



Manuel de l'utilisateur de HP Sure Admin

RESUME

HP Sure Admin permet aux administrateurs informatiques de gérer de manière sécurisée les paramètres de microprogrammes de périphériques sensibles à l'aide de certificats et de cryptographie à clé publique pour une gestion locale et à distance des paramètres plutôt qu'avec un mot de passe.

Informations légales

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

Apple est une marque de commerce d'Apple Computer, Inc., déposée aux États-Unis et dans d'autres pays.

Google Play est une marque commerciale de Google LLC.

Logiciel informatique confidentiel. Licence HP valide requise pour possession, utilisation ou copie. Conformément aux clauses FAR 12.211 et 12.212, une licence est accordée au Gouvernement des États-Unis sous les termes de la licence commerciale standard du fournisseur pour le Logiciel informatique commercial, la Documentation du logiciel informatique et les Données techniques concernant les éléments commerciaux.

Les informations contenues dans ce document peuvent être modifiées sans préavis. Les garanties relatives aux produits et aux services HP sont décrites dans les textes de garantie limitée expresse qui les accompagnent. Aucun élément du présent document ne peut être interprété comme constituant une garantie supplémentaire. HP ne saurait être tenu pour responsable des erreurs ou omissions de nature technique ou rédactionnelle qui pourraient subsister dans le présent document.

Deuxième édition : octobre 2021

Première édition : décembre 2019

Numéro de référence du document :
L83995-052

Sommaire

| | |
|--|----------|
| 1 Mise en route | 1 |
| Utilisation de HP Sure Admin | 1 |
| Désactivation de HP Sure Admin | 1 |
| 2 Création et gestion des clés | 2 |
| Création et exportation de clés | 2 |
| Créer et exporter une clé avec la distribution manuelle | 2 |
| Création et exportation d'une clé avec Azure AD Revocation | 3 |
| Création et envoi d'une clé sur OneDrive du groupe Azure AD | 3 |
| 3 Configuration du téléphone | 5 |
| Utilisation de l'application mobile HP Sure Admin pour déverrouiller le BIOS | 5 |
| Obtention de l'accès à la configuration BIOS après l'inscription | 5 |
| Déverrouillage du BIOS avec Azure AD Group sur OneDrive | 5 |
| 4 Codes d'erreur de HP Sure Admin | 7 |

1 Mise en route

HP Sure Admin permet aux administrateurs informatiques de gérer de manière sécurisée les paramètres de microprogrammes de périphériques sensibles à l'aide de certificats et de cryptographie à clé publique pour une gestion locale et à distance des paramètres plutôt qu'avec un mot de passe.

HP Sure Admin se compose des éléments suivants :

- **PC cible** : Les plates-formes à gérer qui prennent en charge le mode d'authentification BIOS amélioré.
- **HP Manageability Integration Kit (MIK)** : Le plug-in pour System Center Configuration Manager (SCCM) ou l'utilitaire HP BIOS Configuration Utility (BCU) pour la gestion à distance des paramètres du BIOS.
- **HP Sure Admin Local Access Authenticator** : Une application mobile qui remplace le mot de passe afin d'activer l'accès local à la configuration du BIOS en numérisant un code QR pour obtenir un code PIN à usage unique.

Utilisation de HP Sure Admin

Cette section décrit le processus d'utilisation de HP Sure Admin.

1. Ouvrez le plug-in HP Sure Admin à l'intérieur du plug-in HP Manageability Integration Kit (MIK) pour System Configuration Manager (SCCM) ou l'utilitaire Enhanced BIOS Configuration Utility (BCU).
2. Téléchargez l'application mobile HP Sure Admin à partir de la boutique Google Play™ ou de l'App Store® d'Apple.
3. Créez une paire de clés utilisée par le périphérique cible et l'application mobile HP Sure Admin pour obtenir un code PIN à usage unique pour déverrouiller le BIOS.

Désactivation de HP Sure Admin

Cette section décrit les options permettant de désactiver HP Sure Admin.

- Dans les paramètres F10 BIOS, sélectionnez **Restaurer les paramètres de sécurité aux paramètres d'usine par défaut**.



REMARQUE : Cela nécessite une présence physique en fournissant un code PIN d'authentification via l'application mobile HP Sure Admin pour accéder aux paramètres F10.

- Utilisez la commande BCU pour appeler à distance WMI de **Restaurer les paramètres de sécurité aux paramètres d'usine par défaut**.



REMARQUE : Pour plus d'informations, reportez-vous au manuel de l'utilisateur de l'utilitaire HP BIOS Configuration Utility (BCU).

- Dans la page Configuration de sécurité MIK, sélectionnez **Dé-configurer**.

2 Création et gestion des clés

Achevez la Configuration de sécurité dans MIK avant d'activer le mode d'authentification du BIOS amélioré. Le mode d'authentification du BIOS amélioré doit être activé pour créer et exporter des clés. Pour activer le mode d'authentification du BIOS :

- ▲ Ouvrez le plug-in HP Sure Admin et sélectionnez le **Mode d'authentification du BIOS amélioré** pour créer et exporter des clés.

Création et exportation de clés

Il existe 3 façons différentes de sélectionner pour créer des paires de clés d'accès local et activer l'application mobile HP Sure Admin pour accéder à la clé.

- [Créer et exporter une clé avec la distribution manuelle à la page 2](#)
- [Création et exportation d'une clé avec Azure AD Revocation à la page 3](#)
- [Création et envoi d'une clé sur OneDrive du groupe Azure AD à la page 3](#)

Créer et exporter une clé avec la distribution manuelle

Utilisez cette option pour exporter la clé d'autorisation d'accès local, puis distribuez-la manuellement à l'application mobile HP Sure Admin via e-mail ou une autre méthode.



REMARQUE : Cette option n'exige pas l'accès au réseau de l'application mobile HP Sure Admin pour obtenir un code PIN à usage unique.


1. Nommez votre clé dans la zone de saisie du **Nom de la clé**.
2. Saisissez la phrase passe dans la zone de saisie de la **Phrase passe**.



REMARQUE : La phrase passe est utilisée pour protéger la clé exportée et doit être fournie afin que l'utilisateur de l'application mobile HP Sure Admin puisse importer la clé.


3. Sélectionnez **Parcourir**, puis sélectionnez l'emplacement d'exportation du chemin d'accès dans le système.
4. Sélectionnez **Créer une clé**. Votre clé est créée avec succès lorsqu'une icône de notification s'affiche à côté du bouton **Créer une clé** avec le message **Clé créée avec succès**.
5. Sélectionnez **Suivant**. La page récapitulative affiche les paramètres HP Sure Admin que vous avez saisis.
6. Sélectionnez **Enregistrer la stratégie**. La stratégie s'enregistre lorsque le message **Enregistré avec succès** s'affiche.
7. Accédez au dossier où vous avez enregistré la clé et distribuez-la à l'utilisateur de l'application mobile HP Sure Admin à l'aide d'une méthode disponible pour cet utilisateur sur cet appareil, telle que l'e-mail.

Cet utilisateur aura également besoin de la phrase passe pour importer la clé. HP recommande d'utiliser différents mécanismes de distribution pour la clé et la phrase passe.


 **REMARQUE :** Lors de l'envoi du code QR, envoyez-le dans sa taille d'origine. L'application ne peut pas lire correctement l'image si sa taille est inférieure à 800 × 600.

Création et exportation d'une clé avec Azure AD Revocation


Utilisez cette option pour connecter la clé d'accès local à un groupe Azure Active Directory spécifié et exiger de l'application mobile HP Sure Admin qu'elle exige l'authentification de l'utilisateur sur Azure Active Directory et pour confirmer que l'utilisateur est un membre du groupe spécifié avant de fournir un code PIN d'accès local. Cette méthode nécessite également une distribution manuelle de la clé d'autorisation d'accès local à l'application mobile via e-mail ou une autre méthode.

 **REMARQUE :** Cette option nécessite que l'application mobile HP Sure Admin ait accès au réseau afin d'obtenir un code PIN à usage unique.

1. Nommez votre clé dans la zone de saisie du **Nom de la clé**.
2. Saisissez la phrase passe dans la zone de saisie de la **Phrase passe**.

 **REMARQUE :** La phrase passe est utilisée pour protéger la clé exportée et doit être fournie afin que l'utilisateur de l'application mobile HP Sure Admin puisse importer la clé.

3. Sélectionnez **Azure AD Login** et connectez-vous.
4. Sélectionnez le nom de votre groupe dans la liste déroulante **Nom Groupe Azure AD**. Vous devez être un membre du groupe pour accéder à la clé.
5. Sélectionnez **Parcourir**, puis sélectionnez l'emplacement d'exportation du chemin d'accès dans le système.
6. Sélectionnez **Créer une clé**. Votre clé est créée avec succès lorsqu'une icône de notification s'affiche à côté du bouton **Créer une clé** avec le message **Clé créée avec succès**.
7. Sélectionnez **Suivant**. La page récapitulative affiche les paramètres HP Sure Admin que vous avez saisis.
8. Sélectionnez **Enregistrer la stratégie**. La stratégie s'enregistre lorsque le message **Enregistré avec succès** s'affiche.
9. Accédez au dossier où vous avez enregistré la clé et distribuez-la à l'utilisateur de l'application mobile HP Sure Admin à l'aide d'une méthode disponible pour cet utilisateur sur cet appareil, telle que l'e-mail. Cet utilisateur aura également besoin de la phrase passe pour importer la clé. HP recommande d'utiliser différents mécanismes de distribution pour la clé et la phrase passe.

 **REMARQUE :** Lors de l'envoi du code QR, envoyez-le dans sa taille d'origine. L'application ne peut pas lire correctement l'image si sa taille est inférieure à 800 × 600.

Création et envoi d'une clé sur OneDrive du groupe Azure AD

(Recommandé) Utilisez cette option pour éviter de stocker la clé d'autorisation d'accès local sur le téléphone. Lorsque vous choisissez cette option, MIK stocke la clé d'autorisation d'accès local dans le dossier OneDrive spécifié et qui est uniquement accessible au groupe agréé. L'utilisateur de l'application mobile HP Sure Admin devra s'authentifier sur Azure AD à chaque fois qu'un code PIN est requis.

1. Nommez votre clé dans la zone de saisie du **Nom de la clé**.

2. Saisissez la phrase passe dans la zone de saisie de la **Phrase passe**.
3. Sélectionnez **Azure AD Login** et connectez-vous.
4. Sélectionnez le nom de votre groupe dans la liste déroulante **Nom Azure AD Group**.



REMARQUE : Vous devez être un membre du groupe pour accéder à la clé.

5. Saisissez le nom du dossier OneDrive à l'endroit où vous souhaitez enregistrer la clé dans la zone de saisie **OneDrive**.
6. Sélectionnez **Parcourir**, puis sélectionnez l'emplacement d'exportation du chemin d'accès dans le système.
7. Sélectionnez **Créer une clé**.



REMARQUE : Votre clé a été ajoutée avec succès au dossier OneDrive spécifié et exportée vers le dossier local spécifié lorsqu'une icône de notification s'affiche à côté du bouton **Créer une clé** avec le message **Clé créée avec succès**.

8. Sélectionnez **Suivant**. La page récapitulative affiche les paramètres HP Sure Admin que vous avez saisis.
9. Sélectionnez **Enregistrer la stratégie**. La stratégie s'enregistre lorsque le message **Enregistré avec succès** s'affiche.



REMARQUE : Dans ce scénario, il n'est pas nécessaire d'envoyer quoi que ce soit à l'application mobile HP Sure Admin pour la préconfigurer. Les ordinateurs cibles sont configurés pour pointer vers l'emplacement OneDrive qui est inclus dans le code QR. L'application mobile HP Sure Admin utilise ce pointeur pour accéder à l'emplacement OneDrive si l'utilisateur fait partie du groupe autorisé et s'authentifie correctement.

3 Configuration du téléphone

Téléchargez l'application mobile HP Sure Admin à partir de Google Play ou Apple Store.

- Téléchargez HP Sure Admin à partir de Google Store pour les téléphones Android.
- Téléchargez HP Sure Admin à partir de l'Apple Store pour les téléphones iOS.

Utilisation de l'application mobile HP Sure Admin pour déverrouiller le BIOS

L'application mobile HP Sure Admin remplace l'utilisation du mot de passe BIOS pour l'accès local à la configuration du BIOS en fournissant un code PIN à usage unique obtenu en numérisant le code QR présenté par la machine cible.

Suivez ces étapes pour enregistrer la clé localement sur le téléphone dans un scénario où la clé est envoyée à l'utilisateur de l'application mobile. Dans l'exemple suivant, la clé est envoyée par e-mail à l'utilisateur de l'application mobile HP Sure Admin, et l'utilisateur ouvre l'e-mail sur le téléphone.

1. Ouvrez l'e-mail qui contient la clé.
2. Une fois la page **Inscription** affichée, saisissez la phrase passe dans la zone de saisie **Saisir la phrase passe** et votre adresse e-mail dans la zone de saisie **Saisir votre adresse e-mail** pour décrypter la clé et l'ajouter à l'application HP Sure Admin. Le numéro de code PIN de déverrouillage s'affiche sur la page **Votre code PIN**.



REMARQUE : Cette étape permet d'enregistrer la clé sur l'appareil mobile et d'achever l'inscription. À ce stade, vous pouvez utiliser l'application mobile HP Sure Admin pour accéder à n'importe quel périphérique qui a été configuré pour être accessible via cette clé. Une adresse e-mail est requise uniquement si l'administrateur l'exige.

3. Saisissez le code PIN dans la zone de saisie **Code de réponse d'entrée du BIOS**.

Obtention de l'accès à la configuration BIOS après l'inscription

Pour obtenir l'accès à la configuration du BIOS sur une machine cible après l'inscription :

1. Entrez dans la configuration du BIOS au démarrage sur la machine cible.
2. Sélectionnez **Numériser le code QR** dans l'application mobile et numérisez le code QR sur la machine cible.
3. Si vous êtes invité à une authentification de l'utilisateur, présentez vos informations d'authentification.
4. Le numéro de code PIN de déverrouillage s'affiche sur la page **Votre code PIN**.
5. Entrez le code PIN dans la zone de saisie **Entrer le code de réponse du BIOS** sur la machine cible.

Déverrouillage du BIOS avec Azure AD Group sur OneDrive

Pour utiliser HP Sure Admin pour déverrouiller le BIOS avec Azure AD Group sur OneDrive :

1. Sélectionnez **Numériser le code QR**, puis numérisez le code QR du BIOS.



REMARQUE : L'application HP Sure Admin affiche la page d'ouverture de session Azure AD.

2. Connectez-vous à votre compte Azure.
3. Saisissez le code PIN dans la zone de saisie **Code de réponse d'entrée du BIOS**.



REMARQUE : L'application HP Sure Admin n'enregistre pas la clé localement dans ce scénario. L'application mobile HP Sure Admin doit disposer d'un accès au réseau et l'utilisateur doit s'authentifier à chaque fois qu'un code PIN à usage unique est nécessaire.

4 Codes d'erreur de HP Sure Admin

Utilisez le tableau de cette section pour afficher les codes d'erreur HP Sure Admin et de KMS Admin Console, leurs types et leurs descriptions.

Tableau 4-1 Codes d'erreur de l'application HP Sure Admin, leurs types et descriptions

| Code erreur | Type d'erreur | Description |
|-------------|-----------------------------------|--|
| 100 | QRCodeUnknownError | Erreur générale. |
| 101 | QRCodeDeserialization | Impossible de lire le code QR JSON. La chaîne n'est pas un fichier JSON valide ou les données ne sont pas valides. |
| 102 | QRCodeInvalidImage | L'image de code QR numérisée n'est pas valide. Impossible de lire le fichier image du code QR. |
| 103 | QRCodeNoPayload | L'image de code QR numérisée n'est pas valide. Le fichier image n'est pas doté d'une charge utile JSON. |
| 104 | QRCodeInvalid | Impossible de lire le code QR JSON. Soit la chaîne n'est pas un JSON valide, soit les données de l'image QR ne sont pas valides. |
| 105 | QRCodeInvalidKeyIdHash | Le hachage de la clé publique dans le code QR JSON ne correspond pas au hachage de la clé publique du package d'inscription (données KeyID). |
| 106 | QRCodeTampered | L'image de code QR numérisée est falsifiée et n'est pas valide. |
| 107 | QRCodeTamperedOrInvalidPassPhrase | L'image de code QR numérisée est falsifiée et n'est pas valide, et la phrase passe saisie est incorrecte. |

Tableau 4-2 Touche d'accès OneTime à partir des erreurs OneDrive, leurs types et leurs descriptions

| Code erreur | Type d'erreur | Description |
|-------------|------------------------------|---|
| 200 | OneTimeKeyError | Erreur générale. |
| 201 | OneTimeKeyNoUserGroups | L'utilisateur connecté n'appartient à aucun groupe AD qui se trouve dans votre entreprise. |
| 203 | OneTimeKeyInvalidUserGroup | L'utilisateur connecté n'appartient pas au groupe AD auquel cette clé est assignée. |
| 204 | OneTimeKeyQRFileDoesNotExist | Le fichier de la clé OneTime n'existe pas dans le dossier OneDrive du groupe AD. |
| 205 | OneTimeKeyInvalidQRFile | Le fichier de la clé OneTime dans le dossier OneDrive du groupe AD n'est pas valide. |
| 206 | OneTimeKeyInvalidQRpayload | Le fichier de la clé OneTime est existant mais ne peut pas lire la charge utile du fichier. |

Tableau 4-3 Erreurs d'autorisation Azure AD

| Code erreur | Type d'erreur | Description |
|-------------|------------------------------|--|
| 300 | AzureADUnknownError | Erreur générale. |
| 301 | AzureADInvalidDomain | L'adresse e-mail ne correspond pas au nom de domaine spécifié dans l'image de code QR. |
| 302 | AzureADAccessToken | Erreur lors de l'acquisition d'un jeton d'accès à partir d'Azure AD. L'utilisateur ne peut pas se connecter à l'Azure AD de votre entreprise, ou l'application n'a pas les autorisations nécessaires pour se connecter à l'Azure AD de votre entreprise. Il se peut également que l'utilisateur ait annulé l'authentification. |
| 303 | AzureADUserProfile | L'application HP Sure Admin ne parvient pas à acquérir les informations de profil utilisateur depuis l'Azure AD de votre entreprise. |
| 304 | AzureADUserPrincipalMismatch | L'adresse e-mail ne correspond pas au nom utilisateur principal de l'utilisateur connecté. |
| 305 | AzureADUserInvalidUserGroup | L'utilisateur connecté n'appartient pas au groupe Azure AD auquel cette clé est assignée. |

Tableau 4-4 Codes d'erreur KMS Admin Console, types et leurs descriptions

| Code erreur | Type d'erreur | Description |
|-------------|----------------------------------|--|
| 401 | KmsUnauthorized | L'utilisateur n'est pas autorisé à utiliser le service KMS. |
| 402 | KmsKeyDoesNotExist | Une clé privée correspondante n'existe pas dans le coffre à clé KMS. La clé est actuellement dans un état supprimé mais récupérable, et son nom ne peut pas être réutilisable dans cet état. La clé peut uniquement être récupérée ou vidée. |
| 403 | KmsKeyDoesNotExistInTableStorage | La clé n'existe pas dans le stockage de table. |
| 404 | KmsUploadKeyErrorInKeyVault | Une erreur s'est produite lors de l'ajout d'une clé dans le coffre à clé. |
| 405 | KmsUploadKeyUnauthorized | L'utilisateur n'est pas autorisé à charger des clés. L'utilisateur n'appartient pas au groupe AD autorisé à appeler cette API. |
| 406 | KmsInvalidAzureADLogin | L'utilisateur n'est pas connecté dans Azure Tenant AAD. |
| 407 | KmsNoUserGroups | L'utilisateur connecté n'appartient à aucun groupe AD de votre entreprise. |
| 408 | KmsInvalidUserGroup | L'utilisateur connecté n'appartient pas au groupe AD auquel cette clé est assignée. |
| 409 | KmsInvalidAccessToken | Le jeton d'accès fourni dans la demande n'est pas valide. |

Tableau 4-4 Codes d'erreur KMS Admin Console, types et leurs descriptions (suite)

| Code erreur | Type d'erreur | Description |
|-------------|---|--|
| 410 | KmsAccessTokenExpired | Le jeton d'accès fourni a expiré. |
| 411 | KmsAccessTokenInvalidTenantId | Le jeton d'accès fourni a une valeur d'ID Locataire non valide. |
| 412 | KmsAccessTokenTenantIdMismatch | L'ID Locataire dans le jeton d'accès fourni ne correspond pas à l'ID Locataire de l'application de fonction. |
| 413 | KmsInvalidKeyId | L'ID de clé est nul ou vide. |
| 414 | KmsDeleteKeyUnauthorized | L'utilisateur n'est pas autorisé à supprimer des clés. L'utilisateur n'appartient pas au groupe AD autorisé à appeler cette API. |
| 415 | KmsKeyVaultSoftDeleteUnrecoverableState | La récupération du secret a échoué et il n'a pas pu être récupéré. L'utilisateur devrait réessayer. |
| 416 | KmsInvalidGetKeysRequest | La demande d'obtention de clés n'est pas valide. |
| 417 | KmsGetKeysUnauthorized | L'utilisateur n'est pas autorisé à obtenir des clés. L'utilisateur n'appartient pas au groupe AD autorisé à appeler cette API. |
| 418 | KmsInvalidRequestPayload | La demande reçue par l'API n'est pas valide. |
| 419 | KmsRequestRequired | La demande reçue ne doit pas être vide. |
| 420 | KmsKeyNotConcurrent | La clé dans le stockage de table a été mise à jour ou modifiée depuis la dernière récupération d'une copie par l'utilisateur. |