

ProtectTools

用户指南

© 版权所有 2007 Hewlett-Packard
Development Company, L.P.

Microsoft 和 Windows 是 Microsoft Corporation 在美国的注册商标。Intel 是 Intel Corporation 或其子公司在美国和其它国家/地区的商标或注册商标。AMD、AMD 箭头徽标及其组合是 Advanced Micro Devices, Inc. 的商标。Bluetooth 是其所有者拥有的商标，Hewlett-Packard Company 经授权得以使用。Java 是 Sun Microsystems, Inc. 在美国的商标。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 1 版：2007 年 1 月

文档部件号：438371-AA1

目录

1 安全保护简介

HP ProtectTools 功能	2
访问 HP ProtectTools Security	3
实现关键的安全保护目标	4
防范有目的的盗窃行为	4
限制访问敏感数据	4
防止来自内部或外部的未授权访问	5
创建强大可靠的密码策略	5
其它安全保护要素	6
指定安全保护角色	6
管理 HP ProtectTools 密码	6
创建安全的密码	8
HP ProtectTools Backup and Restore	8
备份凭证和设置	8
恢复凭证	10
配置设置	10

2 Credential Manager for HP ProtectTools

设置步骤	12
登录到 Credential Manager	12
使用 Credential Manager 登录向导	12
首次登录	13
注册凭证	13
注册指纹	13
设置指纹识别器	14
使用已注册的指纹登录到 Windows	14
注册 Java 卡、USB eToken 或虚拟身份标记	14
注册 USB eToken	14
注册其他凭证	14
常规任务	15
创建虚拟身份标记	15
更改 Windows 登录密码	15
更改身份标记个人标识号	15
管理标识	16
从系统中清除标识	16
锁定笔记本电脑	17
使用 Windows 登录	17
使用 Credential Manager 登录到 Windows	17
添加帐户	18

删除帐户	18
使用单次登录	18
注册新应用程序	18
使用自动注册功能	18
使用手动（拖放）注册功能	19
管理应用程序和凭证	19
修改应用程序属性	19
从单次登录中删除应用程序	19
导出应用程序	20
导入应用程序	20
修改凭证	20
使用应用程序保护	21
限制对应用程序的访问	21
删除应用程序的保护	22
更改受保护应用程序的限制设置	22
高级任务（仅供管理员使用）	23
指定用户和管理员的登录方式	23
配置自定义验证需求	24
配置凭证属性	24
配置 Credential Manager 设置	25
示例 1 — 使用“Advanced Settings”（高级设置）页允许从 Credential Manager 进行 Windows 登录	25
示例 2 — 使用“Advanced Settings”（高级设置）页要求在单次登录前进行用户验证	26

3 Embedded Security for HP ProtectTools

设置步骤	28
启用嵌入式安全保护芯片	28
初始化嵌入式安全保护芯片	29
建立基本用户帐户	30
常规任务	31
使用个人安全驱动器	31
对文件和文件夹进行加密	31
发送和接收加密的电子邮件	31
更改基本用户密钥密码	32
高级任务	33
备份和恢复	33
创建备份文件	33
通过备份文件恢复认证数据	33
更改主人密码	34
重置用户密码	34
启用和禁用 Embedded Security	34
永久禁用 Embedded Security	34
在永久禁用后启用 Embedded Security	34
使用迁移向导迁移密钥	35

4 Java Card Security for HP ProtectTools

常规任务	38
更改 Java 卡个人标识号	38

选择读卡器	38
高级任务（仅供管理员使用）	39
指定 Java 卡个人标识号	39
为 Java 卡指定名称	40
设置开机验证	40
启用 Java 卡开机验证并创建管理员 Java 卡	41
创建用户 Java 卡	42
禁用 Java 卡开机验证	42

5 BIOS Configuration for HP ProtectTools

常规任务	44
管理引导选项	44
启用和禁用系统配置选项	45
高级任务	47
管理 HP ProtectTools 附加模块设置	47
启用和禁用智能卡开机验证支持	47
启用和禁用 Embedded Security 的开机验证支持	48
启用和禁用驱动器锁自动保护硬盘驱动器功能	49
管理计算机设置实用程序密码	49
设置开机密码	50
更改开机密码	50
设定设置密码	50
更改设置密码	50
设置密码选项	51
启用和禁用严格的安全保护功能	51
启用和禁用 Windows 重新启动时的开机验证功能	51

6 Device Access Manager for HP ProtectTools

启动后台服务	54
简单配置	55
设备类别配置（高级）	56
添加用户或组	56
删除用户或组	56
拒绝用户或组访问	56
允许组中一个用户访问某个设备类别	56
允许组中一个用户访问特定设备	57

7 Drive Encryption for HP ProtectTools

加密管理	60
用户管理	61
恢复	62

8 故障排除

Credential Manager for HP ProtectTools	63
Embedded Security for HP ProtectTools	65
Device Access Manager for HP ProtectTools	70
其他	71

术语表 75

索引 77

1 安全保护简介

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

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools

笔记本电脑中可用的软件模块因机型而异。例如，Embedded Security for HP ProtectTools 软件模块只能用于安装了可信平台模块 (TPM) 嵌入式安全保护芯片的计算机。

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.cn>。



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

下表详细介绍 HP ProtectTools 模块的重要功能：

模块	重要功能
Credential Manager for HP ProtectTools	• Credential Manager 可用作个人密码保护屏障。 • 单次登录可记住多个用于访问各种有密码保护的网站、应用程序和网络资源的密码。 • 单次登录还提供额外的保护，要求使用不同安全技术的组合（比如 Java™ 卡和生物识别器）进行用户身份验证。 • 密码存储通过加密进行保护，并可以利用 TPM 嵌入式安全保护芯片和/或安全设备验证（比如 Java 卡和生物识别器）来加强保护。
Embedded Security for HP ProtectTools	• Embedded Security 模块使用可信平台模块 (TPM) 嵌入式安全保护芯片来帮助防止他人未经授权擅自访问在计算机本地存储的敏感用户数据或凭证。 • Embedded Security 模块允许创建个人安全驱动器 (PSD) 以保护用户数据。 • Embedded Security 模块支持第三方应用程序（如 Microsoft Outlook 和 Internet Explorer）采用数字证书保护措施。
Java Card Security for HP ProtectTools	• 在操作系统加载之前，Java Card Security 模块配置 HP ProtectTools Java 卡进行用户身份验证。 • Java Card Security 模块可以为管理员和用户配置不同的 Java 卡。
BIOS Configuration for HP ProtectTools	• BIOS Configuration 模块用于进行开机用户和管理员密码管理。 • BIOS Configuration 模块可替代预引导 BIOS 配置实用程序（即 f10 设置实用程序）。 • 由于使用了嵌入式安全保护芯片，驱动器锁的功能得到了增强，它可以防止他人未经授权擅自访问硬盘驱动器，即使将其从系统中删除，也无需用户记住除嵌入式安全保护芯片用户密码以外的任何其它密码。
Device Access Manager for HP ProtectTools	• Device Access Manager 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。
Drive Encryption for HP ProtectTools	• Drive Encryption 模块提供全面的整卷硬盘驱动器加密。 • Drive Encryption 模块强制执行预引导验证后，才能解密和访问数据。

访问 HP ProtectTools Security

要从 Windows® 控制面板中访问 HP ProtectTools Security，请执行以下操作：

- ▲ 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。



注： 如果已经配置了 Credential Manager 模块，您还可以通过直接从 Windows 登录屏幕登录到 Credential Manager 来打开 HP ProtectTools。有关详细信息，请参阅“[第 17 页的使用 Credential Manager 登录到 Windows](#)”。

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

防范有目的的盗窃行为

有目的地在机场安检处盗窃保存机密数据和客户信息的笔记本电脑就是这种类型的案例。下列功能有助于防范有目的的盗窃行为：

- 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：
 - “[第 47 页的启用和禁用智能卡开机验证支持](#)”
 - “[第 48 页的启用和禁用 Embedded Security 的开机验证支持](#)”
 - “[第 40 页的为 Java 卡指定名称](#)”
 - “[第 59 页的 Drive Encryption for HP ProtectTools](#)”
- 即使卸下硬盘驱动器，然后将其安装到没有保护的系统，驱动器锁功能也可帮助确保硬盘驱动器上的数据不被未授权用户访问。请参阅“[第 49 页的启用和禁用驱动器锁自动保护硬盘驱动器功能](#)”。
- Embedded Security for HP ProtectTools 模块提供的个人安全驱动器功能可以对敏感数据进行加密，帮助确保未经身份验证不得访问数据。请参阅以下步骤：
 - Embedded Security “[第 28 页的设置步骤](#)”
 - “[第 31 页的使用个人安全驱动器](#)”

限制访问敏感数据

假设合同审核人正在现场工作，并已经获得使用计算机查看敏感财务数据的授权；但您不希望该审核人能够打印文件或将文件保存到可写设备（比如 CD）中。以下功能可帮助限制数据访问：

- IT 经理可以利用 Device Access Manager for HP ProtectTools 来限制使用可写设备的权限，这样就无法从硬盘驱动器打印敏感信息或将其复制到可移动介质上。请参阅“[第 56 页的设备类别配置（高级）](#)”。
- 即使卸下硬盘驱动器，然后将其安装到没有保护的系统，驱动器锁功能也可帮助确保硬盘驱动器上的数据不被未授权用户访问。请参阅“[第 49 页的启用和禁用驱动器锁自动保护硬盘驱动器功能](#)”。

防止来自内部或外部的未授权访问

如果可以从内部或外部访问包含机密数据和客户信息的 PC，那么未授权的用户就可能能够查看公司网络资源或财务部门、执行官或研发团队的数据，或者诸如病历或个人财务数据等私密信息。以下功能可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：
 - “[第 47 页的启用和禁用智能卡开机验证支持](#)”
 - “[第 48 页的启用和禁用 Embedded Security 的开机验证支持](#)”
 - “[第 40 页的为 Java 卡指定名称](#)”
 - “[第 59 页的 Drive Encryption for HP ProtectTools](#)”
- Embedded Security for HP ProtectTools 模块利用以下步骤来帮助保护在 PC 上本地存储的敏感用户数据或凭证：
 - Embedded Security “[第 28 页的设置步骤](#)”
 - “[第 31 页的使用个人安全驱动器](#)”
- 利用以下步骤，Credential Manager for HP ProtectTools 模块帮助确保未经授权的用户不能获取密码或者访问受密码保护的应用程序：
 - Credential Manager “[第 12 页的设置步骤](#)”
 - “[第 18 页的使用单次登录](#)”
- IT 经理可以利用 Device Access Manager for HP ProtectTools 来限制使用可写介质的权限，这样就无法从硬盘驱动器上复制敏感信息。请参阅“[第 55 页的简单配置](#)”。
- 个人安全驱动器功能使用以下步骤对敏感数据进行加密，确保未经身份验证就不能访问数据：
 - Embedded Security “[第 28 页的设置步骤](#)”
 - “[第 31 页的使用个人安全驱动器](#)”

创建强大可靠的密码策略

如果必须对数十个基于 Web 的应用程序和数据库使用强大可靠的密码策略，则 Credential Manager for HP ProtectTools 可使用以下步骤为密码和单次登录功能的存储库：

- Credential Manager “[第 12 页的设置步骤](#)”
- “[第 18 页的使用单次登录](#)”

为提供更强大的安全保护，Embedded Security for HP ProtectTools 还保护用户名和密码的存储库。这允许用户保留多个安全可靠的密码，但无需写下或试图记住这些密码。请参阅 Embedded Security “[第 28 页的设置步骤](#)”。

其它安全保护要素

指定安全保护角色

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



注： 对于小型企业或个人用户，这些角色可能全部由一人担任。

对于 HP ProtectTools，安全责任和权限可以按以下角色划分：

- 安全管理人员 - 定义公司或网络的安全级别，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，请访问 HP 网站：<http://www.hp.com.cn>。

- 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。

管理 HP ProtectTools 密码

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

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

HP ProtectTools 密码	在以下 HP ProtectTools 模块中设置	功能
Credential Manager 登录密码	Credential Manager	此密码提供 2 个选项： ● 可用于在登录到 Windows 后单独登录访问 Credential Manager。 ● 可用于代替 Windows 登录过程，允许同时访问 Windows 和 Credential Manager。
Credential Manager 恢复文件密码	Credential Manager，由 IT 管理员设置并使用	防止他人未经授权擅自访问 Credential Manager 恢复文件。
基本用户密钥密码	Embedded Security	用于访问 Embedded Security 功能，比如为确保安全进行的电子邮件、文件和文件夹加密。如果用于开机验证，还可以在笔记本电脑开启、重新启动或从休眠模式恢复时防止他人擅自访问计算机内容。
急救身份标记密码	Embedded Security，由 IT 管理员设置并使用	防止他人未经授权擅自访问急救身份标记（它是嵌入式安全保护芯片的备份文件）。



注： 也称为：Embedded Security 密码



注： 也称为：急救身份标记密钥密码

HP ProtectTools 密码	在以下 HP ProtectTools 模块中设置	功能
主人密码	Embedded Security, 由 IT 管理员设置并使用	保护系统和 TPM 芯片, 防止他人未经授权擅自访问 Embedded Security 模块的所有主人功能。
Java™ 卡个人标识号	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。
计算机设置实用程序密码  注: 也称为 BIOS 管理员密码、 f10 设置实用程序密码或安全设置实用程序密码	BIOS Configuration, 由 IT 管理员设置并使用	防止他人未经授权擅自访问计算机设置实用程序。
开机密码	BIOS Configuration	在笔记本电脑计算机开启、重新启动或从休眠模式恢复时, 防止他人未经授权擅自对笔记本电脑内容进行访问。
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的密码，降低密码被破解的几率：

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

HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore 提供一个从所有支持的 HP ProtectTools 模块中备份和恢复凭证的便捷方法。

备份凭证和设置

您可以利用以下方法备份凭证：

- 使用 HP ProtectTools 备份向导来选择和备份 HP ProtectTools 模块
- 备份预先选定的 HP ProtectTools 模块



注： 在使用该方法前，您必须先设置备份选项。

- 计划备份时间



注： 在使用该方法前，您必须先设置备份选项。

使用 HP ProtectTools 备份向导来选择和备份 HP ProtectTools 模块

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Backup and Restore（备份和恢复）**。
3. 在右窗格中，单击 **Backup Options（备份选项）**。随即打开 HP ProtectTools 备份向导。按照屏幕上的指示备份凭证。

设置备份选项

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Backup and Restore (备份和恢复)**。
3. 在右窗格中，单击 **Backup Options (备份选项)**。随即打开 HP ProtectTools 备份向导。
4. 按照屏幕上的指示进行操作。
5. 在设置和确认 **Storage File Password (存储文件密码)** 后，选择 **Remember all passwords and authentication values for future automated backups (记住所有密码和验证值以便将来自动备份)**。
6. 单击 **Save Settings (保存设置)**，然后单击 **Finish (完成)**。

备份预先选定的 HP ProtectTools 模块



注： 在使用该方法前，您必须先设置备份选项。

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Backup and Restore (备份和恢复)**。
3. 在右窗格中，单击 **Backup (备份)**。

计划备份时间



注： 在使用该方法前，您必须先设置备份选项。

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Backup and Restore (备份和恢复)**。
3. 在右窗格中，单击 **Schedule Backups (计划备份时间)**。
4. 在 **Task (任务)** 标签上，选择 **Enabled (已启用)** 复选框以执行已计划的备份。
5. 单击 **Set Password (设置密码)**，并在 **Set Password (设置密码)** 对话框中键入密码并确认。单击 **OK (确定)**。
6. 单击 **Apply (应用)**。单击 **Schedule (计划)** 标签。单击 **Schedule Task (计划任务时间)** 箭头，并选择自动备份的频率。
7. 在 **Start time (开始时间)** 下，使用 **Start time (开始时间)** 箭头选择要开始备份的确切时间。
8. 单击 **Advanced (高级)** 选择开始日期、结束日期和重复任务设置。单击 **Apply (应用)**。
9. 单击 **Settings (设置)**，并选择 **Scheduled Task Completed (已完成计划的任务)**、**Idle Time (空闲时间)** 和 **Power Management (电源管理)** 设置。
10. 单击 **Apply (应用)**，然后单击 **OK (确定)** 关闭对话框。

恢复凭证

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Backup and Restore（备份和恢复）**。
3. 在右窗格中，单击 **Restore（恢复）**。随即打开 HP ProtectTools 恢复向导。按照屏幕上的指示进行操作。

配置设置

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **HP ProtectTools**，然后单击 **Settings（设置）**。
3. 在右窗格中，选择您的设置，然后单击 **OK（确定）**。

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools 使用以下安全保护功能防止他人未经允许擅自访问您的计算机：

- 登录 Windows 时不输入密码而使用其它方法，例如使用 Java 卡或生物识别器登录 Windows。有关详细信息，请参阅“[第 13 页的注册凭证](#)”。
- 单次登录功能，可自动记住访问网站、应用程序和受保护网络资源所用的凭证。
- 支持安全保护设备选件，如 Java 卡和生物识别器。
- 支持其它安全保护设置，例如要求在解除计算机锁定前使用安全保护设备选件进行验证。

设置步骤

登录到 Credential Manger

根据配置情况，您可采用以下任意方式登录到 Credential Manger:

- Credential Manager 登录向导（首选）
- 在通知区域中的 HP ProtectTools Security Manager 图标
- HP ProtectTools Security Manager



注： 如果您使用 Windows 登录屏幕上的 Credential Manger 登录提示登录到 Credential Manger，您将同时登录到 Windows。

首次打开 Credential Manger 时，请使用通常的 Windows 登录密码进行登录。然后系统将基于您的 Windows 登录凭证自动创建一个 Credential Manger 帐户。

登录到 Credential Manger 之后，您可以注册其他凭证，例如指纹或 Java 卡。有关详细信息，请参阅“[第 13 页的注册凭证](#)”。

在下次登录时，您可以选择登录策略并使用任意组合形式的注册凭证。

使用 Credential Manager 登录向导

要使用 Credential Manager 登录向导登录到 Credential Manger，请执行以下步骤:

1. 采用以下任意方式打开 Credential Manager 登录向导:
 - 使用 Windows 登录屏幕
 - 双击通知区域中的 **HP ProtectTools Security Manager** 图标
 - 在 ProtectTools Security Manager 的“Credential Manager”页上，单击窗口右上角的 **Log On（登录）** 链接
2. 按照屏幕上的指示登录 Credential Manager。

首次登录

在您开始以前，必须使用管理员帐户登录到 Windows，但不要登录到 Credential Manager。

1. 通过双击通知区域中的 HP ProtectTools Security Manager 图标将其打开。随即打开 HP ProtectTools Security Manager 窗口。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后在右窗格右上角中单击 **Log On（登录）**。随即打开 Credential Manager 登录向导。
3. 在 **Password（密码）** 框中键入您的 Windows 密码，然后单击 **Next（下一步）**。

注册凭证

您可以使用“**My Identity（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到 Credential Manager。

注册指纹

指纹识别器使您可以使用指纹验证（而不是使用 Windows 密码）登录到 Windows 中。

设置指纹识别器

1. 登录 Credential Manager 后，在指纹识别器上扫描您的手指。随即打开 Credential Manager 注册向导。
2. 按照屏幕上的指示完成指纹注册和指纹识别器设置的过程。
3. 要对其他 Windows 用户设置指纹识别器，请以该用户的身份登录到 Windows 中，然后重复步骤 1 和 2。

使用已注册的指纹登录到 Windows

1. 注册完您的指纹后，请立即重新启动 Windows。
2. 出现 Windows Welcome（Windows 欢迎使用）屏幕时，通过扫描您已经注册过的任何手指登录到 Windows。

注册 Java 卡、USB eToken 或虚拟身份标记



注： 您必须在此步骤中配置读卡器。如果还没有安装读卡器，您可以按照“[第 15 页的创建虚拟身份标记](#)”中的说明注册虚拟身份标记。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**。
3. 在右窗格中，单击 **Register Smart Card or Token（注册智能卡或身份标记）**。随即打开 Credential Manager 注册向导。
4. 按照屏幕上的指示进行操作。

注册 USB eToken

1. 确保已安装 USB eToken 驱动程序。



注： 有关详细信息，请参阅 USB eToken 用户指南。

2. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
3. 在左窗格中，单击 **Credential Manager（凭证管理器）**。
4. 在右窗格中，单击 **Register Smart Card or Token（注册智能卡或身份标记）**。随即打开 Credential Manager 注册向导。
5. 按照屏幕上的指示进行操作。

注册其他凭证

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**。
3. 在右窗格中，单击 **Register Credentials（注册凭证）**。随即打开 Credential Manager 注册向导。
4. 按照屏幕上的指示进行操作。

常规任务

所有用户都可以访问 Credential Manager 中的“**My Identity**”（我的标识）页。使用“**My Identity**”（我的标识）页，您可以执行以下任务：

- 创建虚拟身份标记
- 更改 Windows 登录密码
- 管理身份标记个人标识号
- 管理标识
- 锁定笔记本电脑



注： 此选项仅在启用 Credential Manager 经典登录提示时才可用。请参阅“[第 25 页的示例 1 — 使用“Advanced Settings”（高级设置）页允许从 Credential Manager 进行 Windows 登录](#)”。

创建虚拟身份标记

虚拟身份标记的工作原理非常类似于 Java 卡或 USB eToken。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。

要创建新的虚拟身份标记，请执行以下操作：

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器）。
3. 在右窗格中，单击 **Virtual Token**（虚拟身份标记）。随即打开 Credential Manager 注册向导。



注： 如果 **Virtual Token**（虚拟身份标记）不可选，则执行“[第 14 页的注册其他凭证](#)”中的步骤。

4. 按照屏幕上的指示进行操作。

更改 Windows 登录密码

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器）。
3. 在右窗格中，单击 **Change Windows Password**（更改 Windows 密码）。
4. 在 **Old password**（旧密码）框中键入旧密码。
5. 在 **New password**（新密码）和 **Confirm password**（确认密码）框中键入新密码。
6. 单击 **Finish**（完成）。

更改身份标记个人标识号

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器）。

3. 在右窗格中，单击 **Change Token PIN**（更改身份标记个人标识号）。
4. 选择要更改个人标识号的身份标记，然后单击 **Next**（下一步）。
5. 按照屏幕上的指示完成对个人标识号的更改。

管理标识

从系统中清除标识



注： 这不会影响您的 Windows 用户帐户。

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器）。
3. 在右窗格中，单击 **Clear Identity for this Account**（清除此帐户的标识）。
4. 在确认对话框中单击 **Yes**（是）。您的标识即被注销并从系统中删除。

锁定笔记本电脑

如果您使用 Credential Manager 登录到 Windows，则可以使用此功能。要在您离开办公桌时保证您的笔记本电脑的安全，请使用 Lock Workstation（锁定工作站）功能。这可防止他人擅自使用您的计算机。只有您和计算机管理员组的成员可以解除计算机的锁定。



注： 此选项仅在启用 Credential Manager 经典登录提示时才可用。请参阅“[第 25 页的示例 1 — 使用“Advanced Settings”（高级设置）页允许从 Credential Manager 进行 Windows 登录](#)”。

为了进一步提高安全性，您可以配置 Lock Workstation（锁定工作站）功能，以要求必须使用 Java 卡、生物识别器或身份标记才可解除计算机的锁定。有关详细信息，请参阅“[第 25 页的配置 Credential Manager 设置](#)”。

要锁定计算机，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**。
3. 在右窗格中，单击 **Lock Workstation（锁定工作站）**。此时，将显示 Windows 登录屏幕。您必须使用 Windows 密码或 Credential Manager 登录向导才可解除计算机锁定。

使用 Windows 登录

您可以使用 Credential Manager 登录到本地计算机或网络域中的 Windows。当您首次登录到 Credential Manager 时，系统将把您的本地 Windows 用户帐户自动添加为 Windows 登录服务的帐户。

使用 Credential Manager 登录到 Windows

您可以使用 Credential Manager 登录到 Windows 网络或本地帐户。

1. 如果您已经注册用于登录 Windows 的指纹，请使用扫描指纹进行登录。
2. 如果您尚未注册用于登录 Windows 的指纹，则单击屏幕左上角指纹图标旁边的键盘图标。随即打开 Credential Manager 登录向导。
3. 单击 **User name（用户名）** 箭头，然后单击您的用户名。
4. 在 **Password（密码）** 框中键入您的密码，然后单击 **Next（下一步）**。
5. 选择 **More（更多） > Wizard Options（向导选项）**。
 - a. 如果您希望将选中的用户名设置为下次登录计算机时使用的默认用户名，请选择 **Use last user name on next login（下次登录时使用前一次的用户名）** 复选框。
 - b. 如果您希望将此登录策略设置为默认方法，请选择 **Use last policy on next login（下次登录时使用前一次的策略）** 复选框。
6. 按照屏幕上的指示进行操作。如果您的验证信息正确，您将登录到 Windows 帐户和 Credential Manager。

添加帐户

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager (凭证管理器)**，然后单击 **Services and Applications (服务和应用程序)**。
3. 在右窗格中，单击 **Windows Logon (Windows 登录)**，然后单击 **Add a Network Account (添加网络帐户)**。随即打开 Add Network Account Wizard (添加网络帐户向导)。
4. 按照屏幕上的指示进行操作。

删除帐户

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager (凭证管理器)**，然后单击 **Services and Applications (服务和应用程序)**。
3. 在右窗格中，单击 **Windows Logon (Windows 登录)**，然后单击 **Manage Network Accounts (管理网络帐户)**。随即打开 **Manage Network Accounts (管理网络帐户)** 对话框。
4. 单击要删除的帐户，然后单击 **Remove (删除)**。
5. 在确认对话框中单击 **Yes (是)**。
6. 单击 **OK (确定)**。

使用单次登录

Credential Manager 的单次登录功能可以存储多个 Internet 和 Windows 程序的用户名和密码，并可在您访问注册程序时自动输入登录凭证。



注： 单次登录提供了重要的安全保护和隐私保护功能。所有凭证都进行了加密，并且仅在成功登录到 Credential Manager 之后才可用。

注： 您还可以配置单次登录，要求在登录到安全站点或程序之前使用 Java 卡、指纹识别器或身份标记来确认验证凭证是否有效。在登录到包含个人信息（例如银行帐户号码）的程序或网站时，该功能特别有用。有关详细信息，请参阅“[第 25 页的配置 Credential Manager 设置](#)”。

注册新应用程序

在您登录到 Credential Manager 时，该管理器将提示您注册启动的应用程序。您也可以手动注册应用程序。

使用自动注册功能

1. 打开要求您登录的应用程序。
2. 在程序或网站密码对话框中单击 Credential Manager 单次登录图标。
3. 键入程序或网站的密码，然后单击 **OK (确定)**。随即打开 **Credential Manager Single Sign On (凭证管理器单次登录)** 对话框。

4. 单击 **More（更多）**，并从以下选项中选择：
 - Do not use SSO for this site or application.（不要对此网站或应用程序使用单次登录。）
 - Prompt to select account for this application.（提示选择此应用程序的帐户。）
 - Fill in credentials but do not submit.（填写凭证但不提交。）
 - Authenticate user before submitting credentials.（提交凭证之前验证用户。）
 - Show SSO shortcut for this application.（显示此应用程序的单次登录快捷方式。）
5. 单击 **Yes（是）** 完成注册。

使用手动（拖放）注册功能

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Services and Applications（服务和应用程序）**。
3. 在右窗格中，单击 **Single Sign On（单次登录）**，然后单击 **Register New Application（注册新应用程序）**。随即打开 SSO Application Wizard（单次登录应用程序向导）。
4. 按照屏幕上的指示进行操作。

管理应用程序和凭证

修改应用程序属性

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Services and Applications（服务和应用程序）**。
3. 在右窗格中的 **Single Sign On（单次登录）** 下，单击 **Manage Applications and Credentials（管理应用程序和凭证）**。
4. 单击要修改的应用程序项，然后单击 **Properties（属性）**。
5. 单击 **General（常规）** 标签以修改应用程序名称和说明。通过选中或清除相应设置旁的复选框来更改设置。
6. 单击 **Script（脚本）** 标签以查看和编辑单次登录应用程序脚本。
7. 单击 **OK（确定）**。

从单次登录中删除应用程序

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Services and Applications（服务和应用程序）**。
3. 在右窗格中的 **Single Sign On（单次登录）** 下，单击 **Manage Applications and Credentials（管理应用程序和凭证）**。
4. 单击要删除的应用程序项，然后单击 **Remove（删除）**。

5. 在确认对话框中单击 **Yes**（是）。
6. 单击 **OK**（确定）。

导出应用程序

您可以导出应用程序来创建单次登录应用程序脚本的备份副本。此文件随后可用于恢复单次登录数据。该文件是标识备份文件的一个补充，后者仅包含凭证信息。

要导出应用程序，请执行以下操作：

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Services and Applications**（服务和应用程序）。
3. 在右窗格中的 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和凭证）。
4. 单击要导出的应用程序项。然后单击 **More**（更多）> **Applications**（应用程序）> **Export Script**（导出脚本）。
5. 按照屏幕上的指示完成导出操作。
6. 单击 **OK**（确定）。

导入应用程序

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Services and Applications**（服务和应用程序）。
3. 在右窗格中的 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和凭证）。
4. 单击要导入的应用程序项。然后选择 **More**（更多）> **Applications**（应用程序）> **Import Script**（导入脚本）。
5. 按照屏幕上的指示完成导入操作。
6. 单击 **OK**（确定）。

修改凭证

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Services and Applications**（服务和应用程序）。
3. 在右窗格中的 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和凭证）。
4. 单击要修改的应用程序项，然后单击 **More**（更多）。

5. 选择以下任意选项：

- Applications（应用程序）
 - Add New（新添）
 - Remove（删除）
 - Properties（属性）
 - Import Script（导入脚本）
 - Export Script（导出脚本）
- Credentials（凭证）
 - Create New（新建）
- View Password（查看密码）



注： 您必须先验证您的标识才能查看密码。

6. 按照屏幕上的指示进行操作。

7. 单击 **OK**（确定）。

使用应用程序保护

您可以使用此功能配置对应用程序的访问。您可以根据以下标准限制访问：

- 用户类别
- 使用时间
- 用户非活动状态

限制对应用程序的访问

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Services and Applications**（服务和应用程序）。
3. 在右窗格中的 **Application Protection**（应用程序保护）下，单击 **Manage Protected Applications**（管理受保护的应用程序）。随即打开 **Application Protection Service**（应用程序保护服务）对话框。
4. 选择您要管理其访问权限的用户类别。



注： 如果用户类别不是 **Everyone**（所有人），您可能需要选择 **Override default settings**（覆盖默认设置）来覆盖 **Everyone**（所有人）类别的设置。

5. 单击 **Add**（添加）。随即打开 **Add a Program Wizard**（添加程序向导）。
6. 按照屏幕上的指示进行操作。

删除应用程序的保护

要删除应用程序的保护，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Services and Applications（服务和应用程序）**。
3. 在右窗格中的 **Application Protection（应用程序保护）** 下，单击 **Manage Protected Applications（管理受保护的应用程序）**。随即打开 **Application Protection Service（应用程序保护服务）** 对话框。
4. 选择您要管理其访问权限的用户类别。



注： 如果用户类别不是 Everyone（所有人），您可能需要单击 **Override default settings（覆盖默认设置）** 来覆盖 Everyone（所有人）类别的设置。

5. 单击要删除的应用程序项，然后单击 **Remove（删除）**。
6. 单击 **OK（确定）**。

更改受保护应用程序的限制设置

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Services and Applications（服务和应用程序）**。
3. 在右窗格中的 **Application Protection（应用程序保护）** 下，单击 **Manage Protected Applications（管理受保护的应用程序）**。随即打开 **Application Protection Service（应用程序保护服务）** 对话框。
4. 选择您要管理其访问权限的用户类别。



注： 如果用户类别不是 Everyone（所有人），您可能需要单击 **Override default settings（覆盖默认设置）** 来覆盖 Everyone（所有人）类别的设置。

5. 单击要更改的应用程序，然后单击 **Properties（属性）**。随即打开该应用程序的 **Properties（属性）** 对话框。
6. 单击 **General（常规）** 标签。选择以下设置之一：
 - Disabled（禁用）（无法使用）
 - Enabled（启用）（可以无限制使用）
 - Restricted（限制）（使用取决于设置）
7. 当您选择 Restricted（限制）时，以下设置可用：
 - a. 如果您要根据时间、日程或日期限制使用，请单击 **Schedule（日程）** 标签并配置设置。
 - b. 如果您要根据非活动状态限制使用，请单击 **Advanced（高级）** 标签并选择非活动的期限。
8. 单击 **OK（确定）** 关闭应用程序的 **Properties（属性）** 对话框。
9. 单击 **OK（确定）**。

高级任务（仅供管理员使用）

Credential Manager 的 “Authentication and Credentials”（验证和凭证）页和 “Advanced Settings”（高级设置）页仅供具有管理员权限的用户使用。在这些页面中，您可以执行以下任务：

- 指定用户和管理员的登录方式
- 配置自定义验证需求
- 配置凭证属性
- 配置 Credential Manager 设置

指定用户和管理员的登录方式

在 “Authentication and Credentials”（验证和凭证）页，您可以指定用户或管理员需要何种类型的（一种或多种）凭证。

要指定用户和管理员的登录方式，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Authentication and Credentials（验证和凭证）**。
3. 在右窗格中，单击 **Authentication（验证）** 标签。
4. 在类别列表中单击类别（**Users（用户）** 或 **Administrators（管理员）**）。
5. 在列表中单击验证方法类型（一种或多种）。
6. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

配置自定义验证需求

如果“Authentication and Credentials”（验证和凭证）页的 Authentication（验证）标签上未列出您所需的一组验证凭证，那么您可以创建自定义需求。

要配置自定义需求，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Authentication and Credentials（验证和凭证）**。
3. 在右窗格中，单击 **Authentication（验证）** 标签。
4. 在类别列表中单击类别（**Users（用户）** 或 **Administrators（管理员）**）。
5. 在验证方法列表中单击 **Custom（自定义）**。
6. 单击 **Configure（配置）**。
7. 选择要使用的验证方法。
8. 单击以下任一选项选择不同的方法组合：
 - Use AND to combine the authentication methods（使用 AND 组合验证方法）
（用户每次登录时必须使用您选中的所有方法进行验证）。
 - Use OR to require one of two or more authentication methods（使用 OR 要求从两种或更多验证方法中选择一种方法）
（用户每次登录时可以选择您选中的任何一种方法进行验证）。
9. 单击 **OK（确定）**。
10. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

配置凭证属性

在“Authentication and Credentials”（验证和凭证）页的 Credentials（凭证）标签上，您可以查看可用验证方法的列表并修改设置。

要配置凭证，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager（凭证管理器）**，然后单击 **Authentication and Credentials（验证和凭证）**。
3. 在右窗格中，单击 **Credentials（凭证）** 标签。
4. 单击要修改的凭证类型。您可以使用以下方法之一来修改凭证：
 - 要注册凭证，请单击 **Register（注册）**，然后按照屏幕上的指示进行操作。
 - 要删除凭证，请单击 **Clear（清除）**，然后在确认对话框中单击 **Yes（是）**。
 - 要修改凭证属性，请单击 **Properties（属性）**，然后按照屏幕上的指示进行操作。
5. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

配置 Credential Manager 设置

在“Settings”（设置）页中，您可以利用以下标签访问并修改多种设置：

- **General**（常规）— 允许您修改基本配置设置。
- **Single Sign On**（单次登录）— 允许您修改当前用户的单次登录设置，例如检测登录屏幕、自动登录到注册登录对话框以及显示密码等操作的处理方式。
- **Services and Applications**（服务和应用程序）— 允许您查看可用的服务并修改这些服务的相关设置。
- **Security**（安全保护）— 允许您选择指纹识别器软件并调整指纹识别器的安全级别。
- **Smart Cards and Tokens**（智能卡和身份标记）— 允许您查看并修改所有可用的 Java 卡和身份标记的属性。

要修改 Credential Manager 设置，请执行以下操作：

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Settings**（设置）。
3. 在右窗格中，单击要修改的相应标签。
4. 按照屏幕上的指示修改设置。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）。

示例 1 — 使用“**Advanced Settings**”（高级设置）页允许从 **Credential Manager** 进行 Windows 登录

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Settings**（设置）。
3. 在右窗格中，单击 **General**（常规）标签。
4. 在 **Select the way users log on to Windows (requires restart)**（选择用户登录 Windows 的方法（需要重新启动））下，选择 **Use Credential Manager with classic logon prompt**（在经典登录提示下使用凭证管理器）复选框。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）。
6. 重新启动笔记本电脑。



注： 选择 **Use Credential Manager with classic logon prompt**（在经典登录提示下使用凭证管理器）复选框可以让您锁定计算机。请参阅“[第 17 页的锁定笔记本电脑](#)”。

示例 2 — 使用“Advanced Settings”（高级设置）页要求在单次登录前进行用户验证

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Credential Manager**（凭证管理器），然后单击 **Settings**（设置）。
3. 在右窗格中，单击 **Single Sign On**（单次登录）标签。
4. 在 **When registered logon dialog or Web page is visited**（访问注册登录对话框或 Web 页时）下，选中 **Authenticate user before submitting credentials**（提交凭证之前验证用户）复选框。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）。
6. 重新启动笔记本电脑。

3 Embedded Security for HP ProtectTools



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

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

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

TPM 嵌入式安全保护芯片可以增强并支持 Embedded Security for HP ProtectTools 模块的其他安全保护功能。例如，在用户登录 Windows 时，Credential Manager for HP ProtectTools 可以利用嵌入式芯片进行验证。在某些机型上，TPM 嵌入式安全保护芯片还支持增强的 BIOS 安全保护功能，这些功能可通过 BIOS Configuration for HP ProtectTools 模块进行访问。

设置步骤



注意： 为降低安全风险，极力建议 IT 管理员立即初始化嵌入式安全保护芯片。如果未初始化嵌入式安全保护芯片，将可能导致未经授权的用户擅自使用、计算机蠕虫或病毒入侵计算机并控制计算机主人的任务，例如处理急救档案以及配置用户访问设置。

按照下面两节中的步骤操作可以启用并初始化嵌入式安全保护芯片。

启用嵌入式安全保护芯片

必须在计算机设置实用程序中启用嵌入式安全保护芯片。在 BIOS Configuration for HP ProtectTools 中无法执行此步骤。

要启用嵌入式安全保护芯片，请执行以下操作：

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

初始化嵌入式安全保护芯片

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

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

要初始化嵌入式安全保护芯片，请执行以下操作：

1. 在任务栏最右侧的通知区域中右击 HP ProtectTools Security Manager 图标，然后选择 **Embedded Security Initialization**（嵌入式安全保护功能初始化）。

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

2. 按照屏幕上的指示进行操作。

建立基本用户帐户

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

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



注意： 保护基本用户密钥密码。没有此密码将无法访问或恢复加密信息。

要建立基本用户帐户并启用用户安全保护功能，请执行以下操作：

1. 如果 Embedded Security 用户初始化向导没有打开，请选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security (嵌入式安全保护)**，然后单击 **User Settings (用户设置)**。
3. 在右窗格中的 **Embedded Security Features (嵌入式安全保护功能)** 下，单击 **Configure (配置)**。

随即打开 Embedded Security 用户初始化向导。

4. 按照屏幕上的指示进行操作。



注： 要安全地使用电子邮件，必须首先将电子邮件客户端配置为使用由 Embedded Security 模块创建的数字证书。如果没有可用的数字证书，则必须从认证机构获取一个数字证书。有关配置电子邮件和获取数字证书的说明，请参阅电子邮件客户端的联机帮助。

常规任务

在建立基本用户帐户后，您可以执行以下任务：

- 对文件和文件夹进行加密
- 发送和接收加密的电子邮件

使用个人安全驱动器

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

对文件和文件夹进行加密

处理加密文件时，请注意以下规则：

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

要对文件和文件夹进行加密，请执行以下操作：

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

发送和接收加密的电子邮件

使用 Embedded Security 模块，可以发送和接收加密的电子邮件，但对于不同的电子邮件客户端程序，相应的步骤可能会有所不同。有关详细信息，请参阅 Embedded Security 联机帮助和电子邮件客户端程序的联机帮助。

更改基本用户密钥密码

要更改基本用户密钥密码，请执行以下操作：

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

高级任务

备份和恢复

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

创建备份文件

要创建备份文件，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Backup（备份）**。
3. 在右窗格中，单击 **Backup（备份）**。随即打开 HP Embedded Security for ProtectTools 备份向导。
4. 按照屏幕上的指示进行操作。

通过备份文件恢复认证数据

要通过备份文件恢复数据，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Backup（备份）**。
3. 在右窗格中，单击 **Restore（恢复）**。随即打开 HP Embedded Security for ProtectTools 备份向导。
4. 按照屏幕上的指示进行操作。

更改主人密码

要更改主人密码，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Advanced（高级）**。
3. 在右窗格中的 **Owner Password（主人密码）** 下，单击 **Change（更改）**。
4. 键入原来的主人密码，然后设置并确认新的主人密码。
5. 单击 **OK（确定）**。

重置用户密码

管理员可以帮助用户重置忘记的密码。有关详细信息，请参阅联机帮助。

启用和禁用 Embedded Security

如果您希望在无安全保护功能的情况下工作，可以禁用 Embedded Security 功能。

您可以在两个不同的级别启用或禁用 Embedded Security 功能：

- 临时禁用 — 如果选择此选项，在 Windows 重新启动时将自动重新启用 Embedded Security 功能。默认情况下，此选项供所有用户使用。
- 永久禁用 — 如果选择此选项，必须输入主人密码，才可重新启用 Embedded Security 功能。此选项仅供管理员使用。

永久禁用 Embedded Security

要永久禁用 Embedded Security，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Advanced（高级）**。
3. 在右窗格中的 **Embedded Security（嵌入式安全保护）** 下，单击 **Disable（禁用）**。
4. 在系统提示时键入主人密码，然后单击 **OK（确定）**。

在永久禁用后启用 Embedded Security

要在永久禁用 Embedded Security 后启用该功能，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Embedded Security（嵌入式安全保护）**，然后单击 **Advanced（高级）**。
3. 在右窗格中的 **Embedded Security（嵌入式安全保护）** 下，单击 **Enable（启用）**。
4. 在系统提示时键入主人密码，然后单击 **OK（确定）**。

使用迁移向导迁移密钥

迁移是一种高级的管理员任务，允许管理、恢复和传输密钥及证书。

有关迁移的详细信息，请参阅 [Embedded Security 联机帮助](#)。

4 Java Card Security for HP ProtectTools

利用 Java Card Security for HP ProtectTools，可以对配备读卡器选件的笔记本电脑中的 Java 卡进行设置和配置。

利用 Java Card Security，您可以执行以下任务：

- 使用 Java Card Security 功能
- 与计算机设置实用程序一起使用，在开机环境中启用 Java 卡验证
- 为管理员和用户配置不同的 Java 卡。在加载操作系统之前，用户必须插入 Java 卡并键入个人标识号
- 设置和更改用于验证 Java 卡用户的个人标识号

常规任务

您可以通过“General”（常规）页执行以下任务：

- 更改 Java 卡个人标识号
- 选择读卡器



注： 读卡器可以使用 Java 卡 and 智能卡。如果您的笔记本电脑上有多个读卡器，就可以使用此功能。

更改 Java 卡个人标识号

要更改 Java 卡个人标识号，请执行以下操作：



注： Java 卡个人标识号必须介于 4 到 8 位数字字符之间。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **General（常规）**。
3. 将 Java 卡（使用现有的个人标识号）插入读卡器中。
4. 在右窗格中，单击 **Change（更改）**。
5. 在 **Change PIN（更改个人标识号）** 对话框中，将当前的个人标识号键入 **Current PIN（当前个人标识号）** 框。
6. 在 **New PIN（新个人标识号）** 框中键入新的个人标识号，然后在 **Confirm New PIN（确认新个人标识号）** 框中再次键入该个人标识号。
7. 单击 **OK（确定）**。

选择读卡器

在使用 Java 卡之前，请确保在 Java Card Security 模块中选择了正确的读卡器。如果没有选择正确的读卡器，则某些功能将不可用或不能正常显示。此外，必须正确安装读卡器驱动程序，并且在 Windows 设备管理器中显示出来。

要选择读卡器，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **General（常规）**。
3. 将 Java 卡插入读卡器中。
4. 在右窗格中的 **Selected card reader（选择读卡器）** 下，单击正确的读卡器。

高级任务（仅供管理员使用）

您可以通过“Advanced”（高级）页执行以下任务：

- 指定 Java 卡个人标识号
- 为 Java 卡指定名称
- 设置开机验证
- 备份和恢复 Java 卡



注： 您必须拥有 Windows 管理员权限才能显示“Advanced”（高级）页。

指定 Java 卡个人标识号

您必须为 Java 卡指定名称和个人标识号之后，才能将其用于 Java Card Security。

要指定 Java 卡个人标识号，请执行以下操作：



注： Java 卡个人标识号必须介于 4 到 8 位数字字符之间。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **Advanced（高级）**。
3. 将新的 Java 卡插入读卡器中。
4. 当 **New Card（新卡）** 对话框打开时，在 **New display name（新显示名）** 框中键入新名称，在 **New PIN（新个人标识号）** 框中键入新的个人标识号，然后在 **Confirm New PIN（确认新个人标识号）** 框中再次键入该新个人标识号。
5. 单击 **OK（确定）**。

为 Java 卡指定名称

您必须为 Java 卡指定名称之后，才能将其用于开机验证。

要为 Java 卡指定名称，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **Advanced（高级）**。
3. 将 Java 卡插入读卡器中。



注： 如果您还没有为此卡指定个人标识号，则会打开 **New Card（新卡）** 对话框，您可以在此键入新的名称和个人标识号。

4. 在右窗格中的 **Display name（显示名）** 下，单击 **Change（更改）**。
5. 在 **Name（名称）** 框中键入 Java 卡的名称。
6. 在 **PIN（个人标识号）** 框中键入当前的 Java 卡个人标识号。
7. 单击 **OK（确定）**。

设置开机验证

启用开机验证功能后，您需要使用 Java 卡才能启动计算机。

启用 Java 卡开机验证功能的过程包括以下步骤：

1. 在 BIOS Configuration 或计算机设置实用程序中启用 Java 卡开机验证支持。有关详细信息，请参阅“[第 47 页的启用和禁用智能卡开机验证支持](#)”。
2. 在 Java Card Security 模块中启用 Java 卡开机验证功能。
3. 创建并启用管理员 Java 卡。

启用 Java 卡开机验证并创建管理员 Java 卡

要启用 Java 卡开机验证，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security (Java 卡安全保护)**，然后单击 **Advanced (高级)**。
3. 将 Java 卡插入读卡器中。



注： 如果您还没有为此卡指定名称和个人标识号，则会打开 **New Card (新卡)** 对话框，您可以在此键入新的名称和个人标识号。

4. 在右窗格中的 **Power-on authentication (开机验证)** 下，选中 **Enable (启用)** 复选框。
5. 在 **Computer Setup Password (计算机设置实用程序密码)** 对话框中键入您的计算机设置实用程序密码，然后单击 **OK (确定)**。
6. 如果您没有启用驱动器锁保护功能，请键入 Java 卡个人标识号，然后单击 **OK (确定)**。

- 或 -

如果您启用了驱动器锁保护功能，请执行以下操作：

- a. 单击 **Make Java card identity unique (使 Java 卡标识唯一)**。

- 或 -

单击 **Make the Java card identity the same as the DriveLock password (使 Java 卡标识与驱动器锁密码相同)**。



注： 如果在笔记本电脑上启用了驱动器锁保护功能，您可以将 Java 卡标识设置为与驱动器锁用户密码相同，这样，在启动计算机时，只使用 Java 卡就可以同时验证驱动器锁和 Java 卡。

- b. 如果适用，请在 **DriveLock password (驱动器锁密码)** 框中键入驱动器锁用户密码，然后在 **Confirm password (确认密码)** 框中再次键入该密码。
 - c. 键入 Java 卡个人标识号。
 - d. 单击 **OK (确定)**。
7. 如果提示您创建恢复文件，请单击 **Cancel (取消)** 稍后创建恢复文件，或者单击 **OK (确定)**，然后按照 HP ProtectTools 备份向导的屏幕指示立即创建恢复文件。



注： 有关详细信息，请参阅“[第 8 页的 HP ProtectTools Backup and Restore](#)”。

创建用户 Java 卡



注： 必须设置开机验证和管理员卡才能创建用户 Java 卡。

要创建用户 Java 卡，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **Advanced（高级）**。
3. 插入将作为用户卡使用的 Java 卡。
4. 在右窗格中的 **Power-on authentication（开机验证）** 下，单击 **User card identity（用户卡标识）** 旁边的 **Create（创建）**。
5. 为用户 Java 卡键入个人标识号，然后单击 **OK（确定）**。

禁用 Java 卡开机验证

禁用 Java 卡开机验证后，访问计算机便无需再使用 Java 卡。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Java Card Security（Java 卡安全保护）**，然后单击 **Advanced（高级）**。
3. 插入管理员 Java 卡。
4. 在右窗格中的 **Power-on authentication（开机验证）** 下，取消选中 **Enable（启用）** 复选框。
5. 为 Java 卡键入个人标识号，然后单击 **OK（确定）**。

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools 模块允许用户对计算机设置实用程序安全保护功能和配置设置进行访问。这样一来，用户就可以通过 Windows 对计算机设置实用程序所管理的系统安全保护功能进行访问。

利用 BIOS Configuration 模块，您可以实现以下目标：

- 管理开机密码和管理员密码。
- 配置其他开机验证功能，如启用嵌入式安全保护验证支持。
- 启用和禁用硬件功能，如 CD-ROM 引导功能或各个硬件端口。
- 配置引导选项，其中包括启用多重引导功能和改变引导顺序。



注： BIOS Configuration for HP ProtectTools 模块的许多功能在计算机设置实用程序中亦可用。

常规任务

利用 BIOS Configuration，您可以管理各种计算机设置，否则这些设置就只能通过在启动时按 **f10** 键进入计算机设置实用程序进行访问。

管理引导选项

对于在打开或重新启动计算机时运行的任务，您可以使用 BIOS Configuration 来管理多种设置。

要管理引导选项，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration (BIOS 配置)**。
3. 按照 BIOS 管理员密码提示键入计算机设置实用程序的管理员密码，然后单击 **OK (确定)**。



注： 您必须首先设置计算机设置实用程序密码，才会显示 BIOS 管理员密码提示。有关设置计算机设置实用程序密码的详细信息，请参阅“[第 50 页的设定设置密码](#)”一节。

4. 在左窗格中，单击 **System Configuration (系统配置)**。
5. 在右窗格中，为 **f9**、**f10** 和 **f12** 键以及 **Express Boot Popup Delay (Sec) (快速引导弹出延迟 (秒))** 选择延迟时间（以秒计）。
6. 启用或禁用 **MultiBoot (多重引导)**。
7. 如果已启用了多重引导，请选择引导顺序，方法是先选择引导设备，然后单击向上箭头或向下箭头来调整设备在列表中的顺序。
8. 单击 **Apply (应用)**，然后在 HP ProtectTools 窗口中单击 **OK (确定)**。

启用和禁用系统配置选项



注： 您的计算机有可能不支持下面所列的某些项目。

要启用或禁用设备或安全保护选项，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**。
3. 按照 BIOS 管理员密码提示键入计算机设置实用程序的管理员密码，然后单击 **OK（确定）**。
4. 在左窗格中，单击 **System Configuration（系统配置）**，然后在右窗格中启用或禁用系统配置选项，或者配置以下任一系统配置选项：
 - 端口选项
 - 串行端口
 - 红外端口
 - 并行端口
 - SD 插槽
 - USB 端口
 - 1394 端口
 - Cardbus 插槽
 - ExpressCard 插槽
 - 引导选项
 - f9、f10 和 f12 键延迟（秒）
 - 多重引导
 - 快速引导弹出延迟（秒）
 - CD-ROM 引导
 - 软盘引导
 - 内部网络适配器引导
 - 内部网络适配器引导模式（PXE 或 RPL）
 - 引导顺序
 - 设备配置
 - 在引导时打开 NumLock
 - 交换 fn/Ctrl 键的功能
 - 多个指点设备
 - USB 传统支持

- 并行端口模式（标准、双向、EPP 或 ECP）
- 数据执行保护
- SATA 本机模式
- 双核 CPU
- 自动 Intel® SpeedStep 功能支持
- 在接通交流电源的情况下风扇始终开启
- BIOS DMA 数据传输
- Intel 或 AMD PSAE Execution Disable
- 内置设备选项
 - 嵌入式 WLAN 设备的无线功能
 - 嵌入式 WWAN 设备的无线功能
 - 嵌入式 Bluetooth® 设备的无线功能
 - LAN/WLAN 切换
 - 通过 LAN 唤醒处于省电状态的计算机

5. 单击 **Apply**（应用），然后在 HP ProtectTools 窗口中单击 **OK**（确定）以保存更改并退出。

高级任务

管理 HP ProtectTools 附加模块设置

HP ProtectTools Security Manager 的部分功能可以在 BIOS Configuration 模块中进行管理。

启用和禁用智能卡开机验证支持

启用此选项后，可以在开启计算机时使用智能卡进行用户验证。



注： 要完全启用开机验证功能，还必须使用 Java Card Security for HP ProtectTools 模块配置智能卡。

要启用智能卡开机验证支持，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration (BIOS 配置)**。
3. 按照 BIOS 管理员密码提示键入计算机设置实用程序的管理员密码，然后单击 **OK (确定)**。
4. 在左窗格中，单击 **Security (安全保护)**。
5. 在 **Smart Card Security (智能卡安全保护功能)** 下，单击 **Enable (启用)**。



注： 要禁用智能卡开机验证功能，请单击 **Disable (禁用)**。

6. 单击 **Apply (应用)**，然后在 HP ProtectTools 窗口中单击 **OK (确定)**。

启用和禁用 Embedded Security 的开机验证支持

启用此选项后，系统可以在您打开计算机时使用 TPM 嵌入式安全保护芯片（如果可用的话）进行用户验证。



注： 要完全启用开机验证功能，还必须使用 Embedded Security for HP ProtectTools 模块配置 TPM 嵌入式安全保护芯片。

要启用嵌入式安全保护功能的开机验证支持，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**。
3. 按照 BIOS 管理员密码提示键入计算机设置实用程序的管理员密码，然后单击 **OK（确定）**。
4. 在左窗格中，单击 **Security（安全保护）**。
5. 在 **Embedded Security（嵌入式安全保护）** 下，单击 **Enable Power-on Authentication Support（启用开机验证支持）**。



注： 要禁用 Embedded Security（嵌入式安全保护）的开机验证功能，请单击 **Disable（禁用）**。

6. 单击 **Apply（应用）**，然后在 HP ProtectTools 窗口中单击 **OK（确定）**。

启用和禁用驱动器锁自动保护硬盘驱动器功能

启用此选项后，便会在驱动器中自动生成和设置驱动器锁密码，并会利用 TPM 嵌入式安全保护芯片保护该密码。



注： 必须重新启动计算机且在系统提示输入密码时成功键入 TPM 嵌入式安全保护密码，自动生成的密码才会设置到驱动器中。

仅当计算机已安装并初始化了 TPM 安全保护芯片，而且没有启用任何驱动器锁密码时，启用驱动器锁自动保护功能的选项才可用。有关如何启用并初始化 TPM 安全保护芯片的说明，请参阅“[第 28 页的启用嵌入式安全保护芯片](#)”和“[第 29 页的初始化嵌入式安全保护芯片](#)”。



注： 如果您已在计算机上手动设置驱动器锁密码，则必须首先将其禁用，才能设置驱动器锁自动保护功能。

要启用或禁用驱动器锁自动保护功能，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration (BIOS 配置)**。
3. 按照 BIOS 管理员密码提示键入计算机设置实用程序的管理员密码，然后单击 **OK (确定)**。
4. 在左窗格中，单击 **Security (安全保护)**。
5. 在 **Embedded Security (嵌入式安全保护)** 下，单击 **Automatic DriveLock Support (驱动器锁自动保护功能支持)** 旁边的 **Enable (启用)**。



注： 要禁用 Embedded Security 的驱动器锁自动保护功能，请单击 **Disable (禁用)**。

6. 单击 **Apply (应用)**，然后在 HP ProtectTools 窗口中单击 **OK (确定)**。

管理计算机设置实用程序密码

您可以使用 BIOS Configuration 模块来设置并更改计算机设置实用程序中的开机密码和设置密码，以及管理不同的密码设置。



注意： 通过 BIOS Configuration 中的“Passwords”（密码）页设置密码后，单击 HP ProtectTools 窗口中的 **Apply (应用)** 或 **OK (确定)** 按钮将立即保存密码。请务必牢记所设的密码，因为必须提供先前所设的密码方能撤消密码。

开机密码可以阻止他人未经授权擅自使用您的笔记本计算机。



注： 设置了开机密码后，“Passwords”（密码）页上的 Set（设置）按钮将替换为 Change（更改）按钮。

计算机设置实用程序密码用于保护计算机设置实用程序中的配置设置和系统标识信息。设置该密码后，必须使用该密码才能访问计算机设置实用程序。如果您设定了设置密码，系统在打开 HP ProtectTools 的 BIOS Configuration 模块之前将提示您输入密码。



注： 设定了设置密码后，“Passwords”（密码）页上的 Set（设置）按钮将替换为 Change（更改）按钮。

设置开机密码

要设置开机密码，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**，然后单击 **Security（安全保护）**。
3. 在右窗格中，单击 **Power-On Password（开机密码）** 旁边的 **Set（设置）**。
4. 在 **Enter Password（输入密码）** 和 **Verify Password（验证密码）** 框中键入并确认密码。
5. 在 **Passwords（密码）** 对话框中单击 **OK（确定）**。
6. 单击 **Apply（应用）**，然后在 HP ProtectTools 窗口中单击 **OK（确定）**。

更改开机密码

要更改开机密码，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**，然后单击 **Security（安全保护）**。
3. 在右窗格中，单击 **Power-On Password（开机密码）** 旁边的 **Change（更改）**。
4. 在 **Old Password（旧密码）** 框中键入当前的密码。
5. 在 **Enter New Password（输入新密码）** 框中设置并确认新密码。
6. 在 **Passwords（密码）** 对话框中单击 **OK（确定）**。
7. 单击 **Apply（应用）**，然后在 HP ProtectTools 窗口中单击 **OK（确定）**。

设定设置密码

要设定计算机设置实用程序密码，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**，然后单击 **Security（安全保护）**。
3. 在右窗格中，单击 **Setup Password（设置密码）** 旁边的 **Set（设置）**。
4. 在 **Enter Password（输入密码）** 和 **Confirm Password（确认密码）** 框中键入并确认密码。
5. 在 **Passwords（密码）** 对话框中单击 **OK（确定）**。
6. 单击 **Apply（应用）**，然后在 HP ProtectTools 窗口中单击 **OK（确定）**。

更改设置密码

要更改计算机设置实用程序密码，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration（BIOS 配置）**，然后单击 **Security（安全保护）**。
3. 在右窗格中，单击 **Setup Password（设置密码）** 旁边的 **Change（更改）**。
4. 在 **Old Password（旧密码）** 框中键入当前的密码。

5. 在 **Enter New Password**（输入新密码）和 **Verify New Password**（验证新密码）框中键入并确认新密码。
6. 在 **Passwords**（密码）对话框中单击 **OK**（确定）。
7. 单击 **Apply**（应用），然后在 HP ProtectTools 窗口中单击 **OK**（确定）。

设置密码选项

您可以使用 BIOS Configuration for HP ProtectTools 模块来设置密码选项，以增强系统的安全性。

启用和禁用严格的安全保护功能



注意： 为了防止计算机永久不能使用，请记录所配置的设置密码、开机密码或智能卡的个人标识号，并将其存放到远离计算机的安全地点。不输入上述密码或个人标识号，就无法从计算机上解除锁定。

启用严格的安全保护功能后，可以在开机密码和管理员密码以及其他形式的开机验证功能的基础上，进一步强化安全保护性能。

要启用或禁用严格的安全保护功能，请执行以下操作：

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration**（BIOS 配置），然后单击 **Security**（安全保护）。
3. 在右窗格中的 **Password Options**（密码选项）下，启用或禁用 **Stringent Security**（严格的安全保护功能）。



注： 如果您希望禁用严格的安全保护功能，请清除 **Enable Stringent Security**（启用严格的安全保护功能）复选框。

4. 单击 **Apply**（应用），然后在 HP ProtectTools 窗口中单击 **OK**（确定）。

启用和禁用在 Windows 重新启动时的开机验证功能

启用此选项后，Windows 重新启动时会要求用户输入开机密码、TPM 密码或智能卡密码，从而增强安全性。

要启用或禁用在 Windows 重新启动时的开机验证功能，请执行以下操作：

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **BIOS Configuration**（BIOS 配置），然后单击 **Security**（安全保护）。
3. 在右窗格中的 **Password Options**（密码选项）下，启用或禁用 **Require password on restart**（重新启动时需要输入密码）。
4. 单击 **Apply**（应用），然后在 HP ProtectTools 窗口中单击 **OK**（确定）。

6 Device Access Manager for HP ProtectTools

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

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

启动后台服务

要应用设备配置文件，必须运行 HP ProtectTools Device Locking/Auditing 后台服务。当您第一次尝试应用设备配置文件时，HP ProtectTools Security Manager 会打开一个对话框，询问您是否要启动后台服务。单击 **Yes**（是）启动后台服务，并将其设置为每次系统启动时自动启动。

简单配置

您可以使用此功能来拒绝对下类设备的访问：

- 所有非管理员用户对 USB 设备的访问
- 所有非管理员用户对所有可移动介质（软盘、随身驱动盘）的访问
- 所有非管理员用户对所有 DVD/CD-ROM 驱动器的访问
- 所有非管理员用户对所有串行和并行端口的访问

要拒绝所有非管理员用户访问某类设备，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager（设备访问管理器）**，然后单击 **Simple Configuration（简单配置）**。
3. 在右窗格中，选中表示要拒绝访问的设备的复选框。
4. 单击 **Apply（应用）**。



注： 如果后台服务未运行，则它立即尝试启动。单击 **Yes（是）** 允许它启动。

5. 单击 **OK（确定）**。

设备类别配置（高级）

还有更多选项可用来授予或者拒绝特定用户或用户组对多个设备类型的访问。

添加用户或组

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager（设备访问管理器）**，然后单击 **Device Class Configuration（设备类别配置）**。
3. 在设备列表中，单击您想要配置的设备类别。
4. 单击 **Add（添加）**。随即打开 **Select Users or Groups（选择用户或组）** 对话框。
5. 选择 **Advanced（高级） > Find Now（立即查找）** 搜索要添加的用户或组。
6. 单击要添加到有效用户和组列表中的用户或组，然后单击 **OK（确定）**。
7. 单击 **OK（确定）**。

删除用户或组

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager（设备访问管理器）**，然后单击 **Device Class Configuration（设备类别配置）**。
3. 在设备列表中，单击您想要配置的设备类别。
4. 单击您要删除的用户或组，然后单击 **Remove（删除）**。
5. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

拒绝用户或组访问

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager（设备访问管理器）**，然后单击 **Device Class Configuration（设备类别配置）**。
3. 在设备列表中，单击您想要配置的设备类别。
4. 在 **User/Groups（用户/组）** 中，单击要拒绝其访问的用户或组。
5. 单击要拒绝其访问的用户或组旁边的 **Deny（拒绝）**。
6. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

允许组中一个用户访问某个设备类别

您可以允许一个用户访问某个设备类别，同时拒绝该用户所在组中的其他所有成员的访问。

要允许一个用户访问而不允许组访问，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager (设备访问管理器)**，然后单击 **Device Class Configuration (设备类别配置)**。
3. 在设备列表中，单击您想要配置的设备类别。
4. 在 **User/Groups (用户/组)** 中，添加要拒绝其访问的组。
5. 单击要拒绝其访问的组旁边的 **Deny (拒绝)**。
6. 找到所需设备类别下的文件夹，然后添加指定用户。单击 **Allow (允许)** 授予该用户访问权限。
7. 单击 **Apply (应用)**，然后单击 **OK (确定)**。

允许组中一个用户访问特定设备

您可以允许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。

要允许一个用户访问而不允许组访问特定设备，请执行以下操作：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Device Access Manager (设备访问管理器)**，然后单击 **Device Class Configuration (设备类别配置)**。
3. 在设备列表中，单击您想要配置的设备类别，然后找到该类别下的文件夹。
4. 在 **User/Groups (用户/组)** 中，添加要拒绝其访问的组。
5. 单击要拒绝其访问的组旁边的 **Deny (拒绝)**。
6. 在设备列表中找到允许该用户访问的特定设备。
7. 单击 **Add (添加)**。随即打开 **Select Users or Groups (选择用户或组)** 对话框。
8. 选择 **Advanced (高级) > Find Now (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 **OK (确定)**。
10. 单击 **Allow (允许)** 授予该用户访问权限。
11. 单击 **Apply (应用)**，然后单击 **OK (确定)**。

7 Drive Encryption for HP ProtectTools



注意： 如果您决定卸载 Drive Encryption 模块，则必须先对所有已加密的驱动器进行解密。如果您没有解密，则无法访问加密驱动器上的数据，除非您注册了 Drive Encryption 恢复服务（请参阅“[第 62 页的恢复](#)”）。重新安装 Drive Encryption 模块也无法使您能够访问已加密的驱动器。

加密管理

加密驱动器

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption**（驱动器加密），然后单击 **Encryption Management**（加密管理）。
3. 在右窗格中，单击 **Activate**（激活）。打开 Drive Encryption for HP ProtectTools 向导。
4. 按照屏幕上的指示激活加密。



注： 您需要指定用于存储恢复信息的软盘、闪存设备或其他 USB 连接存储介质。

更改加密

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption**（驱动器加密），然后单击 **Encryption Management**（加密管理）。
3. 在右窗格中，单击 **Change encryption**（更改加密）。在 **Change Encryption**（更改加密）对话框中选择要加密的磁盘，然后单击 **OK**（确定）。
4. 再次单击 **OK**（确定）开始加密。

解密驱动器

1. 选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption**（驱动器加密），然后单击 **Encryption Management**（加密管理）。
3. 在右窗格中，单击 **Deactivate**（取消激活）。

用户管理

添加用户

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption (驱动器加密)**，然后单击 **User Management (用户管理)**。
3. 在右窗格中，单击 **Add (添加)**。单击 **User Name (用户名)** 列表中的用户名，或在 **Username (用户名)** 框中键入用户名。单击 **Next (下一步)**。
4. 键入选定用户的 Windows 密码，然后单击 **Next (下一步)**。
5. 选择新用户的验证方法，然后单击 **Finish (完成)**。

删除用户

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption (驱动器加密)**，然后单击 **User Management (用户管理)**。
3. 在右窗格中，单击 **User Name (用户名)** 列表中要删除的用户名。单击 **Remove (删除)**。
4. 单击 **Yes (是)** 确认要删除选定的用户。

更改身份标记

按以下步骤更改用户的验证方法：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption (驱动器加密)**，然后单击 **User Management (用户管理)**。
3. 在右窗格中，从 **User Name (用户名)** 列表中选择用户名，然后单击 **Change Token (更改身份标记)**。
4. 键入该用户的 Windows 密码，然后单击 **Next (下一步)**。
5. 选择新的验证方法，然后单击 **Finish (完成)**。
6. 如果您选择了 Java 卡作为验证方法，请在出现提示时键入 Java 卡密码，然后单击 **OK (确定)**。

设置密码

按以下步骤设置密码或更改用户的验证方法：

1. 选择 **Start (开始) > All Programs (所有程序) > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption (驱动器加密)**，然后单击 **User Management (用户管理)**。
3. 在右窗格中，从 **User Name (用户名)** 列表中选择用户，然后单击 **Set Password (设置密码)**。
4. 键入该用户的 Windows 密码，然后单击 **Next (下一步)**。
5. 选择新的验证方法，然后单击 **Finish (完成)**。
6. 如果您选择了 Java 卡作为验证方法，请在出现提示时键入 Java 卡密码，然后单击 **OK (确定)**。

恢复

您可以使用以下两种安全措施：

- 如果您忘记了密码，则无法访问已加密的驱动器。不过，您可以注册驱动器加密恢复服务，以便您在忘记密码的时候访问计算机。
- 您可以在软盘、闪存设备或其他 USB 连接存储介质上存储驱动器加密密钥。

注册驱动器加密恢复服务

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption（驱动器加密）**，然后单击 **Recovery（恢复）**。
3. 在右窗格中，单击 **Click here to register（单击此处进行注册）**。键入必要的信息以完成安全保护备份过程。

备份驱动器加密密钥

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager**。
2. 在左窗格中，单击 **Drive Encryption（驱动器加密）**，然后单击 **Recovery（恢复）**。
3. 在右窗格中，单击 **Click here to backup your keys（单击此处备份您的密钥）**。
4. 选择用于存储恢复信息的软盘、闪存设备或其他 USB 连接存储介质，然后单击 **Next（下一步）**。打开 Drive Encryption for HP ProtectTools 向导。
5. 按照屏幕上的指示备份驱动器加密密钥。



注： 您需要指定用于存储恢复信息的软盘、闪存设备或其他 USB 连接存储介质。

8 故障排除

Credential Manager for HP ProtectTools

简短说明	详细说明	解决方法
使用 Credential Manager Network Accounts (Credential Manager 网络帐户) 选项, 用户可以选择要登录的域帐户。使用 TPM 验证时, 此选项不可用。所有其他验证方法可以正常使用。	使用 TPM 验证, 用户只能登录本地计算机。	用户可以使用 Credential Manager 的单次登录工具验证其他帐户。
USB 身份标记凭证不可用于登录 Windows XP Service Pack 1。	安装 USB 身份标记软件、注册 USB 身份标记凭证并设置 Credential Manager 作为主登录后, 则 USB 身份标记既不被列出, 也不可用于 Credential Manager/GINA 登录。 在登录返回 Windows, 注销 Credential Manager, 再登录 Credential Manager 并重新选择身份标记作为主登录后, 则身份标记登录操作将正常进行。	通过 Windows Update 将 Windows 更新到 Service Pack 2。 如果保留 Service Pack 1, 则使用其他凭证 (Windows 密码) 登录回 Windows, 以便注销并重新登录回 Credential Manager。
某些应用程序 Web 页出现错误, 阻止用户执行或完成任务。	由于禁用单次登录的功能模式, 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。	Credential Manager 单次登录并不支持所有软件的 Web 界面。通过关闭单次登录支持禁用对特定 Web 页的单次登录支持。请参见 Credential Manager 联机帮助文件提供的有关单次登录的完整文档说明。 如果无法对给定应用程序禁用单次登录功能, 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。	由于为降低安全风险删除了浏览选项, 因此用户不能移动 Credential Manager 中已注册的虚拟身份标记的位置。	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。	当域管理员登录到域中, 并使用一个具有域和本地计算机管理员权限的帐户在 Credential Manager 中注册了域身份之后, 就会发生这种情况。当域管理员试图从 Credential Manager 中修改 Windows 密码时, 管理员将得到登录失败错误: User account restriction (用户帐户限制) 。	Credential Manager 不能通过 Change Windows password (更改 Windows 密码) 来更改域用户的帐户密码。Credential Manager 只能更改本地 PC 帐户密码。域用户可以通过 Windows security (Windows 安全性) > Change password (更改密码) 选项来更改其密码, 但是, 由于域用户在本机 PC 上没有实际帐户, 因此 Credential Manager 只能更改用于登录的密码。
Credential Manager 存在与 Corel WordPerfect 12 密码 GINA 不兼容的问题。	如果用户登录 Credential Manager, 在 WordPerfect 中创建文档, 并用保护密码进行保存, 则无论以手动还是自动方式,	HP 正在研究未来产品增强功能的解决之道。

简短说明	详细说明	解决方法
	Credential Manager 都无法检测或识别密码 GINA。	
Credential Manager 无法识别屏幕上的 Connect (连接) 按钮。	如果将远程桌面连接 (RDP) 的单次登录凭证设置为 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。
用户可能会丢失受 TPM 保护的所有 Credential Manager 凭证。	如果 TPM 模块被删除或损坏，用户将丢失用它来保护的所有凭证。	这是有意设计的。 TPM 模块设计用于保护 Credential Manager 凭证。HP 建议用户在删除 TPM 模块之前，在 Credential Manager 中备份其标识。
仅在 Windows XP Service Pack 1 上，当从睡眠模式转换到休眠模式后，用户无法登录 Credential Manager。	在允许系统切换进入休眠和睡眠模式后，管理员或用户无法登录到 Credential Manager，并且无论选择了哪一种登录凭证（密码、指纹或 Java 卡），都一直显示 Windows 登录屏幕。	通过 Windows Update 将 Windows 更新到 Service Pack 2。有关此问题原因的详细信息，请参阅 Microsoft 网站上的 Microsoft 知识库文章 813301： http://www.microsoft.com。 要进行登录，用户必须选择 Credential Manager 并登录。登录 Credential Manager 后，将提示用户登录 Windows（用户可能需要选择 Windows 登录选项）以完成登录过程。 如果用户先登录 Windows，则必须手动登录到 Credential Manager。
恢复嵌入式安全保护功能会导致 Credential Manager 无法运行。	将 ROM 恢复到出厂设置后，Credential Manager 将无法注册任何凭证。	如果在安装 Credential Manager 后将 ROM 重置为出厂设置，则 Credential Manager 无法访问 TPM。 可以使用 f10 计算机设置实用程序、BIOS Configuration 模块或 HP Client Manager 来启用 TPM 嵌入式安全保护芯片。要使用计算机设置实用程序来启用 TPM 嵌入式安全保护芯片，请执行以下步骤： 1. 打开或重新启动笔记本电脑，当屏幕的左下角显示 f10 = ROM Based Setup (f10 = 基于 ROM 的设置) 消息时，按 f10 键以打开计算机设置实用程序。 2. 使用箭头键选择 Security (安全保护) > Setup Password (设置密码)。设置密码。 3. 选择 Embedded Security Device (嵌入式安全保护设备)。 4. 使用箭头键选择 Embedded Security Device - Disable (嵌入式安全保护设备 - 禁用)。使用箭头键将其更改为 Embedded Security Device - Enable (嵌入式安全保护设备 - 启用)。 5. 选择 Enable (启用) > Save changes and exit (保存更改并退出)。 HP 正在调研未来用户软件版本的解决问题方向。
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，Credential Manager 可能会丢失与登录屏幕上的虚拟身份标记位置的关联性。即使 Credential Manager 已经注册虚拟身份标记，但用户必须注册该身份标记才能恢复关联性。	目前是有意这样设计的。 如果没有保留标识就卸载 Credential Manager，则会破坏身份标记的系统（服务器）部分，因此即使通过标识恢复还原了该身份标记的客户端部分，该身份标记不能再用于登录。 HP 正在研究长远的解决问题方向。

Embedded Security for HP ProtectTools

简短说明	详细说明	解决方法
加密 PSD 上的文件夹、子文件夹和文件时出现错误消息。	如果用户将文件和文件夹复制到 PSD 并尝试加密文件夹/文件或文件夹/子文件夹，则显示 Error Applying Attributes (应用属性时出错) 消息。用户可以加密 C:\ 驱动器和额外安装的硬盘驱动器上的相同文件。	这是有意设计的。 将文件/文件夹移动到 PSD 时会自动对它们进行加密。没有必要对文件/文件夹进行“双重加密”。试图使用 EFS 在 PSD 上对文件/文件夹进行“双重加密”会导致出现此错误消息。
在多引导平台上无法控制其他操作系统。	如果将某个驱动器设置成可以从多个操作系统来引导，则在某一个操作系统中只能使用平台初始化向导来控制该驱动器。	这是出于安全考虑有意这样设计的。
未授权的管理员可以查看、删除、重命名或移动已加密的 EFS 文件夹的内容。	对文件夹进行加密并不能阻止拥有管理权限的未授权用户查看、删除或移动该文件夹的内容。	这是有意设计的。 它是 EFS 的一个功能，而不是嵌入式安全保护 TPM。Embedded Security 模块使用 Microsoft EFS 软件，并且 EFS 为所有管理员保留对文件/文件夹的访问权限。
如果用户试图使用 FAT32 恢复硬盘驱动器，则无法进行加密。	如果用户试图使用 FAT32 恢复硬盘驱动器，则不能使用 EFS 加密文件/文件夹。	这是有意设计的。软件不应当安装在用 FAT32 恢复的分区上。 Microsoft EFS 仅在 NTFS 上受支持，在 FAT32 上不起作用。这是 Microsoft EFS 的一个功能，与 HP ProtectTools 软件无关。
用户能够加密或删除恢复档案 XML 文件。	在设计上没有为此文件夹设置 ACL；因此，用户可以有意无意地加密或删除文件，使该文件不可访问。在加密或删除此文件后，任何用户都无法使用 TPM 软件。	这是有意设计的。 用户有访问急救档案的权限，因此可以保存/更新其基本用户密钥备份副本。应当告知用户绝不要加密或删除急救档案文件。
Embedded Security EFS 与 Symantec Antivirus 或 Norton Antivirus 交互会导致加密/解密和扫描的时间延长。	已加密的文件会干扰 Symantec Antivirus 或 Norton Antivirus 2005 病毒扫描。在扫描过程中，基本用户密码提示要求用户每大约 10 个文件输入一次密码。如果用户没有键入密码，则基本用户密码提示将超时，允许 NAV2005 继续扫描。当 Symantec Antivirus 或 Norton Antivirus 正在运行时，使用 Embedded Security EFS 加密文件需要更长的时间。	要缩短扫描 Embedded Security EFS 文件所需要的时间，用户可以在扫描之前键入加密密码或解密。 要缩短使用 Embedded Security EFS 加密/解密数据所需的时间，用户应当在 Symantec Antivirus 或 Norton Antivirus 上禁用自动保护功能。
急救档案无法保存到移动介质上。	如果用户在 Embedded Security 初始化过程中创建急救档案路径时插入 MMC 或 SD 存储卡，则会显示一条错误消息。	这是有意设计的。 不支持将急救档案存储在移动介质上。急救档案可以存储在网络驱动器或除 C 盘以外的其他本地驱动器上。
掉电产生的错误会中断 Embedded Security 初始化。	如果在初始化嵌入式安全保护芯片过程中出现掉电，则会导致以下问题： - 尝试启动 Embedded Security 初始化向导时，显示以下错误消息： The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner (由于嵌入式安全保护芯片已经有嵌入式安全保护模块主人，无法初始化嵌入式安全保护)。 - 尝试启动用户初始化向导时，显示以下错误消息：The Embedded security is not initialized. To use	要从掉电中恢复，请执行以下步骤：  注： 使用箭头键选择不同的菜单、菜单项，并更改值（除非另有说明）。 1. 启动或重新启动计算机。 2. 当屏幕上出现 f10=Setup (f10= 设置) 消息时，按 f10 键。 3. 选择合适的语言选项。 4. 按 enter 键。 5. 选择 Security (安全保护) > Embedded Security (嵌入式安全保护)。

简短说明	详细说明	解决方法
	the wizard, the Embedded Security must be initialized first. (未初始化嵌入式安全保护。要使用向导, 必须首先初始化嵌入式安全保护)。	6. 将 Embedded Security Device (嵌入式安全保护设备) 选项设置为 Enable (启用)。 7. 按 f10 键接受更改。 8. 选择 File (文件) > Save Changes and Exit (保存更改并退出)。 9. 按 enter 键。 10. 按 f10 键保存更改并退出实用程序。
在启用 TPM 模块后, 可以删除计算机设置 (f10) 实用程序密码。	启用 TPM 模块需要有计算机设置 (f10) 实用程序密码。启用该模块后, 用户可以删除该密码。这允许任何对系统具有直接访问权限的用户重置 TPM 模块, 并可能会导致数据丢失。	这是有意设计的。 只有知道密码的用户才能删除计算机设置 (f10) 实用程序密码。不过, HP 极力建议任何时候都要保护计算机设置 (f10) 实用程序密码。
当系统从等待状态中激活时, 不在显示 PSD 密码框	当用户在创建 PSD 后登录系统时, TPM 要求用户输入基本用户密码。如果用户没有键入该密码并且系统启动等待模式, 则当用户恢复运行时不再显示密码对话框。	这是设计要求的。 用户必须先注销, 然后重新登录, 才能再次看到 PSD password (PSD 密码) 框。
更改 Security Platform Policies (安全平台策略) 不需要密码。	系统中拥有管理权限的用户在访问 Security Platform Policies (安全平台策略) (计算机和用户) 时, 不需要使用 TPM 密码。	这是设计要求的。 任何管理员都有权更改带有或不带有 TPM 用户初始化的 Security Platform Policies (安全平台策略)。
查看证书时, 它显示为不受信任。	在设置 HP ProtectTools 并运行用户初始化向导后, 用户能够查看已签发的证书; 不过在查看证书时, 证书显示为不受信任。尽管可以通过单击安装按钮安装证书, 但此时安装并不能使证书变为受信任。	自签名证书不受信任。在适当配置的企业环境中, 由联机认证机构颁发的 EFS 证书受信任。
出现间断性加密和解密错误: 因为其他进程正在使用文件, 所以此进程无法访问文件。	这是在文件加密或解密过程中出现的罕见间断性错误, 只在文件正在被其他进程使用的情况下才发生, 即使操作系统或其他应用程序未在处理该文件或文件夹。	要解决这一错误, 请执行以下操作: 1. 重新启动系统。 2. 注销退出。 3. 重新登录。
如果在完成新数据生成或传输之前取出存储介质, 就会造成移动存储介质中的数据丢失。	取出诸如多功能插槽硬盘驱动器这类存储介质后仍显示 PSD 可用, 并且在向该 PSD 添加/修改数据时也不生成错误。当系统重新启动后, PSD 没有反映在移动存储设备不可用时发生的文件变更。	不要在数据生成或传输完成之前取出 PSD。这个问题只在以下情况中发生: 用户访问 PSD, 然后在完成新数据生成或传输之前取出硬盘驱动器。如果用户试图在没有移动硬盘驱动器的情况下访问 PSD, 则会显示一条错误消息: the device is not ready (设备未就绪)。
在卸载过程中, 如果用户没有初始化基本用户并打开管理工具, 则 Disable (禁用) 选项不可用, 并且在关闭管理工具之前, 卸载程序不会继续运行。	用户可以选择在没有禁用 TPM 的情况下进行卸载, 或者选择先禁用 TPM (通过管理工具) 然后再卸载的方法。访问管理工具需要基本用户密钥初始化。如果未进行基本的初始化, 则用户无法访问所有选项。 由于用户已经明确选择打开管理工具 (通过在提示 Click Yes to open Embedded Security Administration tool (单击“是”以打开嵌入式安全保护管理工具) 对话框中单击 Yes (是)), 卸载会等到管理工具关闭后才进行。如	管理工具用于禁用 TPM 芯片, 但该选项只有在初始化基本用户密钥后才能使用。如果未进行初始化, 请选择 OK (确定) 或 Cancel (取消) 继续进行卸载。

简短说明	详细说明	解决方法
	果用户在该对话框中单击 No (否) ，则管理工具不会打开，并且卸载继续进行。	
在用两个用户帐户创建 PSD 并在 128 MB 系统配置中使用快速用户切换后，会出现间断性系统锁定。	在最小内存模式下使用快速用户切换时，系统锁定后会出现黑屏，并且键盘和鼠标都没有响应，而不会显示欢迎使用（登录）屏幕。	根本原因可能是低内存配置中的定时问题。 集成图形使用的 UMA 体系结构占用 8 MB 内存，这使得用户只能使用剩余的 120 MB 内存。当两个登录的用户共享这 120 MB 内存并进行快速用户切换时，就会出现此错误。 解决方法是重新引导系统并增加内存配置（HP 没有提供带安全模块的 128 MB 配置）。
EFS 用户验证（密码请求）超时，显示 access denied (访问被拒绝) 。	当用户单击 OK (确定) 或系统退出等待模式后，会重新打开 EFS 用户验证密码。	这是有意设计的，以避免 Microsoft EFS 出现问题（创建一个 30 秒监视程序定时器以生成错误消息）。
在安装日文版过程中，在功能描述中出现小截断。	功能描述在自定义设置安装向导选项过程中被截断。	HP 将在以后的版本纠正这一问题。
EFS 加密无需提示输入密码就可以使用。	通过提示用户密码超时，还可以对文件或文件夹使用加密。	加密功能无需密码验证，因为这是 Microsoft EFS 加密的一个特点。解密时需要用户提供密码。
即使未在用户初始化向导中指定安全电子邮件，或者使用用户策略禁用安全电子邮件配置时，都支持安全电子邮件。	嵌入式安全保护软件和向导并不控制电子邮件客户端（Outlook、Outlook Express 或 Netscape）的设置。	这种方式是有意设计的。TPM 电子邮件设置的配置不会禁止在电子邮件客户端中直接编辑加密设置。安全电子邮件的使用由第三方应用程序设置和控制。HP 向导将这三种参照应用程序联系起来，以便快速进行自定义。
在同一台计算机或以前初始化的计算机上第二次运行 Large Scale Deployment（大规模部署）将覆盖急救和急救身份标记文件。新文件对于恢复没有什么作用。	在任何以前初始化的 HP ProtectTools Embedded Security 系统上运行 Large Scale Deployment（大规模部署）将会使现有的急救档案和恢复身份标记失去作用，除非覆盖这些 XML 文件。	HP 正在努力解决这个 XML 文件覆盖问题，并在将来的 SoftPak 包中提供解决方法。
当用户在 Embedded Security 中恢复时，自动登录脚本不起作用。	在用户执行以下操作后发生错误： - 在 Embedded Security 模块中初始化主人和用户（使用默认位置 - 我的文档）。 - 在 BIOS 中将芯片重置为出厂设置。 - 重新引导计算机。 - 开始恢复 Embedded Security。在恢复过程中，Credential Manager 提示系统是否可以自动登录到 Infineon TPM User Authentication。如果用户选择 Yes (是)，则会在文本框中自动显示 SPemRecToken 的位置。 即使该位置正确，也会显示以下错误消息：No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.（未提供急救身份标记。请选择检索急救身份标记的位置。）	单击屏幕上的 Browse (浏览) 按钮选择一个位置，然后恢复过程继续进行。

简短说明	详细说明	解决方法
多用户 PSD 在快速用户切换环境中不能运行。	当创建多个用户并对 PSD 使用相同的驱动器盘符时就会出现此错误。如果在加载 PSD 时试图在用户之间进行快速用户切换，则第二个用户的 PSD 不可用。	只有在重新配置使用其他驱动器盘符或注销第一个用户后，第二个用户的 PSD 才能使用。
在格式化生成 PSD 所在的硬盘驱动器后，将禁用 PSD，并且无法将其删除。	PSD 图标仍然显示，但在用户尝试访问该 PSD 时显示一条错误消息：drive is not accessible（驱动器不可访问）。 用户无法删除 PSD 并显示以下消息：your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process（您的 PSD 仍在使用，请确保您的 PSD 没有包含打开的文件，并且没有被其他进程访问）。用户必须重新引导系统才能删除 PSD，并且在重新引导后不再加载。	这是有意设计的：如果用户强行删除或从 PSD 数据的存储位置断开连接，则嵌入式安全保护 PSD 驱动器模拟继续运行，并根据缺少通信和丢失数据生成错误。 解决方法：在下次重新引导时，仿真将无法加载，用户可以删除旧的 PSD 仿真，然后创建新的 PSD。
当用户从 Automatic Backup Archive（自动备份档案）恢复时检测出内部错误。	在 Embedded Security 模块中，如果用户单击 Restore under Backup（在备份下恢复） 选项从自动备份档案中恢复，然后选择 SPSystemBackup.xml，则恢复向导无法运行，并显示以下错误消息：The selected Backup Archive does not match the restore reason. Please select another archive and continue.（所选备份档案不符合恢复理由。请选择另一个档案并继续。）	如果用户需要时选择 SpSystemBackup.xml，则 Embedded Security 向导无法运行，并显示以下消息：An internal Embedded Security error has been detected（检测到了 Embedded Security 内部错误）。 用户必须选择符合所需理由的正确的 XML 文件。 上述过程按设计需要工作并且运行正常；但是，Embedded Security 模块内部错误消息不是非常清楚，应该显示一个更准确的消息。HP 正在努力在将来版本中增强此功能。
安全系统在多用户情况下出现恢复错误。	在恢复过程中，如果管理员选择进行恢复的用户，未选择的用户在稍后尝试恢复时，则无法恢复密钥。将显示 decryption process failed（解密过程失败） 错误消息。	可以恢复未选择的用户，方法是：重置 TPM，运行恢复过程，并在下一次默认的日常备份开始运行之前选择所有用户。运行自动备份时，它将覆盖未恢复的用户，这些用户的数据将会丢失。如果存储新系统备份，则无法恢复以前未选择的用户。 此外，用户必须恢复整个系统备份。档案备份可以单独恢复。
将系统 ROM 重置为默认值会隐藏 TPM。	将系统 ROM 重置为默认设置，即对于 Windows 隐藏 TPM。这样会使安全软件无法正常运行，并且使 TPM 加密数据无法访问。	在 BIOS 中取消隐藏 TPM： 打开计算机设置 (f10) 实用程序，浏览找到 Security（安全保护）> Device security（设备安全保护），然后将字段从 Hidden（隐藏） 更改为 Available（可用）。
自动备份不能用于映射的驱动器。	当管理员在 Embedded Security 中设置 Automatic Backup（自动备份）时，它在 Windows > Tasks（任务）> Scheduled Task（已计划的任务） 中创建条目。此 Windows 计划任务被设置为使用 NT AUTHORITY\SYSTEM 权限执行备份。这适用于任何本地驱动器。 而当管理员配置 Automatic Backup（自动备份）使其保存到映射驱动器时，该过程则会失败，因为 NT AUTHORITY\SYSTEM 没有使用映射驱动器的权限。 如果 Automatic Backup（自动备份）安排在登录时执行，则 Embedded Security TNA 图标显示以下消息：The	解决方法为将 NT AUTHORITY\SYSTEM 更改为（计算机名）\（管理员名称）。这是手动创建 Scheduled Task（计划任务）情况下的默认设置。 HP 正在努力在将来产品版本中提供包括计算机名\管理员名称的默认设置。

简短说明	详细说明	解决方法
	Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again （备份档案位置当前不可访问。如果您要在再次访问备份档案之前备份到临时档案，请单击此处）。但是，如果 Automatic Backup（自动备份）安排在特定时间执行，则备份将会失败，并且不显示失败的通知消息。	
在 Embedded Security GUI 中不能暂时禁用 Embedded Security。	当前的 4.0 软件是为 HP Notebook 1.1B 实施设计的，也支持 HP Desktop 1.2 实施。 此要禁用的选项在 TPM 1.1 平台的软件界面中仍然受支持。	HP 将在将来版本中解决此问题。

Device Access Manager for HP ProtectTools

简短说明	详细说明	解决方法
虽然在 Device Access Manager 中已经拒绝用户访问设备，但用户仍可以访问设备。	已经在 Device Access Manager 中使用 Simple Configuration（简单配置）和/或 Device Class Configuration（设备类别配置）来拒绝用户访问设备。尽管已经拒绝访问，但用户仍可以访问设备。	验证是否启动了 HP ProtectTools Device Locking 服务。 作为管理用户，浏览到 Control Panel（控制面板）> Administrative Tools（管理工具）> Services（服务） 。在 Services（服务） 窗口，搜索 HP ProtectTools Device Locking/Auditing（HP ProtectTools 设备锁定/审核） 服务。确保该服务已启动，并且启动类型为 Automatic（自动） 。
用户意外能够访问设备，或者用户被意外拒绝访问设备。	已经使用 Device Access Manager 拒绝用户访问某些设备，并允许用户访问其他设备。当用户正在使用系统时，他可以访问其确信 Device Access Manager 已经拒绝其访问的设备，而拒绝其访问确信 Device Access Manager 应当允许其访问的设备。	应当使用 Device Access Manager 中的 Device Class Configuration（设备类别配置）来查看用户设备设置。 选择 Security Manager（安全管理器）> Device Access Manager（设备访问管理器）> Device Class Configuration（设备类别配置） 。扩展设备类别树中的级别，并查看适用于该用户的设置。检查可以对用户或用户所属的任何 Windows 组（例如，用户、管理员）设置的所有“Deny”（拒绝）权限。
允许或拒绝 — 哪一个优先级更高？	在 Device Class Configuration（设备类别配置）中，已经设置以下配置： 在设备类别层次结构中的同一级别上，已经将 Allow（允许）权限授予一个 Windows 组（例如 BUILTIN\Administrators），并将 Deny（拒绝）权限授予给另外一个 Windows 组（例如 BUILTIN\Users）。 如果用户是这两个组（例如，管理员组）的成员，则哪一个组有更高的优先级？	拒绝用户访问设备。Deny（拒绝）的优先级高于 Allow（允许）。 由于 Windows 运行超出设备的有效权限，因此拒绝访问。虽然拒绝一个组访问，允许另外一个组访问，但是用户是这两个组的成员。由于拒绝访问的优先级别高于允许访问，因此拒绝用户访问。 一种解决方法是拒绝 DVD/CD-ROM 驱动器级别的用户组访问，而允许低于 DVD/CD-ROM 驱动器级别的管理员组访问。 一个更彻底的解决方法是指定 Windows 组，允许一个组访问 DVD/CD，而拒绝另外一个组访问 DVD/CD。然后向相应的组添加特定用户。

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) 。	所有安全保护应用程序，比如 Embedded Security、Java Card Security 和生物识别器是 Security Manager 界面的可扩展插件。必须先安装 Security Manager 后，才能装载 HP 认可的安全插件。	必须先安装 Security Manager 后才能安装任何安全插件。
用于包含支持 Broadcom 的 TPM 的型号的 TPM Firmware Update Utility (TPM 固件更新实用程序) — 通过 HP 支持网站提供的工具报告 ownership required (需要所有权) 。	对于包含支持 Broadcom 的 TPM 型号而言，这是 TPM 固件实用程序的预期行为。 该固件升级工具使得用户在具有或不具有授权密钥 (EK) 的情况下都能升级固件。如果没有 EK，则在完成固件升级时不需要授权。 如果有 EK，则必须存在 TPM 所有者，因为升级需要所有者授权。成功升级之后，必须重新启动平台才能使得新固件生效。 如果出厂时重置了 BIOS TPM，则会删除所有权，必须首先配置嵌入式安全保护软件平台和用户初始化向导之后才能使用固件更新功能。	- 重新安装 Embedded Security 软件。 - 运行平台和用户配置向导。 - 确保系统包含 Microsoft .NET Framework 1.1 安装程序： - 单击开始。 - 单击控制面板。 - 单击添加或删除程序。 - 确保列出了 Microsoft .NET Framework 1.1。 - 检查硬件和软件配置： - 单击开始。 - 单击所有程序。 - 单击 HP ProtectTools Security Manager。 - 从树菜单中选择 Embedded Security (嵌入式安全保护)。 - 单击 More Details (更多详细信息)。系统应该具有下列配置： - Product version (产品版本) = V4.0.1 - Embedded Security State (嵌入式安全保护状态)：Chip State (芯片状态) = Enabled (启用)，Owner State (主人状态) = Initialized (已初始化)，User State (用户状态) = Initialized (已初始化) - Component Info (组件信息)：TCG Spec.Version (TCG 规范版本) = 1.2 - Vendor (供应商) = Broadcom Corporation



注： 始终建议在执行固件更新后进行重启。在重新引导之前，不能正确识别固件版本。

受影响的软件 - 简短说明	详细说明	解决方法
		- FW Version（固件版本）= 2.18（或更高） - TPM Device driver library version（TPM 设备驱动程序库版本）2.0.0.9（或更高） 5. 如果固件版本与 2.18 版不匹配，请下载并更新 TPM 固件。TPM 固件 SoftPaq 是从 HP 网站下载的支持软件包：http://www.hp.com。
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： - 删除 PSD - 恶意修改用户设置 - 禁用安全策略和功能	鼓励管理员在限制最终用户特权和提供限制性用户访问权限时采用“最佳做法”。 对于未授权的用户不应授予管理权限。
BIOS 和 OS Embedded Security 密码不同步。	如果用户没有验证作为 BIOS Embedded Security 密码的新密码，则该密码通过 f10 BIOS 还原为原来的嵌入式安全保护密码。	这按设计要求运行：通过更改操作系统基本用户密码并在 BIOS Embedded Security 密码提示符下对其进行验证，可以重新同步这些密码。
在 BIOS 中启用了 TPM 预引导验证之后，只有一个用户可以登录系统。	TPM BIOS 个人识别号与初始化用户设置的第一个用户关联。如果计算机有多个用户，第一个用户实际上是管理员。第一个用户必须为其他用户提供其 TPM 用户个人标识号，其他用户才能用来进行登录。	这按设计要求运行：HP 建议客户的 IT 部门按照良好的安全策略创建安全解决方案，并确保 BIOS 管理员密码由 IT 管理员进行配置，以获得系统级的保护。
在重置 TPM 出厂设置后，用户必须更改其个人识别号才能使 TPM 预引导工作。	用户必须更改其个人识别号或创建另一个用户以初始化其用户设置，才能使 TPM BIOS 验证在重置后工作。没有其他任何方法可以使 TPM BIOS 验证工作。	这是有意设计的；出厂重置将清除基本用户密码。用户必须更改其个人识别号或创建新用户才能初始化基本用户密钥。
未使用 Embedded Security 的 Reset to Factory Settings（重置为出厂设置） 将 Power-on authentication support（开机验证支持） 设置为默认值	在计算机设置实用程序中，使用 Embedded Security Device（嵌入式安全设备）的选项 Reset to Factory Settings（重置为出厂设置） ，无法将 Power-on authentication support（开机验证支持） 重置为出厂设置。默认情况下， Power-on authentication support（开机验证支持） 设置为 Disable（禁用） 。	Reset to Factory Settings（重置为出厂设置） 选项禁用 Embedded Security Device（嵌入式安全设备），该模块隐藏其他 Embedded Security 选项（包括 Power-on authentication support（开机验证支持））。但是，在重新启用 Embedded Security Device（嵌入式安全保护设备）后，Power-on authentication support（开机验证支持） 保持启用状态。 HP 正在努力寻找一种解决方法，将在以后的基于 Web 的 ROM SoftPaq 产品中提供该方法。

受影响的软件 - 简短说明	详细说明	解决方法
在引导顺序中，Security Power-On Authentication（安全开机验证）覆盖 BIOS 密码。	Power-On Authentication（开机验证）提示用户使用 TPM 密码登录到系统，但是，如果用户按 F10 键访问 BIOS，则仅授予用户只读访问权限。	为了能够写入 BIOS，用户必须在 Power-On Authentication（开机验证）窗口输入 BIOS 密码来代替 TPM 密码。
在更改主人密码后，BIOS 通过计算机设置实用程序要求同时提供新旧密码。	在 Embedded Security Windows 软件中更改主人密码后，BIOS 通过计算机设置实用程序要求同时提供新旧密码。	这是有意设计的。这是因为在操作系统启动并运行后，BIOS 无法与 TPM 通信，并且无法验证 TPM 密码。

术语表

BIOS 安全保护模式 (BIOS security mode) Java Card Security 模块中的设置，启用后要求使用 Java 卡和有效的个人标识号进行用户验证。

BIOS 配置文件 (BIOS profile) 一组可以保存并应用于其他帐户的 BIOS 配置设置。

Java 卡 (Java Card) 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。

USB 身份标记 (USB token) 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，用于验证计算机主人的身份。

Windows 用户帐户 (Windows user account) 有权登录到网络或个人计算机的用户的配置文件。

标识 (Identity) HP ProtectTools Credential 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 (Reboot) 重新启动计算机的过程。

单次登录 (Single Sign On) 存储验证信息并允许您使用 Credential Manager 来访问需要密码验证的 Internet 和 Windows 应用程序的功能。

个人安全驱动器 (Personal secure drive, PSD) 为敏感数据提供的受保护的存储区域。

公共密钥基础结构 (Public Key Infrastructure, PKI) 为创建、使用和管理证书及加密密钥接口进行定义所用的标准。

急救档案 (Emergency recovery archive) 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）。

加密 (Encryption) 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。

加密服务提供程序 (Cryptographic service provider, 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。

加密技术 (Cryptography) 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。

加密文件系统 (Encryption File System, 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。

解密 (Decryption) 在加密技术中用于将加密的数据转换为纯文本的过程。

开机验证 (Power-on authentication) 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。

可信平台模块 (TPM) 嵌入式安全保护芯片 (Trusted Platform Module (TPM) embedded security chip) (仅限某些机型) 可保护高度敏感用户信息免受恶意攻击的集成安全保护芯片。这可以根本地决定给定平台是否可信。TPM 提供的加密算法和运算满足 Trusted Computing Group (TCG) 规范。

凭证 (Credentials) 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 (Migration) 允许管理、恢复和传输密钥及证书的任务。

驱动器锁 (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。

驱动器锁自动保护功能 (Automatic DriveLock) 生成驱动器锁密码并由 TPM 嵌入式安全保护芯片进行保护的安全保护功能。当用户在启动时输入正确的 TPM 基本用户密钥密码，并由 TPM 嵌入式安全保护芯片完成对用户的验证后，BIOS 会为用户解除硬盘驱动器锁定。

认证机构 (Certification authority) 颁发运行公共密钥所需证书的服务机构。

生物 (Biometric) 使用生理特征 (例如指纹) 来识别用户的验证凭证类型。

数字签名 (Digital signature) 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 (Digital certificate) 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。

网络帐户 (Network account) 本地计算机、工作组或域中的 Windows 用户或管理员帐户。

虚拟身份标记 (Virtual token) 与 Java 卡和读卡器功能非常相似的安全保护功能。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。

严格的安全保护功能 (Stringent security) BIOS Configuration 模块中的安全保护功能，为开机密码和设置密码以及其他形式的开机验证提供增强的保护功能。

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

域 (Domain) 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。

智能卡 (Smart card) 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。

索引

A

安全保护

- 关键目标 4
- 角色 6

安全保护角色 6

安全设置实用程序密码 7

B

BIOS Configuration for HP

ProtectTools

- Windows 重新启动时的开机验证 51
- 附加模块设置, 管理 47
- 开机密码, 更改 50
- 开机密码, 设置 50
- 开机验证 48
- 密码选项, 设置 51
- 驱动器锁自动保护功能 49
- 设置密码, 更改 50
- 设置密码, 设置 50
- 系统配置选项 45
- 严格的安全保护功能 51
- 引导选项 44
- 智能卡开机验证 47

BIOS 管理员密码 7

BIOS 设置密码

- 更改 50
- 设置 50

备份和恢复

- Embedded Security 33
- HP ProtectTools 模块 8
- 单次登录数据 20
- 认证信息 33

标识, 管理

- Credential Manager 16

标识, 删除

- Credential Manager 16

C

Credential Manager for HP

ProtectTools

- USB eToken, 注册 14
- Windows 登录 17
- Windows 登录密码, 更改 15
- Windows 登录, 允许 25
- 标识 16
- 标识, 清除 16
- 标识, 删除 16
- 单次登录 (SSO) 18
- 单次登录凭证, 修改 20
- 单次登录手动注册 19
- 单次登录新应用程序 18
- 单次登录应用程序和凭证 19
- 单次登录应用程序, 导出 20
- 单次登录应用程序, 导入 20
- 单次登录应用程序, 删除 19
- 单次登录应用程序, 修改属性 19
- 单次登录自动注册 18
- 登录 12
- 登录密码 6
- 登录向导 12
- 登录指定 23
- 更改应用程序限制设置 22
- 故障排除 63
- 管理员任务 23
- 恢复文件密码 6
- 凭证属性, 配置 24
- 凭证, 注册 13
- 设置步骤 12
- 设置, 配置 25
- 身份标记个人标识号, 更改 15
- 锁定笔记本电脑 17
- 限制应用程序访问 21
- 新帐户, 创建 13
- 虚拟身份标记, 创建 15
- 应用程序保护 21

应用程序保护, 删除 22

用户验证 26

帐户, 删除 18

帐户, 添加 18

指纹登录 14

指纹识别器 14

注册 Java 卡 14

注册其他凭证 14

注册身份标记 14

注册虚拟身份标记 14

注册指纹 13

自定义验证需求 24

初始化嵌入式安全保护芯片 29

D

Device Access Manager for HP

ProtectTools

- 故障排除 70
- 后台服务 54
- 简单配置 55
- 设备类别配置 56
- 设备类别, 允许一个访问 56
- 设备, 允许一个访问 57
- 用户或组, 拒绝访问 56
- 用户或组, 删除 56
- 用户或组, 添加 56

Drive Encryption for HP

ProtectTools

- 更改加密 60
- 更改身份标记 61
- 更改验证 61
- 加密驱动器 60
- 解密驱动器 60
- 驱动器加密恢复服务 62
- 驱动器加密密钥 62
- 删除用户 61
- 设置密码 61
- 添加用户 61

- 单次登录
 - 导出应用程序 20
 - 删除应用程序 19
 - 手动注册 19
 - 修改应用程序属性 19
 - 自动注册 18
 - 对文件和文件夹进行加密 31
- E**
 - Embedded Security for HP
 - ProtectTools
 - 备份文件, 创建 33
 - 重置用户密码 34
 - 初始化芯片 29
 - 对文件和文件夹进行加密 31
 - 个人安全驱动器 31
 - 故障排除 65
 - 基本用户密钥 30
 - 基本用户密钥密码, 更改 32
 - 基本用户帐户 30
 - 加密的电子邮件 31
 - 密码 6
 - 启用 TPM 芯片 28
 - 启用和禁用 34
 - 迁移密钥 35
 - 认证数据, 恢复 33
 - 设置步骤 28
 - 永久禁用 34
 - 在永久禁用后启用 34
 - 主人密码, 更改 34
- F**
 - f10 设置实用程序密码 7
 - 访问
 - 防止未授权 5
 - 控制 53
 - 访问 HP ProtectTools Security 3
- G**
 - 高级任务
 - BIOS Configuration 47
 - Credential Manager 23
 - Device Access Manager 56
 - Embedded Security 33
 - Java 卡 39
 - 个人安全驱动器 (PSD) 31
 - 功能, HP ProtectTools 2
 - 故障排除
 - Credential Manager 63
 - Device Access Manager 70
- Embedded Security 65
 - 其他 71
 - 关键的安全保护目标 4
 - 管理员任务
 - Credential Manager 23
 - Java 卡 39
- H**
 - HP ProtectTools Backup and Restore 8
 - HP ProtectTools Security, 访问 3
 - HP ProtectTools 功能 2
 - 后台服务, Device Access Manager 54
 - 恢复已加密的数据 62
- J**
 - Java Card Security for HP
 - ProtectTools
 - Credential Manager 14
 - 创建管理员 41
 - 读卡器, 选择 38
 - 高级任务 39
 - 个人标识号 7
 - 个人标识号, 更改 38
 - 个人标识号, 指定 39
 - 管理员任务 39
 - 开机验证, 禁用 42
 - 开机验证, 启用 41
 - 开机验证, 设置 40
 - 用户, 创建 42
 - 指定名称 40
 - 基本用户密钥密码
 - 更改 32
 - 设置 30
 - 基本用户帐户 30
 - 急救 29
 - 急救身份标记密码
 - 定义 6
 - 设置 29
 - 计算机设置实用程序
 - 管理员密码 7
 - 密码, 更改 50
 - 密码, 管理 49
 - 密码, 设置 50
 - 加密
 - 方法 60
 - 用户 61
 - 用户验证 61
- 加密驱动器 59
 - 解密驱动器 59
 - 禁用
 - Embedded Security 34
 - Embedded Security, 永久 34
 - Java 卡开机验证 42
 - 开机验证 47
 - 驱动器锁自动保护功能 49
 - 设备选项 45
 - 严格的安全保护功能 51
 - 智能卡验证 47
- K**
 - 开机密码
 - 定义 7
 - 设置和更改 50
 - 开机验证
 - 启用和禁用 47
 - 在 Windows 重新启动时 51
 - 控制设备访问 53
- M**
 - 密码
 - HP ProtectTools 6
 - Windows 登录 15
 - 安全, 创建 8
 - 策略, 创建 5
 - 重置用户 34
 - 更改开机 50
 - 更改设置 50
 - 更改主人 34
 - 管理 6
 - 基本用户密钥 32
 - 急救身份标记密码 29
 - 计算机设置实用程序, 管理 49
 - 设定设置 50
 - 设置开机 50
 - 设置选项 51
 - 主人 29
 - 准则 8
 - 目标, 安全保护 4
- Q**
 - 启用
 - Embedded Security 34
 - Java 卡开机验证 41
 - TPM 芯片 28
 - 开机验证 47
 - 驱动器锁自动保护功能 49
 - 设备选项 45

- 严格的安全保护功能 51
- 在永久禁用后启用 Embedded Security 34
- 智能卡验证 47
- 驱动器锁自动保护功能 49

S

- 设备选项 45
- 身份标记, Credential Manager 14
- 生物识别器 14
- 属性
 - 凭证 24
 - 验证 23
 - 应用程序 19
- 数据, 限制访问 4
- 锁定笔记本电脑 17

T

- TPM 芯片
 - 初始化 29
 - 启用 28

U

- USB eToken, Credential Manager 14

W

- Windows 登录
 - Credential Manager 17
 - 密码 7
- Windows 网络帐户 18
- 网络帐户 18
- 未授权的访问, 防止 5

X

- 限制
 - 访问敏感数据 4
 - 设备访问 53
- 虚拟身份标记 15
- 虚拟身份标记, Credential Manager 14, 15

Y

- 严格的安全保护功能 51
- 引导选项 44
- 有目的的盗窃行为, 防范 4

Z

- 帐户
 - Credential Manager 13
 - 基本用户 30
- 指纹, Credential Manager 13
- 主人密码
 - 定义 7
 - 更改 34
 - 设置 29
- 注册
 - 凭证 13
 - 应用程序 18

