HP Sure Admin felhasználói útmutató

ÖSSZEGZÉS

A HP Sure Admin lehetővé teszi az informatikai rendszergazdák számára, hogy jelszó helyett tanúsítványok és nyilvános kulcson alapuló titkosítás használatával, biztonságosan kezeljék az eszközök bizalmas firmware-beállításait, akár távoli, akár helyi kezelésről van szó.

Jogi információk

Második kiadás: 2021. október

Első kiadás: 2019. december

Dokumentum cikkszáma: L83995-212

Tartalomjegyzék

1 Első lépések 1
A HP Sure Admin használata 1
A HP Sure Admin letiltása 1
2 Kulcsok létrehozása és kezelése 2
Kulcsok létrehozása és exportálása 2
Kulcs létrehozása és exportálása kézi disztribúcióval 2
Kulcs létrehozása és exportálása az Azure AD visszavonási funkciójával 3
Kulcs létrehozása és elküldése az Azure AD-csoport OneDrive-fiókjába 3
3 Telefon beállítása 5
A HP Sure Admin telefonos alkalmazás használata a BIOS zárolásának feloldásához 5
Hozzáférés a BIOS-beállításokhoz a regisztrációt követően 5
A BIOS zárolásának feloldásához az Azure AD-csoport OneDrive-fiókjával 5
4 HP Sure Admin-hibakódok 7

1 Első lépések

A HP Sure Admin lehetővé teszi az informatikai rendszergazdák számára, hogy jelszó helyett tanúsítványok és nyilvános kulcson alapuló titkosítás használatával, biztonságosan kezeljék az eszközök bizalmas firmware-beállításait, akár távoli, akár helyi kezelésről van szó.

A HP Sure Admin a következő részekből áll:

- **Célszámítógép:** Az Enhanced BIOS Authentication Mode-ot (továbbfejlesztett hitelesítési mód) támogató kezelt platformok.
- **HP Manageability Integration Kit (MIK):** A System Center Configuration Manager (SCCM) vagy a HP BIOS Configuration Utility (BCU) eszközhöz készült beépülő modul a BIOS-beállítások távoli kezeléséhez.
- **HP Sure Admin Local Access Authenticator:** Egy telefonos alkalmazás, amely a BIOS beállításához való helyi hozzáférés engedélyezéséhez jelszó helyett beolvas egy QR-kódot, amellyel le lehet kérni egy egyszeri PIN-kódot.

A HP Sure Admin használata

Ez a szakasz a HP Sure Admin használatának folyamatát írja le.

1. Nyissa meg a HP Sure Admin beépülő modult a System Configuration Manager (SCCM) vagy a továbbfejlesztett BIOS Configuration Utility (BCU) eszközhöz készült HP Manageability Integration Kit (MIK) beépülő modulban.
2. Töltse le a HP Sure Admin telefonos alkalmazást a Google Play™ Áruházból vagy az Apple App Store®-ból.
3. A BIOS zárolásának feloldásához hozzon létre egy, a céleszköz és a HP Sure Admin telefonos alkalmazás által használt kulcspárt az egyszeri PIN-kód lekéréséhez.

A HP Sure Admin letiltása

Ez a szakasz azt ismerteti, hogyan tiltható le a HP Sure Admin alkalmazás.

- A BIOS F10-nél válassza a **Restore Security settings to Factory Defaults** (Biztonsági beállítások visszaállítása a gyári alapértékekre) lehetőséget.

MEGJEGYZÉS: Ez megköveteli a fizikai jelenlétet, mivel a HP Sure Admin telefonos alkalmazáson keresztül hitelesítő PIN-kódot biztosít az F10-beállítások eléréséhez.

- A BCU paranccsal meghívhatja távolról a **Restore Security settings to Factory Defaults** (Biztonsági beállítások visszaállítása a gyári alapértékekre) lehetőség WMI-jét.

MEGJEGYZÉS: További információkért tekintse meg a HP BIOS Configuration Utility (BCU) felhasználói útmutatóját.

- Az MIK Security Provisioning (Biztonság kiépítése) lapján válassza a **Deprovision** (Megszüntetés) lehetőséget.

2 Kulcsok létrehozása és kezelése

Az Enhanced BIOS Authentication Mode engedélyezése előtt végezze el az MIK-ban a biztonság kiépítését. A kulcsok létrehozásához és exportálásához engedélyeznie kell az Enhanced BIOS Authentication Mode-ot. A BIOS Authentication Mode engedélyezéséhez:

▲ Nyissa meg a HP Sure Admin beépülő modult, és válassza az **Továbbfejlesztett BIOS-hitelesítési mód** lehetőséget a kulcsok létrehozásához és exportálásához.

Kulcsok létrehozása és exportálása

3 lehetőség kínálkozik a helyi hozzáférési kulcspárok létrehozásához és annak engedélyezéséhez, hogy a HP Sure Admin telefonos alkalmazás hozzáférhessen a kulcshoz.

- Kulcs létrehozása és exportálása kézi disztribúcióval a következő oldalon: 2
- Kulcs létrehozása és exportálása az Azure AD visszavonási funkciójával a következő oldalon: 3
- Kulcs létrehozása és elküldése az Azure AD-csoport OneDrive-fiókjába a következő oldalon: 3

Kulcs létrehozása és exportálása kézi disztribúcióval

Ezzel a beállítással exportálhatja a helyi hozzáférés-engedélyezési kulcsot, majd manuálisan megoszthatja azt a HP Sure Admin telefonos alkalmazásban e-mailen keresztül vagy valamilyen egyéb módon.

MEGJEGYZÉS: Ehhez a lehetőséghez nincs szükség arra, hogy a HP Sure Admin telefonos alkalmazás rendelkezzen hálózati hozzáféréssel az egyszeri PIN-kód lekéréséhez.

1. Nevezze el a kulcsot a **Kulcs neve** szövegmezőben.
2. Adja meg a jelszót a **Jelszó** szövegmezőben.

   MEGJEGYZÉS: A jelszó az exportált kulcs védelmére szolgál, és meg kell adni ahhoz, hogy a HP Sure Admin telefonos alkalmazás felhasználója importálni tudja a kulcsot.

3. Válassza a **Tallózás** lehetőséget, majd válassza ki, mi legyen az exportálási út a rendszeren belül.
4. Válassza a **Kulcs létrehozása** lehetőséget. Ha a **Kulcs létrehozása** gomb mellett megjelenik **A kulcs létrehozása sikerült** üzenetet tartalmazó értesítési ikon, a kulcs sikeresen létrejött.
5. Válassza a **Tovább** elemet. Az összesítő oldal megjeleníti a HP Sure Admin Ön által megadott beállításait.
6. Válassza a **Szabályzat mentése** lehetőséget. Ha megjelenik a **Sikeresen mentve** üzenet, a szabályzat mentése sikerült.
7. Keresse meg a mappát, ahova elmentette a kulcsot, és ossza meg azt a HP Sure Admin telefonos alkalmazás felhasználójával egy olyan módszerrel, amelyet a felhasználó használni tud az eszközén, például e-mailben. A kulcs importálásához a felhasználónak szüksége lesz a jelszóra is. A HP azt javasolja, hogy a kulcshoz és a jelszóhoz eltérő megosztási mechanizmust használjon.

   MEGJEGYZÉS: A QR-kódot eredeti méretben küldje el. Ha a kép 800 × 600 képpontosnál kisebb, az alkalmazás nem tudja megfelelően beolvasni.

Kulcs létrehozása és exportálása az Azure AD visszavonási funkciójával

Ezzel a beállítással hozzákapcsolhatja a helyi hozzáférési kulcsot egy megadott Azure Active Directory-csoporthoz, és megszabhatja, hogy a HP Sure Admin telefonos alkalmazás megkövetelje a felhasználói hitelesítést az Azure Active Directoryban, valamint annak megerősítését még a helyi hozzáférési PIN-kód megadása előtt, hogy a felhasználó a megadott csoport tagja. Ez a módszer azt is megköveteli, hogy manuálisan megossza a helyi hozzáférés-engedélyezési kulcsot a telefonos alkalmazásban e-mailen keresztül vagy egyéb módon.

MEGJEGYZÉS: A lehetőség használatához szükség van arra, hogy a HP Sure Admin telefonos alkalmazás rendelkezzen hálózati hozzáféréssel az egyszeri PIN-kód lekéréséhez.

1. Nevezze el a kulcsot a **Kulcs neve** szövegmezőben.
2. Adja meg a jelszót a **Jelszó** szövegmezőben.

   MEGJEGYZÉS: A jelszó az exportált kulcs védelmére szolgál, és meg kell adni ahhoz, hogy a HP Sure Admin telefonos alkalmazás felhasználója importálni tudja a kulcsot.

3. Válassza a **Bejelentkezés az Azure AD-be** lehetőséget, és jelentkezzen be.
4. Válassza ki a csoport nevét az **Azure AD-csoport neve** legördülő listából. A kulcs eléréséhez a csoport tagjának kell lennie.
5. Válassza a **Tallózás** lehetőséget, majd válassza ki, mi legyen az exportálási út a rendszeren belül.
6. Válassza a **Kulcs létrehozása** lehetőséget. Ha a **Kulcs létrehozása** gomb mellett megjelenik **A kulcs létrehozása sikerült** üzenetet tartalmazó értesítési ikon, a kulcs sikeresen létrejött.
7. Válassza a **Tovább** elemet. Az összesítő oldal megjeleníti a HP Sure Admin Ön által megadott beállításait.
8. Válassza a **Szabályzat mentése** lehetőséget. Ha megjelenik a **Sikeresen mentve** üzenet, a szabályzat mentése sikerült.
9. Keresse meg a mappát, ahova elmentette a kulcsot, és ossza meg azt a HP Sure Admin telefonos alkalmazás felhasználójával egy olyan módszerrel, amelyet a felhasználó használni tud az eszközén, például e-mailben. A kulcs importálásához a felhasználónak szüksége lesz a jelszóra is. A HP azt javasolja, hogy a kulcshoz és a jelszóhoz eltérő megosztási mechanizmust használjon.

   MEGJEGYZÉS: A QR-kódot eredeti méretben küldje el. Ha a kép 800 × 600 képpontosnál kisebb, az alkalmazás nem tudja megfelelően beolvasni.

Kulcs létrehozása és elküldése az Azure AD-csoport OneDrive-fiókjába

(Ajánlott) Ezzel a lehetőséggel elkerülheti, hogy a helyi hozzáférés-engedélyezési kulcsot a telefonon kelljen tárolnia. Ha ezt a megoldást választja, az MIK a helyi hozzáférési engedélyezési kulcsot a megadott OneDrive-mappában tárolja, amely csak az engedéllyel rendelkező csoport számára érhető el. A HP Sure Admin telefonos alkalmazás felhasználójának hitelesítenie kell magát az Azure AD-ben minden egyes alkalommal, amikor PIN-kódra van szüksége.

1. Nevezze el a kulcsot a **Kulcs neve** szövegmezőben.
2. Adja meg a jelszót a **Jelszó** szövegmezőben.
3. Válassza a **Bejelentkezés az Azure AD-be** lehetőséget, és jelentkezzen be.

4. Válassza ki a csoport nevét az Azure AD-csoport neve legördülő listából.

MEGJEGYZÉS: A kulcs eléréséhez a csoport tagjának kell lennie.

5. A **OneDrive** szövegmezőben adja meg annak a OneDrive-mappának a nevét, ahová a kulcsot menteni szeretné.

6. Válassza a **Tallózás** lehetőséget, majd válassza ki, mi legyen az exportálási út a rendszeren belül.

7. Válassza a **Kulcs létrehozása** lehetőséget.

MEGJEGYZÉS: A kulcs akkor kerül be a megadott OneDrive-mappába és kerül exportálásra a megjelölt helyi mappába, amikor egy értesítési ikon jelenik meg a **Kulcs létrehozása** gomb mellett, **A kulcs létrehozása sikerült** üzenettel.

8. Válassza a **Tovább** elemet. Az összesítő oldal megjeleníti a HP Sure Admin Ön által megadott beállításait.

9. Válassza a **Szabályzat mentése** lehetőséget. Ha megjelenik a **Sikeresen mentve** üzenet, a szabályzat mentése sikerült.

MEGJEGYZÉS: Ezen módszer használatakor nem kell semmit küldenie a HP Sure Admin telefonos alkalmazásnak, hogy azt előzetesen kiépítse. A célszámítógépek úgy vannak kiépítve, hogy a QR-kódban megadott OneDrive-helyre mutassanak. A HP Sure Admin telefonos alkalmazás ezt az iránymutatót használja a OneDrive-hely eléréséhez, ha a felhasználó tagja az engedéllyel rendelkező csoportnak, és sikeresen hitelesíti magát.

3 Telefon beállítása

Töltse le a HP Sure Admin telefonos alkalmazást a Google Play Áruházból vagy az Apple Store-ból.

- Android rendszerű telefonokra töltse le a HP Sure Admin alkalmazást a Google Play Áruházból.
- iOS rendszerű telefonokra töltse le a HP Sure Admin alkalmazást az Apple Store-ból.

A HP Sure Admin telefonos alkalmazás használata a BIOS zárolásának feloldásához

A HP Sure Admin mobilalkalmazás lehetővé teszi, hogy a BIOS-beállításokhoz való helyi hozzáféréskor a BIOS-jelszó helyet egy egyszeri PIN-kódot adjon meg, amelyet a célgép által megjelenített QR-kód beolvasásával kérhet le.

Az alábbi lépésekkel helyileg mentheti a kulcsot a telefonra olyan esetben, amikor a kulcsot elküldik a telefonos alkalmazás felhasználójának. A következő példában a kulcsot e-mailben elküldik a HP Sure Admin telefonos alkalmazás felhasználójának, és a felhasználó megnyitja az e-mailt a telefonon.

1. Nyissa meg a kulcsot tartalmazó e-mailt.
2. Amikor megjelenik a **Regisztráció** oldal, adja meg a jelszót az **Adja meg a jelszót**, illetve az e-mail-címét az **Adja meg az e-mail-címét** szövegmezőben a kulcs titkosításának feloldásához és a HP Sure Admin alkalmazáshoz való hozzáadásához. A feloldási PIN-kód **Az Ön PIN-kódja** oldalon jelenik meg.

   MEGJEGYZÉS: Ez a lépés elmenti a kulcsot a mobileszközre, és befejezi a regisztrációt. Ezután a HP Sure Admin telefonos alkalmazás segítségével elérheti azokat az eszközöket, amelyeket a kulccsal elérhetővé tettek. Az e-mail-címet csak akkor kell megadni, ha a rendszergazda kéri.

3. Adja meg a PIN-kódot a BIOS **Enter Response Code** (Adja meg a válaszkódot) beviteli mezőjében.

Hozzáférés a BIOS-beállításokhoz a regisztrációt követően

BIOS-beállítások elérése a célszámítógépen a regisztrációt követően:

1. Lépjen be a BIOS-beállításokba rendszerindításkor a célszámítógépen.
2. Válassza a **QR-kód beolvasása** lehetőséget a telefonos alkalmazásban, és olvassa be a célszámítógépen megjelenő QR-kódot.
3. Ha a rendszer felhasználói hitelesítést kér, adja meg a hitelesítő adatait.
4. A feloldott zárolású PIN-kód megjelenik **Az Ön PIN-kódja** oldalon.
5. Adja meg a PIN-kódot a **BIOS Enter Response Code** (Adja meg a válaszkódot) szövegmezőjében a célszámítógépen.

A BIOS zárolásának feloldásához az Azure AD-csoport OneDrive-fiókjával

HP Sure Admin használata a BIOS zárolásának feloldásához az Azure AD-csoport OneDrive-fiókjával:

1. Válassza a **QR-kód beolvasása** lehetőséget, majd olvassa be a BIOS QR-kódját.

MEGJEGYZÉS: A HP Sure Admin alkalmazás megjeleníti az Azure AD bejelentkezési lapját.

2. Jelentkezzen be az Azure-fiókjába.
3. Adja meg a PIN-kódot a BIOS **Enter Response Code** (Adja meg a válaszkódot) beviteli mezőjében.

MEGJEGYZÉS: A HP Sure Admin alkalmazás ebben az esetben nem menti el helyileg a kulcsot. A HP Sure Admin telefonos alkalmazásnak hálózati hozzáféréssel kell rendelkeznie, és a felhasználónak mindig hitelesítenie kell magát, amikor egyszeri PIN-kódot kell megadni.

4 HP Sure Admin-hibakódok

Az ebben a szakaszban lévő táblázatban a HP Sure Admin- és KMS Admin Console-hibakódok és -hibatípusok, valamint azok leírása látható.

4-1. táblázat: A HP Sure Admin alkalmazás hibakódjai és hibatípusai, valamint azok leírása

Hibakód	Hibatípus	Leírás
100	QRCodeUnknownError	Általános hiba.
101	QRCodeDeserialization	A QR-kód JSON-adatai nem olvashatók. Vagy a karakterlánc nem egy érvényes JSON-fájl, vagy az adat érvénytelen.
102	QRCodeInvalidImage	A beolvasott QR-kód képe érvénytelen. A QR-kód képfájlja nem olvasható.
103	QRCodeNoPayload	A beolvasott QR-kód képe érvénytelen. A képfájl nem tartalmaz JSON-adattartalmat.
104	QRCodeInvalid	A QR-kód JSON-adatai nem olvashatók. Vagy a karakterlánc nem egy érvényes JSON, vagy a QR-képben lévő adat érvénytelen.
105	QRCodeInvalidKeyIdHash	A QR-kód JSON-adataiban lévő nyilvános kulcs kivonata nem egyezik meg a regisztrációs csomag nyilvánoskulcs-kivonatával (kulcsazonosító adat).
106	QRCodeTampered	A beolvasott QR-kód képe manipulált és érvénytelen.
107	QRCodeTamperedOrInvalidPassPhrase	A beolvasott QR-kód képe manipulált és érvénytelen, vagy a megadott jelszó helytelen.

4-2. táblázat: A OneDrive-on lévő egyszeri kulcsfájllal kapcsolatos hibakódok és -hibatípusok, valamint azok leírása

Hibakód	Hibatípus	Leírás
200	OneTimeKeyError	Általános hiba.
201	OneTimeKeyNoUserGroups	A bejelentkezett felhasználó nem tartozik a szervezet egyik AD-csoportjába sem.
203	OneTimeKeyInvalidUserGroup	A bejelentkezett felhasználó nem tartozik abba az AD-csoportba, amelyikhez ez a kulcs hozzá van rendelve.
204	OneTimeKeyQRFileDoesNotExist	Az egyszeri kulcsfájl nem található meg az AD-csoport OneDrive-mappájában.
205	OneTimeKeyInvalidQRFile	Az AD-csoport OneDrive-mappájában lévő egyszeri kulcsfájl érvénytelen.
206	OneTimeKeyInvalidQRpayload	Az egyszeri kulcsfájl létezik, de a fájl adattartalma nem olvasható be.

4-3. táblázat: Azure AD-hitelesítési hibák

Hibakód	Hibatípus	Leírás
300	AzureADUnknownError	Általános hiba.
301	AzureADInvalidDomain	A megadott e-mail-cím nem egyezik meg a QR-kód képében megadott tartománynévvel.
302	AzureADAccessToken	Hiba történt a token Azure AD-ből történő beszerzése során. A felhasználó nem tud bejelentkezni cég vagy szervezet Azure AD-jébe, vagy az alkalmazás nem rendelkezik a szükséges engedélyekkel ahhoz, hogy csatlakozni tudjon a cég vagy szervezet Azure AD-jéhez. Az is lehet, hogy a felhasználó megszakította a hitelesítést.
303	AzureADUserProfile	A HP Sure Admin alkalmazás engedéllyel rendelkezik ahhoz, hogy beszerezze a felhasználói profilokkal kapcsolatos információkat a szervezet Azure AD-jéből.
304	AzureADUserPrincipalMismatch	A megadott e-mail-cím nem egyezik meg a bejelentkezett felhasználó egyszerű nevével.
305	AzureADUserInvalidUserGroup	A bejelentkezett felhasználó nem tartozik abba az AD-csoportba, amelyikhez ez a kulcs hozzá van rendelve.

4-4. táblázat: A KMS Admin Console hibakódjai és hibatípusai, valamint azok leírása

Hibakód	Hibatípus	Leírás
401	KmsUnauthorized	A felhasználó nem jogosult a KMS szolgáltatás használatára.
402	KmsKeyDoesNotExist	A KMS kulcstartóban nem található megfelelő privát kulcs. A kulcs jelenleg törölt de helyreállítható állapotban van, és a nevét nem lehet újrahasználni ebben az állapotban. A kulcsot csak helyreállítani vagy törölni lehet.
403	KmsKeyDoesNotExistInTableStorage	A kulcs nem létezik a táblatárolóban.
404	KmsUploadKeyErrorInKeyVault	Hiba történt egy kulcsnak a kulcstárolóhoz való hozzáadása közben.
405	KmsUploadKeyUnauthorized	A felhasználó nem jogosult kulcsok feltöltésére. A felhasználó nem tartozik ahhoz az AD-csoporthoz, amelyiknek engedélye van meghívni ezt az API-t.
406	KmsInvalidAzureADLogin	A felhasználó nincs bejelentkezve az Azure Tenant AAD-be.
407	KmsNoUserGroups	A bejelentkezett felhasználó nem tartozik a szervezet egyik AD-csoportjába sem.
408	KmsInvalidUserGroup	A bejelentkezett felhasználó nem tartozik abba az AD-csoportba, amelyikhez ez a kulcs hozzá van rendelve.

4-4. táblázat: A KMS Admin Console hibakódjai és hibatípusai, valamint azok leírása (folytatás)

Hibakód	Hibatípus	Leírás
409	KmsInvalidAccessToken	A kérésben megadott hozzáférési token érvénytelen.
410	KmsAccessTokenExpired	A megadott hozzáférési token lejárt.
411	KmsAccessTokenInvalidTenantId	A megadott hozzáférési token érvénytelen TenantId értéket tartalmaz.
412	KmsAccessTokenTenantIdMismatch	A megadott hozzáférési tokenben lévő TenantId nem egyezik a függvényalkalmazás TenantId-jével.
413	KmsInvalidKeyId	A kulcsazonosító üres vagy null.
414	KmsDeleteKeyUnauthorized	A felhasználó nem jogosult kulcsot törölni. A felhasználó nem tartozik ahhoz az AD-csoporthoz, amelyiknek engedélye van meghívni ezt az API-t.
415	KmsKeyVaultSoftDeleteUnrecoverableState	A titkos kulcs helyreállítására vonatkozó kísérlet sikertelen volt, és azt nem sikerült helyreállítani. A felhasználónak újból kell próbálkoznia.
416	KmsInvalidGetKeysRequest	A Get Keys kérés érvénytelen.
417	KmsGetKeysUnauthorized	A felhasználó nem jogosult kulcsokat beszerezni. A felhasználó nem tartozik ahhoz az AD-csoporthoz, amelyiknek engedélye van meghívni ezt az API-t.
418	KmsInvalidRequestPayload	Az API által fogadott kérés érvénytelen.
419	KmsRequestRequired	A fogadott kérés nem lehet üres.
420	KmsKeyNotConcurrent	A táblatárolóban lévő kulcs frissítve vagy módosítva lett azóta, hogy a felhasználó legutóbb beolvasott egy példányt.