



HP Trusted Platform Module

用户指南

版权和许可证

© 2014 Copyright Hewlett-Packard
Development Company, L.P.

未经事先书面许可，严禁进行任何形式的复制、改编或翻译，除非版权法另有规定。

此处包含的信息如有更改，恕不另行通知。

HP 产品及服务的保修仅以随该产品及服务提供的书面保修声明为准。本文所述任何内容不应被视为附加保修。对任何技术或编辑错误或者本文所述内容的遗漏，HP 不承担任何责任。

部件号：F5S62-90908

Edition 1, 11/2014

目录

1 产品概述	1
产品视图	2
产品规格	3
技术规格	3
运行环境规格	3
支持的打印机和 MFP	3
产品尺寸	3
产品硬件设置与软件安装	4
2 管理产品	7
通过 HP 内嵌式 Web 服务器 (EWS) 查看 TPM 状态	8
如何访问 HP 内嵌式 Web 服务器 (EWS)	8
产品安全功能	8
安装确认	8
证书和 TPM	8
EWS	8
停止使用 TPM	9
禁用以前的 TPM 后安装新 TPM 或重新启用现有 TPM	14
3 解决问题	17
与 HP TPM 相关的错误代码	18
软件和固件更新	19
4 服务和故障排除	21
客户支持	21
索引	23

1 产品概述


HP 可信平台模块附件 (TPM) 提供安全的设备身份以及由 TPM 证书生成并保护的私钥。TPM 通过自动将设备加密密钥封装到 TPM，增强对打印机或 MFP 上存储的加密凭据和数据的保护。

TPM 在安装时自动与打印机配装。安装后，打印机和 TPM 即封装在一起，并且打印机拥有 TPM。原打印机不放弃 TPM 所有权即无法将 TPM 移至其他设备。如果移至新打印机且所有权移交给新打印机，则将以加密方式擦除原打印机上的数据。

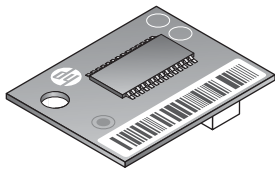
TPM 可创建、使用和存储加密密钥。它自动保护驱动器锁密码、存储的密码以及证书私钥。密钥封装到存储在 TPM 中的主加密密钥，只能通过 TPM 访问。

如果缺少 TPM，则 TPM 阻止打印机启动。如果从打印机上卸下了 TPM，则前控制面板将显示一条错误消息，指示缺少 TPM。

如果执行**停止使用 TPM**过程，则重新启动打印机时将重新安装固件。需要重新加载所有其他已安装的应用程序或解决方案，并需要重新配置打印机。

 **注：**在某些情况下，引导前菜单中可能显示硬盘驱动器错误，要求用 U 盘手动恢复打印机固件。

产品视图



产品规格

技术规格

部件号	F5S62A
包装箱内物品	HP 可信平台模块、《安装指南》
保修	一年现场有限保修
标准和认证	符合可信计算组制定的 TPM 1.2 标准。 ¹

¹ 可信计算组 (TCG) 是一家国际行业标准组织，它组织其成员制定各种规格。TCG 发布各种规格供整个行业使用和实施。

在 www.hp.com/go/printsecurity 了解详情。

运行环境规格

温度	运行：13 至 30° C；存放：0 至 40° C
湿度	湿度：运行：相对湿度 10% 至 80%；存放：相对湿度 10% 至 90%

支持的打印机和 MFP

HP LaserJet：M806

HP LaserJet MFP：M630、M830

HP Color LaserJet：M651、M855

HP Color LaserJet MFP：M680、M880

HP Officejet：X555

HP Officejet MFP：X585

如果未列出您的打印机，请参阅打印机数据表以确认 HP 可信平台模块是否为兼容附件。

产品尺寸

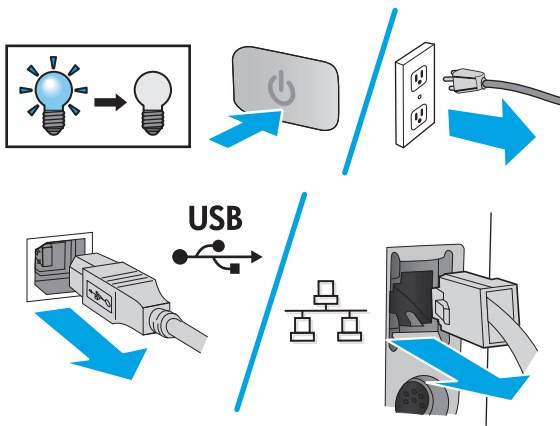
尺寸	21.62 x 18.03 x 6.2 毫米
重量	1.71 克

产品硬件设置与软件安装

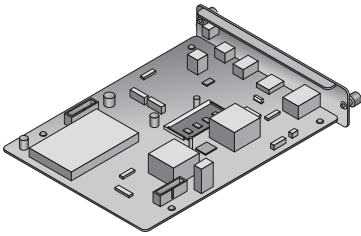
1. 访问 www.hp.com/support 并下载打印机的最新固件版本。升级打印机上的固件。有关说明，请参阅打印机文档。成功安装最新固件后，转到第 2 步。



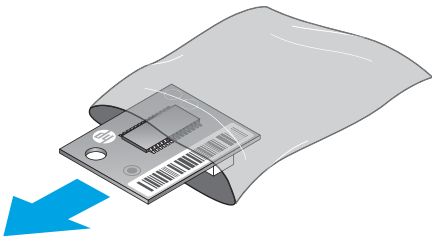
2. 关闭产品电源，然后拔下电源线和网线。




3. 从打印机上拆下格式化板。格式化板的外观和拆卸过程因打印机而异。如果需要其他信息，请参阅 www.hp.com/support 上的打印机产品支持页。

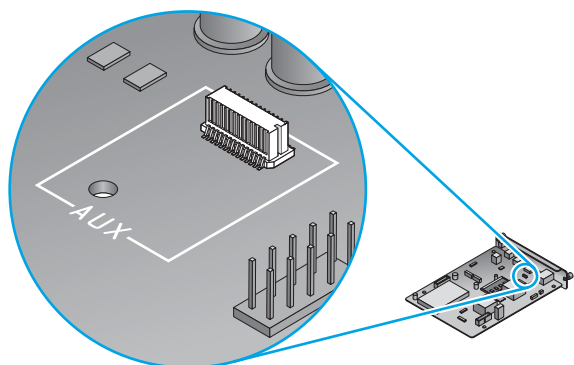


4. 从包装中取出 TPM。

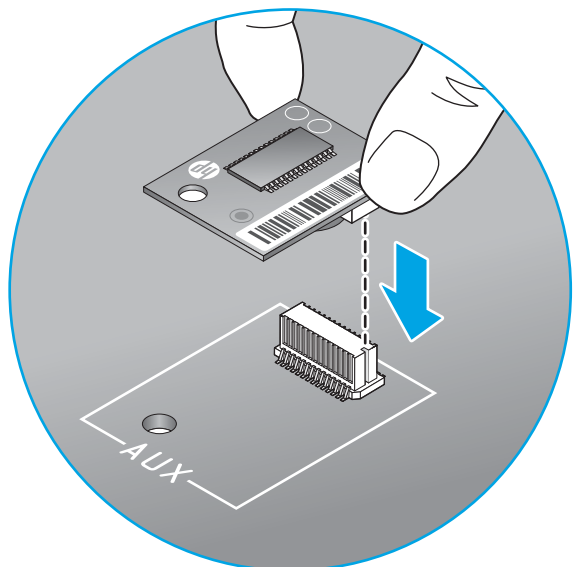


5. 在格式化板上找到正确的接口。格式化板上印有大小与 TPM 相同的白色方形轮廓，它在格式化板中圈住该接口和一个小孔。

 **注：**某些老式板卡上可能没有 **AUX** 字样。您的格式化板上接口的位置可能与所示的位置不同。

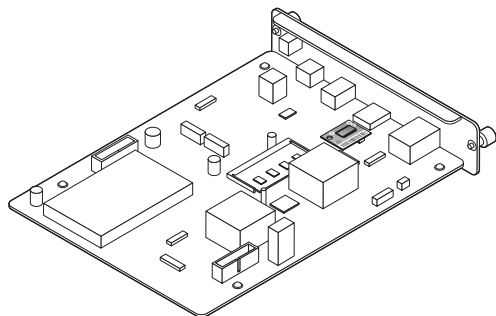


6. 按所示方式握住 TPM 的边缘，然后将 TPM 上的接口与格式化板上的接口对齐。轻轻地将 TPM 放在格式化板上的接口上。慢慢地稳定向下施力。接口完全啮合时，将听到咔嗒一声。

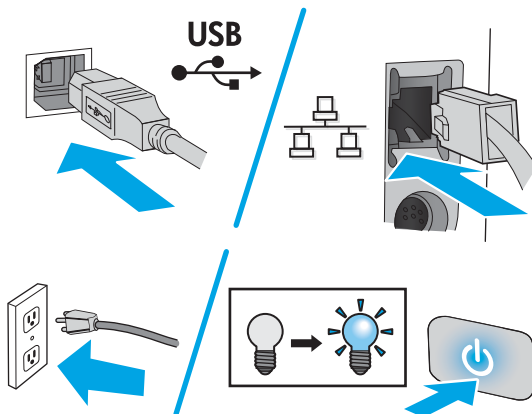


7. 将格式化板装回打印机中。

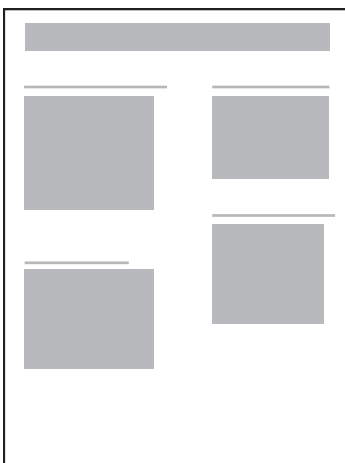
 **注：**建议用 Kensington 锁固定格式化板。



8. 插入电源线和网线，然后开启打印机。



9. 打印机初始化后，打印一张配置页。有关说明，请参阅打印机文档。查看本页上“**安装的个性化和选项**”标题下方的内容，确认列出了 **HP TPM 附件：已启用**。有关其他 TPM 用户信息和故障排除，请访问 www.hp.com/support/。



2 管理产品

- [通过 HP 内嵌式 Web 服务器 \(EWS\) 查看 TPM 状态](#)
- [停止使用 TPM](#)
- [禁用以前的 TPM 后安装新 TPM 或重新启用现有 TPM](#)

通过 HP 内嵌式 Web 服务器 (EWS) 查看 TPM 状态

- [如何访问 HP 内嵌式 Web 服务器 \(EWS\)](#)
- [产品安全功能](#)

 **注：**无法穿越网络防火墙访问 HP 内嵌式 Web 服务器。

如何访问 HP 内嵌式 Web 服务器 (EWS)

有关如何访问 HP 内嵌式 Web 服务器的信息，请参阅打印机的《用户指南》。

产品安全功能

本产品包括多项安全功能以确保其所容纳的信息更安全，减少外部软件攻击和实物被盗的威胁。


- [安装确认](#)
- [证书和 TPM](#)
- [EWS](#)

安装确认

打印机初始化后，打印一张配置页。有关说明，请参阅打印机文档。查看本页上“**安装的个性化和选项**”标题下方的内容，确认列出了 **HP TPM 附件：已启用**。

证书和 TPM


TPM 通过由 TPM 生成和保护证书私钥，确保设备身份的安全。它通过自动将设备加密密钥封装到 TPM，增强对打印机或 MFP 上存储的加密凭据和数据的保护。

 **注：**新证书密钥由 TPM 生成，除非标记为可导出。在生成密钥时指定是否可导出。

EWS

内嵌式 Web 服务器 (EWS) 可用于执行以下任务：

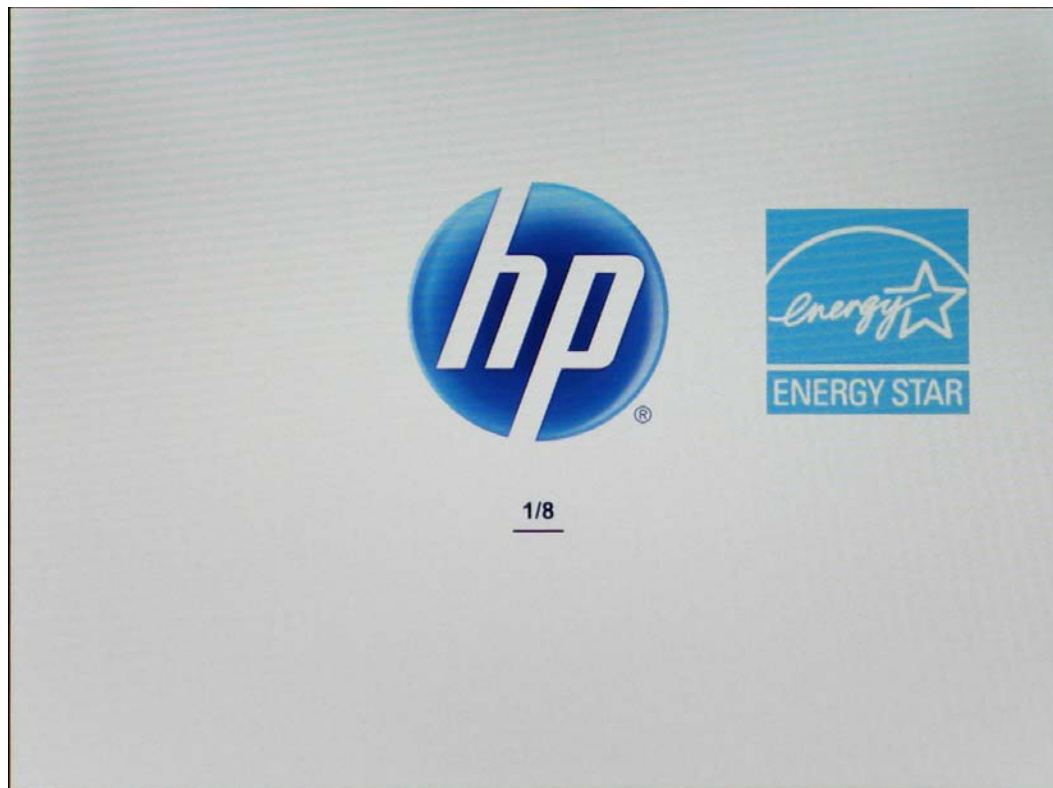
- 判断打印机上的哪些证书受 TPM 保护
- 使用 TPM 创建证书
- 导出证书和私钥（如果其标记为可导出）

 **注：**有关如何访问 HP 内嵌式 Web 服务器 (EWS) 的信息，请参阅打印机的《用户指南》。

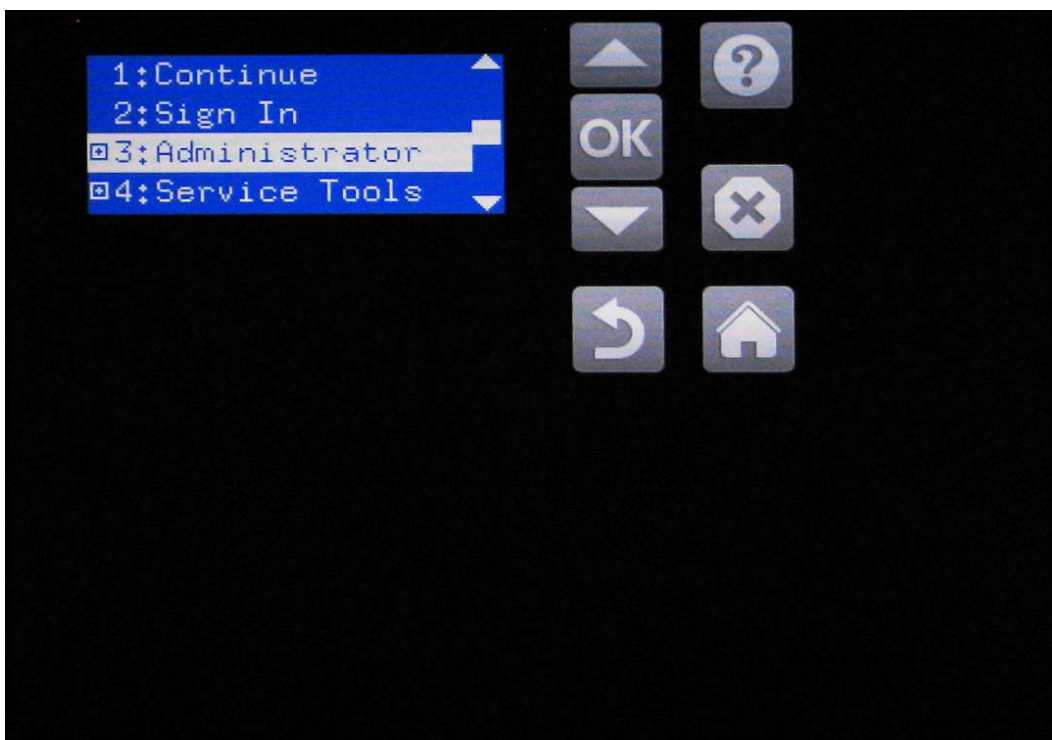
停止使用 TPM

警告！ 执行此过程将丢失所有客户数据，包括安装在设备上的解决方案。

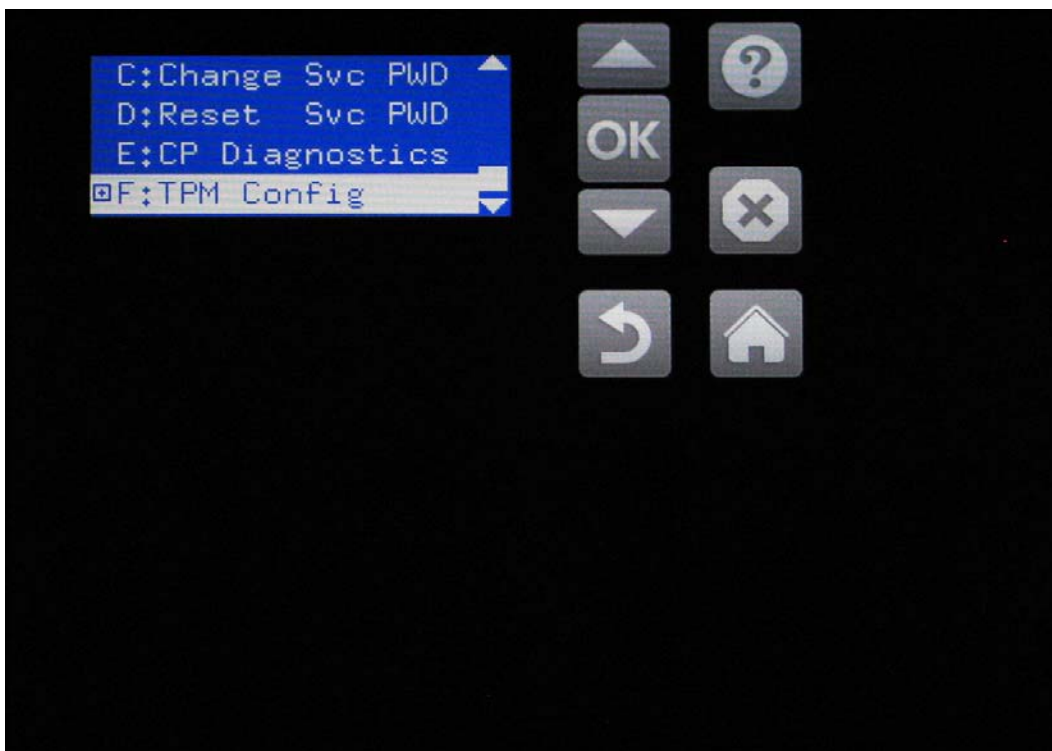
1. 对于多功能打印机，在初始化屏幕到达 **1/8** 时，通过按 HP 徽标，访问引导前菜单。对于单功能打印机，在 **1/8** 之前按 HP 徽标。



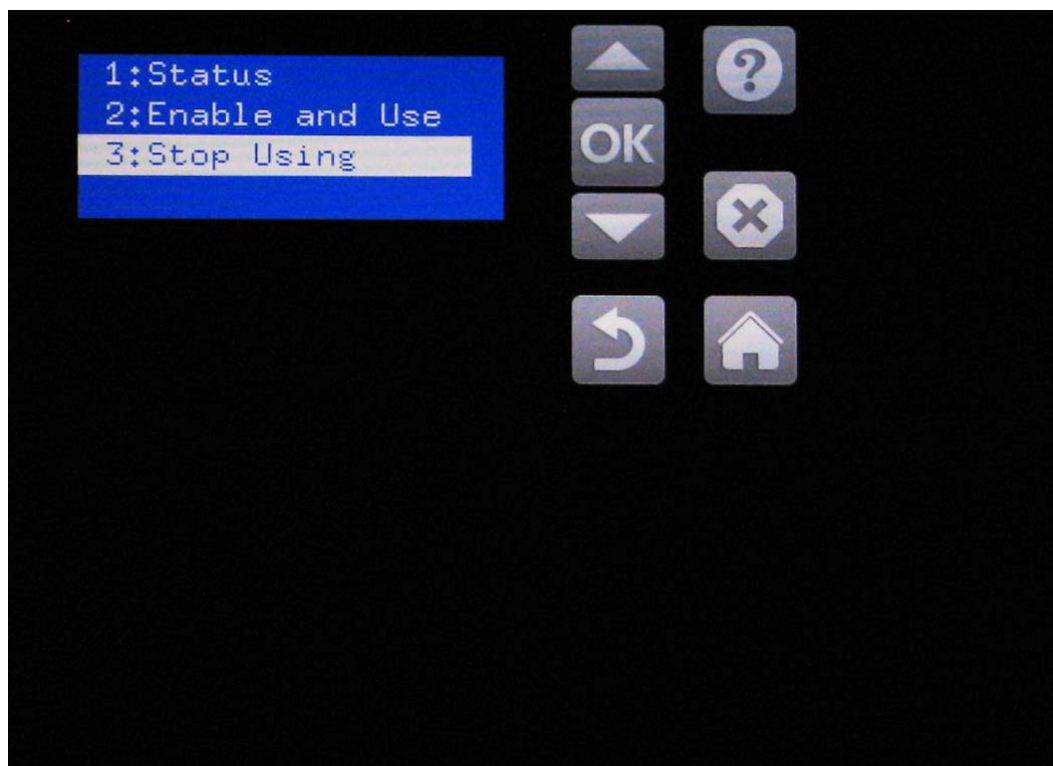
2. 从控制面板上的引导前菜单中，导航至**管理员**，然后按**确定**。如果提示输入管理员口令，请照做。



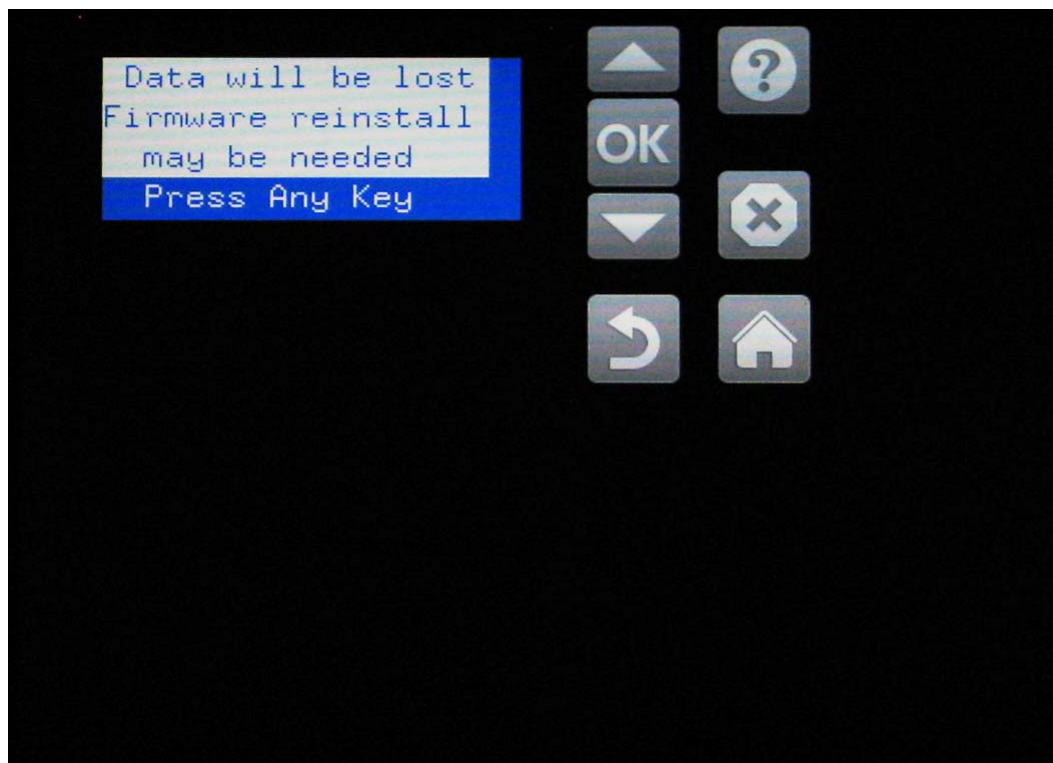
3. 导航至 **F:TPM 配置**，然后按 **确定**。



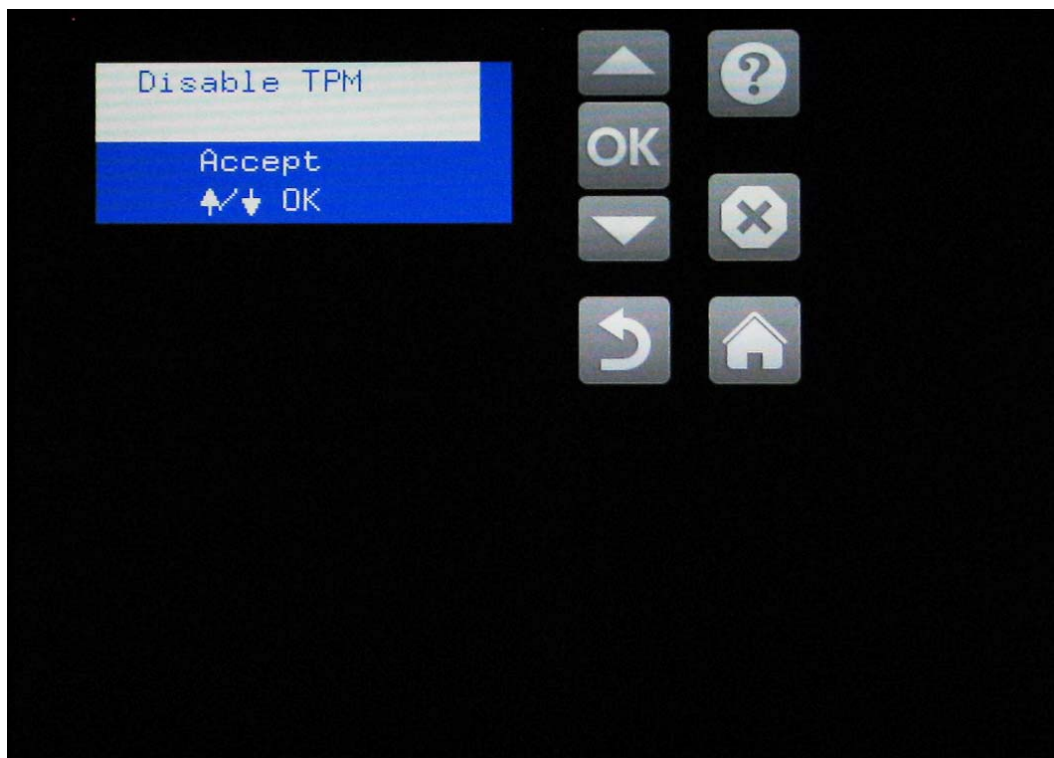
- 依次按停止使用、确定。



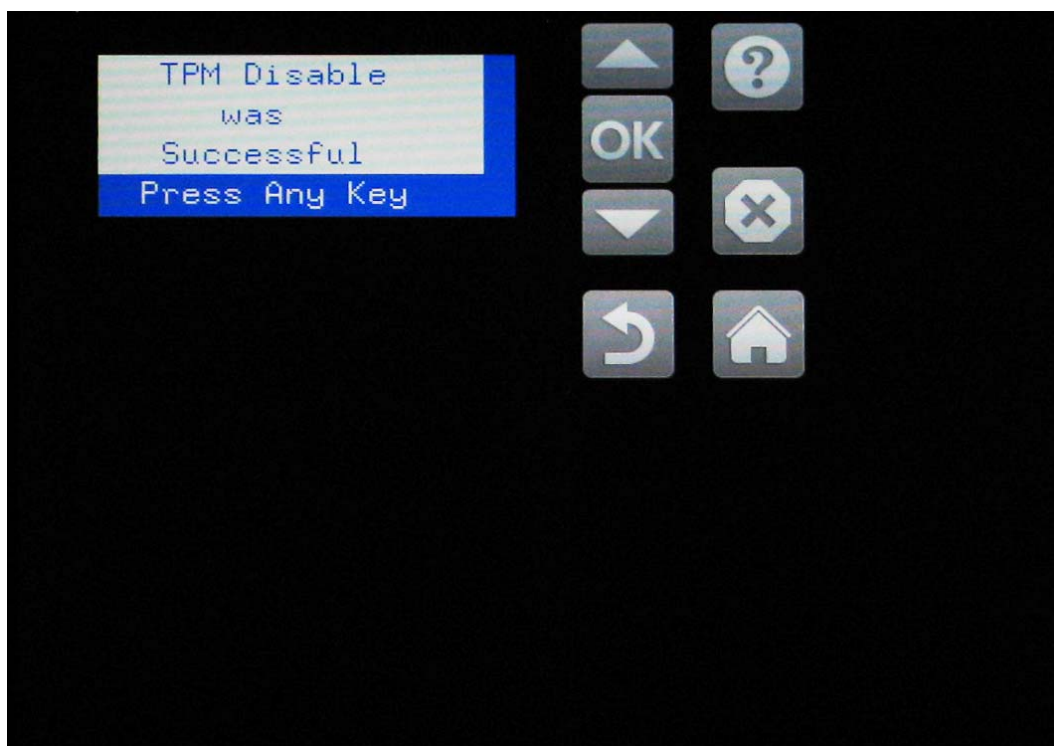
- 随后控制面板将显示数据将丢失，可能需要重新安装固件。按任意键。




6. 依次按禁用 TPM、确定。



7. 随后控制面板将显示 TPM 禁用已成功。按任意键。



 **注：**禁用 TPM 后，可将它留在格式化板上，也可卸下它。如果仍安装在上面，则可按禁用以前的 TPM 后安装新 TPM 或重新启用现有 TPM 一节中的步骤重新启用它。

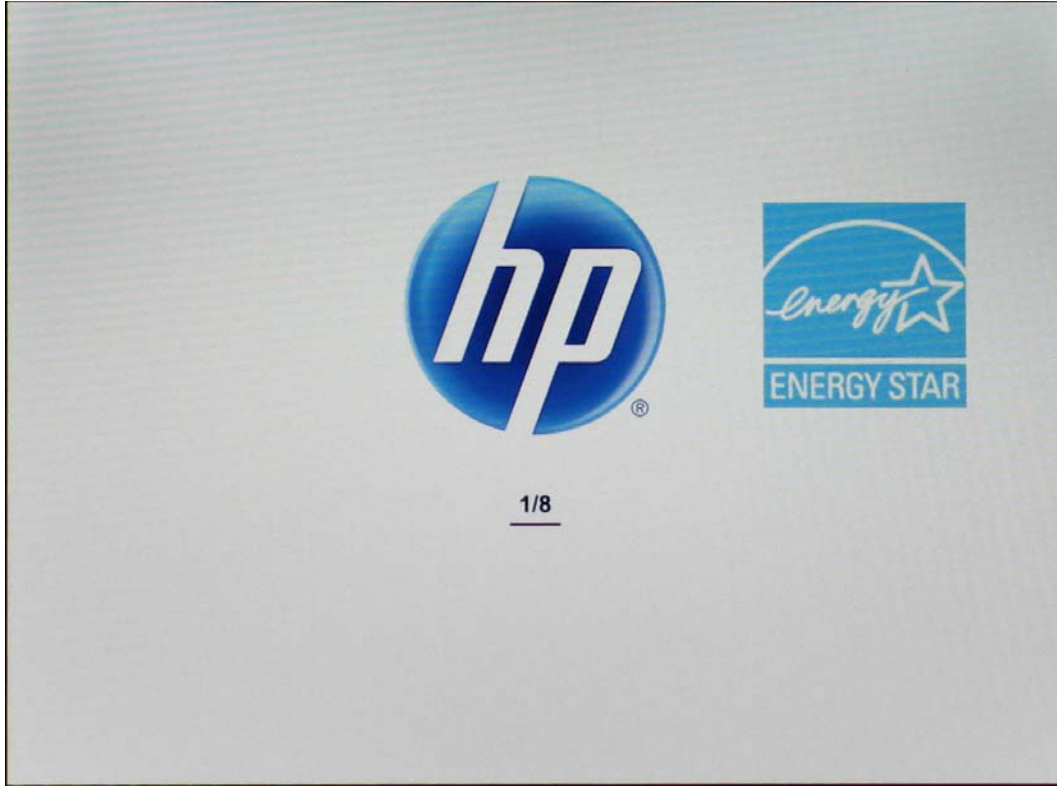
8. 随后打印机将重新启动，并在控制面板上显示正在升级固件和进度条。



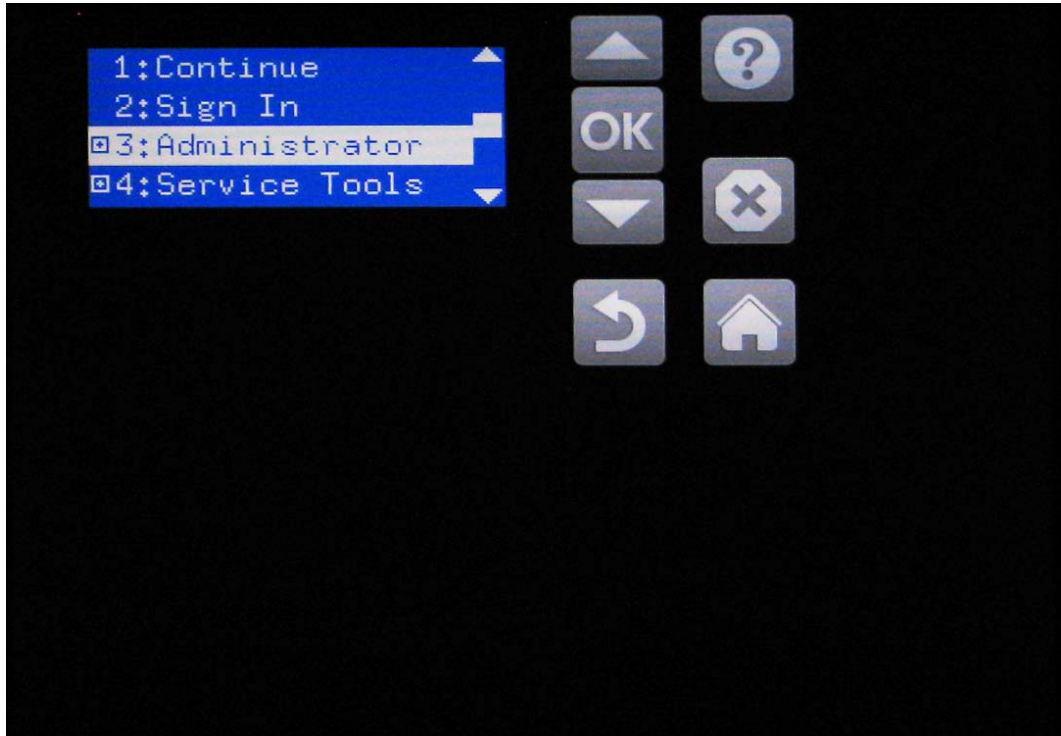
9. 通过打印配置页并寻找 **HP TPM 附件：已禁用**，确认 TPM 已禁用。

禁用以前的 TPM 后安装新 TPM 或重新启用现有 TPM

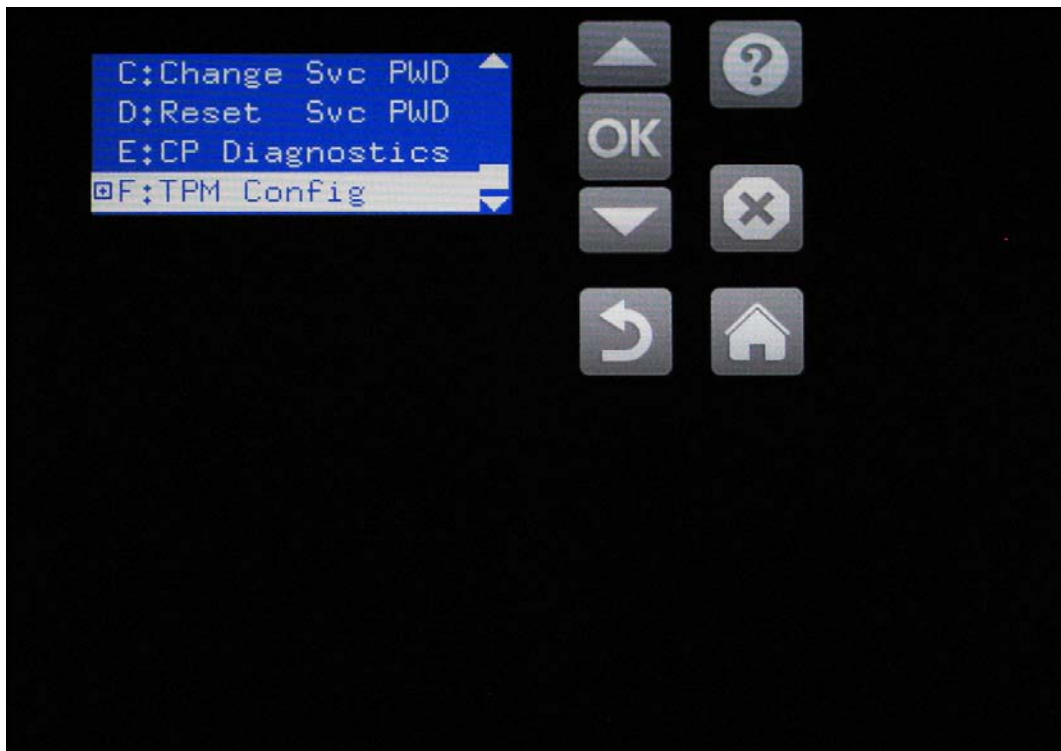
1. 将 TPM 安装在格式化板上，然后将格式化板装入打印机。
2. 对于多功能打印机，在初始化屏幕到达 **1/8** 时，通过按 HP 徽标，访问引导前菜单。对于单功能打印机，在 **1/8** 之前按 HP 徽标。



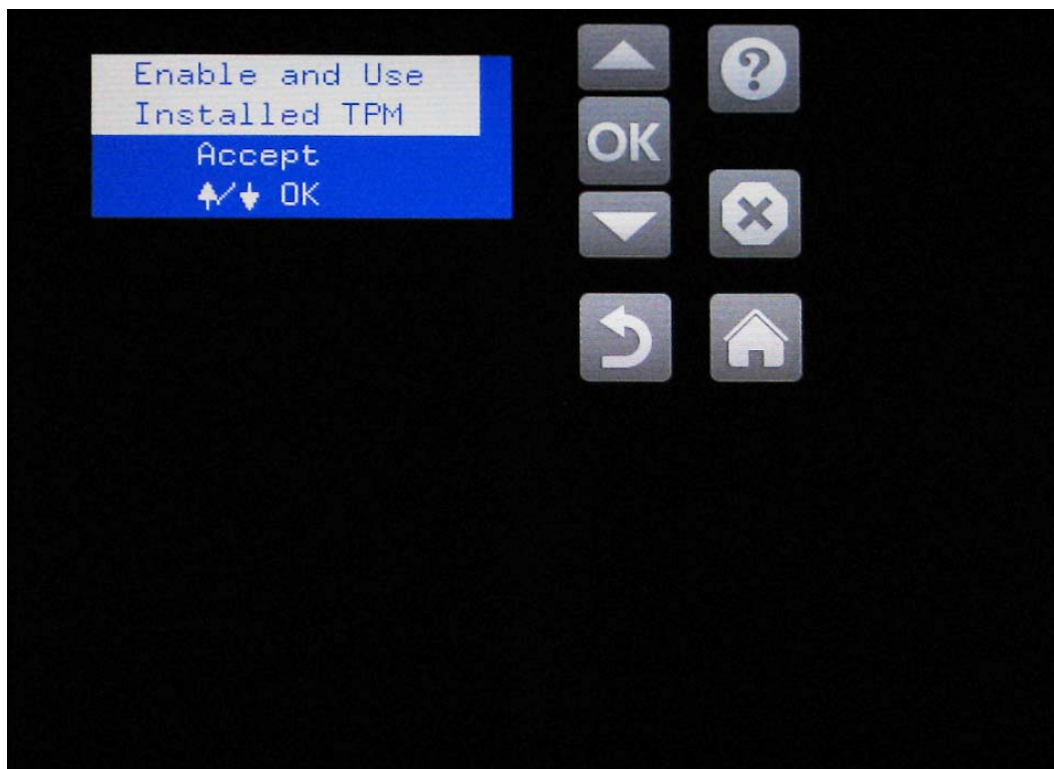
3. 在引导前菜单中，导航至**管理员**，然后按**确定**。如果提示输入管理员口令，请照做。



4. 导航至 **F: TPM 配置**，然后按 **确定**。



5. 依次按启用并使用已安装的 TPM、确定。



6. 随后打印机将重新启动。
7. 打印机初始化后，打印一张配置页。查看本页上“安装的个性化和选项”标题下方的内容，确认列出了 **HP TPM 附件：已启用**。

3 解决问题

- [与 HP TPM 相关的错误代码](#)
- [软件和固件更新](#)

与 HP TPM 相关的错误代码

错误代码	原因	说明	解决方案
33.04.01	缺少 TPM	以前安装过 TPM 的打印机上缺少 TPM。	将缺少的 TPM 模块装回打印机中。重新启动打印机。
33.04.02	未知 TPM	以前安装过其他 TPM 的打印机上现在安装的 TPM 有误。	将原来的 TPM 装回打印机中。重新启动打印机。
33.04.03	未知 TPM	以前未安装过 TPM 的打印机上已安装了旧 TPM。	卸下该 TPM 模块。打印机将不受保护。 或者 如果决定使用旧 TPM 保护打印机，请参阅 禁用以前的 TPM 后安装新 TPM 或重新启用现有 TPM 一节。
33.04.04	未知 TPM	以前安装过其他 TPM 的打印机中安装了新 TPM。	将原来的 TPM 装回打印机中。重新启动打印机。 或者 如果决定用新 TPM 保护打印机，请访问 www.hp.com/support/ 以了解详细说明。

软件和固件更新

有关软件和固件更新的信息，请参阅打印机文档。

4 服务和故障排除

客户支持

保修期内可从您所在的国家/地区获得免费的电话支持。

产品包装箱中随附的小册子或 www.hp.com/support 网站上列有国家/地区电话号码

准备好打印机名称、序列号、购买日期和问题说明。

获得对 Macintosh 电脑的产品支持

www.hp.com/go/macosex

订购原装 HP 部件或附件

www.hp.com/buy/parts

订购其他 HP 服务或维护协议

www.hp.com/go/carepack

索引

符号/编号

33.04.01 18
33.04.02 18
33.04.03 18
33.04.04 18

A

安全
 功能 8
安装 4
 确认 8
 新 14

B

Bonjour
 确定 8
帮助 21
保修 3
标准 3
部件号 3

C

重量 3
尺寸 3
错误
 代码 18

D

打印机
 支持 3
代码
 错误 18

E

Explorer，支持的版本
 HP 内嵌式 Web 服务器 8

G

概述
 产品 1
高度 3
更新
 固件 19
 软件 19
固件
 更新 19
关于
 产品 1
规格
 产品 3

H

HP 内嵌式 Web 服务器 (EWS)
 网络连接 8

I

Internet Explorer，支持的版本
 HP 内嵌式 Web 服务器 8

K

可信计算组 3
宽度 3

L

浏览器要求
 HP 内嵌式 Web 服务器 8

M

密钥证书 8

N

Netscape Navigator，支持的版本
 HP 内嵌式 Web 服务器 8
内嵌式 Web 服务器 (EWS)
 安全 8
 网络连接 8

Q

取消 9

R

认证 3
软件
 安装 4
 操作方法 4
 更新 19
 设置 4

S

设置 4
 新 TPM 14
湿度
 存放 3
 运行 3
视图
 产品 2
私钥 8

T

停止使用 9

W

Web 浏览器要求
 HP 内嵌式 Web 服务器 8
温度
 存放 3
 运行 3

X

系统要求
 HP 内嵌式 Web 服务器 8

Y

隐私
 功能 8

硬件

安装 4

操作方法 4

设置 4

运行

湿度 3

温度 3

Z

证书

安全 8

支持 21



F5562-90908

