

参考指南

ProtectTools Security Manager

文档部件号：389171-AA1

2005 年 5 月

© 版权所有 2005 Hewlett-Packard Development Company, L.P.

Microsoft 和 Windows 是 Microsoft Corporation 在美国的注册商标。

本文档中包含的信息如有变更，恕不另行通知。随 HP 产品和服务附带的明示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。

参考指南

ProtectTools Security Manager

第一版 2005 年 5 月

文档部件号：389171-AA1

目录

1 简介

| | |
|--|-----|
| ProtectTools Security Manager | 1-1 |
| 访问 ProtectTools Security Manager | 1-2 |
| 了解安全角色 | 1-3 |
| 管理 ProtectTools 密码 | 1-4 |
| 创建安全的密码 | 1-7 |

2 ProtectTools 的智能卡安全保护功能

| | |
|---------------------|------|
| 基本概念 | 2-1 |
| 对智能卡进行初始化 | 2-2 |
| 智能卡 BIOS 安全模式 | 2-3 |
| 启用智能卡 BIOS 安全模式和 | |
| 设置智能卡管理员密码 | 2-4 |
| 更改智能卡管理员密码 | 2-6 |
| 设置和更改智能卡用户密码 | 2-7 |
| 存储管理员或用户卡密码 | 2-8 |
| 常规任务 | 2-10 |
| 更新 BIOS 智能卡设置 | 2-10 |
| 选择智能卡读卡器 | 2-11 |
| 更改智能卡 PIN | 2-11 |
| 备份和恢复智能卡 | 2-12 |

3 ProtectTools 的嵌入式安全保护功能

| | |
|--|------|
| 基本概念 | 3-1 |
| 设置步骤 | 3-2 |
| 启用嵌入式安全保护芯片 | 3-2 |
| 初始化嵌入式安全保护芯片 | 3-3 |
| 建立基本用户帐户 | 3-4 |
| 常规任务 | 3-6 |
| 使用个人安全驱动器 | 3-6 |
| 对文件和文件夹进行加密 | 3-6 |
| 发送和接收加密的电子邮件 | 3-7 |
| 更改基本用户密钥密码 | 3-7 |
| 高级任务 | 3-8 |
| 备份和恢复 | 3-8 |
| 更改主人密码 | 3-10 |
| 启用和禁用嵌入式安全保护功能 | 3-10 |
| 使用 Migration Wizard (迁移向导) 迁移密钥 | 3-12 |

4 ProtectTools 的 BIOS 配置

| | |
|--------------------------|------|
| 基本概念 | 4-1 |
| 常规任务 | 4-2 |
| 管理引导选项 | 4-2 |
| 启用和禁用设备或安全保护选项 | 4-3 |
| 高级任务 | 4-4 |
| 管理 ProtectTools 设置 | 4-4 |
| 管理配置文件 | 4-7 |
| 管理计算机设置实用程序密码 | 4-11 |

5 ProtectTools 的身份管理器

| | |
|-------------------------|------|
| 基本概念 | 5-1 |
| 设置步骤 | 5-2 |
| 登录到身份管理器 | 5-2 |
| 注册身份 | 5-5 |
| 常规任务 | 5-7 |
| 创建虚拟令牌 | 5-7 |
| 更改 Windows 登录密码 | 5-8 |
| 更改令牌 PIN | 5-8 |
| 管理标识 | 5-9 |
| 锁定计算机 | 5-11 |
| 使用 Microsoft 网络登录 | 5-12 |
| 使用单次登录 | 5-15 |
| 高级任务（仅供管理员使用） | 5-20 |
| 指定用户和管理员的登录方式 | 5-20 |
| 配置自定义验证需求 | 5-21 |
| 配置身份属性 | 5-22 |
| 配置身份管理器设置 | 5-23 |

术语表

索引

ProtectTools Security Manager

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：

- ProtectTools 的智能卡安全保护功能
- ProtectTools 的嵌入式安全保护
- ProtectTools 的 BIOS 配置
- ProtectTools 的身份管理器

计算机中可用的软件模块因机型而异。例如，ProtectTools 的嵌入式安全保护功能要求计算机必须安装可信平台模块 (TPM) 嵌入式安全保护芯片（仅限于某些机型），ProtectTools 的智能卡安全保护功能要求计算机必须安装智能卡和读卡器选件。

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



本指南中的说明假设您已经安装了适用的 ProtectTools 软件模块。

访问 **ProtectTools Security Manager**

要通过 Microsoft® Windows® 控制面板访问 ProtectTools Security Manager，请执行以下操作：

- » 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器）。



如果已经配置身份管理器模块，还可以通过直接从 Windows 登录屏幕登录到身份管理器来打开 ProtectTools。有关详细信息，请参阅第 5 章“[ProtectTools 的身份管理器](#)”中的“[使用身份管理器登录到 Windows](#)”。

了解安全角色

管理计算机安全性（尤其是对于大型企业）时，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。



对于小型企业或个人用户，这些角色可能全部为一人拥有。

对于 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，如智能卡、生物读卡器或 USB 令牌等。




通过与 HP 合作，安全管理人员可以自定义 ProtectTools 中的许多功能。有关详细信息，请访问 <http://www.hp.com>。

- IT 管理员 — 应用并管理安全管理人员定义的安全功能。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智能卡，IT 管理员可以启用智能卡 BIOS 安全模式。
- 用户 — 使用安全功能。例如，如果安全管理人员和 IT 管理员已经为系统启用了智能卡，用户可以设置智能卡 PIN，并使用该卡进行身份验证。





管理 ProtectTools 密码

大多数 ProtectTools Security Manager 功能都是受密码保护的。下表列出了常用的密码、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。

| ProtectTools 密码 | 在此 ProtectTools 模块中设置 | 功能 |
|--|-----------------------|--|
| 计算机设置实用程序管理员密码 | BIOS 配置，由 IT 管理员设置并使用 | 防止他人擅自访问计算机设置实用程序。 |
|  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 | | |
| 驱动器锁的主人密码 | BIOS 配置，由 IT 管理员设置并使用 | 防止他人擅自访问受驱动器锁保护的内置硬盘驱动器。还可以用于解除驱动器锁保护。 |
| 驱动器锁的用户密码 | BIOS 配置 | 防止他人擅自访问受驱动器锁保护的内置硬盘驱动器。 |
| 开机密码 | BIOS 配置 | 在笔记本电脑开启、重新启动或从休眠模式恢复时，防止对笔记本电脑内容进行访问。 |
| 配置文件密码 | BIOS 配置，由 IT 管理员设置并使用 | 对保存 BIOS 系统设置的配置文件进行加密（和解锁）。 |

(续)

| ProtectTools 密码 | 在此 ProtectTools 模块中设置 | 功能 |
|---|-------------------------|---|
| 智能卡管理员密码  也称为 BIOS 管理员卡密码 | 智能卡安全保护功能，由 IT 管理员设置并使用 | 将智能卡与计算机关联在一起，以便于标识。 允许计算机管理员启用或禁用计算机设置实用程序密码、生成新的管理员卡，以及创建恢复文件以恢复用户或管理员卡。 |
| 智能卡的 PIN | 智能卡安全保护功能 | 使用智能卡和读卡器选件时，防止他人擅自访问智能卡内容和计算机内容。 |
| 智能卡恢复文件密码 | 智能卡安全保护功能 | 防止他人擅自访问包含 BIOS 密码的恢复文件。 |
| 智能卡用户密码  也称为 BIOS 用户卡密码 | 智能卡安全保护功能 | 将智能卡与计算机关联在一起，以便于标识。 允许用户创建恢复文件，以恢复用户卡。 |
| 基本用户密钥密码  也称为：嵌入式安全保护功能密码 | 嵌入式安全保护功能 | 在启用为 BIOS 开机验证支持密码时，防止他人在计算机开启、重新启动或从休眠模式恢复时擅自访问计算机内容。 |
| 急救令牌密码  也称为：急救令牌密钥密码 | 嵌入式安全保护功能，由 IT 管理员设置并使用 | 防止他人擅自访问急救令牌（它是嵌入式安全保护芯片的备份文件）。 |
| 主人密码 | 嵌入式安全保护功能，由 IT 管理员设置并使用 | 保护系统和 TPM 芯片，防止他人擅自访问嵌入式安全保护功能模块的所有主人功能。 |

(续)

| ProtectTools 密码 | 在此 ProtectTools 模块中设置 | 功能 |
|------------------------|------------------------------|--|
| 身份管理器登录密码 | 身份管理器 | 此密码提供有 2 个选项： <ul style="list-style-type: none">■ 用于在登录到 Microsoft Windows 后单独登录，以访问身份管理器。■ 用于 Windows 登录过程中，允许同时访问 Windows 和身份管理器。 |
| 身份管理器恢复文件密码 | 身份管理器，由 IT 管理员设置并使用 | 防止他人擅自访问身份管理器恢复文件。 |
| Windows 登录密码 | Windows 控制面板 | 可用于手动登录，或保存在智能卡中。 |

创建安全的密码

创建密码时，首先必须遵循程序设置的所有密码规范。不过，一般而言，应遵守下列准则以便创建安全的密码，减少密码被破解的机率：

- 使用的密码要长于 6 个字符（最好长于 8 个字符）。
- 密码要包含大小写字母。
- 如果可能的话，最好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 I 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”。
- 请不要使用可在字典中查到的词作为密码。
- 请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。
- 如果写下密码，请不要将其存放在距计算机很近的明显位置。
- 请不要在计算机上的文件（如电子邮件）中保存密码。
- 请不要与他人共用帐户或将密码告诉别人。

ProtectTools 的智能卡 安全保护功能

基本概念

利用 ProtectTools 的智能卡安全保护功能，可以对配备智能卡读卡器选件的计算机中的智能卡进行设置和配置。

使用智能卡安全保护功能模块，您可以实现以下目标：

- 使用智能卡安全保护功能。
- 对智能卡进行初始化，以便与其它 ProtectTools 模块配合使用，例如 ProtectTools 的身份管理器。
- 与计算机设置实用程序配合使用可在预引导环境中启用智能卡验证功能，并为管理员和用户分别配置智能卡。这需要用户在允许装载操作系统之前插入智能卡并输入（或不输入）PIN。
- 设置和更改用于验证智能卡用户的密码。
- 备份和恢复智能卡中存储的智能卡 BIOS 密码。

对智能卡进行初始化

必须对智能卡进行初始化，才可以使用智能卡。

要对智能卡进行初始化，请执行以下操作：


1. 将智能卡插入读卡器中。
2. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
3. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **Smart Card**（智能卡）。
4. 单击 **Initialize**（初始化）。
5. 在 **Initialize the smart card**（初始化智能卡）对话框内的第一个框中键入您的姓名。
6. 在相应的框中设置并确认智能卡 PIN。PIN 代码必须介于 4 到 8 位数字字符之间。
 要使用计算机，必须记住智能卡 PIN。如果忘记智能卡 PIN，将无法使用计算机。必须在 5 次尝试内正确输入智能卡 PIN，否则智能卡将锁定并且无法使用。输入正确的 PIN 后，将重置尝试计数。
7. 单击 **OK**（确定）完成初始化。

智能卡 BIOS 安全模式


在启用智能卡 BIOS 安全模式后，您需要使用智能卡才能登录到计算机。

启用智能卡 BIOS 安全模式包含以下步骤：

1. 在 BIOS 配置中启用智能卡开机验证支持。请参阅第 4 章“[ProtectTools 的 BIOS 配置](#)”中的“[启用和禁用智能卡开机验证支持](#)”。

 启用此设置后，可以使用智能卡进行开机验证。只有在启用智能卡开机验证支持后，智能卡 BIOS 安全模式功能才可用。

2. 在智能卡安全保护功能模块中启用智能卡 BIOS 安全模式。请参阅本章稍后部分中的“[启用智能卡 BIOS 安全模式和设置智能卡管理员密码](#)”。
3. 设置智能卡管理员密码。

 智能卡管理员密码是在启用智能卡 BIOS 安全模式的过程中设置的。

智能卡管理员密码与计算机设置实用程序管理员密码不同。智能卡管理员密码可以将智能卡与计算机关联在一起，以便于标识，另外还允许您执行以下操作：

- 启用或禁用计算机设置实用程序密码
- Create（创建）新的管理员和用户智能卡
- 创建恢复文件以恢复用户或管理员智能卡

只有在智能卡安全保护功能模块中启用智能卡 BIOS 安全模式之后，才能设置智能卡管理员密码。

启用智能卡 BIOS 安全模式和设置智能卡管理员密码

要启用智能卡 BIOS 安全模式和设置智能卡管理员密码，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **BIOS**。
3. 在 **BIOS Security Mode**（BIOS 安全模式）下，单击 **Enable**（启用）。
4. 单击 **Next**（下一步）。
5. 按照提示输入计算机设置实用程序管理员密码，然后单击 **Next**（下一步）。
6. 请先插入新管理员智能卡，然后按照屏幕上的说明操作。不同情况下的说明各不相同，可能会包括以下任务：
 - ❑ 对智能卡进行初始化。有关详细信息，请参阅“[对智能卡进行初始化](#)”。
 - ❑ 设置智能卡管理员密码。有关详细信息，请参阅“[存储管理员或用户卡密码](#)”。
 - ❑ 创建恢复文件。有关详细信息，请参阅“[创建恢复文件](#)”。

禁用智能卡 BIOS 安全模式

禁用智能卡 BIOS 安全模式后，智能卡管理员和用户密码也将禁用，并且无需使用智能卡即可使用计算机。



如果以前已启用智能卡 BIOS 安全模式，Smart Card Security BIOS（智能卡安全保护功能 BIOS）页上的按钮将变为 Disable（禁用）状态。

要禁用智能卡安全保护功能，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager（HP ProtectTools 安全管理器） > Smart Card Security（智能卡安全保护功能）**。
2. 选择加号 (+) 展开 Smart Card Security（智能卡安全保护功能）菜单，然后选择 **BIOS**。
3. 在 **BIOS Security Mode（BIOS 安全模式）** 下，单击 **Disable（禁用）**。
4. 插入带当前智能卡管理员密码的卡，然后单击 **Next（下一步）**。
5. 按照提示输入智能卡 PIN，然后单击 **Finish（完成）**。

更改智能卡管理员密码

智能卡管理员密码是在启用智能卡 BIOS 安全模式的过程中设置的。在设置智能卡管理员密码后，可以更改该密码。有关智能卡管理员密码的详细信息，请参阅本章前面部分中的“智能卡 BIOS 安全模式”。



通过以下步骤可以更新智能卡和计算机设置实用程序中存储的智能卡管理员密码。


要更改智能卡管理员密码，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **BIOS**。
3. 在 **BIOS Security Mode**（BIOS 安全模式）下的 **BIOS administrator card**（BIOS 管理员卡）旁，单击 **Change**（更改）。
4. 输入智能卡 PIN，然后单击 **Next**（下一步）。
5. 插入新管理员卡，然后单击 **Next**（下一步）。
6. 输入智能卡 PIN，然后单击 **Finish**（完成）。


设置和更改智能卡用户密码

要设置或更改智能卡用户密码，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **BIOS**。
3. 在 **BIOS Security Mode**（BIOS 安全模式）下的 **BIOS user card**（BIOS 用户卡）旁，单击 **Set**（设置）按钮。

 如果计算机设置实用程序中已存在用户密码，请单击 **Change**（更改）按钮。


4. 输入智能卡 PIN，然后单击 **Next**（下一步）。
5. 插入新用户卡，然后单击 **Next**（下一步）。
 - 如果该卡中已存在用户密码，将显示 **Finish**（完成）对话框。跳过第 6 步到第 8 步，然后转到第 9 步。
 - 如果该卡没有用户密码，将打开 **BIOS Password Wizard**（BIOS 密码向导）。
6. 在 **BIOS Password Wizard**（BIOS 密码向导）中，可以执行以下操作：
 - 手动输入密码。
 - 生成随机的 32 字节密码。

 使用已知的密码时，无需使用恢复文件即可创建备份卡。生成随机的密码可以增强安全性；但是，必须使用恢复文件才能制作备份卡。

7. 如果要求在启动时输入智能卡 PIN，请选中 **Boot Requirements**（引导要求）下的复选框。

 如果不要要求在启动时输入智能卡 PIN，请清除此复选框。

8. 输入智能卡 PIN，然后单击 **OK**（确定）。系统将提示您创建恢复文件。

 强烈建议您创建恢复文件。有关详细信息，请参阅本章稍后部分中的“[创建恢复文件](#)”。

9. 在 **Finish**（完成）对话框中输入智能卡 PIN，然后单击 **Finish**（完成）。

存储管理员或用户卡密码

如果希望创建备份卡，并且已经设置管理员密码，则可以在新卡中存储密码。



注意：此步骤只更新卡中的密码，而不更新计算机设置实用程序中的密码。使用新卡将无法使用计算机。

要存储管理员或用户卡密码，请执行以下操作：

1. 将智能卡插入读卡器中。
2. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
3. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **BIOS**。

4. 在 **BIOS Password on Smart Card**（智能卡中的 BIOS 密码）下，单击 **Store**（存储）。
5. 在 BIOS Password Wizard（BIOS 密码向导）中，可以执行以下操作：
 - 手动输入密码。
 - 生成随机的 32 字节密码。

 使用已知的密码时，无需使用恢复文件即可创建备份卡。生成随机的密码可以增强安全性；但是，必须使用恢复文件才能制作备份卡。
6. 在 **Access Privilege**（访问权限）下，单击 **Administrator**（管理员）或 **User**（用户）作为卡的类型。
7. 如果要求在启动时输入智能卡 PIN，请选中 **Boot Requirements**（引导要求）下的复选框。

 如果不要在启动时输入智能卡 PIN，请清除此复选框。
8. 输入智能卡 PIN，然后单击 **OK**（确定）。
9. 在 **Finish**（完成）对话框中再次输入智能卡 PIN，然后单击 **Finish**（完成）。系统将提示您创建恢复文件。



强烈建议您创建智能卡恢复文件。有关详细信息，请参阅本章稍后部分中的“[创建恢复文件](#)”。

常规任务

更新 BIOS 智能卡设置

要在重新启动计算机时要求输入智能卡 PIN，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 单击加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **BIOS**。
3. 在 **Smart Card BIOS Password Properties**（智能卡 BIOS 密码属性）下，单击 **Settings**（设置）。
4. 选中该复选框将要求在重新引导时输入 PIN。
 要取消此要求，请清除该复选框。
5. 输入智能卡 PIN，然后单击 **OK**（确定）。

选择智能卡读卡器

在使用智能卡之前，请确保在智能卡安全保护功能模块中选择了正确的智能卡读卡器。如果未在智能卡安全保护功能模块中选择正确的读卡器，某些功能将不可用或不能正常显示。

要选择智能卡读卡器，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **General**（常规）。
3. 在 **Smart Card Reader**（智能卡读卡器）下，选择正确的读卡器。
4. 将智能卡插入读卡器中。读卡器信息将自动刷新。

更改智能卡 PIN

要更改智能卡 PIN，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **Smart Card**（智能卡）。
3. 单击 **Change PIN**（更改 PIN）。
4. 键入您当前的智能卡 PIN。
5. 设置并确认新的 PIN。
6. 在确认对话框中单击 **OK**（确定）。

备份和恢复智能卡

在智能卡进行初始化并且可用之后，强烈建议您创建智能卡恢复文件。恢复文件可用来将智能卡数据从一个智能卡传输到另一个智能卡中。此文件也可用于备份原始智能卡或者在智能卡丢失或被盗时恢复数据。



注意：为了避免恢复文件与更新信息后的智能卡不符，请及时创建新的恢复文件并将其存储在安全位置。如果具有备份的智能卡，还必须通过将新恢复文件恢复到备份智能卡中来更新备份智能卡中的信息。

创建恢复文件

要创建恢复文件，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **Smart Card**（智能卡）。
3. 在 **Recovery**（恢复）下，单击 **Create**（创建）。
4. 输入智能卡 PIN，然后单击 **OK**（确定）。
5. 在 **Filename**（文件名）字段中输入文件路径和文件名。



为了能够使用计算机，请不要将恢复文件保存到计算机硬盘驱动器上；没有智能卡，您将无法访问该文件。另外，其他人也能够访问保存到硬盘驱动器上的恢复文件，这会增加安全风险。

6. 设置并确认恢复文件密码，然后单击 **OK**（确定）。



注意：为避免丢失智能卡恢复文件数据，请不要忘记恢复文件密码。如果忘记密码，将无法基于恢复文件重新创建卡。

恢复智能卡数据

您可以通过恢复文件恢复智能卡数据。在卡丢失或被盗时或者您希望创建备份智能卡时，这非常有用。如果使用的卡以前保存有数据，以前保存的数据将被覆盖。

开始之前，您需要具有以下几项：

- 对安装有智能卡安全保护功能软件的计算机的访问权
- 智能卡恢复文件
- 智能卡恢复文件密码
- 智能卡

要恢复智能卡，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Smart Card Security**（智能卡安全保护功能）。
2. 选择加号 (+) 展开 **Smart Card Security**（智能卡安全保护功能）菜单，然后选择 **Smart Card**（智能卡）。
3. 插入包含智能卡恢复文件的磁盘或其它介质。
4. 将智能卡插入读卡器中。如果卡没有初始化，将提示您对其进行初始化。有关对智能卡进行初始化的详细说明，请参阅本章前面部分中的“[对智能卡进行初始化](#)”。
5. 在 **Recovery**（恢复）部分中，单击 **Restore**（恢复）。
6. 确保选择正确的恢复文件名，然后输入恢复文件密码。
7. 输入智能卡 PIN。
8. 单击 **OK**（确定）。原始智能卡内容将恢复到新的智能卡中。

创建备份智能卡

强烈建议您创建备份智能卡，以便备份。根据智能卡密码是手动创建还是随机生成，有两种方法创建备份卡。

要创建具有随机生成的智能卡密码的备份智能卡，请执行以下操作：

- » 将智能卡插入读卡器中，然后将相应的恢复文件装载到其中。有关详细信息，请参阅本章前面部分中的“[恢复智能卡数据](#)”。

要创建具有手动生成的智能卡密码的备份智能卡，请执行以下操作：

1. 对新智能卡进行初始化。有关说明，请参阅本章前面部分中的“[对智能卡进行初始化](#)”。
2. 将管理员或用户卡密码存储到新智能卡中。有关说明，请参阅本章前面部分中的“[存储管理员或用户卡密码](#)”。

ProtectTools 的嵌入式安全保护功能

基本概念



计算机中必须安装有集成可信平台模块 (TPM) 嵌入式安全保护芯片，才能使用 ProtectTools 的嵌入式安全保护功能。

ProtectTools 的嵌入式安全保护功能可以防止他人擅自访问用户数据或身份信息。此软件模块提供有以下安全功能：

- 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
- 使用嵌入式安全保护功能软件时，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 ProtectTools Security Manager 的其它安全保护功能。例如，在用户登录 Windows 时，ProtectTools 的身份管理器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 ProtectTools 的 BIOS 配置进行访问。

设置步骤



注意：为降低安全风险，强烈建议 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、计算机蠕虫或病毒侵占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。

按照以下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 ProtectTools 的 BIOS 配置中无法执行此步骤。

要启用嵌入式安全保护芯片，请执行以下操作：

1. 在打开或重新启动计算机后，打开计算机设置实用程序。当屏幕的左下角显示“**F10 = ROM Based Setup**”（**F10 = 基于 ROM 的设置**）信息时，按 **F10** 键。
2. 如果尚未设置管理员密码，请使用箭头键选择 **Security**（**安全**）> **Administrator password**（**管理员密码**），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**）菜单中，使用箭头键选择 **Embedded Security**（**嵌入式安全保护功能**），然后按 **Enter** 键。
5. 在 **Embedded Security**（**嵌入式安全保护功能**）下，选择 **Embedded security device state**（**嵌入式安全保护设备状态**），将其更改为 **Enable**（**启用**）。
6. 按 **F10** 键接受对嵌入式安全保护功能配置的更改。
7. 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**）。然后按照屏幕上的说明操作。

初始化嵌入式安全保护芯片

在嵌入式安全保护功能的初始化过程中，您将完成以下操作：

- 为嵌入式安全保护芯片设置一个主人密码，以防止他人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嵌入式安全保护功能图标，然后选择 **Embedded Security Initialization（嵌入式安全保护功能初始化）**。此时，将打开 ProtectTools Embedded Security Initialization Wizard（ProtectTools 嵌入式安全保护功能初始化向导）。
2. 单击 **Next（下一步）**。
3. 设置并确认主人密码，然后单击 **Next（下一步）**。此时，将打开 **Setup Emergency Recovery（建立急救档案）** 对话框。
4. 单击 **Next（下一步）** 接受默认的急救档案位置，或单击 **Browse（浏览）** 按钮选择其它位置，然后单击 **Next（下一步）**。
5. 设置并确认急救令牌密码，然后单击 **Next（下一步）**。
6. 单击 **Browse（浏览）** 并选择急救档案的位置，然后单击 **Next（下一步）**。

7. 在“Summary”（摘要）页面中单击 **Next**（下一步）。
 - ❑ 如果此时不想建立基本用户帐户，请清除 **Start the Embedded Security User Initialization Wizard**（启动嵌入式安全保护功能用户初始化向导）复选框，然后单击 **Finish**（完成）。您可以按照下一节中的说明随时手动启动该向导以建立基本用户帐户。
 - ❑ 如果希望建立基本用户帐户，请选中 **Start the Embedded Security User Initialization Wizard**（启动嵌入式安全保护功能用户初始化向导）复选框，然后单击 **Finish**（完成）。此时，将打开 Embedded Security User Initialization Wizard（嵌入式安全保护功能用户初始化向导）。有关详细信息，请参阅下一节中的说明。

建立基本用户帐户

在嵌入式安全保护功能中建立基本用户帐户

- 生成一个保护加密数据的基本用户密钥，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数据。

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 User Initialization Wizard（嵌入式安全保护功能用户初始化向导）没有打开，请选择 **Start**（开始）> **All Programs**（所有程序）> **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器）> **Embedded Security**（嵌入式安全保护功能）> **User Settings**（用户设置）。

2. 在 **Embedded Security Features**（嵌入式安全保护功能）下，单击 **Configure**（配置）。此时，将打开 Embedded Security User Initialization Wizard（嵌入式安全保护功能用户初始化向导）。
3. 单击 **Next**（下一步）。
4. 设置并确认基本用户密钥密码，然后单击 **Next**（下一步）。
5. 单击 **Next**（下一步）确认设置。
6. 选择所需的安全保护功能，然后单击 **Next**（下一步）。
7. 再次单击 **Next**（下一步）。

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

8. 如果有多个加密证书，请选择适合的证书，然后单击 **Next**（下一步）。
9. 为 PSD 选择驱动器号和标签，然后单击 **Next**（下一步）。
10. 选择 PSD 的大小和位置，然后单击 **Next**（下一步）。
11. 在“Summary”（摘要）页面中单击 **Next**（下一步）。
12. 单击 **Finish**（完成）。

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

在 Windows XP Professional 中使用加密文件时，需要考虑以下规则：

- 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数据。

要加密文件和文件夹，请执行以下操作：

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

发送和接收加密的电子邮件

使用嵌入式安全保护功能，可以发送和接收加密的电子邮件，但对于不同的电子邮件客户端程序，相应的步骤可能会有所不同。有关详细信息，请参阅嵌入式安全保护功能的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**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **User Settings**（用户设置）。
2. 在 **Basic User Key password**（基本用户密钥密码）下，单击 **Change**（更改）。
3. 键入原密码，然后设置并确认新密码。
4. 单击 **OK**（确定）。

高级任务

备份和恢复

嵌入式安全保护功能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**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **Backup**（备份）。
2. 选择 **Backup**（备份）。
3. 单击 **Browse**（浏览）选择要保存备份文件的位置。
4. 选择是否将急救档案添加到备份数据中。
5. 单击 **Next**（下一步）。
6. 单击 **Finish**（完成）。

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**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **Backup**（备份）。
2. 单击 **Restore**（恢复）。
3. 单击 **Browse**（浏览）从存储位置选择备份文件。
4. 单击 **Next**（下一步）。
5. 选择是否启动 **Embedded Security User Initialization Wizard**（嵌入式安全保护功能用户初始化向导）。
 - 如果选择启动该初始化向导，请单击 **Finish**（完成），然后按照屏幕上的说明完成初始化。有关详细信息，请参阅本章前面部分中的“[建立基本用户帐户](#)”。
 - 如果选择不启动该初始化向导，请单击 **Finish**（完成）。

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**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **Advanced**（高级）。
2. 在 **Owner Password**（主人密码）下，单击 **Change**（更改）。
3. 键入原主人密码，然后设置并确认新主人密码。
4. 单击 **OK**（确定）。

启用和禁用嵌入式安全保护功能

如果希望在无安全保护功能的情况下工作，可以禁用嵌入式安全保护功能。

您可以在两个不同的级别启用或禁用嵌入式安全保护功能。

- **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嵌入式安全保护功能。默认情况下，此选项对所有用户都可用。
- **永久禁用** — 如果选择此选项，必须输入主人密码，才可重新启用嵌入式安全保护功能。此选项仅对管理员可用。

临时禁用嵌入式安全保护功能

要临时禁用嵌入式安全保护功能，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **User Settings**（用户设置）。
2. 在 **Embedded Security**（嵌入式安全保护功能）下，单击 **Disable**（禁用）。

在临时禁用后启用嵌入式安全保护功能

如果通过 **User Settings**（用户设置）禁用了嵌入式安全保护功能，则在 Windows 重新启动时将自动重新启用该功能。



如果您注销了 Windows 帐户但未重新启动计算机，那么，在您或另一用户登录 Windows 时，嵌入式安全保护功能将仍为禁用状态，直至重新启动计算机为止。

永久禁用嵌入式安全保护功能

要永久禁用嵌入式安全保护功能，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **Advanced**（高级）。
2. 在 **Embedded Security**（嵌入式安全保护功能）下，单击 **Disable**（禁用）。
3. 在系统提示时输入主人密码，然后单击 **OK**（确定）。

在永久禁用后启用嵌入式安全保护功能

要在永久禁用嵌入式安全保护功能后启用该功能，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Embedded Security**（嵌入式安全保护功能） > **Advanced**（高级）。
2. 在 **Embedded Security**（嵌入式安全保护功能）下，单击 **Enable**（启用）。
3. 在系统提示时输入主人密码，然后单击 **OK**（确定）。

使用 **Migration Wizard**（迁移向导）迁移密钥

迁移是一种高级的管理员任务，允许管理、恢复和传输密钥及证书。

有关迁移的详细信息，请参阅嵌入式安全保护功能的联机帮助。

ProtectTools 的 BIOS 配置

基本概念

ProtectTools 的 BIOS 配置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。

使用 BIOS 配置，您可以实现以下目标：

- 管理开机密码和管理员密码。
- 配置其它预引导验证功能，如启用智能卡密码和嵌入式安全保护功能进行验证。
- 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。



计算机设置实用程序也具有 ProtectTools 的 BIOS 配置中的许多功能。

常规任务

通过 BIOS 配置，您可以管理多种计算机设置，否则，您只能通过启动时按 **F10** 进入计算机设置实用程序来管理。

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 配置来管理多种设置。

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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 按照 BIOS 管理员密码提示输入计算机设置实用程序的管理员密码，然后单击 **OK**（确定）。



您必须首先设置计算机设置实用程序的管理员密码，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管理员密码的详细信息，请参阅本章稍后部分中的“设置管理员密码”。

3. 选中或清除 **Enable Quick boot**（启用快速引导）复选框。
4. 为 **F10**、**F12** 和 **Express Boot Popup**（快速引导弹出）选择延迟秒数。
5. 选中或清除 **Enable MultiBoot**（启用多重引导）复选框。
6. 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 **Move Up**（上移）或 **Move Down**（下移）来调整设备在列表中的顺序。
7. 单击 **Apply**（应用），然后在 ProtectTools 窗口中单击 **OK**（确定）保存更改。

启用和禁用设备或安全保护选项

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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 按照 BIOS 管理员密码提示输入计算机设置实用程序的管理员密码，然后单击 **OK**（确定）。
3. 单击 **Device Options**（设备选项）。
4. 选择或清除以下任意一个或多个选项：
 - 在引导时打开数码锁定
 - 交换 Fn/Ctrl 键的功能
 - 多个指点设备
 - USB 传统支持
 - 自动 SpeedStep 功能支持
 - 在接通交流电源的情况下风扇始终开启
5. 从下拉框中选择并行端口模式。
6. 单击 **Security**（安全保护）。
7. 选择或清除以下任意一个或多个选项：
 - 串行端口
 - 红外端口
 - 并行端口
 - SD 插槽
 - CD-ROM 引导
 - 软盘引导
 - 内部网络适配器引导
8. 单击 **Apply**（应用），然后在 ProtectTools 窗口中单击 **OK**（确定）以保存更改并退出。

高级任务

管理 ProtectTools 设置

ProtectTools Security Manager 的部分功能可以在 BIOS 配置中管理。

启用和禁用智能卡开机验证支持

启用此选项后，您可以在打开计算机时使用智能卡进行用户验证。

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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 按照 BIOS 管理员密码提示输入计算机设置实用程序的管理员密码，然后单击 **OK**（确定）。
3. 选择 **Security**（安全保护）。
4. 单击 **Advanced**（高级）。
5. 在 **Smart Card Security**（智能卡安全保护功能）下，选中 **Enable Smart Card Power-on Authentication Support**（启用智能卡开机验证支持）复选框。
 要禁用智能卡开机验证功能，请清除此复选框。
6. 单击 **Apply**（应用），然后在 ProtectTools 窗口中单击 **OK**（确定）保存更改。

启用和禁用嵌入式安全保护功能的开机验证支持

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。

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（HP ProtectTools 安全管理器） > BIOS Configuration（BIOS 配置）**。
2. 按照 BIOS 管理员密码提示输入计算机设置实用程序的管理员密码，然后单击 **OK（确定）**。
3. 选择 **Security（安全保护）**。
4. 单击 **Advanced（高级）**。
5. 在 **Embedded Security（嵌入式安全保护功能）** 下，选中 **Enable Power-on Authentication Support（启用开机验证支持）** 复选框。



要禁用嵌入式安全保护功能的开机验证功能，请清除此复选框。

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

启用和禁用驱动器锁自动保护硬盘驱动器的功能

启用此选项后，便可生成驱动器锁密码，并利用 TPM 嵌入式安全保护芯片进行保护。驱动器锁主人密码被设置为与计算机设置实用程序的管理员密码相匹配，而驱动器锁用户密码由 TPM 随机生成并由 TPM 进行保护。

除非是以下情况，否则，启用驱动器锁自动保护功能的选项不可用：

- 计算机已安装并初始化了 TPM 安全保护芯片。有关如何启用并初始化 TPM 安全保护芯片的说明，请参阅第 3 章“[ProtectTools 的嵌入式安全保护功能](#)”中的“[启用嵌入式安全保护芯片](#)”和“[初始化嵌入式安全保护芯片](#)”。
- 尚未启用任何驱动器锁密码。



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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 按照 BIOS 管理员密码提示输入计算机设置实用程序的管理员密码，然后单击 **OK**（确定）。
3. 选择 **Security**（安全保护）。
4. 单击 **Advanced**（高级）。
5. 在 **Embedded Security**（嵌入式安全保护功能）下，选中 **Enable Automatic DriveLock Protection**（启用驱动器锁自动保护功能）复选框。



要禁用嵌入式安全保护功能的开机验证功能，请清除此复选框。

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

管理配置文件

在 ProtectTools 的 BIOS 配置中设置了首选项后，可以将相关设置保存到指定的配置文件中。系统将利用您提供的密码来加密这个保存上述设置的文件。该配置文件随后将应用到多个平台上。



您必须重新启动计算机，这些设置才会生效。

使用命令行管理配置文件

您可以使用命令行界面管理 BIOS 配置的配置文件中。使用命令行可以执行以下操作：


- 更改设置以在 ProtectTools 的 BIOS 配置中显示 Profiles（配置文件）页，该页面默认状态下为隐藏状态。
- 访问并打开配置方案
- 将配置文件应用于多台计算机

要从命令行访问和修改配置文件设置，请执行以下操作：

1. 选择 **Start（开始） > Run（运行）**。
2. 在 **Open（打开）** 框中输入 `cmd.exe`。
3. 单击 **OK（确定）**。
4. 在命令提示符后，使用 `cd` 命令浏览至 BIOS 配置实用程序所在的以下路径：

`C:\Program Files\HPQ\HP BIOS Configuration for ProtectTools`

5. 输入 `hpqsetup.exe`，然后添加开关参数以自定义请求，如下表所示：


| 开关参数 | 功能 | 示例 |
|--|--|--|
| <code>/f</code> 和 <code>/k</code> | /f: 指定 INI 文件路径 /k: 指定用于解密 BIOS 配置工具中所创建文件的密码。 | <code>Hpqsetup.exe /f:c:\test.ini /kxxxx</code> (其中 <i>test</i> 为 INI 文件的名称, <i>xxxx</i> 为密码) |
|  这两个开关参数结合使用。 | | |
| <code>/p</code> | 显示 ProtectTools 的 BIOS 配置页上的 Profiles (配置文件) 页, 该页面默认情况下为隐藏状态 (需要重新启动 ProtectTools) | <code>Hpqsetup.exe /p</code> |

6. 按 **Enter** 键。

保存新的配置方案

要保存新的配置方案，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 单击 **Profiles**（配置文件）。

 如果 **Profiles**（配置文件）页不可见，您必须从命令行更改显示设置。有关说明，请参阅上一节中的“[使用命令行管理配置文件](#)”。

3. 单击 **Save As**（另存为）。
4. 在对话框中键入配置文件的名称。
5. 设置并确认用于加密文件的密码。
6. 在 **Add Profile**（添加配置文件）对话框中单击 **OK**（确定）。
7. 单击 **Apply**（应用），然后在 ProtectTools 窗口中单击 **OK**（确定）保存更改。

删除配置方案

要删除配置方案，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Profiles**（配置文件）。
3. 从下拉列表中选择要删除的配置文件。
4. 单击 **Delete**（删除）。
5. 在确认对话框中单击 **Yes**（是）。

将从以下位置删除该配置文件创建的 INI 文件：

C:\Program Files\HPQ\HP BIOS Configuration for ProtectTools \INIFiles

应用配置方案

您可以通过 HP BIOS Configuration for ProtectTools 在新的平台上应用任何配置方案。

要应用配置方案，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Profiles**（配置文件）。
3. 从下拉列表中选择要应用的配置方案。
4. 单击 **Apply**（应用）。
5. 单击 **OK**（确定）。XXX.ini 文件将保存到以下位置：

C:\Documents and Settings\All Users\Application Data\BIOS Configuration\INIFiles

将配置方案应用到多台计算机

IT 管理员可以使用 HPQSetup 应用程序和开发工具将 BIOS 配置的配置文件应用到网络中的多个平台。HPQSetup 应用程序只能与开发工具结合使用，并且只能通过命令行运行。有关详细信息，请参阅本文档前面部分中的“[使用命令行管理配置文件](#)”。

管理计算机设置实用程序密码

您可以使用 BIOS 配置来设置并更改计算机设置实用程序中的开机密码和管理员密码，以及管理不同的密码设置。



注意：通过 BIOS 配置中的 Passwords（密码）页设置了密码后，单击 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。



设置了开机密码后，Passwords（密码）页上的 Set（设置）按钮将更换为 Change（更改）按钮。

计算机设置实用程序的管理员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，必须输入该密码才能访问计算机设置实用程序。如果您设置了管理员密码，系统在打开 ProtectTools 的 BIOS 配置模块之前将提示您输入密码。



设置了管理员密码后，Passwords（密码）页上的 Set（设置）按钮将更换为 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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 在 **Power-On Password**（开机密码）下，选择 **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 ProtectTools 窗口中单击 **OK**（确定）保存更改。

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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 在 **Power-On Password**（开机密码）下，单击 **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 ProtectTools 窗口中单击 **OK**（确定）保存更改。

设置管理员密码

要设置计算机设置实用程序的管理员密码，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 在 **Administrator Password**（管理员密码）下，选择 **Set**（设置）。
4. 在 **Enter Password**（输入密码）和 **Confirm Password**（确认密码）框中设置并确认密码。
5. 在 **Passwords**（密码）对话框中单击 **OK**（确定）。
6. 单击 **Apply**（应用），然后在 ProtectTools 窗口中单击 **OK**（确定）保存更改。

更改管理员密码

要更改计算机设置实用程序的管理员密码，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 在 **Administrator Password**（管理员密码）下，单击 **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 ProtectTools 窗口中单击 **OK**（确定）保存更改。

设置密码选项

您可以利用 ProtectTools 的 BIOS 配置来设置密码选项，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，请记录所配置的管理员密码、开机密码或智能卡的 PIN，并将其存放到远离计算机的安全地点。不输入上述密码或 PIN，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它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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 选中 **Enable Stringent Security**（启用严格的安全保护功能）复选框。



如果您希望禁用严格的安全保护功能，请清除此复选框。

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

启用和禁用在 Windows 重新启动时的开机验证功能

此选项可要求用户在 Windows 重新启动时输入开机密码、TPM、驱动器锁或智能卡密码，从而增强安全保护性能。

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**（HP ProtectTools 安全管理器） > **BIOS Configuration**（BIOS 配置）。
2. 选择 **Passwords**（密码）。
3. 选中 **Enable Power-on Authentication on Windows restart**（启用在 Windows 重新启动时的开机验证功能）复选框。

 如果希望禁用在 Windows 重新启动时的开机验证功能，请清除此复选框。

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

ProtectTools 的身份管理器

基本概念

ProtectTools 的身份管理器提供的安全保护功能可以防止他人擅自访问您的计算机。这些功能包括：

- 登录 Microsoft Windows 时不输入密码而使用其它方法，例如使用智能卡或生物识别器登录 Windows。
- 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身份。
- 支持的安全保护设备选件，如智能卡和生物识别器。
- 支持其他安全保护设置，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

登录到身份管理器

根据配置情况，您可采用以下任意方式登录到身份管理器：

- Credential Manager Logon Wizard（身份管理器登录向导，首选）
- 通知区域中的身份管理器图标
- ProtectTools Security Manager



如果您使用 Windows Logon（Windows 登录）屏幕上的身份管理器登录提示登录到身份管理器，您将在同时登录到 Windows。

首次登录

首次打开身份管理器时，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 登录身份自动创建一个身份管理器帐户。

登录到身份管理器之后，您可以注册其他身份，例如指纹或智能卡。

在下一次登录时，您可以选择登录策略并使用任意组合形式的注册身份。

使用 Credential Manager Logon Wizard (身份管理器登录向导)

要使用 Credential Manager Logon Wizard (身份管理器登录向导) 登录到身份管理器, 请执行以下操作:

1. 采用以下任意方式打开 Credential Manager Logon Wizard (身份管理器登录向导):
 - ❑ 使用 Windows Logon (Windows 登录) 屏幕
 - ❑ 双击通知区域中的 ProtectTools 图标。
 - ❑ 在 Protect Tools Security Manager 的 Credential Manager (身份管理器) 页上, 单击窗口右上角的 **Log On (登录)** 链接。
2. 在 **User name (用户名)** 框中输入您的用户名, 然后单击 **Next (下一步)**。
3. 选择要使用的验证方法, 然后单击 **Next (下一步)**。
4. 按照屏幕上的说明, 使用所选的验证方法进行登录。
5. 单击 **Finish (完成)**。

创建新帐户

您可以使用 Credential Manager Logon Wizard（身份管理器登录向导）创建新的用户帐户。在您开始以前，必须使用管理员帐户登录到 Windows，但不要登录到身份管理器。

要创建新帐户，请执行以下操作：

1. 通过双击通知区域中的图标打开身份管理器。此时，将打开 Credential Manager Logon Wizard（身份管理器登录向导）。
2. 在 Introduce Yourself（个人信息）页上，单击 **More（更多）** 按钮，然后单击 **Sign Up for a New Account（申请新帐户）**。
3. 单击 **Next（下一步）**。
4. 在 Registration（注册）页上，键入用户名、用户的姓名和帐户说明。然后单击 **Next（下一步）**。
5. 在 Authentication Methods（验证方法）页上，选择要注册的验证方法（并清除不希望注册使用的其它验证方法的复选框），然后单击 **Next（下一步）**。
6. 按照屏幕上的说明注册所选的身份。
7. 单击 **Finish（完成）**。

注册身份

您可以使用 **My Identity**（我的标识）页注册不同的验证方法或身份。注册完成后，您可以使用这些方法登录身份管理器。

注册指纹

要注册指纹，请执行以下操作：

1. 将指纹识别器连接到计算机。
2. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
3. 单击 **My Identity**（我的标识）。
4. 在 **I Want To**（要执行的操作）下，单击 **Register Fingerprints**（注册指纹）。
5. 按照屏幕上的说明完成注册。

注册智能卡或令牌

要注册智能卡或令牌，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Register Credentials**（注册身份）。
4. 单击要注册的验证方法，然后单击 **Next**（下一步）。
5. 按照屏幕上的说明完成注册。

注册其它身份

要注册其它身份，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Register Credentials**（注册身份）。
4. 单击要注册的验证方法，然后单击 **Next**（下一步）。
5. 按照屏幕上的说明完成注册。

常规任务

所有用户都可以访问身份管理器中的 **My Identity**（我的标识）页。使用 **My Identity**（我的标识）页，可以执行以下操作：

- 创建并注册验证身份。
- 管理密码。
- 管理 Microsoft 网络帐户。
- 管理单次登录身份。

创建虚拟令牌

虚拟令牌的工作方式非常类似于智能卡或 USB 令牌。该令牌保存在计算机硬盘驱动器或 Windows 注册表中。使用虚拟令牌登录后，将要求您输入用户 PIN 以完成验证。

要创建新的虚拟令牌，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Register Credentials**（注册身份）。
4. 单击 **Next**（下一步）。
5. 单击 **Virtual Token**（虚拟令牌），然后单击 **Next**（下一步）。
6. 单击 **Create New**（新建），然后单击 **Next**（下一步）。
7. 输入虚拟令牌文件的名称和位置（或单击 **Browse**（浏览）按钮定位到文件位置），然后单击 **Next**（下一步）。
8. 设置并确认主人 PIN 和用户 PIN。
9. 单击 **Finish**（完成）。

更改 Windows 登录密码

您可以从身份管理器中的 My Identity（我的标识）页更改 Windows 登录密码。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager（HP ProtectTools 安全管理器） > Credential Manager（身份管理器）**。
2. 单击 **My Identity（我的标识）**。
3. 在 **I Want To（要执行的操作）** 下，单击 **Change Windows Logon Password（更改 Windows 登录密码）**。
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）** 框中设置并确认新密码。
6. 单击 **Finish（完成）**。

更改令牌 PIN

您可以从身份管理器中的 My Identity（我的标识）页更改智能卡或虚拟令牌的 PIN。

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager（HP ProtectTools 安全管理器） > Credential Manager（身份管理器）**。
2. 单击 **My Identity（我的标识）**。
3. 在 **I Want To（要执行的操作）** 下，单击 **More（更多）**，然后单击 **Change Token PIN（更改令牌 PIN）**。
4. 单击 **Next（下一步）**。
5. 选择要更改 PIN 的令牌，然后单击 **Next（下一步）**。
6. 按照屏幕上的说明完成对 PIN 的更改。

管理标识

备份标识

建议您在身份管理器中备份标识，以便在丢失或意外删除数据时使用。

要备份标识，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Backup Identity**（备份标识）。
4. 单击 **Next**（下一步）。
5. 选择要备份的元素，然后单击 **Next**（下一步）。
6. 在 **Device Type**（设备类型）页上，选择要用于存储备份的设备类型，然后单击 **Next**（下一步）。



您需要了解选择用于备份文件的设备的密码或 PIN 代码。

7. 按照屏幕上对所选设备的说明进行操作，然后单击 **Finish**（完成）。

恢复标识

要恢复标识，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Restore Identity**（恢复标识）。
4. 单击 **Next**（下一步）。
5. 在 **Device Type**（设备类型）页上，选择存储备份的设备类型，然后单击 **Next**（下一步）。
6. 按照屏幕上对所选设备的说明进行操作，然后单击 **Finish**（完成）。
7. 在确认对话框中单击 **Yes**（是）。

从系统中删除标识

您可以从身份管理器中完全删除标识。



这不会影响 Windows 用户帐户。

要从系统中删除标识，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 选择 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Remove My Identity from the System**（从系统中删除标识）。
4. 在确认对话框中单击 **Yes**（是）。该标识即被注销并从系统中删除。

锁定计算机

要在您离开办公桌时保证计算机的安全，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。只有您和计算机的管理员组的成员可以解除计算机的锁定。



为了进一步提高安全性，您可以配置 **Lock Workstation**（锁定工作站）功能，以要求必须使用智能卡、生物识别器或令牌才可解除计算机的锁定。有关详细信息，请参阅本章稍后部分中的“[配置身份管理器设置](#)”。

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**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **I Want To**（要执行的操作）下，单击 **More**（更多），然后单击 **Lock Workstation**（锁定工作站）。此时，将显示 Windows Logon（Windows 登录）屏幕。您必须使用 Windows 密码或 **Credential Manager Logon Wizard**（身份管理器登录向导）才可解除计算机锁定。


使用 Microsoft 网络登录

您可以使用身份管理器登录到本地计算机或网络域中的 Windows。当您首次登录到身份管理器时，系统将把您的本地 Windows 用户帐户自动添加为网络登录服务的网络帐户。有关详细信息，请参阅本章前面部分中的“首次登录”。

使用身份管理器登录到 Windows

您可以使用身份管理器登录到 Windows 网络或本地帐户。

1. 从 Windows Logon（Windows 登录）屏幕中，选择 **Log on to Credential Manager（登录到身份管理器）**。
2. 如果显示 Welcome（欢迎）页，请在该页面上单击 **Next（下一步）**。
3. 在 **User name（用户名）** 框中键入您的用户名。

 如果您希望将输入的用户名设置为默认的用户名，请选择 **Use this name next time you log on（下次登录时使用此名称）**。

4. 从 **Log on to（登录到）** 列表中选择 **Credential Manager（身份管理器）**。
5. 单击 **Next（下一步）**。在 Logon Policy（登录策略）页上，选择要使用的验证方法。

 如果您希望将此方法设置为默认的方法，请选择 **Use this policy next time you log on（下次登录时使用此策略）**。

6. 按照所选验证方法的说明进行操作。如果您的验证信息正确，您将登录到 Windows 帐户和身份管理器。

添加帐户

您可以在登录到身份管理器之后添加其它本地帐户或域帐户。

要添加帐户，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Microsoft Network Logon**（Microsoft 网络登录）下，单击 **Add a Network Account**（添加网络帐户）。
4. 在 **User name**（用户名）框中设置新帐户的用户名。
5. 在可用域列表中单击所需的域。
6. 键入并确认密码。

 如果您希望将其设置为默认的用户帐户，请选择 **Use these credentials by default**（默认情况下使用这些身份）。

7. 单击 **Finish**（完成）。

删除帐户

您可以在登录到身份管理器之后删除本地帐户或域帐户。

要删除帐户，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Microsoft Network Logon**（Microsoft 网络登录）下，单击 **Manage Network Accounts**（管理网络帐户）。
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）。

设置默认用户

您可以在登录到身份管理器之后设置或更改默认用户。

要设置默认用户，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Microsoft Network Logon**（Microsoft 网络登录）下，单击 **Manage Network Accounts**（管理网络帐户）。
4. 单击要设为默认帐户的帐户，然后单击 **Properties**（属性）。
5. 在 **Account Properties**（帐户属性）对话框的 **Set Up Account**（设置帐户）选项卡上，选择 **Use these credentials by default**（默认情况下使用这些身份）复选框。
6. 单击 **Apply**（应用），然后单击 **OK**（确定）。

使用单次登录

身份管理器的单次登录功能可以存储多个 Internet 和 Windows 应用程序的用户名和密码，并可在您访问注册应用程序时自动输入登录身份。



单次登录提供了重要的安全保护和隐私保护功能。所有身份都进行了加密，并且仅在成功登录到身份管理器之后才可用。



您还可以配置单次登录功能，要求在登录到安全站点或应用程序之前使用智能卡、生物识别器或令牌来确认验证身份是否有效。在登录到包含个人信息（例如银行帐户号码）的应用程序或网站时，该功能特别有用。有关详细信息，请参阅本章稍后部分中的“[配置身份管理器设置](#)”。

注册新应用程序

在您登录到身份管理器时，身份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

要使用自动注册功能来注册应用程序，请执行以下操作：


1. 打开要求您登录的应用程序。
2. 在 **Credential Manager Single Sign On**（身份管理器单次登录）对话框中，单击 **Options**（选项）来配置以下注册设置：
 - 不建议将 SSO 用于此网站或应用程序。
 - 请仅填写身份。不要提交。
 - 在提交身份前请求确认。
3. 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**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Register New Application**（注册新应用程序）。
4. 运行要注册的应用程序，直到显示提示输入密码的页面。
5. 在 **SSO Registration Wizard**（SSO 注册向导）的 **Drag and Drop Registration**（拖放注册）页上，选择要自动完成的操作的类型。

 在大多数情况下，要自动完成的操作都是 **Logon dialog**（登录对话框）中的操作。

6. 单击图标并将其从向导页拖动到应用程序的密码输入框所在的区域。当该区域成为当前焦点后，释放鼠标。

 您将不会看到手指图标在页面上移动，但在将鼠标指针拖动到应用程序的登录框时，将显示一个矩形图标。

7. 在 **SSO Registration Wizard**（SSO 注册向导）的 **Application Information**（应用程序信息）页上，输入应用程序的名称和说明。
8. 单击 **Finish**（完成）。
9. 在应用程序框中输入登录身份（例如用户名和密码）。
10. 在确认对话框中，确认或修改身份名称，然后单击 **Yes**（是）。

管理应用程序和身份

修改应用程序属性

要修改应用程序属性，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和身份）。
4. 单击要修改的应用程序项，然后单击 **Properties**（属性）。
 - a. 单击 **General**（常规）选项卡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。
 - b. 单击 **Script**（脚本）选项卡以查看和编辑 SSO 应用程序脚本。
5. 单击 **OK**（确定）保存更改。

从单次登录中删除应用程序

要从单次登录中删除应用程序，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和身份）。
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，后者仅包含身份信息。

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**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和身份）。
4. 单击要导出的应用程序项。然后单击 **More**（更多），再单击 **Export Application**（导出应用程序）。
5. 按照屏幕上的说明完成导出操作。
6. 单击 **OK**（确定）。

导入应用程序

要导入应用程序，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和身份）。
4. 单击要导入的应用程序项。然后单击 **More**（更多），再单击 **Import Application**（导入应用程序）。
5. 按照屏幕上的说明完成导入操作。
6. 单击 **OK**（确定）。

修改身份

要修改身份，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **My Identity**（我的标识）。
3. 在 **Single Sign On**（单次登录）下，单击 **Manage Applications and Credentials**（管理应用程序和身份）。
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：
 - 添加新身份
 - 删除身份
 - 删除未使用的身份
 - 编辑身份
6. 按照屏幕上的说明进行操作。
7. 单击 **OK**（确定）保存更改。

高级任务（仅供管理员使用）

身份管理器的 Authentication and Credentials（验证和身份）页和 Advanced Settings（高级设置）页仅供具有管理员权限的用户使用。使用这些页面，您可以执行以下操作：

- 指定用户和管理员的登录方式。
- 配置身份属性。
- 配置身份管理器的程序设置。

指定用户和管理员的登录方式

从 Authentication and Credentials（验证和身份）页，您可以指定用户或管理员需要何种类型的（一种或多种）身份。

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（HP ProtectTools 安全管理器） > Credential Manager（身份管理器）**。
2. 单击 **Authentication and Credentials（验证和身份）**。
3. 单击 **Authentication（验证）** 选项卡。
4. 在类别列表中单击类别，即 **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 **OK（确定）**。
7. 单击 **Apply（应用）**，然后单击 **OK（确定）** 保存更改。

配置自定义验证需求

如果 **Authentication and Credentials**（验证和身份）页的 **Authentication**（验证）选项卡上未列出您所需的一组验证身份，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**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **Authentication and Credentials**（验证和身份）。
3. 单击 **Authentication**（验证）选项卡。
4. 在类别列表中单击类别，即 **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 combine the authentication methods**（使用 OR 组合验证方法）
（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）保存更改。

配置身份属性

从 Authentication and Credentials（验证和身份）页的 **Credentials（身份）** 选项卡上，您可以查看可用验证方法的列表并修改设置。

要配置身份，请执行以下操作：

1. 选择 **Start（开始） > All Programs（所有程序） > HP ProtectTools Security Manager（HP ProtectTools 安全管理器） > Credential Manager（身份管理器）**。
2. 单击 **Authentication and Credentials（验证和身份）**。
3. 单击 **Credentials（身份）** 选项卡。
4. 单击要修改的身份类型。
 - ❑ 要注册身份，请单击 **Register（注册）**，然后按照屏幕上的说明操作。
 - ❑ 要删除身份，请单击 **Clear（清除）**，然后在确认对话框中单击 **Yes（是）**。
 - ❑ 要修改身份属性，请单击 **Properties（属性）**，然后按照屏幕上的说明操作。
5. 单击 **Apply（应用）**，然后单击 **OK（确定）**。

配置身份管理器设置

在 **Advanced Settings**（高级设置）页中，您可以通过以下选项卡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、自动登录注册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。
- **Biometric Settings**（生物设置）— 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**（智能卡和令牌）— 允许您查看并修改所有可用的智能卡和令牌的属性。

要修改身份管理器设置，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **Advanced Settings**（高级设置）。
3. 根据要修改的设置，单击相应的选项卡。
4. 按照屏幕上的说明修改设置。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）保存更改。

示例 1 — 使用 **Advanced Settings**（高级设置）页允许从身份管理器进行 **Windows** 登录

要允许从身份管理器登录到 Windows，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **Advanced Settings**（高级设置）。
3. 单击 **General**（常规）选项卡。
4. 选中 **Use Credential Manager to log on to Windows**（使用身份管理器登录到 Windows）复选框。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）保存更改。
6. 重新启动笔记本电脑。

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

若要求在登录注册对话框或 Web 页之前使用单次登录来验证身份，请执行以下操作：

1. 选择 **Start**（开始） > **All Programs**（所有程序） > **HP ProtectTools Security Manager**（HP ProtectTools 安全管理器） > **Credential Manager**（身份管理器）。
2. 单击 **Advanced Settings**（高级设置）。
3. 单击 **Single Sign On**（单次登录）选项卡。
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 **Validate user before submitting credentials**（提交身份之前验证用户）复选框。
5. 单击 **Apply**（应用），然后单击 **OK**（确定）保存更改。
6. 重新启动笔记本电脑。

术语表

本文档和 ProtectTools Security Manager（HP ProtectTools 安全管理器）中使用了下列术语：

Authentication（验证） — 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。

Automatic DriveLock（驱动器锁自动保护功能） — 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。

Biometric（生物） — 使用物理特征（例如指纹）来识别用户的身份验证类型。

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

BIOS security mode（BIOS 安全模式） — 智能卡安全保护功能中的设置，启用后要求使用智能卡和有效的 PIN 进行用户验证。

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

Credentials（身份） — 用户在验证过程中证明其有资格执行特定任务的方法。

Cryptographic service provider (CSP)（加密服务提供程序 (CSP)） — 可用于适当定义的接口来实现特定加密功能的加密算法提供程序或库。

Cryptography（加密技术） — 对数据进行加密和解密的手段，以保证只有指定的用户才能解码数据。

Decryption（解密） — 在加密技术中用于将加密的数据转换为一般文本的过程。

DriveLock（驱动器锁） — 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输入驱动器锁密码的安全保护功能。

Digital certificate（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标识个人或公司身份的电子身份证书。

Digital signature（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。

Domain（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。

Emergency recovery archive（急救档案） — 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）。

Encryption（加密） — 加密技术中将普通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。

Encryption File System (EFS)（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。

Identity（标识） — ProtectTools 的身份管理器中的一组身份和设置，其用途类似于特定用户的帐户或配置文件。

Migration（迁移） — 允许管理、恢复和传输密钥及证书的任务。

Network account（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。

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

Power-on authentication (开机验证) — 打开计算机时要求使用某种验证方式（例如智能卡、安全保护芯片或密码）的安全保护功能。

Public Key Infrastructure (PKI) (公共密钥基础结构 (PKI)) — 为创建、使用和管理证书及加密密钥定义接口的标准。

Reboot (重新引导) — 重新启动计算机的过程。

Single Sign On (单次登录) — 存储验证数据并允许您使用身份管理器来访问需要密码验证的 Internet 和 Windows 应用程序的功能。

Smart card (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。

Smart card administrator password (智能卡管理员密码) — 在计算机设置实用程序中将管理员智能卡与计算机相关联的密码，用于在启动或重新启动时验证身份。此密码可由管理员手动设置或随机生成。

Smart card user password (智能卡用户密码) — 在计算机设置实用程序中将用户智能卡与计算机相关联的密码，用于在启动或重新启动时验证身份。此密码可由管理员手动设置或随机生成。

Stringent security (严格的安全保护功能) — BIOS 配置中的安全保护功能，为开机验证、管理员密码或其他形式的开机验证提供增强的保护功能。

Trusted Platform Module (TPM) embedded security chip (select models only) (可信平台模块 (TPM) 嵌入式安全保护芯片，仅限于某些机型) — 可保护高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。

USB token (USB 令牌) — 存储用户身份信息的安全设备。该设备类似于智能卡或生物识别器，用于验证计算机主人的身份。

Virtual token (虚拟令牌) — 与智能卡或读卡器功能非常相似的安全保护功能。该令牌保存在计算机硬盘驱动器或 Windows 注册表中。使用虚拟令牌登录后，将要求您输入用户 PIN 以完成验证。

Windows user account (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。

索引

字母

BIOS 管理员卡密码

定义 1-5

更改 2-6

设置 2-4

BIOS 管理员密码

定义 1-4

更改 4-13

设置 4-13

BIOS 用户卡密码

定义 1-5

设置和更改 2-7

BIOS 智能卡安全保护功能
2-3

F10 设置实用程序密码 1-4

ProtectTools Security

Manager 1-1

ProtectTools 的 BIOS 配置
4-1

ProtectTools 的嵌入式安全
保护 3-1

ProtectTools 的身份管理器
5-1

ProtectTools 的智能卡安全
保护功能 2-1

TPM 芯片

初始化 3-3

启用 3-2

Windows 登录密码 1-6

Windows 网络帐户 5-13

A

安全设置实用程序密码 1-4

B

备份

标识 5-9

单次登录 5-18

嵌入式安全保护功能 3-8

智能卡 2-12

标识 5-9

C

初始化

嵌入式安全芯片 3-3

智能卡 2-2

D

单次登录

导出应用程序 5-18

删除应用程序 5-17

手动注册 5-16

修改应用程序属性 5-17

自动注册 5-15

对文件和文件夹进行加密
3-6

G

- 个人安全驱动器 (PSD) 3-6
- 管理
 - 标识 5-9
 - 配置文件 4-7

H

- 恢复
 - 标识 5-10
 - 单次登录 5-18
 - 智能卡 2-13

J

- 基本用户密钥密码
 - 定义 1-5
 - 更改 3-7
 - 设置 3-5
- 基本用户帐户 3-4
- 急救 3-3
- 急救令牌密码
 - 定义 1-5
 - 设置 3-3
- 计算机设置实用程序的管理员密码
 - 更改 4-13
 - 设置 4-13
- 计算机设置实用程序管理员密码
 - 定义 1-4
- 禁用
 - 开机验证 4-4
 - 嵌入式安全保护功能 3-11
 - 驱动器锁自动保护功能 4-5
 - 设备选项 4-3

- 严格的安全保护功能 4-14
- 智能卡 BIOS 安全保护功能 2-5
- 智能卡验证 4-4

K

- 开机密码
 - 定义 1-4
 - 设置和更改 4-12
- 开机验证
 - 启用和禁用 4-4
 - 在 Windows 重新启动时 4-15

M

- 密码
 - 管理 1-4
 - 使用指南 1-7
- 命令行 4-7
- 默认用户 5-14

P

- 配置文件
 - 保存 4-9
 - 删除 4-9
 - 显示菜单 4-8
 - 应用 4-10
- 配置文件密码
 - 定义 1-4
 - 设置 4-9

Q

- 启用
 - TPM 芯片 3-2
 - 开机验证 4-4
 - 嵌入式安全保护功能 3-11

- 驱动器锁自动保护功能 4-5
- 设备选项 4-3
- 严格的安全保护功能 4-14
- 智能卡 BIOS 安全保护功能 2-3
- 智能卡验证 4-4
- 驱动器锁密码 1-4
- 驱动器锁自动保护功能 4-5
- S**
- 设备选项 4-3
- 身份管理器
 - 登录密码 1-6
 - 登录向导 5-3
 - 恢复文件密码 1-6
 - 帐户 5-4
- 生物识别器 5-5
- 属性
 - 身份 5-22
 - 验证 5-20
 - 应用程序 5-17
- 锁定工作站 5-11
- W**
- 网络帐户 5-13
- 我的标识 5-9
- X**
- 虚拟令牌 5-7
- Y**
- 严格的安全保护功能 4-14
- 引导选项 4-2
- Z**
- 帐户
 - 基本用户 3-4
 - 身份管理器 5-4
- 指纹 5-5
- 智能卡 BIOS 安全保护功能 2-3
- 智能卡的 PIN
 - 定义 1-5
 - 更改 2-11
- 智能卡管理员密码
 - 定义 1-5
 - 更改 2-6
 - 设置 2-3
- 智能卡恢复文件密码
 - 定义 1-5
 - 设置 2-12
- 智能卡用户密码
 - 存放 2-8
 - 定义 1-5
 - 设置和更改 2-7
- 主人密码
 - 定义 1-5
 - 更改 3-10
 - 设置 3-3
- 注册
 - 身份 5-5
 - 应用程序 5-15