HP Sure Admin 用户指南

摘要

HP Sure Admin 使 IT 管理员能够使用证书和公共密钥加密（而非密码）进行远程和本地设置管理，以安全地管理敏感的设备固件设置。

法律信息

Apple 是 Apple Computer, Inc. 在美国和其他国家/地区的注册商标。

Google Play 是 Google LLC 公司的商标。

保密的计算机软件。需要有 HP 颁发的有效许可证才能拥有、使用或复制。与 FAR 12.211 和 12.212 相一致，依据供应商的标准商业许可将“商业计算机软件、计算机软件文档和用于商业单位的技术数据”许可给美国政府使用。

本文档中包含的信息如有更改，恕不另行通知。HP 产品和服务附带的明示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构成任何额外保修服务。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任何责任。

第二版：2021 年 10 月

第一版：2019 年 12 月

文档部件号：L83995-AA2

目录

1 使用入门

HP Sure Admin 使 IT 管理员能够使用证书和公共密钥加密（而非密码）进行远程和本地设置管理，以安全地管理敏感的设备固件设置。

HP Sure Admin 由以下部分组成：

- **目标 PC：**支持增强型 BIOS 身份验证模式的管理平台。
- **HP Manageability Integration Kit (MIK)：**System Center Configuration Manager (SCCM) 或 HP BIOS Configuration Utility (BCU) 的插件，可用于远程管理 BIOS 设置。
- **HP Sure Admin Local Access Authenticator：**一款手机应用程序，可通过扫描二维码获取一次性 PIN 来代替密码，以启用对 BIOS 设置的本地访问。

使用 HP Sure Admin

本节介绍使用 HP Sure Admin 的过程。

1. 在适用于 System Center Configuration Manager (SCCM) 或增强型 BIOS Configuration Utility (BCU) 的 HP Manageability Integration Kit (MIK) 插件中，打开 HP Sure Admin 插件。
2. 从 Google Play™ 商店或 Apple App Store® 下载 HP Sure Admin 手机应用程序。
3. 创建目标设备和 HP Sure Admin 手机应用程序使用的密钥对，以获取用于解锁 BIOS 的一次性 PIN。

禁用 HP Sure Admin

本节介绍禁用 HP Sure Admin 的各种选项。

- 在 BIOS F10 设置中，选择**将安全设置恢复为出厂默认值**。

注：这需要检验物理存在，方法是通过 HP Sure Admin 手机应用程序提供身份验证 PIN 来访问 F10 设置。

- 使用 BCU 命令远程调用**将安全设置恢复为出厂默认值**的 WMI。

注：有关详细信息，请参阅 HP BIOS Configuration Utility (BCU) 用户指南。

- 在“MIK 安全性配置”页面中，选择**取消设置**。

2 创建和管理密钥

在启用增强型 BIOS 身份验证模式之前，先在 MIK 中完成安全性配置。要创建和导出密钥，必须启用增强型 BIOS 身份验证模式。要启用 BIOS 身份验证模式，请执行以下操作：

▲ 打开 HP Sure Admin 插件，然后选择**增强型 BIOS 身份验证模式**以创建和导出密钥。

创建和导出密钥

有三种不同的方式可以创建本地访问密钥对，然后启用 HP Sure Admin 手机应用程序来访问密钥。

- 第 2 页的通过手动分发创建和导出密钥
- 第 3 页的使用 Azure AD 吊销创建和导出密钥
- 第 3 页的创建密钥并将其发送至 Azure AD 组 OneDrive

通过手动分发创建和导出密钥

使用此选项导出本地访问授权密钥，然后通过电子邮件或其他途径将密钥手动分发到 HP Sure Admin 手机应用程序。

注：此选项无需 HP Sure Admin 手机应用程序访问网络即可获取一次性 PIN。

1. 在**密钥名称**输入框中为密钥命名。
2. 在**密码**输入框中输入密码。

   注：此密码可用于保护导出的密钥，HP Sure Admin 手机应用程序用户必须提供该密码才能导入密钥。

3. 选择**浏览**，然后选择系统中的导出路径。
4. 选择**创建密钥**。当**创建密钥**按钮旁边显示通知图标和**密钥创建成功**的消息时，即表示您的密钥创建成功。
5. 选择**下一步**。摘要页面会显示您输入的 HP Sure Admin 设置。
6. 选择**保存策略**。当显示**保存成功**的消息时，即表示策略已保存。
7. 导航至保存密钥的文件夹，使用 HP Sure Admin 手机应用程序用户在该设备上可以使用的方法（如电子邮件），将密钥分发给该用户。此用户还需要密码才能导入密钥。HP 建议针对密钥和密码使用不同的分发机制。

   注：发送二维码时，请以其原始尺寸发送。如果图像尺寸小于 800 × 600，应用程序将无法正确读取图像。

使用 Azure AD 吊销创建和导出密钥

使用此选项不但可将本地访问密钥连接到指定的 Azure Active Directory 组，还需要使用 HP Sure Admin 手机应用程序向 Azure Active Directory 验证用户身份，并在提供本地访问 PIN 之前确认用户为指定组成员。此方法还需要通过电子邮件或其他途径，将本地访问授权密钥手动分发到手机应用程序。

注：此选项要求 HP Sure Admin 手机应用程序接入网络，才能获取一次性 PIN。

1. 在**密钥名称**输入框中为密钥命名。
2. 在**密码**输入框中输入密码。

   注：此密码可用于保护导出的密钥，HP Sure Admin 手机应用程序用户必须提供该密码才能导入密钥。

3. 选择 **Azure AD 登录**，然后登录。
4. 从 **Azure AD 组名称**下拉框中选择您的组名。您必须是组成员才能访问密钥。
5. 选择**浏览**，然后选择系统中的导出路径。
6. 选择**创建密钥**。当**创建密钥**按钮旁边显示通知图标和**密钥创建成功**的消息时，即表示您的密钥创建成功。
7. 选择**下一步**。摘要页面会显示您输入的 HP Sure Admin 设置。
8. 选择**保存策略**。当显示**保存成功**的消息时，即表示策略已保存。
9. 导航至保存密钥的文件夹，使用 HP Sure Admin 手机应用程序用户在该设备上可以使用的方法（如电子邮件），将密钥分发给该用户。此用户还需要密码才能导入密钥。HP 建议针对密钥和密码使用不同的分发机制。

   注：发送二维码时，请以其原始尺寸发送。如果图像尺寸小于 800 × 600，应用程序将无法正确读取图像。

创建密钥并将其发送至 Azure AD 组 OneDrive

（推荐）使用此选项可避免在手机上存储本地访问授权密钥。选择此选项时，MIK 会将本地访问授权密钥存储到指定的 OneDrive 文件夹中，该文件夹仅可由授权组访问。每当需要 PIN 时，HP Sure Admin 手机应用程序都会要求向 Azure AD 验证用户身份。

1. 在**密钥名称**输入框中为密钥命名。
2. 在**密码**输入框中输入密码。
3. 选择 **Azure AD 登录**，然后登录。
4. 从 Azure AD 组名称下拉框中选择您的组名。

   注：您必须是组成员才能访问密钥。

5. 在 **OneDrive** 输入框中，输入您希望保存密钥的 OneDrive 文件夹的名称。
6. 选择**浏览**，然后选择系统中的导出路径。

7. 选择**创建密钥**。

注：当**创建密钥**按钮旁边显示通知图标和**密钥创建成功**的消息时，即表示您的密钥已成功添加到指定的 OneDrive 文件夹，并已导出到指定的本地文件夹。

8. 选择**下一步**。摘要页面会显示您输入的 HP Sure Admin 设置。

9. 选择**保存策略**。当显示**保存成功**的消息时，即表示策略已保存。

注：在这种情况下，无需将任何内容发送到 HP Sure Admin 手机应用程序，即可对其进行预配置。目标 PC 经配置将指向二维码中包含的 OneDrive 位置。如果用户为授权组成员并已成功通过身份验证，HP Sure Admin 手机应用程序将使用此指针访问该 OneDrive 位置。

3 手机设置

从 Google Play 或 Apple Store 下载 HP Sure Admin 手机应用程序。

- 从 Google 商店下载适用于 Android 手机的 HP Sure Admin。
- 从 Apple Store 下载适用于 iOS 手机的 HP Sure Admin。

使用 HP Sure Admin 手机应用程序解锁 BIOS

HP Sure Admin 手机应用程序可通过扫描目标机器所示的二维码获得一次性 PIN，并使用该一次性 PIN 代替 BIOS 密码，方便您在本地访问 BIOS 设置。

在将密钥发送到手机应用程序用户的情况下，使用以下步骤将密钥保存在手机本地。在以下示例中，密钥通过电子邮件发送至 HP Sure Admin 手机应用程序用户，用户可在手机上打开该电子邮件。

1. 打开包含密钥的电子邮件。
2. 显示**注册**页面后，请在**输入密码**输入框中输入密码，然后在**输入电子邮件地址**输入框中输入您的电子邮件地址，以解密密钥，并将其添加到 HP Sure Admin 应用程序中。解锁 PIN 码显示在**您的 PIN** 页面上。

> **注：**此步骤可将密钥保存在移动设备中，并完成注册。此时，您可以使用 HP Sure Admin 手机应用程序访问通过此密钥配置为可访问的任何设备。仅当管理员要求时，才需要提供电子邮件地址。

3. 在 **BIOS 输入响应代码**输入框中输入 PIN。

注册后获取 BIOS 设置访问权限

要在注册后获得目标机器上 BIOS 设置的访问权限，请执行以下操作：

1. 在启动时进入目标机器的 BIOS 设置。
2. 在手机应用程序中选择**扫描二维码**，然后扫描目标机器上的二维码。
3. 如果系统提示您进行用户身份验证，请出示您的凭证。
4. 已解锁的 PIN 码显示在**您的 PIN** 页面上。
5. 在目标机器上的 **BIOS 输入响应代码**输入框中输入 PIN。

使用 Azure AD 组 OneDrive 解锁 BIOS

要通过 Azure AD Group OneDrive 使用 HP Sure Admin 解锁 BIOS，请执行以下操作：

1. 选择**扫描二维码**，然后扫描 BIOS 二维码。

> **注：**HP Sure Admin 应用程序将显示 Azure AD 登录页面。

2. 登录您的 Azure 帐户。

3. 在 **BIOS 输入响应代码**输入框中输入 PIN。

注：在这种情况下，HP Sure Admin 应用程序不会在本地保存密钥。HP Sure Admin 手机应用程序必须可以接入网络，而且每当需要提供一次性 PIN 时，用户都必须进行身份验证。

4 HP Sure Admin 错误代码

使用本节中的表查看 HP Sure Admin 和 KMS 管理控制台的错误代码、类型及其说明。

表 4-1 HP Sure Admin 应用程序错误代码、类型及其说明

错误代码	错误类型	说明
100	QRCodeUnknownError	常规错误。
101	QRCodeDeserialization	无法读取 QR 码 JSON。字符串并非有效的 JSON 文件，或数据无效。
102	QRCodeInvalidImage	扫描的二维码图像无效。无法读取二维码图像文件。
103	QRCodeNoPayload	扫描的二维码图像无效。图像文件没有 JSON 负载。
104	QRCodeInvalid	无法读取 QR 码 JSON。字符串并非有效的 JSON，或 QR 码图像中的数据无效。
105	QRCodeInvalidKeyIdHash	QR 码 JSON 中的公共密钥哈希与注册程序包的公共密钥哈希（KeyID 数据）不匹配。
106	QRCodeTampered	扫描的 QR 码图像被篡改且无效。
107	QRCodeTamperedOrInvalidPassPhrase	扫描的 QR 码图像被篡改且无效，或者输入的密码不正确。

表 4-2 OneDrive 的 OneTime 访问密钥错误、类型及其说明

错误代码	错误类型	说明
200	OneTimeKeyError	常规错误。
201	OneTimeKeyNoUserGroups	已登录的用户不属于贵组织中的任何 AD 组。
203	OneTimeKeyInvalidUserGroup	已登录的用户不属于为此密钥分配的 AD 组。
204	OneTimeKeyQRFileDoesNotExist	AD 组的 OneDrive 文件夹中不存在该一次性密钥文件。
205	OneTimeKeyInvalidQRFile	AD 组的 OneDrive 文件夹中的 OneTime 密钥文件无效。
206	OneTimeKeyInvalidQRpayload	OneTime 密钥文件已存在，但无法读取文件负载。

表 4-3 Azure AD Authorization errors

错误代码	错误类型	说明
300	AzureADUnknownError	常规错误。

表 4-3 Azure AD Authorization errors （续）

错误代码	错误类型	说明
301	AzureADInvalidDomain	输入的电子邮件地址与 QR 码图像中指定的域名不匹配。
302	AzureADAccessToken	从 Azure AD 获取访问令牌时出错。用户无法登录到贵组织的 Azure AD，或该应用程序没有连接贵组织 Azure AD 所需的权限。也可能是用户取消了身份验证。
303	AzureADUserProfile	HP Sure Admin 应用程序已启用，能够从贵组织的 Azure AD 中获取用户配置文件信息。
304	AzureADUserPrincipalMismatch	输入的电子邮件地址与已登录用户的用户主体名称不匹配。
305	AzureADUserInvalidUserGroup	已登录的用户不属于为此密钥分配的 Azure AD 组。

表 4-4 KMS 管理控制台错误、类型及其说明

错误代码	错误类型	说明
401	KmsUnauthorized	用户无权使用 KMS 服务。
402	KmsKeyDoesNotExist	KMS 密钥库中不存在匹配的私钥。密钥当前处于已删除但可恢复状态，其名称不能在此状态下重复使用。密钥只能恢复或被清除。
403	KmsKeyDoesNotExistInTableStorage	表存储中不存在密钥。
404	KmsUploadKeyErrorInKeyVault	向密钥库添加密钥时出现错误。
405	KmsUploadKeyUnauthorized	用户无权上传密钥。用户不属于允许调用此 API 的被授权 AD 组。
406	KmsInvalidAzureADLogin	用户未登录 Azure 租户 AAD。
407	KmsNoUserGroups	已登录的用户不属于贵组织中的任何 AD 组。
408	KmsInvalidUserGroup	已登录的用户不属于为此密钥分配的 AD 组。
409	KmsInvalidAccessToken	请求中提供的访问令牌无效。
410	KmsAccessTokenExpired	提供的访问令牌已过期。
411	KmsAccessTokenInvalidTenantId	提供的访问令牌具有无效的租户 ID 值。
412	KmsAccessTokenTenantIdMismatch	提供的访问令牌中的租户 ID 与功能应用程序租户 ID 不匹配。
413	KmsInvalidKeyId	密钥 ID 为 Null 或空。
414	KmsDeleteKeyUnauthorized	用户无权删除密钥。用户不属于允许调用此 API 的被授权 AD 组。
415	KmsKeyVaultSoftDeleteUnrecoverableState	试图恢复密钥失败，密钥无法恢复。用户应该重试。
416	KmsInvalidGetKeysRequest	获取密钥请求无效。

表 4-4 KMS 管理控制台错误、类型及其说明 （续）

错误代码	错误类型	说明
417	KmsGetKeysUnauthorized	用户无权获取密钥。用户不属于允许调用此 API 的被授权 AD 组。
418	KmsInvalidRequestPayload	API 收到的请求无效。
419	KmsRequestRequired	收到的请求不得为空。
420	KmsKeyNotConcurrent	自从用户上次检索副本以来，表存储中的密钥已更新或已修改。