



# HP Sure Admin 使用指南

## 摘要

HP Sure Admin 讓 IT 管理員得以使用認證和公開金鑰加密技術，安全地管理遠端和本機設定管理上的敏感裝置韌體設定，而無需使用密碼。

## 法律資訊

© Copyright 2019, 2021 HP Development Company, L.P.

Apple 是 Apple Computer, Inc. 在美國及其他國家/地區的註冊商標。

Google Play 是 Google LLC 的商標。

此為機密電腦軟體。持有、使用或複製均需要 HP 的有效授權。與 FAR 12.211 和 FAR 12.212 相同，「商業電腦軟體」、「電腦軟體文件」和「商業項目技術資料」皆依據廠商的標準商用授權規定授權予美國政府。

本文件包含的資訊如有變更，恕不另行通知。HP 產品和服務的保固僅列於此類產品和服務隨附的明示保固聲明中。不可將本文件的任何部分解釋為構成額外保固。HP 對本文件中的技術或編輯錯誤或疏失概不負責。

第二版：2021 年 10 月

第一版：2019 年 12 月

文件編號：L83995-AB2

---

# 目錄

<b>1 快速入門</b> .....	<b>1</b>
使用 HP Sure Admin .....	1
停用 HP Sure Admin .....	1
<b>2 建立和管理金鑰</b> .....	<b>2</b>
建立和匯出金鑰 .....	2
透過手動分派的方式建立及匯出金鑰.....	2
透過 Azure AD Revocation 建立和匯出金鑰 .....	2
建立並傳送金鑰至 Azure AD Group OneDrive.....	3
<b>3 手機設定</b> .....	<b>5</b>
使用 HP Sure Admin 手機應用程式解鎖 BIOS .....	5
在註冊後存取 BIOS 設定.....	5
使用 Azure AD Group OneDrive 解鎖 BIOS .....	5
<b>4 HP Sure Admin 錯誤代碼</b> .....	<b>7</b>

# 1 快速入門

HP Sure Admin 讓 IT 管理員得以使用認證和公開金鑰加密技術，安全地管理遠端和本機設定管理上的敏感裝置韌體設定，而無需使用密碼。

HP Sure Admin 由以下項目組成：

- **目標電腦**：要管理的平台，支援「增強型 BIOS 驗證模式」。
- **HP Manageability Integration Kit (MIK)**：System Center Configuration Manager (SCCM) 或 HP BIOS Configuration Utility (BCU) 的外掛程式，用於遠端管理 BIOS 設定。
- **HP Sure Admin Local Access Authenticator**：一個可取代密碼的手機應用程式，能透過掃描 QR 碼取得一次性 PIN 碼，以允許本機存取 BIOS 設定。

## 使用 HP Sure Admin

本節說明使用 HP Sure Admin 的程序。


1. 開啟 System Configuration Manager (SCCM) 或增強型 BIOS Configuration Utility (BCU) 的 HP Manageability Integration Kit (MIK) 外掛程式內的 HP Sure Admin 外掛程式。
2. 從 Google Play™ 商店或 Apple App Store® 下載 HP Sure Admin 手機應用程式。
3. 建立目標裝置和 HP Sure Admin 手機應用程式使用的金鑰來取得一次性 PIN 碼，以解鎖 BIOS。

## 停用 HP Sure Admin

本節說明停用 HP Sure Admin 的選項。

- 在 BIOS F10 設定中，選擇**將安全性設定還原至原廠預設值**。

---

 **附註：**這需要透過 HP Sure Admin 手機應用程式以實體狀態提供身份驗證 PIN 碼，以存取 F10 設定。

---

- 使用 BCU 指令來遠端呼叫**將安全性設定還原至原廠預設值**的 WMI。

---

 **附註：**若您需要更多資訊，請參見「HP BIOS Configuration Utility (BCU) 使用指南」。

---

- 在 MIK 安全佈建頁面，選擇**取消佈建**。

## 2 建立和管理金鑰

在啟用增強型 BIOS 驗證模式之前，在 MIK 中完成安全性佈建。為了建立和匯出金鑰，必須先啟用增強型 BIOS 驗證模式。啟用 BIOS 驗證模式：

▲ 開啟 HP Sure Admin 外掛程式並選擇**增強型 BIOS 驗證模式**，即可建立並匯出金鑰。

### 建立和匯出金鑰

有 3 種不同的方式可以建立本機存取金鑰對，並允許 HP Sure Admin 手機應用程式存取金鑰。


- [位於第 2 頁的透過手動分派的方式建立及匯出金鑰](#)
- [位於第 2 頁的透過 Azure AD Revocation 建立和匯出金鑰](#)
- [位於第 3 頁的建立並傳送金鑰至 Azure AD Group OneDrive](#)

### 透過手動分派的方式建立及匯出金鑰


使用此選項可以匯出本機存取授權金鑰，然後透過電子郵件或其他方法將其手動分派至 HP Sure Admin 手機應用程式。

 **附註：**此選項不需要 HP Sure Admin 手機應用程式網路存取權限，即可獲得一次性 PIN 碼。

1. 在**金鑰名稱**輸入方塊中為您的金鑰命名。
2. 在**複雜密碼**輸入方塊中輸入複雜密碼。


 **附註：**複雜密碼適用於保護匯出的金鑰，您必須提供以便 HP Sure Admin 手機應用程式能夠匯入該金鑰。

3. 選擇**瀏覽**，然後在系統中選擇您希望匯出的路徑。
4. 選擇**建立金鑰**。當**建立金鑰**按鈕旁出現**金鑰已成功建立**訊息時，即代表您的金鑰已成功建立。
5. 選取**下一步**。概要頁面會顯示您已輸入的 HP Sure Admin 設定。
6. 選擇**儲存原則**。當系統顯示**儲存成功**訊息時，表示原則已成功儲存。
7. 前往您儲存金鑰的資料夾，並透過使用者在該裝置上可用的方式，例如電子郵件，將其分派至 HP Sure Admin 手機應用程式使用者。該使用者也需要複雜密碼，才能匯入金鑰。HP 建議針對金鑰和複雜密碼使用不同的分派機制。


 **附註：**在傳送 QR 碼時，請以原始尺寸傳送。如果圖片尺寸小於 800 × 600，應用程式將無法正確讀取該圖片。

### 透過 Azure AD Revocation 建立和匯出金鑰

使用此選項將本機存取密鑰連接到指定的 Azure Active Directory 群組，並使 HP Sure Admin 手機應用程式要求對 Azure Active Directory 進行使用者身份驗證，並在提供本機存取 PIN 碼之前，確認使用者是指定群組的成員。此方法也需要透過電子郵件或其他方法將本機存取授權密鑰手動分派至手機應用程式。

 **附註：**此選項需要 HP Sure Admin 手機應用程式具有網路存取權限，以便獲得一次性 PIN 碼。

1. 在**金鑰名稱**輸入方塊中為您的金鑰命名。
2. 在**複雜密碼**輸入方塊中輸入複雜密碼。

 **附註：**複雜密碼適用於保護匯出的金鑰，您必須提供以便 HP Sure Admin 手機應用程式能夠匯入該金鑰。

3. 選擇 **Azure AD 登入** 並登入。
4. 從 **Azure AD 群組名稱** 下拉式方塊中選擇您的群組名稱。您必須是群組的成員才能存取該金鑰。
5. 選擇 **瀏覽**，然後在系統中選擇您希望匯出的路徑。
6. 選擇 **建立金鑰**。當 **建立金鑰** 按鈕旁出現 **金鑰已成功建立** 訊息時，即代表您的金鑰已成功建立。
7. 選取 **下一步**。概要頁面會顯示您已輸入的 HP Sure Admin 設定。
8. 選擇 **儲存原則**。當系統顯示 **儲存成功** 訊息時，表示原則已成功儲存。
9. 前往您儲存金鑰的資料夾，並透過使用者在該裝置上可用的方式，例如電子郵件，將其分派至 HP Sure Admin 手機應用程式使用者。該使用者也需要複雜密碼，才能匯入金鑰。HP 建議針對金鑰和複雜密碼使用不同的分派機制。

 **附註：**在傳送 QR 碼時，請以原始尺寸傳送。如果圖片尺寸小於 800 × 600，應用程式將無法正確讀取該圖片。


## 建立並傳送金鑰至 Azure AD Group OneDrive

(建議) 使用此選項以避免將本機存取授權金鑰儲存於手機上。在您選擇此選項時，MIK 會將本機存取授權密鑰儲存至指定的 OneDrive 資料夾中，該資料夾只能由授權群組存取。HP Sure Admin 手機應用程式使用者每次需要取得 PIN 碼時都要經過 Azure AD 驗證。

1. 在**金鑰名稱**輸入方塊中為您的金鑰命名。
2. 在**複雜密碼**輸入方塊中輸入複雜密碼。
3. 選擇 **Azure AD 登入** 並登入。
4. 從 **Azure AD 群組名稱** 下拉式方塊中選擇您的群組名稱。

 **附註：**您必須是群組的成員才能存取該金鑰。

5. 在 **OneDrive** 輸入方塊中，輸入您希望儲存金鑰的 OneDrive 資料夾名稱。
6. 選擇 **瀏覽**，然後在系統中選擇您希望匯出的路徑。
7. 選擇 **建立金鑰**。

 **附註：**當 **建立金鑰** 按鈕旁出現 **金鑰已成功建立** 訊息時，代表您的金鑰已成功儲存於指定的 OneDrive 資料夾，並且已匯出至指定的本機資料夾。

8. 選取 **下一步**。概要頁面會顯示您已輸入的 HP Sure Admin 設定。

9. 選擇**儲存原則**。當系統顯示**儲存成功**訊息時，表示原則已成功儲存。



**附註：**在此情況下，使用者不需要傳送任何預佈建設定到 HP Sure Admin 手機應用程式。目標電腦已佈建為向至包含在 QR 碼當中的 OneDrive 位置。如果使用者是授權群組的成員並且已成功授權，HP Sure Admin 手機應用程式會使用此指標來存取 OneDrive 位置。

## 3 手機設定

從 Google Play 或 Apple Store 下載 HP Sure Admin 手機應用程式。


- Android 手機使用者，請從 Google 商店下載 HP Sure Admin 手機應用程式。
- iOS 手機使用者，請從 Apple Store 下載 HP Sure Admin 手機應用程式。

### 使用 HP Sure Admin 手機應用程式解鎖 BIOS

HP Sure Admin 手機應用程式透過提供一次性 PIN 碼 (透過掃描目標電腦顯示的 QR 碼獲得) 來代替 BIOS 密碼，用於本機存取 BIOS 設定。

在金鑰已傳送至手機應用程式使用者的情況下，請使用以下步驟將金鑰保存在手機本機上。以下範例中，我們使用電子郵件將金鑰傳送給 HP Sure Admin 手機應用程式使用者，然後使用者在手機上開啟電子郵件。

1. 開啟包含金鑰的電子郵件。
2. 當系統顯示註冊頁面，請於**輸入複雜密碼**輸入方塊中輸入複雜密碼，然後在**輸入您的電子郵件地址**輸入方塊中輸入您的電子郵件地址，即可解密金鑰並將其加入 HP Sure Admin 應用程式。解鎖 PIN 碼顯示於您的 PIN 碼頁面。

 **附註：**此步驟會將金鑰儲存於行動裝置並完成註冊。在這個階段，您可以使用 HP Sure Admin 手機應用程式存取任何已經透過此金鑰佈建為可存取的裝置。只有在管理員要求提供電子郵件地址時，才需要輸入。

3. 在 BIOS 輸入回應代碼輸入方塊中輸入 PIN 碼。

### 在註冊後存取 BIOS 設定

若您希望在註冊後存取目標裝置上的 BIOS 設定：

1. 在目標裝置開機時進入 BIOS 設定。
2. 在手機應用程式中選擇**掃描 QR 碼**，並且掃描目標裝置上的 QR 碼。
3. 如果系統要求輸入使用者認證資訊，請輸入您的認證資訊。
4. 已解鎖的 PIN 碼會顯示在您的 PIN 碼頁面。
5. 在目標裝置的 BIOS 輸入回應代碼輸入方塊中輸入 PIN 碼。

### 使用 Azure AD Group OneDrive 解鎖 BIOS

若您要在 Azure AD Group OneDrive 中使用 HP Sure Admin 解鎖 BIOS：

1. 選擇**掃描 QR 碼**然後掃描 BIOS QR 碼。


 **附註：**HP Sure Admin 應用程式顯示 Azure AD 登入頁面。

2. 登入您的 Azure 帳戶。



3. 在 BIOS 輸入回應代碼輸入方塊中輸入 PIN 碼。

---

 **附註：** HP Sure Admin 在此情況下不會將金鑰儲存於本機。每次需要一次性 PIN 碼時，HP Sure Admin 手機應用程式都必須具備網路存取權限並且使用者必須進行驗證。

---

## 4 HP Sure Admin 錯誤代碼

使用本節中的表格來查看 HP Sure Admin 與 KMS Admin Console 錯誤代碼、類型及其說明。

**表格 4-1** HP Sure Admin 應用程式錯誤代碼、類型及其說明

錯誤代碼	錯誤類型	說明
100	QRCodeUnknownError	一般錯誤。
101	QRCodeDeserialization	無法讀取 QR 碼 JSON。字串不是有效的 JSON 或資料無效。
102	QRCodeInvalidImage	掃描到的 QR 碼圖像無效。無法讀取 QR 碼圖像檔案。
103	QRCodeNoPayload	掃描到的 QR 碼圖像無效。此圖像檔案沒有 JSON 內容。
104	QRCodeInvalid	無法讀取 QR 碼 JSON。字串不是有效的 JSON 或 QR 圖像中的資料無效。
105	QRCodeInvalidKeyIdHash	QR 碼 JSON 中的公開金鑰雜湊不符合註冊包中的公開金鑰雜湊 (KeyID 資料)。
106	QRCodeTampered	掃描到的 QR 碼圖像遭竄改且無效。
107	QRCodeTamperedOrInvalidPassPhrase	掃描到的 QR 碼圖像遭竄改且無效，或輸入的複雜密碼不正確。

**表格 4-2** OneDrive 中的一次性存取金鑰錯誤、類型及其說明

錯誤代碼	錯誤類型	說明
200	OneTimeKeyError	一般錯誤。
201	OneTimeKeyNoUserGroups	登入使用者不屬於您組織中的任何 AD 群組。
203	OneTimeKeyInvalidUserGroup	登入使用者不屬於被指派此金鑰的 AD 群組。
204	OneTimeKeyQRFileDoesNotExist	一次性金鑰檔案不存在於 AD 群組的 OneDrive 資料夾。
205	OneTimeKeyInvalidQRFile	AD 群組 OneDrive 資料夾中的一次性金鑰檔案無效。
206	OneTimeKeyInvalidQRpayload	一次性金鑰檔案存在，但是無法讀取檔案內容。

**表格 4-3** Azure AD 授權錯誤

錯誤代碼	錯誤類型	說明
300	AzureADUnknownError	一般錯誤。

**表格 4-3 Azure AD 授權錯誤 (續)**

錯誤代碼	錯誤類型	說明
301	AzureADInvalidDomain	輸入的電子郵件地址不符合在 QR 碼圖像中指定的網域名稱。
302	AzureADAccessToken	試圖從 Azure AD 取得存取權杖時發生錯誤。使用者可能無法登入您組織的 Azure AD，或者該應用程式沒有連接到您組織的 Azure AD 所需的權限。也可能是使用者取消了驗證。
303	AzureADUserProfile	HP Sure Admin 應用程式無法從您組織的 Azure AD 中取得使用者檔案資訊。
304	AzureADUserPrincipalMismatch	輸入的電子郵件地址不符合登入使用者的主體名稱。
305	AzureADUserInvalidUserGroup	登入使用者不屬於被指派此金鑰的受指派 Azure AD 群組。

**表格 4-4 KMS Admin Console 錯誤、類型及其說明**

錯誤代碼	錯誤類型	說明
401	KmsUnauthorized	使用者未獲授權使用 KMS 服務。
402	KmsKeyDoesNotExist	相符私密金鑰不存在於 KMS 金鑰 Vault 中。金鑰目前處於已刪除但可復原的狀態，且在此狀態下無法重複使用其名稱。只能復原或清除金鑰。
403	KmsKeyDoesNotExistInTableStorage	金鑰不存在於表格儲存中。
404	KmsUploadKeyErrorInKeyVault	將金鑰加入至金鑰 Vault 時發生錯誤。
405	KmsUploadKeyUnauthorized	使用者未獲授權上傳金鑰。使用者不屬於獲准呼叫此 API 的授權 AD 群組。
406	KmsInvalidAzureADLogin	使用者未登入 Azure Tenant AAD。
407	KmsNoUserGroups	登入使用者不屬於您組織中的任何 AD 群組。
408	KmsInvalidUserGroup	登入使用者不屬於被指派此金鑰的 AD 群組。
409	KmsInvalidAccessToken	在要求中提供的存取權杖無效。
410	KmsAccessTokenExpired	提供的 accessToken 已過期。
411	KmsAccessTokenInvalidTenantId	提供的 accessToken 具有無效的 TenantId 值。
412	KmsAccessTokenTenantIdMismatch	所提供 accessToken 中的 TenantId 與功能應用程式 TenantId 不符。
413	KmsInvalidKeyId	keyId 為 null 或空。
414	KmsDeleteKeyUnauthorized	使用者未獲授權刪除金鑰。使用者不屬於獲准呼叫此 API 的授權 AD 群組。
415	KmsKeyVaultSoftDeleteUnrecoverableState	嘗試復原祕密失敗，且其無法復原。使用者應再試一次。
416	KmsInvalidGetKeysRequest	取得金鑰要求無效。

**表格 4-4 KMS Admin Console 錯誤、類型及其說明 (續)**

錯誤代碼	錯誤類型	說明
417	KmsGetKeysUnauthorized	使用者未獲授權取得金鑰。使用者不屬於獲准呼叫此 API 的授權 AD 群組。
418	KmsInvalidRequestPayload	API 接收的要求無效。
419	KmsRequestRequired	接收的要求不得為空。
420	KmsKeyNotConcurrent	自使用者上次擷取副本以來，表格儲存中的金鑰已更新或修改。