细信息，请参阅第 40 页的 Trust Circles。

Trust Circles

可以在输入电子邮件地址之后的初始设置过程中或者在 Trust Circle 视图上创建信任圈：

▲ 从 Trust Circle 视图上，单击或点击**创建 Trust Circle**，然后输入信任圈的名称。

- 要为信任圈添加成员，单击或点击**成员**旁边的 **M+** 图标，然后按照屏幕上的说明进行操作。
- 要为信任圈添加文件夹，单击或点击**文件夹**旁边的 **+** 图标，然后按照屏幕上的说明进行操作。

添加文件夹至信任圈

添加文件夹至新的信任圈：

- 在创建信任圈过程中，可以通过单击或点击**文件夹**旁边的**+**图标，然后按照屏幕上的说明进行操作，来添加文件夹。

  - 或 -

- 在 Windows Explorer 中，右击或点击当前不属于某个信任圈文件夹不放，选择 **Trust Circle**，然后选择**从文件夹中创建 Trust Circle**。

提示： 可以选择一个或多个文件夹。

添加文件夹至现有的 Trust Circle：

- 从 Trust Circle 视图中，单击**您的 Trust Circles**，双击或双点击现有的信任圈以显示当前的文件夹，单击或点击**文件夹**旁边的 **+** 图标，然后按照屏幕上的说明进行操作。

  - 或 -

- 在 Windows Explorer 中，右击或点击当前不属于某个信任圈文件夹不放，选择 **Trust Circle**，然后选择**此文件夹添加至现有 Trust Circle**。

提示： 可以选择一个或多个文件夹。

文件夹一经添加至信任圈，Trust Circles 自动加密文件夹及其内容。所有文件加密之后，即显示通知。此外，文件夹内所有加密的文件夹图标和文件图标上都显示绿色锁符号，指示它们受完全保护。

添加成员至信任圈

将成员添加至信任圈需要三个步骤：

1. **邀请** — 首先，信任圈主人邀请成员。邀请电子邮件可以发送至多个用户或分配列表/组。
2. **接受** — 受邀者接收邀请并选择是接受还是拒绝。如果受邀者接受邀请，邀请者将收到电子邮件回复。如果向组发送邀请，每个成员接收邀请，并选择接受还是拒绝。
3. **注册** — 邀请者最后有机会决定是否将成员添加至信任圈。如果邀请者决定注册成员，系统将发送电子邮件给受邀者确认回复。邀请者和受邀者可选地验证邀请过程的安全性。受邀者将看到验证码，并通过电话读给邀请者。验证码经过验证，邀请者可以发送最终的注册电子邮件。

添加成员至新的信任圈：

▲ 在创建信任圈过程中，可以通过单击或点击**成员**旁边的 **M+** 图标，然后按照屏幕上的说明进行操作，来添加成员。

- 如果使用 Outlook，从 Outlook 地址簿中选择联系人，然后单击**确定**
- 如果使用其他电子邮件服务，可手动将新的电子邮件地址添加至 Trust Circle，或者从在 Trust Circle 注册的电子邮件地址中检索。

添加成员至现有的信任圈：

▲ 从 Trust Circle 视图中，单击**您的 Trust Circles**，双击或双点击现有的信任圈以显示当前的成员，单击或点击**成员**旁边的 **M+** 图标，然后按照屏幕上的说明进行操作。

- 如果使用 Outlook，从 Outlook 地址簿中选择联系人，然后单击**确定**。
- 如果使用其他电子邮件服务，可手动将新的电子邮件地址添加至 Trust Circle，或者从在 Trust Circle 注册的电子邮件地址中检索。

添加文件至信任圈

您可以使用以下某种方法添加文件至信任圈：

- 复制或移动文件至现有的信任圈文件夹。

  - 或 -

- 在 Windows Explorer 中，右击或点击当前未加密的文件不放，选择 **Trust Circle**，然后选择**加密**。系统将提示您选择要添加文件的信任圈。

提示： 可以选择一个或多个文件。

加密的文件夹

信任圈的任何成员可以查看和编辑属于该信任圈的文件。

注： Trust Circle Manager/Reader 不在成员之间同步文件。

文件必须通过现有方式共享，例如，电子邮件、FTP 或云存储提供商。复制、移动至信任圈文件夹中或者在其中创建的文件立即受到保护。

从信任圈移除文件夹

从信任圈移除文件夹，此文件夹及其所有内容即被解密，不受保护。

- 从 Trust Circle 视图中，单击**您的 Trust Circles**，双击或双点击现有的信任圈以显示当前的文件夹，单击或点击文件夹旁边的**回收站**图标。

  - 或 -

- 在 Windows Explorer 中，右击或点击当前属于某个信任圈的文件夹不放，选择 **Trust Circle**，然后选择**从信任圈中移除**。

提示： 可以选择一个或多个文件夹。

从信任圈移除文件

要从信任圈中移除文件，在 Windows Explorer，右击或点击当前加密的文件不放，选择 **Trust Circle**，选择**解密文件**。

从信任圈移除成员

完全注册的成员不能从信任圈中移除。替代做法是创建带有所有其他成员的新信任圈，将所有文件和文件夹移至新的信任圈，然后删除旧的信任圈。这将确保成员接收的任何新文件不会被访问，但是旧信任圈的成员依然可以访问之前共享的任何内容。

如果成员未完全注册（成员被要求加入信任圈或还未接受加入信任圈的邀请），您可以通过以下任一方式将成员从信任圈中移除：

- 从 Trust Circle 视图中，单击或点击**您的 Trust Circles**，然后双击或双点击信任圈以显示当前成员列表。单击或点击要移除的成员名称旁边的**回收站**图标。
- 从 Trust Circle 视图中，单击或点击**成员**，然后双击或双点击成员以显示其所属的信任圈。单击或点击信任圈旁边的**回收站**图标，以将成员从信任圈中移除。

删除信任圈

要删除信任圈，需要有所有权。

▲ 从 Trust Circle 视图中，单击或点击**您的 Trust Circles**，单击或点击要删除的信任圈旁边的**回收站**图标。

这将信任圈从页面中移除，并发送电子邮件给信任圈的所有成员，告知此信任圈已经被删除。该信任圈中包含的任何文件或文件夹都被解密。

设置首选项

从 Trust Circle 视图，单击或点击**首选项**。显示三个标签

- **电子邮件设置**

选项	说明
用户名	显示当前使用的用户名。要更改，在文本框中输入新的用户名。自动保存更改。
电子邮件地址	显示当前使用的电子邮件帐户。要更改，单击或点击**更改电子邮件设置**，然后按照屏幕上的说明进行操作。
新成员确认	从以下选项中进行选择： ◦ **自动确认** — 收到受邀者的接受之后，他们确认进入信任圈，无需手动输入，确认电子邮件发送至受邀者。 ◦ **手动确认** — 从受邀者接收接受之后，需要手动输入以将新成员注册到信任圈，然后确认电子邮件发送至受邀者。 ◦ **需要验证** — 在接收受邀者的接受之后，需要验证码以完全注册受邀者。信任圈的所有者必须联系受邀者并要求其提供验证码。输入正确的验证码之后，发送确认电子邮件。
定期验证	定期验证要求用户在特定超时（以分钟记录）之后以及执行敏感的操作时输入 Windows 密码。此设置允许用户开启或关闭验证。
验证超时	在需要验证之前，选择特定的超时期间（以分钟记录）。

选项	说明
不要显示确认消息	选中复选框以禁用显示确认消息，或清除复选框以显示确认消息。
我愿意通过匿名使用跟踪帮助改进 HP Trust Circle	选择复选框参与计划，或若不愿意参与，清除复选框。

- **备份/还原**

选项	说明
备份	复制 Trust Circle Manager/Reader 应用程序数据（设置和信任圈）至备份文件。如果出现崩溃或系统故障，可以使用此文件将新安装的 Trust Circles 还原至文件保存的状态。 **注：** 仅保存 Trust Circle 应用程序数据（信任圈、设置和成员）。信任圈文件夹中的实际文件不备份。那些文件应单独备份。 要备份 Trust Circle 设置和用户数据： 1. 单击或点击**备份**。 2. 选择备份文件的文件名和目录，然后单击或点击**保存**。 3. 输入密码，确认，然后单击或点击**确定**。还原此文件将需要此密码。
还原	从备份文件中还原设置和信任圈，通常在系统崩溃或迁移至另一台计算机之后执行。 要还原 Trust Circle Manager 的设置和用户数据： 1. 单击或点击**还原**。 2. 导航至备份文件的目录和文件名，然后单击或点击**打开**。 3. 输入在进行备份时设置的密码。

- **关于** — 显示 Trust Circle Manager/Reader 软件版本。显示链接以允许您升级 Trust Circle Manager 至 Pro 版本或显示 HP 隐私声明。

9 失窃找回（仅限某些机型）

Computrace（需单独购买）允许您远程监视、管理和跟踪您的笔记本计算机。

激活后，在 Absolute Software 客户中心中对 Computrace 进行配置。在该客户中心中，管理员可以配置 Computrace 以监视或管理笔记本计算机。如果系统失窃或者将其放错位置，则客户中心可以帮助本地主管机构查找并恢复该计算机。如果配置，则 Computrace 可持续发挥作用，即使清除或更换硬盘驱动器也是如此。

要激活 Computrace，请执行以下操作：

1. 连接到 Internet。
2. 打开 HP Client Security。有关详细信息，请参阅第 7 页的打开 HP Client Security。
3. 单击 **Theft Recovery**。
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 的详细信息，请单击**了解更多信息**。

10 本地化的密码例外情况

在开机验证级别和 HP Drive Encryption 级别，仅提供有限的密码本地化支持。有关详细信息，请参阅第 45 页的开机验证级别或 Drive Encryption 级别不支持 Windows IME。

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. 启动 HP Client Security，然后输入 Windows 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更多信息，请参阅第 46 页的特殊按键处理。
  2. 启动 HP Client Security，然后输入 Windows 密码。

开机验证级别或 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。

开机验证级别或 Drive Encryption 级别不支持 IME。无法在开机验证或 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 Client Security 可以支持该配置。

⚠ **警告！** 如果部署了 HP Client Security，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 Client Security 用户页面（从主页面的**齿轮**图标访问）从 HP Client Security 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 HP Client Security 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

  当用户选择上述一种键盘布局，然后输入密码（例如 abcdef），在按以下键时必须输入同样的密码：shift 键小写，shift 键和 caps lock 键大写（开机验证和 HP Drive Encryption）。数字密码必须使用数字小键盘进行输入。

- 韩语

  当用户选择支持的韩语键盘布局，然后输入密码（例如 abcdef），在按以下键时必须输入同样的密码：右 alt 键小写，右 alt 键和 caps lock 键大写（开机验证和 HP Drive Encryption）。

- 下表列出了不支持的字符：

Language（语言）	Windows	BIOS	Drive Encryption
阿拉伯语	ﻻ ,ﻷ, 和 ﻹ 键生成两个字符。	ﻻ ,ﻷ, 和 ﻹ 键生成一个字符。	ﻻ ,ﻷ, 和 ﻹ 键生成一个字符。
加拿大法语	使用 caps lock 输入的 ç、è、à 和 é 在 Windows 中为 Ç、È、À 和 É。	使用 caps lock 输入 ç、è、à 和 é 在开机验证中为 ç、è、à 和 é 。	使用 caps lock 输入的 ç、è、à 和 é 在 HP Drive Encryption 中为 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

Language（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
斯洛伐克语	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
Japanese（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

Bluetooth
该技术利用无线传输使支持 Bluetooth 的计算机、打印机、鼠标、手机以及其它设备在短距离内进行无线通信。

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
请参阅 Drive Encryption 预引导验证。

Drive Encryption 预引导验证。
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，或者扫描经过注册的手指。如果选择了一步登录，则在 Drive Encryption 登录屏幕上输入正确信息后便可直接访问 Windows，而无需在 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。

PIN
用于验证的注册用户个人标识号。

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。

Trust Circle
通过将数据绑定至定义的信任用户组，提供数据密闭。可防止数据被意外或有意地落入不当之手。配有 CryptoMill’s Zero Overhead Key Management 技术，数据被密码地约束在信任圈内。防止解密信任圈之外的文档或其他敏感信息。

Trust Circle Manager/Reader。
Trust Circle Reader 仅可接受由 Trust Circle Manager 用户发送的邀请。但是，Trust Circle Manager 允许创建信任圈。其功能包含通过电子邮件邀请某人至信任圈和接受其他人的信任圈邀请。在对等用户之间建立了信任圈之后，受此信任圈保护的文件即可被安全地共享。

Trust Circle 文件夹。
受信任圈保护的任何文件夹。

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
授权登录到网络或个别计算机的用户。

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 Client Security 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。

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

登录
HP Client Security 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）。

非接触卡
一张塑料材质的卡，其中含有可用于进行验证的计算机芯片。

管理员
请参阅 *Windows 管理员*。

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，才能使用 Drive Encryption 的功能。管理员可以使用 HP Client Security 设置向导或 HP Client Security 激活 Drive Encryption。激活过程包括激活软件、加密驱动器，以及在可移动存储设备上创建初始备份加密密钥。

及时验证。
参见 HP Device Access Manager 软件帮助。

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。

接近卡
一张塑料材质的卡，其中含有可用于进行验证的计算机芯片，与其它凭证配合使用可提供额外的安全保护。

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。

可用空间清理
在已删除的资产和未用空间上写入随机数据。这个过程可以减少已删除资产的存在，从而使原始资产更加难以恢复。

连接的设备。
连接到计算机端口上的硬件设备。

凭证

用于验证单个用户的一些特定信息或硬件设备。

软件加密
使用软件逐扇区加密硬盘驱动器。该过程比硬件加密慢。

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。

手动碎化
立即碎化某一资产或选定资产，这将跳过预先设定的碎化时间。

受信任的平台模块 (TPM) 嵌入式安全保护芯片
TPM 对计算机（而不是对用户）进行身份验证，方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 可最大限度降低笔记本计算机上由于物理窃取或外部黑客攻击而危及信息的风险。

碎化
执行一种算法以使用无意义的数据覆盖资产中包含的数据。

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
该过程通过使用凭证（包括 Windows 密码、指纹、智能卡、非接触卡或接近卡）验证您是否为所声称的人。

硬件加密
使用满足可信计算组 OPAL 规范的自我加密驱动器完成瞬时加密，该规范针对管理自我加密驱动器而制定。硬件加密是瞬时的，可能需要几分钟，但是软件加密可能需要几个小时的时间。

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。

指纹
提取的数字指纹图像。HP Client Security 并不存储实际的指纹图像。

智能卡
可用于验证并配合 PIN 使用的硬件设备。

主页
一个中心位置，您可以从中访问和管理 HP Client Security 中的功能和设置。

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
在 File Sanitizer 中计划的碎化。

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