



[HP Sure Admin]ユーザー ガイド

概要

[HP Sure Admin]により、IT 管理者はパスワードではなく、リモートおよびローカル双方の設定管理向けの証明書および公開キーの暗号化を使用して、機密性の高いデバイスファームウェアの設定を安全に管理することができます。

法的情報

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

Apple は、米国およびその他の国における Apple Computer, Inc.の商標または登録商標です。

Google Play は、Google LLC の商標または登録商標です。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、HP から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェア資料、および商業用製品の技術データは、ベンダー標準の商業用ライセンスのもとで米国政府に使用許諾が付与されます。

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

改訂第 1 版 : 2021 年 10 月

初版 : 2019 年 12 月

製品番号 : L83995-292

目次

| | |
|------------------------------------------------|---|
| 1 お使いになる前に..... | 1 |
| [HP Sure Admin]の使用..... | 1 |
| [HP Sure Admin]の無効化..... | 1 |
| 2 キーの作成および管理..... | 2 |
| キーの作成およびエクスポート..... | 2 |
| 手動配布でキーを作成およびエクスポートする..... | 2 |
| Azure AD Revocation を使用してキーを作成およびエクスポートする..... | 3 |
| キーを作成して Azure AD Group OneDrive に送信する..... | 3 |
| 3 スマートフォンのセットアップ..... | 5 |
| [HP Sure Admin]アプリを使用した BIOS のロック解除..... | 5 |
| 登録後に BIOS セットアップへのアクセスを取得する..... | 5 |
| Azure AD Group OneDrive で BIOS のロックを解除する..... | 6 |
| 4 [HP Sure Admin]のエラー コード..... | 7 |

1 お使いになる前に

[HP Sure Admin]により、IT 管理者はパスワードではなく、リモートおよびローカル双方の設定管理向けの証明書および公開キーの暗号化を使用して、機密性の高いデバイスファームウェアの設定を安全に管理することができます。

[HP Sure Admin]は、以下の要素で構成されています。

- **対象 PC** : HP の BIOS エンハンスド認証モードをサポートする管理用プラットフォーム。
- **[HP Manageability Integration Kit] (MIK)** : BIOS 設定をリモート管理するための[System Center Configuration Manager] (SCCM) または[HP BIOS Configuration Utility] (BCU) のプラグイン。
- **[HP Sure Admin]の[Local Access Authenticator]** : パスワードの代わりに、QR コードをスキャンしてワンタイム PIN を取得することで、BIOS セットアップへのローカル アクセスを可能にするスマートフォンアプリ。



[HP Sure Admin]の使用

このセクションでは、[HP Sure Admin]を使用するプロセスについて説明します。

1. [System Configuration Manager] (SCCM) または[Enhanced BIOS Configuration Utility] (BCU) 向けの[HP Manageability Integration Kit] (MIK) プラグイン内で、[HP Sure Admin]プラグインを開きます。
2. Google Play™ ストアまたは Apple App Store® から、[HP Sure Admin]アプリをダウンロードします。
3. BIOS をロック解除するためのワンタイム PIN を入手するために、対象デバイスと[HP Sure Admin]スマートフォンアプリによって使用されるキーのペアを作成します。

[HP Sure Admin]の無効化

このセクションでは、[HP Sure Admin]を無効にするオプションについて説明します。

- セットアップユーティリティ (BIOS) の設定で、**[Restore Security settings to Factory Defaults]** (セキュリティ設定を工場出荷時の初期設定に復元) を選択します。
-
-  **注記** : これには、実際にその場で操作することが必要になります。[HP Sure Admin]アプリを使用して認証 PIN を入力し、セットアップユーティリティ (BIOS) の設定にアクセスします。
-
- [BIOS Configuration Utility] (BCU) コマンドを使用して、**[Restore Security settings to Factory Defaults]** (セキュリティ設定を工場出荷時の初期設定に復元) の WMI をリモートで呼び出します。
-
-  **注記** : 詳しくは、[HP BIOS Configuration Utility]のユーザー ガイドを参照してください。
-
- [MIK Security Provisioning] (MIK セキュリティ プロビジョニング) ページで、**[Deprovision]** (プロビジョニング解除) を選択します。

2 キーの作成および管理

BIOS エンハンスド認証モードを有効にする前に、MIK 内でセキュリティ プロビジョニングを完了します。キーを作成およびエクスポートするには、BIOS エンハンスド認証モードを有効にする必要があります。BIOS 認証モードを有効にするには、以下の操作を行います。

- ▲ [HP Sure Admin]プラグインを開き、[Enhanced BIOS Authentication Mode] (BIOS エンハンスド認証モード) を選択して、キーを作成およびエクスポートします。


キーの作成およびエクスポート

ローカル アクセスキーのペアを作成し、キーにアクセスするために[HP Sure Admin]アプリを有効にするには、3 種類の方法があります。


- [2 ページの「手動配布でキーを作成およびエクスポートする」](#)
- [3 ページの「Azure AD Revocation を使用してキーを作成およびエクスポートする」](#)
- [3 ページの「キーを作成して Azure AD Group OneDrive に送信する」](#)

手動配布でキーを作成およびエクスポートする

このオプションを使用し、ローカル アクセス承認キーをエクスポートし、電子メールまたはその他の方法を使用して[HP Sure Admin]アプリに手動でキーを配布します。


 **注記:** このオプションでは、ワンタイム PIN を取得するために[HP Sure Admin]アプリでネットワークにアクセスする必要はありません。

1. **[Key Name]** (キー名) 入力ボックスにキーの名前を入力します。
2. **[Passphrase]** (パスフレーズ) 入力ボックスにパスフレーズを入力します。

 **注記:** パスフレーズは、エクスポートされたキーを保護するために使用されます。[HP Sure Admin]アプリのユーザーがキーをインポートできるようにするには、このパスフレーズを提供する必要があります。


3. **[Browse]** (参照) を選択し、システム内でパスをエクスポートする場所を選択します。
4. **[Create Key]** (キーの作成) を選択します。キーが正常に作成されると、**[Create Key]** (キーの作成) ボタンの横に通知アイコンが表示され、**[Key successfully created]** (キーが正常に作成されました) というメッセージが表示されます。
5. **[Next]** (次へ) を選択します。概要ページに、入力した[HP Sure Admin]の設定が表示されます。
6. **[Save Policy]** (ポリシーの保存) を選択します。ポリシーが保存されると、**[Saved successfully]** (正常に保存されました) というメッセージが表示されます。
7. キーを保存したフォルダーに移動し、電子メールなどのデバイスで利用可能な方法を使用して、[HP Sure Admin]アプリのユーザーにキーを配布します。このユーザーがキーをインポートすると

きにもパスフレーズが必要になります。キーとパスフレーズで異なる配布メカニズムを使用することをお勧めします。


 **注記：** QR コードを送る場合は、元のサイズで送信してください。サイズが 800 × 600 より小さい場合、アプリケーションは画像を正しく読み取ることができません。

Azure AD Revocation を使用してキーを作成およびエクスポートする


このオプションを使用して、ローカルアクセスキーを、指定された Azure Active Directory グループに接続します。さらに、ローカルアクセス PIN を提供する前に、[HP Sure Admin]アプリで、Azure Active Directory へのユーザー認証、およびユーザーが指定されたグループのメンバーであることの確認の両方が必要になります。この方法では、電子メールまたはその他の方法でアプリにローカルアクセス認証キーを手動で配布する処理も必要になります。

 **注記：** このオプションでは、ワンタイム PIN を取得するために[HP Sure Admin]アプリでネットワークにアクセスする必要があります。

1. **[Key Name]** (キー名) 入力ボックスにキーの名前を入力します。
2. **[Passphrase]** (パスフレーズ) 入力ボックスにパスフレーズを入力します。

 **注記：** パスフレーズは、エクスポートされたキーを保護するために使用されます。[HP Sure Admin]アプリのユーザーがキーをインポートできるようにするには、このパスフレーズを提供する必要があります。


3. **[Azure AD Login]** (Azure AD ログイン) を選択してログインします。
4. **[Azure AD Group Name]** (Azure AD グループ名) ドロップダウン ボックスからグループ名を選択します。キーにアクセスするには、このグループのメンバーである必要があります。
5. **[Browse]** (参照) を選択し、システム内でパスをエクスポートする場所を選択します。
6. **[Create Key]** (キーの作成) を選択します。キーが正常に作成されると、**[Create Key]** (キーの作成) ボタンの横に通知アイコンが表示され、**[Key successfully created]** (キーが正常に作成されました) というメッセージが表示されます。
7. **[Next]** (次へ) を選択します。概要ページに、入力した[HP Sure Admin]の設定が表示されます。
8. **[Save Policy]** (ポリシーの保存) を選択します。ポリシーが保存されると、**[Saved successfully]** (正常に保存されました) というメッセージが表示されます。
9. キーを保存したフォルダーに移動し、電子メールなどのデバイスで利用可能な方法を使用して、[HP Sure Admin]アプリのユーザーにキーを配布します。このユーザーがキーをインポートするときにもパスフレーズが必要になります。キーとパスフレーズで異なる配布メカニズムを使用することをお勧めします。

 **注記：** QR コードを送る場合は、元のサイズで送信してください。サイズが 800 × 600 より小さい場合、アプリケーションは画像を正しく読み取ることができません。


キーを作成して Azure AD Group OneDrive に送信する

(推奨) このオプションを使用して、ローカルアクセス認証キーがスマートフォンに保存されないようにします。このオプションを選択すると、認証されたグループのみがアクセスできる、指定された OneDrive フォルダーにローカルアクセス認証キーが MIK によって保存されます。PIN が必要になるたびに、[HP Sure Admin]アプリのユーザーが Azure AD に対して認証される必要があります。


1. **[Key Name]** (キー名) 入力ボックスにキーの名前を入力します。
2. **[Passphrase]** (パスフレーズ) 入力ボックスにパスフレーズを入力します。
3. **[Azure AD Login]** (Azure AD ログイン) を選択してログインします。
4. **[Azure AD Group Name]** (Azure AD グループ名) ドロップダウン ボックスからグループ名を選択します。

 **注記** : キーにアクセスするには、このグループのメンバーである必要があります。

5. **[OneDrive]**入力ボックスに、キーを保存する OneDrive フォルダーの名前を入力します。
6. **[Browse]** (参照) を選択し、システム内でパスをエクスポートする場所を選択します。
7. **[Create Key]** (キーの作成) を選択します。

 **注記** : 指定した OneDrive フォルダーにキーが正常に追加され、指定したローカルフォルダーにエクスポートされると、**[Create Key]** (キーの作成) ボタンの横に通知アイコンが表示され、**[Key successfully created]** (キーが正常に作成されました) というメッセージが表示されます。

8. **[Next]** (次へ) を選択します。概要ページに、入力した[HP Sure Admin]の設定が表示されます。
9. **[Save Policy]** (ポリシーの保存) を選択します。ポリシーが保存されると、**[Saved successfully]** (正常に保存されました) というメッセージが表示されます。

 **注記** : このシナリオでは、事前プロビジョニングのために[HP Sure Admin]アプリに何かを送信する必要はありません。対象 PC は、QR コードに含まれている OneDrive の場所を示すようにプロビジョニングされます。ユーザーが、承認されたグループに属していて認証に成功した場合、[HP Sure Admin]アプリがこのポインターを使用して OneDrive の場所にアクセスします。

3 スマートフォンのセットアップ

Google Play または Apple Store から[HP Sure Admin]アプリをダウンロードします。


- Android スマートフォンの場合は、Google ストアから[HP Sure Admin]をダウンロードします。
- iOS スマートフォンの場合は、Apple ストアから[HP Sure Admin]をダウンロードします。

[HP Sure Admin]アプリを使用した BIOS のロック解除

[HP Sure Admin]モバイルアプリは、BIOS パスワードを使用する代わりに、対象マシンから提供される QR コードをスキャンして取得されるワンタイム PIN を提供することで、BIOS のセットアップにローカルでアクセスできるようにします。

アプリのユーザーにキーが送信されるシナリオで、スマートフォンのローカルにキーを保存するには、以下の操作を行います。以下の例では、このキーが[HP Sure Admin]アプリのユーザーに電子メールで送信され、ユーザーがスマートフォンで電子メールを開きます。

1. キーが記載されている電子メールを開きます。
2. [登録]ページが表示されたら、[パスフレーズを入力してください]ボックスにパスフレーズを入力して、[電子メールアドレスを入力してください]ボックスに電子メールアドレスを入力し、キーを復号して[HP Sure Admin]アプリケーションに追加します。ロック解除 PIN 番号が[お使いの PIN]ページに表示されます。

 **注記：**この手順を実行すると、モバイルデバイスにキーが保存され、登録が完了します。この時点で、[HP Sure Admin]アプリを使用して、このキーでアクセスできるようにプロビジョニングされているすべてのデバイスにアクセスできます。電子メールアドレスは、管理者が要求するように指定している場合にのみ必要です。

3. BIOS の[Enter Response Code] (応答コードの入力) ボックスに PIN を入力します。

登録後に BIOS セットアップへのアクセスを取得する


登録後に対象コンピューターで BIOS セットアップへのアクセスを取得するには、以下の操作を行います。

1. 対象コンピューターの起動時に BIOS セットアップを表示します。
2. アプリで[QR コードのスキャン]を選択して、対象コンピューターで QR コードをスキャンします。
3. ユーザー認証を求められた場合は、認証情報を入力します。
4. ロック解除された PIN 番号が、[お使いの PIN]ページに表示されます。
5. 対象コンピューターで BIOS の[Enter Response Code] (応答コードの入力) 入力ボックスに PIN を入力します。

Azure AD Group OneDrive で BIOS のロックを解除する


[HP Sure Admin]を使用して、Azure AD Group OneDrive で BIOS のロックを解除するには、以下の操作を行います。

1. **[QR コードのスキャン]**を選択して、BIOS QR コードをスキャンします。

 **注記** : [HP Sure Admin]アプリによって、Azure AD ログインページが表示されます。

2. ご自分の Azure アカウントにログインします。

3. BIOS の**[Enter Response Code]** (応答コードの入力) ボックスに PIN を入力します。

 **注記** : このシナリオでは、[HP Sure Admin]アプリによってキーがローカルに保存されることはありません。[HP Sure Admin]アプリがネットワークにアクセスできる必要があり、ユーザーはワンタイム PIN が必要になるたびに認証する必要があります。

4 [HP Sure Admin]のエラーコード

このセクションの表を使用すると、[HP Sure Admin]および KMS 管理コンソールのエラーコード、種類、およびその説明を確認できます。

表 4-1 [HP Sure Admin]アプリのエラーコード、種類、およびその説明

| エラーコード | エラーの種類 | 説明 |
|--------|-----------------------------------|----------------------------------------------------------------|
| 100 | QRCodeUnknownError | 一般的なエラー。 |
| 101 | QRCodeDeserialization | QR コード JSON を読み取れません。文字列が有効な JSON ファイルでないか、データが無効です。 |
| 102 | QRCodeInvalidImage | スキャンされた QR コードイメージが無効です。QR コードイメージファイルを読み取れません。 |
| 103 | QRCodeNoPayload | スキャンされた QR コードイメージが無効です。イメージファイルに JSON ペイロードがありません。 |
| 104 | QRCodeInvalid | QR コード JSON を読み取れません。文字列が有効な JSON でないか、QR イメージのデータが無効です。 |
| 105 | QRCodeInvalidKeyIdHash | QR コード JSON の公開キーのハッシュが、登録パッケージの公開キーのハッシュ (KeyID データ) と一致しません。 |
| 106 | QRCodeTampered | スキャンされた QR コードイメージが改ざんされて無効です。 |
| 107 | QRCodeTamperedOrInvalidPassPhrase | スキャンされた QR コードイメージが改ざんされて無効であるか、入力されたパスワードが正しくありません。 |

表 4-2 OneDrive からワンタイムアクセスキーのエラー、種類、およびその説明

| エラーコード | エラーの種類 | 説明 |
|--------|------------------------------|-----------------------------------------------|
| 200 | OneTimeKeyError | 一般的なエラー。 |
| 201 | OneTimeKeyNoUserGroups | ログインしているユーザーは、組織内のどの AD グループにも属していません。 |
| 203 | OneTimeKeyInvalidUserGroup | ログインしているユーザーは、このキーが割り当てられている AD グループに属していません。 |
| 204 | OneTimeKeyQRFileDoesNotExist | ワンタイムキーファイルが、AD グループの OneDrive フォルダーに存在しません。 |
| 205 | OneTimeKeyInvalidQRFile | AD グループの OneDrive フォルダーにあるワンタイムキーファイルが無効です。 |

表 4-2 OneDrive からのワンタイム アクセスキーのエラー、種類、およびその説明 (続き)

| エラーコード | エラーの種類 | 説明 |
|--------|----------------------------|-----------------------------------------------|
| 206 | OneTimeKeyInvalidQRpayload | ワンタイム キー ファイルは存在しますが、ファイルのペイロードを読み取ることができません。 |

表 4-3 Azure AD の認証エラー

| エラーコード | エラーの種類 | 説明 |
|--------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 300 | AzureADUnknownError | 一般的なエラー。 |
| 301 | AzureADInvalidDomain | 入力された電子メールアドレスが、QR コードイメージで指定されたドメイン名と一致しません。 |
| 302 | AzureADAccessToken | Azure AD からアクセストークンを取得するときにエラーが発生しました。ユーザーが組織の Azure AD にログインすることができないか、またはアプリが、組織の Azure AD に接続するために必要な権限を持っていません。ユーザーが認証をキャンセルした可能性もあります。 |
| 303 | AzureADUserProfile | [HP Sure Admin]アプリによって組織の Azure AD からユーザー プロファイル情報を取得する機能が有効化されました。 |
| 304 | AzureADUserPrincipalMismatch | 入力された電子メールアドレスが、ログインしているユーザーのプリンシパル名と一致しません。 |
| 305 | AzureADUserInvalidUserGroup | ログインしているユーザーは、このキーが割り当てられている Azure AD グループに属していません。 |

表 4-4 KMS 管理コンソールのエラー、種類、およびその説明

| エラーコード | エラーの種類 | 説明 |
|--------|----------------------------------|---------------------------------------------------------------------------------------------------------------|
| 401 | KmsUnauthorized | ユーザーに KMS サービスを使用する権限がありません。 |
| 402 | KmsKeyDoesNotExist | KMS キー ヴォールトに、一致する秘密キーが存在しません。キーは現在削除されており、復元可能な状態ですが、この状態ではこのキー名を再使用することはできません。このキーに対してできる操作は、復元または完全削除のみです。 |
| 403 | KmsKeyDoesNotExistInTableStorage | キーはテーブルストレージに存在しません。 |
| 404 | KmsUploadKeyErrorInKeyVault | キー ヴォールトへのキーの追加中にエラーが発生しました。 |
| 405 | KmsUploadKeyUnauthorized | このユーザーはキーのアップロードを行う権限がありません。ユーザーは、この API の呼び出しが許可されている認証済み AD グループに属していません。 |

表 4-4 KMS 管理コンソールのエラー、種類、およびその説明 (続き)

| エラー コード | エラーの種類 | 説明 |
|---------|-----------------------------------------|-------------------------------------------------------------------------|
| 406 | KmsInvalidAzureADLogin | ユーザーは、Azure テナント AAD にログインしていません。 |
| 407 | KmsNoUserGroups | ログインしているユーザーは、組織内のどの AD グループにも属していません。 |
| 408 | KmsInvalidUserGroup | ログインしているユーザーは、このキーが割り当てられている AD グループに属していません。 |
| 409 | KmsInvalidAccessToken | リクエストで提供されたアクセストークンが無効です。 |
| 410 | KmsAccessTokenExpired | 提供されたアクセストークンの有効期限が切れています。 |
| 411 | KmsAccessTokenInvalidTenantId | 提供されたアクセストークンに無効な TenantId 値があります。 |
| 412 | KmsAccessTokenTenantIdMismatch | 提供されたアクセストークンの TenantId が機能アプリの TenantId と一致しません。 |
| 413 | KmsInvalidKeyId | keyId が NULL または空です。 |
| 414 | KmsDeleteKeyUnauthorized | このユーザーはキーの削除を行う権限がありません。ユーザーは、この API の呼び出しが許可されている認証済み AD グループに属していません。 |
| 415 | KmsKeyVaultSoftDeleteUnrecoverableState | 秘密の復元に失敗したため、復元できませんでした。もう一度試してください。 |
| 416 | KmsInvalidGetKeysRequest | キーの取得リクエストが無効です。 |
| 417 | KmsGetKeysUnauthorized | このユーザーはキーの取得を行う権限がありません。ユーザーは、この API の呼び出しが許可されている認証済み AD グループに属していません。 |
| 418 | KmsInvalidRequestPayload | API で受け取ったリクエストが無効です。 |
| 419 | KmsRequestRequired | 受信したリクエストは空であってはなりません。 |
| 420 | KmsKeyNotConcurrent | テーブルストレージ内のキーは、ユーザーが最後にコピーを取得した後に更新または変更されました。 |