

HP ProtectTools

用户指南

© Copyright 2009 Hewlett-Packard
Development Company, L.P.

Bluetooth 是其所有者拥有的商标，Hewlett-Packard Company 按许可协议中的规定进行使用。Java 是 Sun Microsystems, Inc. 在美国的商标。Microsoft 和 Windows 是 Microsoft Corporation 在美国的注册商标。SD 徽标是其所有者的商标。

本文档中包含的信息如有更改，恕不另行通知。随 HP 产品和服务附带的明确有限保修声明中阐明了此类产品和服务的全部保修服务。本文档中的任何内容均不应理解为构成任何额外保证。HP 对本文档中出现的技术错误、编辑错误或遗漏之处不承担责任。

第一版：2009 年 10 月

文档部件号：572661-AA1

目录

1 安全保护简介

HP ProtectTools 功能	2
实现关键的安全保护目标	3
防范目标性窃取	3
限制对敏感数据的访问	3
防止来自内部或外部的未授权访问	3
创建强密码策略	3
其他安全保护要素	4
指定安全保护角色	4
管理 HP ProtectTools 密码	4
创建安全的密码	5
备份和恢复 HP ProtectTools 凭证	5

2 使用入门

打开 HP ProtectTools 管理控制台	7
启用安全保护功能	8
注册指纹	9
设置智能卡	10
使用管理控制台	11

3 配置系统

为计算机设置验证	13
登录策略	13
会话策略	13
设置	14
管理用户	15
指定设备设置	16
指纹	16
智能卡	16

4 配置应用程序

“常规”标签	18
应用程序标签	19

5 添加管理工具

6 HP ProtectTools Security Manager

设置步骤	22
使用入门	22
注册凭证	22
注册指纹	22
更改 Windows 密码	23
设置智能卡	23
使用 Security Manager 控制板	23
打开 HP ProtectTools Security Manager	24
常规任务	25
Password Manager	25
对于尚未创建登录的网页或程序	25
对于已创建登录的网页或程序	25
添加登录	26
编辑登录	26
使用“登录”菜单	27
将登录划分到不同类别中	27
管理登录	27
评估您的密码强度	28
Password Manager 图标设置	28
设置	28
凭证	28
个人 ID 卡	30
设置首选项	30
备份和恢复数据	31
添加应用程序	31
安全应用程序状态	31

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

设置步骤	33
打开 Drive Encryption	33
常规任务	34
激活 Drive Encryption	34
停用 Drive Encryption	34
在激活 Drive Encryption 后登录	34
通过加密硬盘驱动器保护您的数据	35
显示加密状态	35
高级任务	36
管理 Drive Encryption (管理员任务)	36
加密或解密各个驱动器	36
备份和恢复 (管理员任务)	36

创建备份密钥	36
执行恢复	37

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

设置步骤	39
打开 Privacy Manager	39
管理 Privacy Manager 证书	39
请求并安装 Privacy Manager 证书	39
申请 Privacy Manager 证书	39
获取预先指定的 Privacy Manager 企业证书	40
安装 Privacy Manager 证书	40
查看 Privacy Manager 证书详细信息	40
续订 Privacy Manager 证书	41
设置默认 Privacy Manager 证书	41
删除 Privacy Manager 证书	41
恢复 Privacy Manager 证书	41
吊销 Privacy Manager 证书	42
管理可信联系人	42
添加可信联系人	42
添加可信联系人	43
使用 Microsoft Outlook 联系人添加可信联系人	43
查看可信联系人详细信息	44
删除可信联系人	44
检查可信联系人的吊销状态	44
常规任务	45
在 Microsoft Outlook 中使用 Privacy Manager	45
为 Microsoft Outlook 配置 Privacy Manager	45
对电子邮件进行签名并发送	45
密封并发送电子邮件	46
查看密封的电子邮件	46
在 Microsoft Office 2007 文档中使用 Privacy Manager	46
为 Microsoft Office 配置 Privacy Manager	46
对 Microsoft Office 文档进行签名	47
在对 Microsoft Word 或 Microsoft Excel 文档进行签名时添加签名行	47
在 Microsoft Word 或 Microsoft Excel 文档中添加建议的签名者	47
添加建议的签名者的签名行	48
加密 Microsoft Office 文档	48
从 Microsoft Office 文档中删除加密	48
发送加密的 Microsoft Office 文档	49
查看签名的 Microsoft Office 文档	49
查看加密的 Microsoft Office 文档	49
在 Windows Live Messenger 中使用 Privacy Manager	49
启动 Privacy Manager Chat 会话	50

为 Windows Live Messenger 配置 Privacy Manager	50
在 Privacy Manager Chat 窗口中聊天	51
查看聊天历史记录	51
显示所有会话	52
显示特定帐户的会话	52
查看会话 ID	52
查看会话	52
在会话中搜索特定文本	52
删除会话	53
添加或删除列	53
过滤显示的会话	53
高级任务	54
将 Privacy Manager 证书和可信联系人迁移到其他计算机上	54
备份 Privacy Manager 证书和可信联系人	54
恢复 Privacy Manager 证书和可信联系人	54
Privacy Manager 集中管理	54

9 HP ProtectTools File Sanitizer

碎化	56
可用空间清理	57
设置步骤	58
打开 File Sanitizer	58
设置碎化计划	58
设置可用空间清理计划	58
选择或创建碎化配置文件	59
选择预定义碎化配置文件	59
自定义碎化配置文件	59
自定义简单删除配置文件	60
常规任务	61
使用按键序列启动碎化	61
使用 File Sanitizer 图标	61
手动碎化一个资产	62
手动碎化所有选定项目	62
手动激活可用空间清理	62
终止碎化或可用空间清理操作	63
查看日志文件	63

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

设置步骤	65
打开 Device Access Manager	65
配置设备访问权限	65
设备管理员组	65
简单配置	65

启动后台服务	66
设备类别配置	66
拒绝用户或组访问	68
允许用户或组访问	68
删除用户或组的访问权限	69
允许组中一个用户访问某个类别设备	69
允许组中一个用户访问特定设备	69
重置配置	70
高级任务	71
控制对配置设置的访问权限	71
授予现有组或用户的访问权限	71
拒绝现有组或用户的访问	71
添加新组或用户	72
删除组或用户访问权限	72
相关文档	72

11 HP ProtectTools LoJack Pro

12 故障排除

HP ProtectTools Security Manager	74
HP ProtectTools Device Access Manager	76
其他	78

术语表	79
-----------	----

索引	83
----------	----

1 安全保护简介


HP ProtectTools Security Manager (HP ProtectTools 安全管理器) 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 的管理通过“管理控制台”功能实现。

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
- 注册此计算机用户的指纹
- 设置智能卡
- 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 (安全管理器) 应用程序
- 添加其他 Security Manager 应用程序

笔记本电脑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 Credential Manager (HP ProtectTools 凭证管理器)	<ul style="list-style-type: none">• Password Manager (密码管理器) 用作个人密码库, 利用“单一登录”功能简化登录过程, 该功能会自动记住并应用用户凭证。• “单一登录”需要采用多种不同类型的安全技术 (如 Java™ 卡和生物识别器) 来对用户进行身份验证, 从而还能提供更多保护。• 通过软件加密保护密码存储, 并且使用安全设备验证 (例如 Java 卡或生物识别器) 使其得到增强。 <p>注: Credential Manager (凭证管理器) 功能位于 HP ProtectTools Security Manager 的 Password Manager 选项内</p>
HP ProtectTools Drive Encryption (HP ProtectTools 驱动器加密, 仅限某些机型)	<ul style="list-style-type: none">• Drive Encryption (驱动器加密) 提供硬盘驱动器的整卷全面加密。• Drive Encryption 强制执行预引导验证, 以便解密和访问数据。
HP ProtectTools Privacy Manager (HP ProtectTools 隐私管理器, 仅限某些机型)	<ul style="list-style-type: none">• 在使用电子邮件、Microsoft® Office 文档或即时通讯 (IM) 时, Privacy Manager (隐私管理器) 利用高级登录技术验证通信来源、完整性和安全性。
HP ProtectTools File Sanitizer (HP ProtectTools 文件清除工具)	<ul style="list-style-type: none">• 通过使用 File Sanitizer (文件清除工具), 您可以安全地碎化计算机上的数字资产 (包括应用程序文件、历史数据或与 Web 有关的内容, 或其他机密数据等敏感信息), 并定期清理硬盘驱动器。
HP ProtectTools Device Access Manager (HP ProtectTools 设备访问管理器, 仅限某些机型)	<ul style="list-style-type: none">• Device Access Manager (设备访问管理器) 模块允许 IT 管理人员基于用户配置文件控制对设备的访问。• Device Access Manager 模块不仅可防止未经授权的用户擅自删除使用外部存储介质保存的数据, 还防止用户从外部介质中将病毒引入系统中。• 管理员可以禁止特定个人用户或用户组访问可写设备。

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：

- 防范有目的的盗窃行为
- 限制访问敏感数据
- 防止来自内部或外部的未授权访问
- 创建强大可靠的密码策略
- 符合管制安全要求

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：

- 启用预引导验证功能有助于防止他人未经授权擅自访问操作系统。请参阅以下步骤：
 - Security Manager
 - Drive Encryption

限制对敏感数据的访问

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文件或将其保存到可写设备，例如 CD。下列功能可帮助限制对数据的访问：

- HP ProtectTools Device Access Manager 可让 IT 管理员限制对可写设备的访问，使敏感信息无法打印或从硬盘驱动器复制到可移动介质。

防止来自内部或外部的未授权访问

未经授权而访问未采取安全措施的商业 PC 会给公司网络资源（如财务服务、管理人员或研发团队的信息）以及个人信息（如病史记录或个人财务记录）带来切实的危险。以下功能可以帮助防止未经授权的访问：

- 启用预引导验证功能有助于防止他人未经授权擅自访问操作系统。请参阅以下步骤：
 - Password Manager
 - Drive Encryption
- 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。
- HP ProtectTools Device Access Manager 可让 IT 管理员限制对可写设备的访问，以便无法复制硬盘驱动器中的敏感信息。
- DriveLock 可帮助确保即使将硬盘驱动器卸下并安装到未受保护的系统中也无法访问数据。

创建强密码策略

如果施行命令要求对数十个基于 Web 的应用程序和数据库使用强密码策略，Security Manager 可提供受保护的密码存储库和单一登录便利。

其他安全保护要素

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级别，确定要部署的安全功能，如 Java™ 卡、生物识别器或 USB 身份标记等。

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 - 应用并管理安全管理人员定义的安全保护功能。IT 管理员还可以启用或禁用某些功能。例如，如果安全管理人员已决定部署 Java 卡，IT 管理员可以启用 Java 卡 BIOS 安全保护模式。
- 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了 Java 卡，用户可以设置 Java 卡个人标识号，并使用该卡进行身份验证。

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。

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。所有其他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 HP ProtectTools 模块中设置	功能
Security Manager 登录密码	Security Manager	此密码提供两个选项： <ul style="list-style-type: none">● 可用作 Security Manager 登录以在登录到 Windows 后访问 Security Manager。● 可用来允许同时访问 Windows 和 Security Manager。
Security Manager 恢复文件密码	Security Manager, 由 IT 管理员	防止他人未经授权擅自访问 Security Manager 恢复文件。
Java™ 卡 PIN	Java Card Security	防止他人未经授权擅自访问 Java 卡内容并验证 Java 卡用户的身份。用于开机验证时，Java 卡个人标识号还可以防止他人未经授权擅自访问计算机设置实用程序和计算机内容。 如果选择了 Java 卡身份标记，则验证 Drive Encryption 模块的用户。
Windows 登录密码	Windows® 控制面板	可用于手动登录，或保存在 Java 卡中。

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词中的字母。例如，可以使用数字 1 代替字母 l 或 L。
- 混合使用两种或更多种语言的字词。
- 将数字或特殊字符置于单词或短语的中间，如“Mary2-2Cat45”。
- 不要使用可在字典中查到的词作为密码。
- 不要使用姓名或其他个人信息（如生日、宠物名称或母亲的姓氏）作为密码，即使反过来拼写也不可以。
- 定期更改密码。您可以只递增地更改几个字符。
- 如果您写下了密码，请不要将其存放在距离计算机很近的显眼位置。
- 不要在计算机上的文件（如电子邮件）中保存密码。
- 不要与他人共享帐户或将密码告诉别人。

备份和恢复 HP ProtectTools 凭证

可以使用 HP ProtectTools Drive Encryption 来选择和备份 HP ProtectTools 凭证。

2 使用入门

 **注：** HP ProtectTools 管理需要具有管理权限。

“HP ProtectTools 设置向导”可引导您设置 Security Manager 的最常用功能。但是，通过 HP ProtectTools 管理控制台还可以使用其他许多功能。向导中的相同设置以及其他安全保护功能都可以通过该控制台来配置，可从 Windows® “开始”菜单访问该控制台。这些设置应用到该计算机以及共享该计算机的所有用户。

1. 在“欢迎使用”页中，您可以选择其中一个选项以禁止继续显示此向导。
2. 设置完计算机一周后或具有管理权限的用户第一次在指纹识别器上扫描手指时，“HP ProtectTools 设置向导”将自动启动以引导您完成配置程序的基本步骤。有关设置计算机的视频教程会自动启动。
3. 按照屏幕上的说明进行操作，直至完成设置。

如果未完成此向导，它将会再自动启动两次。之后，可通过任务栏通知区域旁边显示的通知气球访问该向导（除非已按照上述步骤 2 将其禁用），直至完成设置。

要使用 HP ProtectTools Security Manager 应用程序，请从“开始”菜单中启动 HP ProtectTools Security Manager，或者右击任务栏最右侧的通知区域中的 Security Manager 图标。共享此计算机的所有用户均可使用 HP ProtectTools 管理控制台及其应用程序。

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**。

对于用户任务，例如注册指纹或使用 Security Manager，请按以下步骤打开控制台：

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

- 或 -

双击任务栏最右侧的通知区域中的 **HP ProtectTools Security Manager** 图标。

启用安全保护功能

“设置向导”将要求您验证您的身份。


1. 阅读“欢迎使用”屏幕内容，然后单击**下一步**。
2. 验证您的身份：键入您的 Windows 密码（如果尚未注册指纹），或者使用指纹识别器扫描您的指纹。单击**下一步**。

如果您的 Windows 密码为空，则会要求您创建一个密码。要使用 HP ProtectTools Security Manager 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。

“设置向导”将引导您完成启用安全保护功能（应用到该计算机的所有用户）的过程：

- 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 — 可在 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。


要启用安全保护功能，请选中相应的复选框。选择的功能越多，您的计算机就越安全。

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


注册指纹

如果您选择了“指纹”，并且计算机具有内置的指纹识别器或连接了指纹识别器，将会指导您完成设置或“注册”指纹的过程：

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，请单击相应的手指。

2. 在选择要注册的手指后，系统将提示您扫描该指纹，直至成功注册该手指。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。对于其他手指，请重复步骤 1 至步骤 3。
4. 单击**下一步**。

 **注：** 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。如果计算机处于非活动状态一段时间或者关闭了控制板，则**不会**保存所做的更改。

设置智能卡

如果您选择了“智能卡”且如果您的计算机内置或连接了智能卡读卡器，则“HP ProtectTools 设置向导”将提示您设置智能卡 PIN（个人标识号）。

要设置智能卡 PIN，请执行以下操作：

1. 在“设置智能卡”页中，输入并确认 PIN。

您也可以更改 PIN：提供旧 PIN，然后选择新 PIN。

2. 要继续操作，请单击**下一步**。

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。

该控制台包含以下组件：

- **工具** — 显示以下类别，用于在计算机上配置安全保护功能：
 - **主页** — 用于选择要执行的安全任务。
 - **系统** — 用于为用户和设备配置安全保护功能和验证。
 - **应用程序** — 显示 HP ProtectTools Security Manager 和 Security Manager 应用程序的常规设置。
 - **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。
- **管理工具** — 提供其他工具的相关信息。下面的面板显示以下选项：
 - **HP ProtectTools 设置向导** — 引导您设置 HP ProtectTools Security Manager。
 - **帮助** — 显示帮助文件，其中提供了有关 Security Manager 及其预安装的应用程序的信息。您可以添加的应用程序的帮助在那些应用程序中提供。
 - **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。

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**。

3 配置系统

可以从 HP ProtectTools 管理控制台屏幕左侧的“工具”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。
- **设备** — 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，您可以选择应在此计算机上实现的安全保护功能、设置控制计算机访问的策略并配置其他高级设置。您可以指定在登录到 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“安全保护”面板菜单中，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“工具”菜单中，单击**安全保护**，然后单击**验证**。
2. 在**登录策略**标签上，单击一个用户类别。
3. 指定选定用户类别所需的验证凭证。您必须至少指定一个凭证。
4. 选择需要任意一个（仅一个）指定的凭证还是需要所有指定的凭证，以验证用户。您还可以阻止任意用户访问计算机。
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“工具”菜单中，单击**安全保护**，然后单击**验证**。
2. 在**会话策略**标签上，单击一个用户类别。
3. 指定选定用户类别所需的验证凭证。
4. 选择需要任意一个（仅一个）指定的凭证还是需要所有指定的凭证，以验证用户。您还可以要求无需验证即可访问 HP ProtectTools 软件。
5. 单击**应用**。

设置

您可以允许使用下面的一种或多种安全设置：

- **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。
- **允许使用 HP SpareKey 验证进行 Windows 登录** — 允许此计算机的用户使用 HP SpareKey 功能登录到 Windows，而不管 Security Manager 所需的任何其他验证策略。

要编辑设置，请执行以下操作：

1. 单击以启用或禁用特定设置。
2. 单击**应用**以保存所做的更改。

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**。

要为用户注册指纹或设置其他凭证，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，然后单击**查看策略**。

指定设备设置

在“设备”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。

指纹

“指纹”页中包含三个标签：“注册”、“灵敏度”和“高级”。

注册

您可以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。

警告！ 所有用户包括管理员的指纹数据都将会被清除。如果登录策略仅需要指纹，则所有用户都将会被禁止登录到此计算机。

灵敏度

要调整指纹识别器在扫描指纹时使用的灵敏度，请移动滑块。

如果始终无法识别您的指纹，则可能需要降低灵敏度设置。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

您可以将指纹识别器配置为在计算机依靠电池供电时节省电能。

智能卡

您可以将计算机配置为在取下智能卡时自动锁定。不过，只有在登录到 Windows 时将智能卡用作验证凭证时，才会锁定计算机。取下登录到 Windows 时未使用的智能卡并不会锁定计算机。

▲ 选中相应的复选框以允许或禁止在取下智能卡时锁定计算机。

4 配置应用程序

可以从 HP ProtectTools 管理控制台左侧的“安全应用程序”菜单面板中访问“应用程序”组。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“工具”菜单中，从**应用程序**组中单击**设置**。
2. 单击以启用或禁用特定设置。
3. 单击**应用**以保存所做的更改。

“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** — 选择此选项可阻止在登录时向导自动打开。
- ▲ **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：

- **Security Manager** — 为计算机的所有用户启用 Security Manager 应用程序。
- **启用“查找更多”按钮** — 允许此计算机的所有用户通过单击 **[+] 查找更多** 按钮，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。

5 添加管理工具

可以通过其他应用程序在 Security Manager 中添加新的管理工具。此计算机的管理员可通过“设置”应用程序禁用此功能。

要添加其他管理工具，请单击 **[+] 管理工具**。

您可以访问 DigitalPersona 网站查看是否有新的应用程序，或者设置一个自动更新的计划。

6 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他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
- 为验证设置智能卡
- 备份和恢复程序数据
- 添加更多应用程序

设置步骤

使用入门

在设置完成之前，“HP ProtectTools 设置向导”会自动显示为 HP ProtectTools Security Manager 的默认页。

要设置 Security Manager，请执行以下步骤：

 **注：** 如果指纹识别器和智能卡均无法使用，请仅执行步骤 1、5 和 6。

1. 在“欢迎使用”页中，单击**下一步**。
2. 下一页将列出可以在此计算机上使用的验证方法。单击**下一步**继续。
3. 在“验证您的身份”页中，键入您的 Windows 密码，然后单击**下一步**。
4. 请参阅下面的一个或多个主题，具体取决于计算机的配置。
 - 如果指纹识别器可用，则请参阅[第 22 页的注册指纹](#)。
 - 如果智能卡可用，则请参阅[第 23 页的设置智能卡](#)。
5. 如果指纹识别器和智能卡均无法使用，则会要求您输入 Windows 密码。以后，只要需要进行验证，就必须使用该密码。
6. 在向导的最后一页中，单击**完成**。

将显示 Security Manager 控制板。

注册凭证

您可以使用“我的标识”页注册不同的验证方法或凭证。注册完成后，您可以使用这些方法登录 Security Manager。


注册指纹

如果您的计算机内置或连接了指纹识别器，则“HP ProtectTools 设置向导”将引导您完成设置或“注册”您的指纹的过程。


1. 阅读“欢迎使用”屏幕内容，然后单击**下一步**。
2. 验证您的身份：键入您的 Windows 密码（如果尚未注册指纹），或者使用指纹识别器扫描您的指纹。单击**下一步**。

如果您的 Windows 密码为空，则会要求您创建一个密码。要使用 HP ProtectTools Security Manager 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。

3. 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，请单击相应的指纹。

4. 在选择要注册的手指后，系统将提示您扫描该指纹，直至成功注册该手指。将使用绿色在轮廓上突出显示注册的手指。
5. 您必须至少注册两根手指；最好是食指或中指。对于其他手指，请重复步骤 3 和 4。
6. 单击**下一步**。

 **注：** 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。如果计算机处于非活动状态一段时间或者关闭了控制板，则**不会**保存所做的更改。

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，依次单击**我的身份、凭证和密码**。
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。

设置智能卡

如果计算机具有内置或连接的智能卡读卡器，Security Manager 将提示您设置智能卡 PIN（个人标识号）。

- 要设置智能卡 PIN，请在“设置智能卡”页中输入并确认 PIN。
- 要更改 PIN，请先键入旧 PIN，然后选择新 PIN。

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。

控制板包含以下组件：

- **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：
 - **我的身份**
 - **我的数据**
 - **我的电脑**
- **查找更多** — 打开一个页面，可以在其中查找其他应用程序以提高身份、数据以及通信的安全性。
- **主区域** — 显示应用程序特定的屏幕。
- **管理** — 打开 HP ProtectTools 管理控制台。
- **帮助按钮** — 显示当前屏幕的相关信息。
- **高级** — 用于访问以下选项：
 - **首选项** — 用于对 Security Manager 设置进行个性化设置。
 - **备份和恢复** — 用于备份或恢复数据。
 - **关于** — 显示 Security Manager 的版本信息。

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

打开 HP ProtectTools Security Manager

可以通过以下任一方式打开 HP ProtectTools 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。
- 右键单击 **HP ProtectTools** 图标，然后单击**打开 HP ProtectTools Security Manager**。
- 单击 Windows 边栏上的 **Security Manager ID 卡** 小工具。
- 按 **ctrl+alt+h** 组合热键以打开“Security Manager 快速链接”菜单。

常规任务

该组中包含的应用程序可帮助您管理数字身份的几个方面。

- **Security Manager** — 创建并管理快速链接，这些链接允许您通过 Windows 密码、您的指纹或智能卡进行验证以启动并登录网站和程序。
- **凭证** — 提供一种轻松更改 Windows 密码、注册指纹或设置智能卡的方法。

要添加更多应用程序，请单击控制板左下角的 [+] **查找更多** 按钮。管理员可能已禁用该按钮。

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。

还可以通过 Password Manager 图标来使用很多 Password Manager 功能，在网页或程序登录屏幕具有焦点时将显示该图标。单击该图标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 Password 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，然后提交该页面（如果在创建登录或上次编辑登录时指定了提交）。
- **编辑登录** — 用于编辑此网站的登录数据。
- **添加新帐户** — 用于在登录中添加帐户。
- **打开 Password Manager** — 启动 Password Manager 应用程序。
- **帮助** — 显示 Password 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**添加登录**来显示此对话框。某些选项取决于计算机连接的安全保护设备；例如，使用 **ctrl+alt+H** 热键、扫描指纹或插入智能卡。
 - 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。
 - 要将屏幕上的其他字段添加到登录中，请单击**选择其他字段**。
 - 要填充登录字段，但不提交，请清除**提交登录数据**复选框。
 - 要查看此登录的密码，请单击**显示密码**。
4. 单击**确定**。

将从 Password Manager 图标中删除加号，以通知您已创建登录。

每次访问该网站或打开该程序时，将显示 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。
 - 要将屏幕上的其他字段添加到登录中，请单击**选择其他字段**。
 - 要填充登录字段，但不提交，请清除**提交登录数据**复选框。
 - 要查看此登录的密码，请单击**显示密码**。
4. 单击**确定**。

使用“登录”菜单

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+alt+h 是出厂设置。要更改组合热键，请单击 **Password Manager**，然后单击**设置**。
2. 扫描指纹（在具有内置或连接的指纹识别器的计算机上）。

将登录划分到不同类别中

可通过创建一个或多个类别，使用类别秩序井然地划分登录。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。在将鼠标移到类别上时，将会突出显示这些类别。
4. 在突出显示所需的类别时，松开鼠标按钮。

不会将登录移到该类别中，而只是将其复制到选定类别中。您可以将相同登录添加到多个类别中，并通过单击**全部**显示所有登录。

管理登录

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

“管理”标签中列出了您的登录。如果为同一网站创建了多个登录，则会在登录列表中该网站名称下面以缩进方式列出每个登录。

要管理登录，请执行以下操作：

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。
- **编辑登录** — 单击某个登录，单击**编辑**，然后更改登录数据。
- **删除登录** — 单击某个登录，然后单击**删除**。

要为网站或程序添加其他登录，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** 图标以显示其快捷菜单。
3. 单击**添加其他登录**，然后按照屏幕上的说明进行操作。

评估您的密码强度

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。

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 不再提示您为此登录屏幕添加登录。

要访问其他 Password Manager 设置，请单击 **Password Manager**，然后单击 Security Manager 控制板上的**设置**。

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+alt+H 打开 Password Manager** — 打开“Password Manager 快速链接”菜单的默认热键是 **ctrl+alt+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。

凭证

可以使用 Security Manager 凭证验证您是否为所声称的那个人。此计算机的本地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。

可用的凭证可能会因此计算机内置或连接的安全保护设备而有所不同。每个支持的凭证在**我的身份、凭证**组中具有一个条目。

将列出可用凭证、要求和当前状态，并且可能包含以下内容：

- 指纹
- 密码
- 智能卡

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。

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，并且还会以 Windows 边栏小工具形式进行显示。

可以使用很多方法快速访问 Security Manager，单击 Windows 边栏中的 ID 卡就是其中的一种。

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. 从 Security Manager 控制板中，单击左上角的 **ID 卡**。
2. 单击显示为 Windows 中的帐户输入的名称的框。系统将显示该帐户的 Windows 用户名。
3. 要更改此名称，请键入新名称，然后单击**保存按钮**。

要更改显示的图片，请执行以下操作：

1. 从 Security Manager 控制板中，单击**我的身份**，然后单击左上角的 **ID 卡**。
2. 单击**选择图片按钮**，单击一个图像，然后单击**保存按钮**。

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

“常规”标签上提供了以下设置：

外观 — 在任务栏上显示图标

要允许在任务栏上显示图标，请选中该复选框。

要禁止在任务栏上显示图标，请清除该复选框。

指纹

“指纹”标签上提供了以下设置：

快速操作 — 可以使用快速操作选择在扫描指纹的同时按住指定键时执行的 Security Manager 任务。

要为列出的某个键指定快速操作，请执行以下操作：

- 单击一个（键）+**指纹**选项，然后单击菜单中的某个可用任务。


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声音，或者清除此选项以禁用声音反馈。
- **显示扫描质量反馈** — 默认情况下，只要指纹扫描质量无法满足身份验证要求，Security Manager 就会显示一个带有问号的指纹图像。可通过清除此选项来禁止显示此图像。

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. 在左面板中，单击**高级**，然后单击**备份和恢复**。
2. 单击**备份数据**。
3. 选择要包含在备份中的模块。大多数情况下，您希望选择所有模块。
4. 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。
5. 输入密码以保护该文件。
6. 验证您的身份。
7. 单击**完成**。


要恢复数据，请执行以下操作：

1. 在左面板中，单击**高级**，然后单击**备份和恢复**。
2. 单击**恢复数据**。
3. 选择以前创建的存储文件。您可以在提供的字段中输入路径，或者单击**编辑**。
4. 输入用于保护该文件的密码。
5. 选择要恢复数据的模块。大多数情况下，将选择列出的所有模块。
6. 单击**完成**。

添加应用程序

可以添加其他应用程序，以便为此程序提供新功能。

从 Security Manager 控制板中，单击 **[+] 查找更多** 以浏览其他应用程序。

 **注：** 如果控制板左下角没有 **[+] 查找更多** 链接，则说明此计算机的管理员已将其禁用。

安全应用程序状态

“Security Manager 应用程序状态”页显示安装的安全应用程序的总体状态。它显示设置的应用程序及其设置状态。在打开 Security Manager 控制板或单击**安全应用程序**时，将自动显示该摘要。

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

△ **注意：** 如果决定卸载 Drive Encryption 模块，您必须首先解密所有已加密的驱动器。如果未成功解密，您将无法访问加密驱动器上的数据，除非已注册使用 Drive Encryption 恢复服务。重新安装 Drive Encryption 模块也无法访问加密驱动器。

Drive Encryption for HP ProtectTools 模块通过加密笔记本电脑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 设置向导”，Windows 管理员可以激活 Drive Encryption、备份加密密钥、添加和删除用户以及停用 Drive Encryption。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：

- 加密管理
 - 加密或解密各个驱动器
-
- 🔑 **注：** 只能加密内置硬盘驱动器。
- 恢复
 - 创建备份密钥
 - 执行恢复操作

设置步骤


打开 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

激活 Drive Encryption

使用 HP ProtectTools 设置向导激活 Drive Encryption。

 **注：** 还可以使用此向导添加和删除用户。

- 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**，然后单击**功能**。
3. 选择 **Drive Encryption** 复选框，然后单击**下一步**。
4. 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。
5. 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。

6. 在**用于保存加密密钥的外部存储设备**下，选择用于保存加密密钥的存储设备旁的复选框。
7. 单击**应用**。

Drive Encryption 启用。

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

停用 Drive Encryption

请使用“HP ProtectTools 设置向导”停用 Drive Encryption。有关详细信息，请参阅 HP ProtectTools Security Manager 软件帮助。


- 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**，然后单击**功能**。
3. 清除 **Drive Encryption** 复选框，然后单击**应用**。


Drive Encryption 启用。

在激活 Drive Encryption 后登录

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

 **注：** 如果 Windows 管理员在 HP ProtectTools Security Manager 中启用了启动前安全保护功能，将在打开笔记本电脑后立即登录到笔记本电脑，而不是在 Drive Encryption 登录屏幕上登录。


1. 单击您的用户名，然后键入 Windows 密码或 Java™ 卡个人标识号，或者扫描经过注册的手指。
2. 单击**确定**。

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

通过加密硬盘驱动器保护您的数据


使用“HP ProtectTools 设置向导”通过加密硬盘驱动器保护您的数据：

1. 在 Security Manager 中，单击**使用入门**，然后单击 **Security Manager 设置**图标。将启动一个介绍 Security Manager 功能的演示（也可以从“Drive Encryption”页中启动 Security Manager）。
2. 在左窗格中单击 **Drive Encryption**，然后单击**加密管理**。
3. 单击**更改加密**。
4. 选择要加密的驱动器。

 **注：** 强烈建议您加密硬盘驱动器。

显示加密状态

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

 **注：** 必须使用 HP ProtectTools 管理控制台更改驱动器加密状态。

1. 打开 **HP ProtectTools Security Manager**。
2. 在**我的数据**下，单击**加密状态**。

如果激活了 Drive Encryption，驱动器状态将显示以下一种状态代码：

- 活动
- 不活动
- 未加密
- 已加密
- 正在加密
- 正在解密

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）


管理员可以通过“加密管理”页查看和更改 Drive Encryption 的状态（活动或非活动），以及查看笔记本计算机上所有硬盘驱动器的加密状态。

- 如果状态为“非活动”，则表明 Windows 管理员尚未在 HP ProtectTools Security Manager 中激活 Drive Encryption，而没有为硬盘驱动器提供保护。请使用“HP ProtectTools Security Manager 设置向导”激活 Drive Encryption。
- 如果状态为“活动”，表明已经激活并配置了 Drive Encryption。驱动器处于以下状态之一：
 - 未加密
 - 已加密
 - 正在加密
 - 正在解密

加密或解密各个驱动器

如果您要对笔记本计算机上的一个或多个硬盘驱动器加密或者要解密已经加密的驱动器，请使用“更改加密”功能：

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

 **注：** 在加密或解密驱动器时，进度栏会显示完成当前会话过程所需的剩余时间。如果在加密过程中，笔记本计算机关机或进入了睡眠或休眠模式，重新启动后剩余时间显示会重置到开头，不过实际上加密会从上次停止的位置继续。剩余时间和进度显示会很快发生变化，以反映之前的进度。


备份和恢复（管理员任务）

管理员可以通过“恢复”页备份和恢复加密密钥。

本地 Drive Encryption 密钥备份 — 激活 Drive Encryption 后，可将加密密钥备份到可移动介质中。

创建备份密钥

您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：** 确保将包含备份密钥的存储设备存放在安全位置，因为如果您忘记密码或丢失了 Java 卡，则只能使用该设备访问硬盘驱动器。

1. 打开 **HP ProtectTools 管理控制台**，单击 **Drive Encryption**，然后单击**恢复**。
2. 单击**备份密钥**。
3. 在“选择备份磁盘”页上，选择要用来备份加密密钥的设备旁的复选框，然后单击**下一步**。


4. 阅读下一页显示的信息，然后单击**下一步**。加密密钥随即保存在您选择的存储设备上。
5. 确认对话框打开时，请单击**完成**。

执行恢复

要在忘记密码时执行恢复，请执行以下步骤：

1. 打开笔记本电脑。
2. 插入包含备份密钥的可移动存储设备。
3. 在打开 Drive Encryption for HP ProtectTools 登录对话框时，单击**取消**。
4. 在屏幕左下角单击**选项**，然后单击**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**。

笔记本电脑将启动。

 **注：** 极力建议您执行恢复操作后重置密码。

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

借助于 HP ProtectTools Privacy Manager，您可以在使用电子邮件、Microsoft® Office 文档或即时消息 (IM) 时使用高级安全登录（验证）方法保证通信的来源、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
- HP ProtectTools Java™ 卡

您可以在 Privacy Manager 中使用以上任何安全登录方法。

Privacy Manager 要求具备下列条件：

- HP ProtectTools Security Manager 5.00 或更高版本
- Windows® 7、Windows Vista® 或 Windows XP 操作系统
- Microsoft Outlook 2007 或 Microsoft Outlook 2003
- 有效电子邮件帐户

 **注：** 必须先从 Privacy Manager 中请求并安装 Privacy Manager 证书（一种数字证书），然后才能访问安全保护功能。有关请求 Privacy Manager 证书的信息，请参阅[第 39 页的请求并安装 Privacy Manager 证书](#)。

设置步骤

打开 Privacy Manager

要打开 Privacy Manager，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. 单击 **Privacy Manager**。

- 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 **Configuration**（配置）。

- 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**证书或可信联系人**。

- 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**证书或可信联系人**。

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。

您可以执行以下任务：

- 申请并安装 Privacy Manager 证书
- 查看 Privacy Manager 证书详细信息
- 续订 Privacy Manager 证书
- 设置 Privacy Manager 使用的默认 Privacy Manager 证书（如果有多个可用证书）
- 删除并吊销 Privacy Manager 证书（高级）

请求并安装 Privacy Manager 证书

在使用 Privacy Manager 功能之前，您必须使用有效的电子邮件地址申请并安装 Privacy Manager 证书（从 Privacy Manager 中）。在从中申请 Privacy Manager 证书的不同计算机上，必须在 Microsoft Outlook 中将此电子邮件地址设置为帐户。

申请 Privacy Manager 证书

1. 打开 Privacy Manager，然后单击**证书**。
2. 单击**申请 Privacy Manager 证书**。
3. 阅读“欢迎使用”页上的文本，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**选中此框以接受此许可协议的条款**旁边的复选框，然后单击**下一步**。
6. 在“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**。
8. 单击**确定**以关闭证书。

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

获取预先指定的 Privacy Manager 企业证书

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**。
3. 将会在 Microsoft Outlook 中收到一封电子邮件，其中附加了 Privacy Manager 证书。
4. 要安装证书，请参阅[第 40 页的安装 Privacy Manager 证书](#)。

安装 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，请从[第 43 页的使用 Microsoft Outlook 联系人添加可信联系人](#)主题的第 2 步开始按照屏幕上的说明进行操作。

- 或 -

如果单击**取消**，请参阅[第 43 页的添加可信联系人](#)以了解有关以后添加可信联系人的信息。

查看 Privacy Manager 证书详细信息

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

续订 Privacy Manager 证书

当 Privacy Manager 证书快要过期时，将会通知您需要续订证书：

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


 **注：** Privacy Manager 证书续订过程并不会替换旧 Privacy Manager 证书。您需要购买新的 Privacy Manager 证书，并使用与[第 39 页的请求并安装 Privacy Manager 证书](#)相同的过程安装证书。

设置默认 Privacy Manager 证书

Privacy Manager 中只显示 Privacy Manager 证书，即使在计算机上安装了来自其他认证机构的其他证书。

如果在计算机上通过 Privacy Manager 安装了多个 Privacy Manager 证书，您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**设置默认值**。
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 Privacy Manager 证书，则无法打开使用该证书加密的任何文件，也无法查看使用该证书加密的任何数据。如果误删了 Privacy Manager 证书，可使用在安装该证书时创建的备份文件进行恢复。有关详细信息，请参阅[第 41 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**。
6. 单击**确定**。

有关详细信息，请参阅[第 40 页的安装 Privacy Manager 证书](#)或[第 54 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 证书安全受到了危害，您可以吊销您自己的证书：

 **注：** 并不会删除吊销的 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 通讯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其计算机上安装 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>。

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一个或多个电子邮件地址。
5. 编辑文本并签上您的名字（可选）。
6. 单击**发送**。

 **注：** 如果尚未获得 Privacy Manager 证书，则会显示一条消息，通知您必须具有 Privacy Manager 证书才能发送可信联系人请求。请单击**确定**以启动证书请求向导。有关详细信息，请参阅[第 39 页的请求并安装 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**邀请我的所有 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. 当打开“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：** 如果尚未获得 Privacy Manager 证书，则会显示一条消息，通知您必须具有 Privacy Manager 证书才能发送可信联系人请求。请单击**确定**以启动证书请求向导。有关详细信息，请参阅[第 39 页的请求并安装 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
- Windows Live Messenger

在 Microsoft Outlook 中使用 Privacy Manager

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

- 签名并发送（仅“安全发送”按钮）—此选项可在电子邮件中添加数字签名并在您使用选择的安全登录方法进行验证后发送该电子邮件。
- 为可信联系人密封并发送（仅“安全发送”按钮）—此选项可在电子邮件中添加数字签名，加密电子邮件，并在您使用选择的安全登录方法进行验证后发送该电子邮件。
- 邀请联系人—此选项允许您发送可信联系人邀请。有关详细信息，请参阅[第 43 页的添加可信联系人](#)。
- 邀请 Outlook 联系人—此选项允许您向 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 43 页的使用 Microsoft Outlook 联系人添加可信联系人](#)。
- 打开 Privacy Manager 软件—“证书”、“可信联系人”和“设置”选项允许您打开 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 45 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**旁边的向下箭头（在 Outlook 2003 中为**隐私**），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

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**旁边的向下箭头（在 Outlook 2003 中为**隐私**），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。

密封并发送电子邮件

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**旁边的向下箭头（在 Outlook 2003 中为**隐私**），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凭证
- 用于验证电子邮件签名者的凭证的产品

在 Microsoft Office 2007 文档中使用 Privacy Manager

 **注：** Privacy Manager 只能与 Microsoft Office 2007 文档配合使用。

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—此选项向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，对 Microsoft Word 或 Microsoft Excel 文档进行签名或加密时会添加签名行。要禁用此选项，请单击**添加签名行**以清除复选标记。
- 加密文档—此选项添加数字签名并加密文档。
- 删除加密—此选项从文档中删除加密。
- 打开 Privacy Manager 软件—“证书”、“可信联系人”和“设置”选项允许您打开 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 39 页的管理 Privacy Manager 证书](#)、[第 42 页的管理可信联系人](#)或[第 46 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。

在对 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。

在 Microsoft Word 或 Microsoft Excel 文档中添加建议的签名者


可通过指定建议的签名者，在文档中添加多个签名行。建议的签名者是指由 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，也可以是另一个您希望其对文档进行签名的人。例如，如果您准备一份需要由部门的所有成员签名的文档，则可以在文档的最后一页底部包含这些用户的签名行，并提供按特定日期签名的说明。

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：** 由于文档所有者为其文档指定了建议的签名者，因此，如果未选中**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，建议的签名者将无法在签名行中显示日期和/或职务，即使将建议的签名者的文档设置配置为显示这些信息。

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。在加密文档并将其关闭后，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，请执行第 48 页的**从 Microsoft Office 文档中删除加密**中的步骤。在删除加密后，您可以对文档进行编辑。请按照此部分中的步骤重新加密文档。

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，这与通常发送带有附件的普通电子邮件完全一样。

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 46 页的密封并发送电子邮件](#)。

查看签名的 Microsoft Office 文档

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

打开签名的 Microsoft Office 文档后，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**图标可切换“签名”对话框的显示，其中显示对文档进行签名的所有用户的名称和每个用户的签名日期。
2. 要查看有关每个签名的其他详细信息，请右键单击“签名”对话框中的名称，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。另外，还必须恢复用于加密该文件的 Privacy Manager 证书。


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。

在 Windows Live Messenger 中使用 Privacy Manager

Privacy Manager 在 Windows Live Messenger 中添加了以下安全通信功能：

- **安全聊天**—使用 XML 协议的 SSL/TLS（安全套接字层/传输层安全性）来传输消息，该技术同样确保电子商务交易的安全。
- **收件人标识**—您可以在发送消息前确认收件人是否存在及其身份。
- **签名的消息**—您可以以电子方式对消息进行签名。此后，如果消息被篡改，在收件人收到消息时，它将被标记为无效。
- **显示/隐藏功能**—您可以隐藏 Privacy Manager Chat 窗口中的任意或全部消息。也可以发送隐藏内容的消息。需要先进行验证，然后才能显示消息。
- **安全聊天历史记录**—您的聊天会话日志在保存之前会进行加密，而且需要验证才能查看。
- **自动锁定/取消锁定**—您可以锁定和取消锁定 Privacy Manager Chat 窗口或将其设置为指定的不活动时间后自动锁定。

启动 Privacy Manager Chat 会话

 **注：** 要使用 Privacy Manager Chat，双方必须安装 Privacy Manager 和 Privacy Manager 证书。有关安装 Privacy Manager 证书的详细信息，请参阅[第 39 页的请求并安装 Privacy Manager 证书](#)。


1. 要在 Windows Live Messenger 中启动 Privacy Manager Chat，请执行以下任一过程：
 - a. 在 Live Messenger 中右键单击某个在线联系人，然后选择 **Start an Activity**（开始一个活动）。
 - b. 单击 **Start Chat**（开始聊天）。

- 或 -

 - a. 在 Live Messenger 中双击某个在线联系人，然后选择 **See a list of activities**（查看活动列表）菜单。
 - b. 单击 **Action**（操作），然后单击 **Start Chat**（开始聊天）。

- 或 -

 - a. 右键单击通知区域中的 ProtectTools 图标，再单击 **HP ProtectTools Privacy Manager**，然后选择 **Start Chat**（开始聊天）。
 - b. 在 Live Messenger 中，单击 **Actions:Start an Activity**（操作：开始一个活动），然后选择 **Privacy Manager Chat**。

 **注：** 每个用户都必须在 Live Messenger 中在线，而且必须显示在彼此的 Live Messenger 在线窗口中。单击以选择在线用户。

Privacy Manager 将向该联系人发送邀请以启动 Privacy Manager Chat。当被邀请的联系人接受邀请时，将打开 Privacy Manager Chat 窗口。如果被邀请的联系人没有 Privacy Manager，系统将提示他或她进行下载。

2. 单击**开始**以开始安全聊天。

为 Windows Live Messenger 配置 Privacy Manager

1. 在 Privacy Manager Chat 中，单击**设置**按钮。

- 或 -

在 Privacy Manager 中，单击**设置**，然后单击**聊天**标签。

- 或 -

在 Privacy Manager Live Messenger 历史记录查看器中，单击**设置**按钮。
2. 要指定 Privacy Manager Chat（隐私管理器聊天）锁定会话之前等待的时间，请从 **Lock session after _ minutes of inactivity**（在处于不活动状态 _ 分钟后锁定会话）框中选择一个数字。
3. 要为聊天会话指定历史记录文件夹，请单击**浏览**以查找文件夹，然后单击**确定**。
4. 要在关闭会话时自动加密并保存会话，请选中**自动保存安全聊天历史记录**复选框。
5. 单击**确定**。

在 Privacy Manager Chat 窗口中聊天

在启动 Privacy Manager Chat 后，将在 Windows Live Messenger 中打开 Privacy Manager Chat 窗口。Privacy Manager Chat 的使用方式与基本 Windows Live Messenger 类似，所不同的是 Privacy Manager Chat 窗口中提供了以下附加功能：

- **保存**—单击此按钮可将您的聊天会话保存到在配置设置中指定的文件夹。也可以将 Privacy Manager Chat 设置为在关闭每个会话时自动对其进行保存。
- **全部隐藏和全部显示**—单击相应按钮可展开或折叠“安全通信”窗口中的所有消息。也可以通过单击消息标题隐藏或显示各条消息。
- **在吗?**—单击此按钮可要求您的联系人进行验证。
- **锁定**—单击此按钮可关闭 Privacy Manager Chat 窗口并返回 Chat Entry（聊天入口）窗口。要再次显示“安全通信”窗口，请单击**恢复会话**，然后使用所选的安全登录方法进行验证。
- **发送**—单击此按钮可将加密的消息发送给您的联系人。
- **发送签名的**—选中此复选框可以电子方式对消息进行签名并加密。此后，如果消息被篡改，在收件人收到消息时，它将被标记为无效。每次发送签名的消息时，都必须对其进行验证。
- **发送隐藏的**—选中此复选框可加密并发送仅显示消息标题的消息。联系人必须进行验证才能阅读消息的内容。

查看聊天历史记录

Privacy Manager Chat: Live Messenger 历史记录查看器会显示加密的 Privacy Manager Chat 会话文件。可通过在 Privacy Manager Chat 窗口中单击**保存**来保存会话，或者在 Privacy Manager 的“聊天”标签中配置自动保存。在此查看器中，每个会话显示（加密的）联系人屏幕名称以及会话的开始和结束日期和时间。默认情况下，为设置的所有电子邮件帐户显示会话。可以使用**显示历史记录**菜单仅选择要查看的特定帐户。

在此查看器中，您可以执行以下任务：

- [第 52 页的显示所有会话](#)
- [第 52 页的显示特定帐户的会话](#)
- [第 52 页的查看会话 ID](#)
- [第 52 页的查看会话](#)
- [第 52 页的在会话中搜索特定文本](#)
- [第 53 页的删除会话](#)
- [第 53 页的添加或删除列](#)
- [第 53 页的过滤显示的会话](#)

要启动 Live Messenger 历史记录查看器，请执行以下操作：

- ▲ 在工具栏最右侧的通知区域，右键单击 **HP ProtectTools** 图标，再单击 **HP ProtectTools Privacy Manager**，然后单击 **Live Messenger 历史记录查看器**。

- 或 -

- ▲ 在聊天会话中，单击**历史记录查看器**或**历史记录**。

显示所有会话

通过显示所有会话，可为当前选定的会话以及相同帐户中的所有会话显示解密的联系人屏幕名称。

要显示所有保存的聊天历史记录会话，请执行以下操作：


1. 在 Live Messenger 历史记录查看器中，右键单击任何会话，然后选择**显示所有会话**。
2. 使用所选的安全登录方法进行验证。
将解密联系人屏幕名称。
3. 双击任何会话以查看其内容。

显示特定帐户的会话

通过显示某个会话，可为当前选定的会话显示解密的联系人屏幕名称。

要显示特定聊天历史记录会话，请执行以下操作：

1. 在 Live Messenger 历史记录查看器中，右键单击任何会话，然后选择**显示会话**。
2. 使用所选的安全登录方法进行验证。
将解密联系人屏幕名称。
3. 双击显示的会话以查看其内容。

 **注：** 使用相同证书加密的其他会话将显示解锁图标，表明通过双击其中的任何会话即可进行查看，而无需进行额外的验证。使用不同证书加密的会话将显示锁定图标，表明这些会话需要进行进一步的验证，然后才能查看联系人屏幕名称或内容。

查看会话 ID

要查看会话 ID，请执行以下操作：

- ▲ 在 Live Messenger 历史记录查看器中，右键单击显示的任何会话，然后选择**查看会话 ID**。

查看会话

查看会话时，将打开要查看的文件。如果以前未显示该会话（显示解密的联系人屏幕名称），将会同时显示该会话。

要查看 Live Messenger 历史记录会话，请执行以下操作：

1. 在 Live Messenger 历史记录查看器中，右键单击任何会话，然后选择**查看**。
2. 如果出现提示，请使用所选的安全登录方法进行验证。
将解密会话内容。

在会话中搜索特定文本

只能在查看器窗口中显示的（解密）会话中搜索文本。在这些会话中，将以纯文本显示联系人屏幕名称。

要在聊天历史记录会话中搜索文本，请执行以下操作：

1. 在 Live Messenger 历史记录查看器中，单击**搜索**按钮。
2. 输入搜索文本，配置所需的任何搜索参数，然后单击**确定**。

将在查看器窗口中突出显示包含该文本的会话。

删除会话

1. 选择一个聊天历史记录会话。
2. 单击**删除**。

添加或删除列

默认情况下，Live Messenger 历史记录查看器中显示三个最常用的列。可以添加要显示的其他列，也可以删除显示的列。

要添加显示的列，请执行以下操作：

1. 右键单击任何列标题，然后选择**添加/删除列**。
2. 在左面板中选择一个列标题，然后单击**添加**以将其移到右面板中。

要删除显示的列，请执行以下操作：

1. 右键单击任何列标题，然后选择**添加/删除列**。
2. 在右面板中选择一个列标题，然后单击**删除**以将其移到左面板中。

过滤显示的会话

Live Messenger 历史记录查看器中显示所有帐户的会话列表。也可以按以下条件过滤显示的会话：

- 特定帐户。有关详细信息，请参阅[第 53 页的显示特定帐户的会话](#)。
- 日期范围。有关详细信息，请参阅[第 53 页的显示某个日期范围的会话](#)。
- 不同的文件夹。有关详细信息，请参阅[第 53 页的显示非默认文件夹中保存的会话](#)。

显示特定帐户的会话

- ▲ 在 Live Messenger 历史记录查看器中，从**显示历史记录**菜单中选择一个帐户。

显示某个日期范围的会话

1. 在 Live Messenger 历史记录查看器中，单击**高级过滤器**图标。
将打开“高级过滤器”对话框。
2. 选中**仅显示指定日期范围内的会话**复选框。
3. 在**起始日期**和**截至日期**框中，输入日、月和/或年，或者单击日历旁边的箭头以选择日期。
4. 单击**确定**。

显示非默认文件夹中保存的会话

1. 在 Live Messenger 历史记录查看器中，单击**高级过滤器**图标。
2. 选中**使用备用历史记录文件文件夹**复选框。
3. 输入文件夹位置，或者单击**浏览**以查找文件夹。
4. 单击**确定**。

高级任务


将 Privacy Manager 证书和可信联系人迁移到其他计算机上

可以安全地将 Privacy Manager 证书和可信联系人迁移到其他计算机上，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“已保存迁移文件”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他证书颁发机构颁发的数字证书。
- **加密策略** — 可能在 Microsoft Office 或 Outlook 以及 Windows Live Messenger 中分别启用或禁用了加密功能。

9 HP ProtectTools File Sanitizer

通过 File Sanitizer 工具，您可以安全地碎化计算机上的资产（个人信息或文件、历史数据或与 Web 有关的数据或其他数据组件），并定期清理硬盘驱动器。


 **注：** 这一版本的 File Sanitizer 只支持系统硬盘驱动器。

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），因为在使用 File Sanitizer 碎化资产时，将调用一个遮盖数据的算法，此算法使得您几乎无法检索原始资产。在硬盘驱动器上或在可以使用取证方法恢复文件（或资产）的情况下，Windows 简单删除操作可使文件（或资产）保持完好无损。

当您选择碎化配置文件（高安全保护、中安全保护或低安全保护）后，将自动选择用于进行碎化的预定义资产列表和清除方法。也可以自定义碎化配置文件，通过该文件可以指定碎化周期数、包括在碎化中的资产、碎化前要确认的资产以及要从碎化中排除的资产。有关详细信息，请参阅[第 59 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，也可以在需要时手动碎化资产。有关详细信息，请参阅[第 58 页的设置碎化计划](#)、[第 62 页的手动碎化一个资产](#)或[第 62 页的手动碎化所有选定项目](#)。

 **注：** 仅当将 .dll 文件移到回收站时，才能对其进行碎化并从系统中删除。

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，直至其他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：** 可用空间清理适用于使用 Windows 回收站删除的资产或手动删除的资产。可用空间清理没有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，也可以使用任务栏最右侧通知区域中的 **HP ProtectTools** 图标手动激活可用空间清理。有关详细信息，请参阅 [第 58 页的设置可用空间清理计划](#) 或 [第 62 页的手动激活可用空间清理](#)。

设置步骤

打开 File Sanitizer

要打开 File Sanitizer，请执行以下操作：

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

2. 单击 **File Sanitizer**。


- 或 -

▲ 双击位于桌面上的 **File Sanitizer** 图标。

- 或 -

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

设置碎化计划


 **注：** 有关选择预定义碎化配置文件或创建碎化配置文件的信息，请参阅[第 59 页的选择或创建碎化配置文件](#)。

注： 有关手动碎化资产的信息，请参阅[第 62 页的手动碎化一个资产](#)。


1. 打开 File Sanitizer，然后单击**碎化**。

2. 选择一个碎化选项：

- **Windows 关机** — 选择此选项可在 Windows 关机时碎化所有所选资产。


 **注：** 选择此选项后，将在关机时显示一个对话框，询问您是否继续碎化所选资产，或是否跳过此过程。单击**是**可跳过碎化过程，单击**否**可继续碎化。

- **打开 Web 浏览器** — 选择此选项可以在打开 Web 浏览器时碎化所有与 Web 有关的所选资产（如浏览器 URL 历史记录）。
- **退出 Web 浏览器** — 选择此选项可以在关闭 Web 浏览器时碎化所有与 Web 有关的所选资产（如浏览器 URL 历史记录）。
- **按键序列** — 选择此选项可使用按键序列启动碎化。
- **调度程序** — 选中**激活调度程序**复选框，输入 Windows 密码，然后输入要碎化所选资产的日期和时间。

 **注：** 仅当将 .dll 文件移到回收站时，才能对其进行碎化并从系统中删除。


3. 单击**应用**，然后单击**确定**。

设置可用空间清理计划

 **注：** 可用空间清理适用于使用 Windows 回收站删除的资产或手动删除的资产。可用空间清理没有为碎化的资产提供额外的安全保护。

要设置可用空间清理计划，请执行以下操作：

1. 打开 File Sanitizer，然后单击**可用空间清理**。
2. 选中**激活计划程序**复选框，输入 Windows 密码，然后输入清理硬盘驱动器的日期和时间。
3. 单击**应用**，然后单击**确定**。

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

选择或创建碎化配置文件

通过选择预定义配置文件或创建您自己的配置文件，可以指定一种清除方法并选择要碎化的资产。

选择预定义碎化配置文件

在选择预定义碎化配置文件（高安全保护、中安全保护或低安全保护）时，将会自动选择一种预定义清除方法和一个资产列表。可以单击**查看详细信息**按钮，以查看为碎化选择的预定义资产列表。


要选择预定义碎化配置文件，请执行以下操作：

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。
3. 单击**查看详细信息**以查看为碎化选择的资产列表。
4. 在**碎化以下内容**下，选中要在碎化之前进行确认的每个资产旁边的复选框。
5. 单击**应用**，然后单击**确定**。


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，单击**设置**，单击**高级安全设置**，然后单击**查看详细信息**。
2. 指定碎化周期数。

 **注：** 将对每个资产执行所选碎化周期数。例如，如果您选择 3 个碎化周期，则将单独执行 3 次遮盖数据的算法。如果您选择的安全保护碎化周期数较大，则碎化可能需要相当长的时间；然而，您指定的碎化周期数越大，所能检索的数据就越少。


3. 选择要碎化的资产：
 - 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**，然后浏览至文件名或文件夹，或键入文件名或文件夹的路径。单击**打开**，然后单击**确定**。在**可用碎化选项**下，单击自定义资产，然后单击**添加**。

 **注：** 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. 在**碎化以下内容**下，选中要在碎化前进行确认的每个资产旁边的复选框。

 **注：** 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不被自动碎化，在**不要碎化以下内容**下，单击**添加**，然后浏览至文件名或文件夹，或键入文件名或文件夹的路径。单击**打开**，然后单击**确定**。

 **注：** 要从排除列表中删除资产，请单击该资产，然后单击**删除**。

6. 配置完碎化配置文件时，单击**应用**，然后单击**确定**。


自定义简单删除配置文件

简单删除配置文件只执行标准资产删除，而不进行碎化。当您自定义简单删除配置文件时，可以为简单删除指定要包括的资产、执行简单删除前要确认的资产以及要从简单删除中排除的资产。


 **注：** 如果使用简单删除选项，则可不定期执行可用空间清理功能清理通过 Windows 回收站删除的资产或手动删除的资产。

要自定义简单删除配置文件，请执行以下操作：


1. 打开 File Sanitizer，单击**设置**，单击**简单删除设置**，然后单击**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**，输入文件名或文件夹名，然后单击**确定**。单击自定义资产，然后单击**添加**。

 **注：** 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. 在**删除以下内容**下，选中要在删除之前进行确认的每个资产旁边的复选框。

 **注：** 要从删除列表中删除资产，请单击该资产，然后单击**删除**。

4. 在**不要删除以下内容**下，单击**添加**以选择要从碎化中排除的特定资产。


 **注：** 要从排除列表中删除资产，请单击该资产，然后单击**删除**。

5. 配置完简单删除配置文件时，单击**应用**，然后单击**确定**。

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 61 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 61 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 62 页的手动碎化一个资产](#)或[第 62 页的手动碎化所有选定项目](#)。
- 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 62 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 63 页的终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 63 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

要指定按键序列，请执行以下步骤：

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他按键序列。

要使用按键序列启动碎化，请执行以下操作：

1. 在按下所选字符的同时，按住 **shift** 键和 **ctrl** 键或 **alt** 键（或指定的任何组合键）。
2. 如果打开确认对话框，请单击**是**。

使用 File Sanitizer 图标

 **注意：** 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. 把资产拖放到桌面中的 File Sanitizer 图标上。
3. 在打开确认对话框时，单击**是**。

手动碎化一个资产

△ **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键单击 **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：** 所选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**。

手动碎化所有选定项目

1. 在任务栏最右侧的通知区域中右键单击 **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. 右键单击桌面上的**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键单击 **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**。

终止碎化或可用空间清理操作


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

要终止该操作，请执行以下操作：

- ▲ 单击该消息，然后单击**停止**以取消该操作。

查看日志文件

每次执行碎化或可用空间清理操作时，都会生成任何错误或故障的日志文件。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。

为碎化操作创建一个日志文件，并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的以下路径中：

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

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

Windows® 操作系统管理员可使用 HP ProtectTools 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。
- 还可以将用户组成若干个组（例如预定义的“设备管理员”组），或者使用“控制面板”的“管理工具”部分中的“计算机管理”选项定义组。
- 可以根据组成员资格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。

还可向有限的用户授予读取和修改设备访问控制策略的权限。

设置步骤

打开 Device Access Manager

要打开 Device Access Manager，请按照下列步骤进行操作：

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 **Device Access Manager**。

配置设备访问权限


HP ProtectTools Device Access Manager 提供三个视图：

- “简单配置”视图，用于允许或拒绝“设备管理员”组成员对各类别设备的访问。
- “设备类别配置”视图，用于授予或拒绝特定用户或组对各类型设备或特定设备的访问权限。
- “用户访问设置”视图，用于指定哪些用户可以查看或修改“简单配置”和“设备类别配置”信息。

设备管理员组

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

系统管理员可以实施简单的设备访问控制策略，即除非用户被归类为可信（关于设备访问），否则拒绝其对一组设备类别的访问。区分“设备信任的”用户和“非设备信任的”用户的建议方法是使所有“设备信任的”用户成为“设备管理员”组成员。通过“简单配置”或“设备类别配置”视图授予“设备管理员”组成员对设备的访问权限，可确保“设备信任的”用户具有对指定组的设备类别的完全访问权限。


 **注：** 将用户添加到“设备管理员”组并不会自动允许用户访问设备。但是，可以使用“简单配置”视图来授予“设备信任的”用户对所需设备类别组的访问权限。

要将用户添加到“设备管理员”组，请执行以下步骤：

- 对于 Windows 7、Vista 或 XP Professional，请使用标准“本地用户和组”MMC 管理单元。
- 对于 Windows 7、Vista® 或 XP 家庭版，可以使用特权帐户，在命令提示符窗口中输入：
`c:\> net localgroup "Device Administrators" username /ADD`

简单配置

管理员和授权用户可以使用“简单配置”视图修改所有非设备管理员对下列类别设备的访问权限：

 **注：** 为了使用此视图读取设备访问信息，必须在**用户访问设置**视图中授予用户或组“读”访问权限。为了使用此视图修改设备访问信息，必须在**用户访问设置**视图中授予用户或组“更改”访问权限。

- 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
- 所有红外设备


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

要允许或拒绝所有非设备管理员对一类设备的访问，请执行以下步骤：

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. 在右窗格中，要拒绝访问，请选中设备类别或特定设备的复选框。清除该复选框可允许对该设备类别或特定设备的访问。

如果复选框为灰白，则影响访问模式的值已从“设备类别配置”视图内部进行更改。要将该值重设回简单设置，请单击该复选框以清除或设置该值，然后单击**是**确认。


3. 单击**保存**图标。

 **注：** 如果后台服务未运行，将打开一个对话框，询问您是否要启动。单击**是**。

4. 单击**确定**。

启动后台服务

在应用设备配置文件之前，HP ProtectTools Security Manager 将打开一个对话框，询问您是否要启动 HP ProtectTools 设备锁定/审核后台服务。单击**是**。后台服务将启动且以后会在每次系统启动时自动启动。

 **注：** 必须定义设备配置文件，然后才会显示后台服务提示。

管理员也可以启动或停止此服务：

1. 单击**开始**，然后单击**控制面板**。
2. 单击**管理工具**，然后单击**服务**。
3. 搜索 **HP ProtectTools 设备锁定/审核服务**。

停止设备锁定/审核服务不会停止设备锁定。有两个组件可以强制设备锁定：

- 设备锁定/审核服务
- DAMDrv.sys 驱动程序


启动该服务可以启动设备驱动程序，但是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，请打开命令提示符窗口，然后输入 `sc query flicdlock`。

要确定设备驱动程序是否正在运行，请打开命令提示符窗口，然后输入 `sc query damdrv`。

设备类别配置


管理员和授权用户可以查看和修改被允许或拒绝访问各类别设备或特定设备的用户和组列表。

 **注：** 为了使用此视图读取设备访问信息，必须在**用户访问设置**视图中授予用户或组“读”访问权限。为了使用此视图修改设备访问信息，必须在**用户访问设置**视图中授予用户或组“更改”访问权限。

“设备类别配置”视图包括下列几个部分：

- **设备列表**—显示系统中安装或者以前可能在系统中安装的所有设备类别和设备。
 - 通常会对设备类别应用保护。选定用户或组能够访问设备类别中的任意设备。
 - 也可以对特定设备应用保护。
- **用户列表**—显示允许或拒绝对选定设备类别或特定设备进行访问的所有用户和组。
 - “用户列表”条目可能是针对特定用户，也可能是针对该用户是其中成员的组。
 - 如果“用户列表”中的用户或组条目不可用，则该设置已从“类别”文件夹或“设备列表”中的设备类别继承。
 - 某些设备类别，例如 DVD 和 CD-ROM，可以通过分别允许或拒绝读操作和写操作的访问权限进行进一步控制。

对于其他设备和类别，可以继承读/写访问权限。例如，“读”访问权限可以从更高级别的类继承，但是可能要特别针对用户或组拒绝“写”访问权限。

 **注：** 如果“写”复选框为空白，则该访问控制条目对该设备的读访问权限无效。既不会授予也不会拒绝对设备的读访问权限。

示例 1—如果用户或组被拒绝对设备或设备类别的写访问权限：

可以仅授予该用户、该组或该组成员对设备层次结构中此设备的下层设备的写访问权限或读+写访问权限。

示例 2—如果用户或组被允许对设备或设备类别的写访问权限：

可以仅拒绝该用户、该组或该组成员对此设备或设备层次结构中此设备的下层设备的写访问权限或读+写访问权限。

示例 3—如果用户或组被允许对设备或设备类别的读访问权限：

可以仅拒绝该用户、该组或该组成员对此设备或设备层次结构中此设备的下层设备的读访问权限或读+写访问权限。

示例 4—如果用户或组被拒绝对设备或设备类别的读访问权限：

可以仅授予该用户、该组或该组成员对设备层次结构中此设备的下层设备的读访问权限或读+写访问权限。

示例 5—如果用户或组被允许对设备或设备类别的读+写访问权限：

可以仅拒绝该用户、该组或该组成员对此设备或设备层次结构中此设备的下层设备的写访问权限或读+写访问权限。


示例 6—如果用户或组被拒绝对设备或设备类别的读+写访问权限：

可以仅授予该用户、该组或该组成员对设备层次结构中此设备的下层设备的读访问权限或读+写访问权限。

拒绝用户或组访问

要阻止用户或组访问设备或设备类别，请执行以下步骤：

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，单击您想要配置的设备类别。
 - 设备类别
 - 所有设备
 - 各个设备
3. 在 **用户/组** 中，单击要拒绝其访问的用户或组。
4. 单击用户或组旁边的 **拒绝**。
5. 单击 **保存** 图标。

 **注：** 在同一设备级别同时对用户设置了拒绝和允许设置时，拒绝访问优先于允许访问。

允许用户或组访问

要授予用户或组访问设备或设备类别的权限，请执行以下步骤：

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，单击下列选项之一：
 - 设备类别
 - 所有设备
 - 各个设备
3. 单击 **添加**。

将打开 **选择用户或组** 对话框。
4. 单击 **高级**，然后单击 **立即查找** 搜索要添加的用户或组。
5. 单击要添加到可用用户和组列表中的用户或组，然后单击 **确定**。
6. 再次单击 **确定**。
7. 单击 **允许** 授予该用户或组访问权限。
8. 单击 **保存** 图标。

删除用户或组的访问权限

要删除用户或组访问设备或设备类别的权限，请执行以下步骤：

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，单击您想要配置的设备类别。
 - 设备类别
 - 所有设备
 - 各个设备
3. 在 **用户/组** 下，单击您要删除的用户或组，然后单击 **删除**。
4. 单击 **保存** 图标。

允许组中一个用户访问某个类别设备

要允许用户访问某个类别设备，同时拒绝该用户所在组的其他所有成员访问该类别设备，请执行以下步骤：

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，单击您想要配置的设备类别。
 - 设备类别
 - 所有设备
 - 各个设备
3. 在 **用户/组** 中，选择要拒绝其访问的组，然后单击 **拒绝**。
4. 浏览到所需类别下的文件夹，然后添加指定用户。
5. 单击 **允许** 授予该用户访问权限。
6. 单击 **保存** 图标。

允许组中一个用户访问特定设备

管理员可以授予一个用户访问特定设备，同时拒绝该用户所在组中的其他所有成员访问该设备类别中的所有设备。

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，单击您想要配置的设备类别，然后浏览到该类别下的文件夹。
3. 单击 **添加**。将打开 **选择用户或组** 对话框。
4. 单击 **高级**，然后单击 **立即查找** 搜索要拒绝访问该类别中所有设备的用户组。
5. 单击该组，然后单击 **确定**。
6. 浏览到要允许该用户访问的设备类别下的特定设备。

7. 单击**添加**。将打开**选择用户或组**对话框。
8. 单击**高级**，然后单击**立即查找**搜索要添加的用户或组。
9. 单击要允许其访问的用户，然后单击**确定**。
10. 单击**允许**授予该用户访问权限。
11. 单击**保存**图标。

重置配置

△ **注意：** 重置配置将放弃所有已进行的设备配置更改，并将所有设置恢复为出厂时设置的值。


要将配置重置为出厂值，请执行以下步骤：

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**按钮。
3. 单击**是**确认。
4. 单击**保存**图标。


高级任务

控制对配置设置的访问权限

在**用户访问设置**视图中，管理员可以指定允许使用“简单配置”和“设备类别配置”页的组或用户。

 **注：** 用户或组必须具有“完全用户管理员权限”才能修改“用户访问设置”视图中的设置。

- 用户或组必须在“用户访问设置”视图中被授予“查看（只读）配置设置”访问权限，才能查看“简单配置”和“设备类别配置”信息。
- 用户或组必须在“用户访问设置”视图中被授予“更改配置设置”访问权限，才能更改“简单配置”和“设备类别配置”信息。


 **注：** 即使是“管理员”组成员，也必须被授予“读”访问权限，才能查看“简单配置”和“设备类别配置”视图；被授予“更改”访问权限，才能使用“简单配置”和“设备类别配置”视图更改数据。

注： 在评估所有用户和组的访问级别后，如果某用户对特定访问级别既没有选择“允许”也没有选择“拒绝”，则该用户在该级别将被拒绝。

授予现有组或用户的访问权限

要授予现有组或用户查看或更改配置设置的权限，请执行以下步骤：

1. 在 **HP ProtectTools 管理控制台** 的左窗格中，单击 **Device Access Manager**，然后单击**用户访问设置**。
2. 单击要允许访问的组或用户。
3. 在**权限**下，针对要授予选定组或用户的每个权限类型单击**允许**：

 **注：** 所授予的权限是累积的。例如，被授予“更改配置设置”权限的用户自动拥有“查看（只读）配置设置”权限。被授予“完全用户管理员权限”的用户也会被授予“更改配置设置”和“查看（只读）配置设置”权限。

- 完全用户管理员权限
 - 更改配置设置
 - 查看（只读）配置设置
4. 单击**保存**图标。

拒绝现有组或用户的访问

要拒绝现有组或用户查看或更改配置设置的权限，请执行以下步骤：

1. 在 **HP ProtectTools 管理控制台** 的左窗格中，单击 **Device Access Manager**，然后单击**用户访问设置**。
2. 单击要拒绝访问的组或用户。

3. 在**权限**下，针对要拒绝选定组或用户的每个权限类型单击**拒绝**:
 - 完全用户管理员权限
 - 更改配置设置
 - 查看（只读）配置设置
4. 单击**保存**图标。

添加新组或用户

要授予新组或用户查看或更改配置设置的权限，请执行以下步骤：

1. 在 **HP ProtectTools 管理控制台** 的左窗格中，单击 **Device Access Manager**，然后单击**用户访问设置**。
2. 单击**添加**。将打开**选择用户或组**对话框。
3. 单击**高级**，然后单击**立即查找**搜索要添加的用户或组。
4. 单击组或用户，然后单击**确定**，再次单击**确定**。
5. 单击**允许**授予该用户访问权限。
6. 单击**保存**图标。

删除组或用户访问权限

要删除组或用户查看或更改配置设置的权限，请执行以下步骤：

1. 在 **HP ProtectTools 管理控制台** 的左窗格中，单击 **Device Access Manager**，然后单击**用户访问设置**。
2. 单击组或用户，然后单击**删除**。
3. 单击**保存**图标。

相关文档

HP ProtectTools Device Access Manager 与企业版产品 HP ProtectTools Enterprise Device Access Manager 兼容。当与该企业版产品一起使用时，HP ProtectTools Device Access Manager 允许对其功能的只读访问。


有关 HP ProtectTools Device Access Manager 的详细信息可以从网页 <http://www.hp.com/hps/security/products> 上获得。

11 HP ProtectTools LoJack Pro

由 Absolute Software 公司推出的 Computrace LoJack Pro（需单独购买）可以解决越来越多的计算机丢失或被盜问题。

激活此软体可启用 Computrace 代理，即使硬盘驱动器被重新格式化或更换，该代理也会在您的计算机中保持作用中。

LoJack Pro 允许远程监控、管理和跟踪您的计算机。如果您的计算机丢失或被盜，Absolute 公司的“恢复团队”将帮助其恢复。*

 **注：** *此功能取决于地理位置。有关其他详细信息，请参阅 Absolute Software 公司的订阅协议。

12 故障排除

HP ProtectTools Security Manager

简短说明	详细说明	解决方法
安装 Security Manager 后才安装的智能卡和 USB 身份标记，在 Security Manager 中不可用。	为了在 Security Manager 中使用智能卡或 USB 身份标记，必须在安装 Security Manager 之前安装支持软件（驱动程序、PKCS#11 提供程序等）。 如果您已安装 Security Manager，请在安装智能卡或身份标记支持软件后，执行以下步骤：	登录 Password Manager。 在 HP ProtectTools Security Manager 中，依次单击 Password Manager、凭证及智能卡 。 根据提示，重新启动笔记本电脑。
某些应用程序 Web 页出现错误，阻止用户执行或完成任务。	由于禁用单一登录的功能模式，导致某些基于 Web 的应用程序停止运行并报告错误。例如，在 Internet Explorer 中会出现一个中间有 ! 的黄色三角形，表明发生了错误。	Security Manager 单一登录不支持所有软件 Web 界面。通过关闭单一登录支持可禁用特定网页的单一登录支持。请参阅有关单一登录的完整文档，位于 Security Manager 软件帮助文件中。 如果无法对给定应用程序禁用单一登录功能，请致电 HP 技术支持部门，并通过您的 HP 服务联系人请求第三级支持。
登录过程中不会显示 Browse for Virtual Token (浏览虚拟身份标记) 选项。	用户无法在 Password Manager 中移动注册虚拟身份标记的位置，因为为了降低安全风险，已删除浏览选项。	之所以删除浏览选项是因为不允许用户删除和重命名文件并操控 Windows。
域管理员即使有授权也不能修改 Windows 密码。	域管理员使用在域和本地计算机中具有管理员权限的帐户登录域并注册 Password Manager 的域身份后就会发生此情况。域管理员尝试从 Password Manager 更改 Windows 密码时，会收到登录失败的错误： 用户帐户限制 。	Password Manager 无法通过 更改 Windows 密码 更改域用户的帐户密码。Security Manager 只能更改本地计算机的帐户密码。域用户可以通过 Windows 安全的更改密码 选项更改其密码，但是，由于域用户在本地计算机上没有物理帐户，Password Manager 只能更改用于登录的密码。
Password Manager 存在与 Corel WordPerfect 12 密码 GINA 不兼容的问题。	如果用户登录 Password Manager，在 WordPerfect 中创建文档并使用密码保护保存该文档，则无论通过手动还是自动，Password Manager 都无法检测到或识别密码 GINA。	HP 正在研究未来产品增强功能的解决之道。
Password Manager 无法识别屏幕上的 连接 按钮。	如果将远程桌面连接 (RDP) 的单一登录凭证设置为 Connect (连接) ，则在重新启动单次登录时，它总是进入 Save As (另存为) ，而不是 Connect (连接) 。	HP 正在研究未来产品增强功能的解决之道。
在 Windows XP Service Pack 1 上（仅在此操作系统上）从睡眠模式转换到休眠模式后，用户无法登录 Password Manager。	允许系统转换为休眠和睡眠模式后，无论选择哪种登录凭据（密码、指纹还是 Java 卡），管理员或用户都无法登录 Password Manager 且 Windows 登录屏幕继续显示。	通过 Windows 更新将 Windows 更新至 Service Pack 2。请参阅 Microsoft 知识库中的文件 813301（网址为： http://www.microsoft.com ），以获取有关问题原因的详细信息。

简短说明	详细说明	解决方法
安全保护 Restore Identity (恢复标识) 进程丢失与虚拟身份标记的关联性。	当用户恢复标识时，在登录屏幕上，Password Manager 可能失去与虚拟身份标记位置的关联。即使 Password Manager 已注册虚拟身份标记，用户必须重新注册该身份标记才能恢复关联。	<p>为了登录，用户必须选择 Password Manager 并登录。登录到 Password Manager 后，系统将提示用户登录 Windows (用户可能必须选择 Windows 登录选项) 以完成登录过程。</p> <p>如果用户是第一次登录 Windows，则必须手动登录 Password Manager。</p> <p>目前是有意这样设计的。</p> <p>如果卸载 Security Manager 且不保留标识，身份标记的系统 (服务器) 部分将被破坏，因此无法再使用该身份标记进行登录，即使通过标识恢复来恢复该身份标记的客户端部分。</p> <p>HP 正在研究长远的解决问题方向。</p>

HP ProtectTools Device Access Manager

已在 Device Access Manager 中拒绝用户访问设备，但用户仍可访问设备。

- **说明** - 已在 Device Access Manager 中使用 Simple Configuration（简单配置）和/或 Device Class Configuration（设备类别配置）以拒绝用户访问设备。尽管拒绝访问，但用户仍可访问设备。
- **解决方案:**
 - 验证 HP ProtectTools Device Locking 服务是否已启动。
 - 以管理用户的身份，单击**控制面板**，然后单击**系统和维护**。在“管理工具”窗口中，单击**服务**，然后搜索 **HP ProtectTools Device Locking/Auditing** 服务。确保该服务已启动且启动类型是**自动**。

用户意外地拥有某设备的访问权，或者用户被意外地拒绝访问某设备。

- **说明** - 已使用 Device Access Manager 来拒绝用户访问某些设备并允许用户访问其他设备。当用户使用系统时，可以访问他们认为 Device Access Manager 已经拒绝访问的设备，而被拒绝访问他们认为 Device Access Manager 应该允许访问的设备。
- **解决方案:**
 - 使用 Device Access Manager 中的 Device Class Configuration（设备类别配置）来检查用户的设备设置。
 - 单击 **Security Manager**，单击 **Device Access Manager**，然后单击 **Device Class Configuration**（设备类别配置）。展开 Device Class（设备类别）树中的级别，并检查此用户适用的设置。检查是否可能对此用户或其所属的任何 Windows 组（例如，“用户”、“管理员”）设置了“拒绝”权限。

允许或拒绝，哪一个优先？

- **说明** - 在 Device Class Configuration（设备类别配置）中，已设置以下配置：
 - 在设备类别层次结构（例如 DVD/CD-ROM 驱动器）中的同一级别，已授予一个 Windows 组（例如，BUILTIN\管理员）“允许”权限，同时授予另一个 Windows 组（例如，BUILTIN\用户）“拒绝”权限。
 - 如果用户同时属于这两个组（例如，管理员），哪一个权限优先？
- **解决方案:**
 - 拒绝用户访问设备。Deny（拒绝）优先于 Allow（允许）。
 - 由于 Windows 计算设备有效权限的方式，访问将被拒绝。一个组被拒绝，一个组被允许，但该用户同时属于这两个组。因为拒绝访问优先于允许访问，所以用户被拒绝。
 - 一种解决方法是在 DVD/CD-ROM 驱动器级别拒绝“用户”组，而在 DVD/CD-ROM 驱动器下的级别允许“管理员”组。
 - 另一种解决方法是创建特定的 Windows 组，一个组用于允许访问 DVD/CD，一个组用于拒绝访问 DVD/CD。之后将特定用户分别添加到相应的组。

已使用 **Simple Configuration**（简单配置）视图定义设备访问控制策略，但管理用户无法访问设备。

- **说明** - Simple Configuration（简单配置）拒绝“用户”和“来宾”访问，而允许“设备管理员”访问。
- **解决方案：** 将管理用户添加到 Device Administrators（设备管理员）组。

其他

受影响的软件 - 简短说明	详细说明	解决方法
收到 Security Manager 警告消息： The security application can not be installed until the HP Protect Tools Security Manager is installed (安装 HP Protect Tools Security Manager 后才能安装安全保护应用程序) 。	所有安全应用程序，例如 Java Card Security 和生物技术，都是 Security Manager 接口的可扩展插件。必须先安装 Security Manager，然后才能加载 HP 许可的安全插件。	必须先安装 Security Manager 后才能安装任何安全插件。
HP ProtectTools Security Manager - 关闭 Security Manager 界面时偶尔会返回错误消息。	在没有完成加载所有插件应用程序之前，使用屏幕右上角的关闭按钮关闭 Security Manager 时，偶尔会产生错误（12 个例程中出现 1 次）。	这与关闭和重新启动 Security Manager 时与插件服务加载时间的计时相关性有关。因为 PTHOST.exe 是承载其他应用程序（插件）的 shell，所以它依赖于插件的能力才能完成其加载时间（服务）。在插件还没有时间完成加载时就关闭该 shell，是造成这种情况的根本原因。 允许 Security Manager 完成装载消息（在 Security Manager 窗口顶部显示）和左栏列出的所有插件。为避免失败，允许有合理的时间装载这些插件。
HP ProtectTools 未限制的访问权限或未控制的管理员特权构成安全风险。	不限制对客户端 PC 的访问可能会带来许多风险，包括以下： <ul style="list-style-type: none">● 删除 PSD● 恶意修改用户设置● 禁用安全策略和功能	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。

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 启动之前显示的屏幕。用户必须输入他们的 Windows 用户名和密码或 Java 卡个人标识号。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 将硬盘驱动器与用户相关联，并要求用户在计算机启动时正确键入驱动器锁密码的安全保护功能。

HP SpareKey 驱动器加密密钥的备份副本。

ID 卡 Windows 边栏小工具，使用您的用户名和选择的图片形象地标识您的桌面。单击 ID 卡可打开 HP ProtectTools 管理控制台。

Java 卡 插入笔记本电脑的可移动卡。它包含登录所用的标识信息。在 Drive Encryption 登录屏幕上使用 Java 卡登录时，您需要插入 Java 卡，并键入您的用户名和 Java 卡个人标识号。

Live Messenger 历史记录查看器 这是一个 Privacy Manager Chat 组件，用于搜索和查看加密的聊天历史记录会话。

PKI 公共密钥基础结构标准，其定义用于创建、使用和管理证书及加密密钥的接口。

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，为敏感信息提供受保护的存储区域。

SATA 设备模式 笔记本电脑与大容量存储设备（如硬盘驱动器和光驱）之间的数据传输模式。

TXT 可信执行技术。

USB 身份标记 存储用户身份信息的安全设备。该设备类似于 Java 卡或生物识别器，用于验证笔记本电脑主人的身份。

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。

安全登录方法 用于登录到计算机的方法。

按键序列 这是一组特定键组合，按下时会启动自动碎化 — 例如，[ctrl+alt+s](#)。

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他计算机上。

标识 HP ProtectTools Security Manager 中的一组凭证和设置，其用途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 存储验证信息并允许您使用 Security Manager 来访问需要密码验证的 Internet 和 Windows 应用程序的功能。

登录 Security Manager 内由用于登录网站或其他程序的用户名和密码（以及可能选择的其他信息）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 请参见 Windows 管理员。

后台服务 HP ProtectTools 设备锁定/审核后台服务，必须运行该服务，才能应用设备访问控制策略。可以从“控制面板”的“管理工具”选项下的“服务”应用程序内查看该服务。如果该服务未运行，HP ProtectTools Security Manager 将在应用设备访问控制策略时尝试启动它。

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 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 对数据进行加密和解密以保证只有指定用户才能解码数据的手段。

加密 加密技术中将纯文本转换为密码文本以防止未经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 Data Encryption Standard（数据加密标准）和公用密钥加密。

加密服务提供商 (CSP) 可用于适当定义的接口来执行特定加密功能的加密算法提供程序或库。

加密文件系统 (EFS) 对选定文件夹中的所有文件和子文件夹进行加密的系统。

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 在加密技术中用于将加密的数据转换为纯文本的过程。

紧急恢复档案 受保护的存储区域，允许重新加密基本用户密钥（从一个平台主人密钥到另一个平台主人密钥）。

开机验证 打开计算机时要求使用某种验证方式（例如 Java 卡、安全保护芯片或密码）的安全保护功能。

可信 IM 通信 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 可以访问和管理此程序的功能和设置的中心位置。

聊天历史记录会话 这是一个加密文件，其中包含聊天会话中双方的对话记录。

面板 可以访问和管理此程序的功能和设置的中心位置。

凭证 用户在验证过程中证明其有资格执行特定任务的方法。

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。通过单击此按钮，可在 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。

认证机构 颁发运行公共密钥所需证书的服务机构。

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 请参见安全登录方法。

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。

授权用户 已在“用户访问设置”视图中被授权查看或修改“简单配置”或“设备类别配置”视图上的配置设置的用户。

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主人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 本地计算机、工作组或域中的 Windows 用户或管理员帐户。

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。

显示 通过执行此任务，用户可以解密一个或多个聊天历史记录会话，以便以纯文本显示联系人屏幕名称并可查看会话。

虚拟身份标记 一种安全保护功能，与 Java 卡和智能卡识别器的功能非常相似。该身份标记保存在计算机硬盘驱动器或 Windows 注册表中。使用虚拟身份标记登录后，将要求您输入用户个人标识号以完成验证。

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

用户 Drive Encryption 中注册的任何人。非管理员用户在 Drive Encryption 中只拥有有限的权限。他们只能注册（经管理员许可）和登录。

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

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 大小和形状类似信用卡的小型硬件，用于存储主人的身份信息。用于验证计算机主人的身份。

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

符号/编号

- “常规” 标签, 设置 18
- “应用程序” 标签设置 31

A

- 安全
 - 摘要 31
- 安全保护
 - 关键目标 3
 - 角色 4
- 安全保护功能, 启用 8
- 安全保护角色 4
- 安全应用程序状态 31
- 按键序列 61

B

- 保护资产不被自动碎化 60
- 备份
 - HP ProtectTools 凭证 5
 - Privacy Manager 证书 54
 - 可信联系人 54
 - 数据 31
- 备份密钥, 创建 36

C

- 重置 70
- 查看
 - 加密的 Microsoft Office 文档 49
 - 聊天历史记录 51
 - 密封的电子邮件 46
 - 签名的 Microsoft Office 文档 49
 - 日志文件 63
- 创建
 - 备份密钥 36
 - 碎化配置文件 59
- 从自动删除中排除资产 60

D

- 打开
 - HP ProtectTools Device Access Manager 65
 - HP ProtectTools Drive Encryption 33
 - HP ProtectTools File Sanitizer 58
 - HP ProtectTools Privacy Manager 39
 - HP ProtectTools Security Manager 24
 - HP ProtectTools 管理控制台 7

登录

- 编辑 26
- 菜单 27
- 管理 27
- 类别 27
- 添加 26
- 登录到笔记本电脑 34
- 电子邮件
 - 查看密封的邮件 46
 - 签名 45
 - 为可信联系人密封 46
- 定义
 - 在删除之前进行确认的资产 60
 - 在碎化之前进行确认的资产 59

E

- Excel, 添加签名行 47

F

- 访问
 - 防止未授权 3
 - 拒绝 68
 - 拒绝现有组或用户 71
 - 控制 64
 - 授予现有组或用户 71
 - 允许 68

G

- 工具, 添加 20
- 功能, HP ProtectTools 2
- 故障排除
 - Device Access Manager 76
 - Security Manager 74
 - 其他 78
- 关键的安全保护目标 3
- 管理
 - 密码 19, 25
 - 凭证 28
 - 用户 15
- 管理工具, 添加 20

H

- HP ProtectTools Device Access Manager
 - 打开 65
 - 故障排除 76
- HP ProtectTools Drive Encryption
 - 备份和恢复 36
 - 打开 33
 - 管理 Drive Encryption 36
 - 激活 34
 - 加密各个驱动器 36
 - 解密各个驱动器 36
 - 停用 34
 - 在激活 Drive Encryption 后登录 34
- HP ProtectTools File Sanitizer
 - 打开 58
 - 设置步骤 58
 - 图标 61
- HP ProtectTools Java Card Security, PIN 4
- HP ProtectTools LoJack Pro 73
- HP ProtectTools Privacy Manager
 - Privacy Manager 证书 39
 - 安全登录方法 38

- 打开 39
- 管理 Privacy Manager 证书 39
- 管理可信联系人 42
- 将 Privacy Manager Certificates (隐私管理器证书) 和 Trusted Contacts (可信联系人) 迁移到其他计算机上 54
- 将 Privacy Manager 证书和可信联系人迁移到其他计算机上 54
- 设置步骤 39
- 系统要求 38
- 验证方法 38
- HP ProtectTools Security Manager
 - 打开 24
 - 故障排除 74
 - 恢复文件密码 4
 - 设置步骤 22
 - 设置向导 6
- HP ProtectTools 功能 2
- HP ProtectTools 管理控制台
 - 打开 7
 - 配置 12
 - 使用 11
- 后台服务 66
- 恢复
 - HP ProtectTools 凭证 5
 - Privacy Manager 证书和可信联系人 54
 - 数据 31
- 恢复, 执行 37

I
ID 卡 30

J
激活

- Drive Encryption 34
- 可用空间清理 62

集中管理 54
加密

- Microsoft Office 文档 48
- 驱动器 32, 35, 36

加密状态, 显示 35
简单配置 65
简单删除 60
建议的签名者

- 添加 47
- 添加签名行 48

- 解密驱动器 32, 36
- 拒绝访问 68

K
可信联系人

- 查看详细信息 44
- 检查吊销状态 44
- 删除 44
- 添加 42

可用空间清理 58
控制板设置 23
控制设备访问 64

L
聊天历史记录, 查看 51

M
Microsoft Excel, 添加签名行 47
Microsoft Office

- 查看加密的文档 49
- 查看签名的文档 49
- 对文档进行签名 47
- 加密文档 48
- 删除加密 48
- 通过电子邮件发送加密的文档 49

Microsoft Word, 添加签名行 47
密封 46
密码

- HP ProtectTools 4
 - 安全的 5
 - 策略 3
 - 更改 23
 - 管理 4
 - 强度 28
 - 准则 5

目标, 安全保护 3

P
Password Manager 25
Privacy Manager

- 与 Microsoft Office 2007 文档配合使用 46
- 与 Microsoft Outlook 配合使用 45
- 在 Windows Live Messenger 中使用 49

Privacy Manager 证书

- 安装 40
- 查看详细信息 40

- 存储 41
- 吊销 42
- 删除 41
- 设置默认 41
- 申请 39
- 收到 40
- 续订 41

配置

- HP ProtectTools 管理控制台 12
- 重置 70
- 简单 65
- 控制访问权限 71
- 设备访问权限 65
- 设备类别 66
- 设置 71
- 应用程序 17
- 针对 Microsoft Office 文档的 Privacy Manager 46
- 针对 Microsoft Outlook 的 Privacy Manager 45
- 针对 Windows Live Messenger 的 Privacy Manager 50

凭证 28, 30
凭证, 注册 22

Q
启动 Privacy Manager Chat 会话 50
签名

- Microsoft Office 文档 47
- 电子邮件 45

窃取, 防范 3, 73

S
Security Manager

- 登录密码 4
- 设置向导 22

删除

- 从 Microsoft Office 文档中删除加密 48
- 用户访问权限 72
- 组访问权限 72

设备类别

- 配置 66
- 允许用户访问 69

设备设置

- 指定 16
- 指纹 16
- 智能卡 16

- 设备, 允许用户访问 69
- 设置
 - 可用空间清理计划 58
 - 碎化计划 58
 - 添加 19, 23, 31
 - 图标 28
 - 应用程序 19, 23, 31
 - “常规”标签 18
- 设置向导 6, 22
- 申请数字证书 39
- 手动碎化
 - 所有选定项目 62
 - 一个资产 62
- 首选项, 设置 30
- 数据
 - 备份 31
 - 恢复 31
 - 限制访问 3
- 数字证书
 - 安装 40
 - 查看详细信息 40
 - 存储 41
 - 吊销 42
 - 删除 41
 - 设置默认 41
 - 申请 39
 - 收到 40
 - 续订 41
- 碎化周期 59

T

- 添加
 - 建议的签名者 47
 - 建议的签名者的签名行 48
 - 签名行 47
 - 用户 72
 - 组 72
- 停用 Drive Encryption 34
- 通过电子邮件发送加密的 Microsoft Office 文档 49

W

- Windows Live Messenger, 聊天 51
- Windows 登录密码 4
- Word, 添加签名行 47
- 未授权的访问, 防止 3

X

- 系统要求 38

- 限制
 - 对敏感数据的访问 3
 - 设备访问 64
- 向导
 - HP ProtectTools 设置 6
- 选择
 - 碎化配置文件 59
 - 要碎化的资产 59

Y

- 验证 13
- 应用程序标签设置 19
- 应用程序, 配置 17
- 用户
 - 拒绝访问 68
 - 删除 69
 - 允许访问 68
- 预定义碎化配置文件 59
- 允许访问 68

Z

- 在“通信”窗口中聊天 51
- 证书, 预先指定的 40
- 指定安全设置 14
- 指纹
 - 设置 16
 - 注册 9, 22
- 智能卡
 - 设置 10, 16
- 终止碎化或清理操作 63
- 注册凭证 22
- 自定义
 - 简单删除配置文件 60
 - 碎化配置文件 59
- 组
 - 拒绝访问 68
 - 删除 69
 - 允许访问 68

