



# Ghidul pentru utilizator HP Sure Admin

## SUMAR

HP Sure Admin le dă administratorilor IT posibilitatea de a gestiona în siguranță setările sensibile ale firmware-ului dispozitivelor, utilizând certificate și criptografia cu cheie publică, atât pentru gestionarea la distanță, cât și locală a setărilor, în loc să folosească o parolă.

## Informații juridice

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

Apple este marcă comercială a Apple Computer, Inc., înregistrată în S.U.A. și în alte țări/regiuni.

Google Play este marcă comercială a Google LLC.

Software confidențial. Pentru posesie, utilizare și copiere este necesară o licență validă din partea HP. În conformitate cu FAR 12.211 și 12.212, software-ul comercial pentru computer, documentația software-ului pentru computer și datele tehnice pentru bunurile comerciale sunt licențiate Guvernului S.U.A. conform cu licența comercială standard a furnizorului.

Informațiile din acest document pot fi modificate fără înștiințare prealabilă. Singurele garanții pentru produsele și serviciile HP sunt cele specificate în declarațiile speciale de garanție care însoțesc respectivele produse și servicii. Nimic din conținutul de față nu trebuie interpretat ca reprezentând o garanție suplimentară. Compania HP nu va fi răspunzătoare pentru erorile tehnice sau editoriale ori pentru omisiunile din documentul de față.

Ediția a doua: Octombrie 2021

Prima ediție: Decembrie 2019

Cod document: L83995-272

---

# Cuprins

<b>1</b>	<b>Noțiuni introductive .....</b>	<b>1</b>
	Utilizarea aplicației HP Sure Admin .....	1
	Dezactivarea aplicației HP Sure Admin .....	1
<b>2</b>	<b>Crearea și gestionarea cheilor .....</b>	<b>2</b>
	Crearea și exportul cheilor .....	2
	Creați și exportați Cheia cu distribuție manuală .....	2
	Crearea și exportarea cheii cu Azure AD Revocation .....	3
	Creați și trimiteți o cheie către Azure AD Group OneDrive .....	3
<b>3</b>	<b>Configurarea telefonului .....</b>	<b>5</b>
	Utilizarea aplicației pentru telefon HP Sure Admin pentru a debloca BIOS-ul .....	5
	Obținerea accesului la configurația BIOS-ului după înscriere .....	5
	Deblocarea BIOS-ului cu Azure AD Group OneDrive .....	5
<b>4</b>	<b>Codurile de eroare HP Sure Admin .....</b>	<b>7</b>

# 1 Noțiuni introductive

HP Sure Admin le dă administratorilor IT posibilitatea de a gestiona în siguranță setările sensibile ale firmware-ului dispozitivelor, utilizând certificate și criptografia cu cheie publică, atât pentru gestionarea la distanță, cât și locală a setărilor, în loc să folosească o parolă.

HP Sure Admin are următoarele componente:

- **PC-ul vizat:** Platformele de gestionat care acceptă Modul îmbunătățit de autentificare pe BIOS.
- **HP Manageability Integration Kit (MIK):** Plug-in pentru System Center Configuration Manager (SCCM) sau HP BIOS Configuration Utility (BCU) pentru gestionarea de la distanță a setărilor pentru BIOS.
- **HP Sure Admin Local Access Authenticator:** Aplicație pentru telefon care înlocuiește parola pentru a permite accesul local la configurarea BIOS-ului prin scanarea unui cod QR cu scopul de a obține un PIN unic.

## Utilizarea aplicației HP Sure Admin


Această secțiune descrie procesul de utilizare a HP Sure Admin.

1. Deschideți plug-in-ul HP Sure Admin în plug-in-ul HP Manageability Integration Kit (MIK) pentru System Configuration Manager (SCCM) sau Enhanced BIOS Configuration Utility (BCU).
2. Descărcați aplicația pentru telefon HP Sure Admin din Magazinul Google Play™ sau din Apple App Store®.
3. Creați o pereche de chei utilizată de dispozitivul vizat și de aplicația pentru telefon HP Sure Admin pentru a obține codul PIN unic ca să deblocați BIOS-ul.

## Dezactivarea aplicației HP Sure Admin

Această secțiune descrie opțiunile pentru a dezactiva HP Sure Admin.

- În setarea F10 pentru BIOS, selectați **Restabiliți setările de securitate la valorile implicite din fabrică**.

 **NOTĂ:** Pentru aceasta este necesară prezența fizică prin introducerea codului PIN de autentificare în aplicația pentru telefon HP Sure Admin ca să accesați setările F10.

- Utilizați comanda BCU pentru a apela de la distanță WMI folosind comanda **Restabiliți setările de securitate la valorile implicite din fabrică**.

 **NOTĂ:** Pentru mai multe informații, consultați Ghidul de utilizare pentru HP BIOS Configuration Utility (BCU).

- În pagina Asigurarea accesului la setările de securitate MIK, selectați **Anulați asigurarea accesului**.

## 2 Crearea și gestionarea cheilor

Finalizați asigurarea accesului la setările de securitate în MIK înainte de a activa Modul îmbunătățit de autentificare pe BIOS. Modul îmbunătățit de autentificare pe BIOS trebuie să fie activat pentru a crea și a exporta chei. Pentru a activa Modul de autentificare pe BIOS:

- ▲ Deschideți plug-in-ul HP Sure Admin și selectați **Mod îmbunătățit de autentificare pe BIOS** pentru a crea și a exporta chei.

### Crearea și exportul cheilor

Există 3 moduri diferite de a crea perechi de chei de acces locale și de a activa aplicația de telefon HP Sure Admin în vederea accesării cheii.

- [Creați și exportați Cheia cu distribuție manuală, la pagina 2](#)
- [Crearea și exportarea cheii cu Azure AD Revocation, la pagina 3](#)
- [Creați și trimiteți o cheie către Azure AD Group OneDrive, la pagina 3](#)

### Creați și exportați Cheia cu distribuție manuală

Utilizați această opțiune pentru a exporta cheia de autorizare pentru acces local, apoi distribuiți-o manual către aplicația pentru telefon HP Sure Admin prin e-mail sau printr-o altă metodă.



**NOTĂ:** Această opțiune nu necesită accesul la rețea al aplicației pentru telefon HP Sure Admin pentru a obține un cod PIN unic.

1. Denumiți cheia în caseta de introducere **Nume cheie**.
2. Introduceți fraza de acces în caseta de introducere **Frază de acces**.



**NOTĂ:** Fraza de acces este utilizată pentru a proteja cheia exportată și trebuie introdusă astfel încât utilizatorul aplicației pentru telefon HP Sure Admin să poată importa cheia.

3. Selectați **Răsfoire** și alegeți locația în care să exportați cheia pe sistem.
4. Selectați **Creare cheie**. Cheia dvs. a fost creată cu succes atunci când o pictogramă de notificare apare lângă butonul **Creare cheie** cu mesajul **Cheia s-a creat cu succes**.
5. Selectați **Următorul**. Pagina cu rezumatul afișează setările pentru HP Sure Admin pe care le-ați introdus.
6. Selectați **Salvați politica**. Politica se salvează când apare mesajul **Salvare reușită**.
7. Navigați la folderul în care ați salvat cheia și distribuiți-l către utilizatorul aplicației pentru telefon HP Sure Admin, utilizând o metodă disponibilă pentru acel utilizator pe dispozitivul respectiv, cum ar fi e-mailul. Utilizatorul va avea nevoie de fraza de acces pentru a importa cheia. HP recomandă să utilizați mecanisme de distribuire diferite pentru cheie și fraza de acces.



**NOTĂ:** Când trimiteți codul QR, folosiți dimensiunea inițială. Aplicația nu poate citi corect imaginea dacă are o dimensiune mai mică de 800 × 600.

## Crearea și exportarea cheii cu Azure AD Revocation

Utilizați această opțiune pentru a conecta cheia pentru acces local la un anumit grup Azure Active Directory și setați aplicația pentru telefon HP Sure Admin să solicite atât autentificarea utilizatorului în Azure Active Directory, cât și confirmarea faptului că utilizatorul este membru al grupului indicat înainte de a introduce un cod PIN pentru acces local. Această metodă necesită, de asemenea, distribuirea manuală a cheii de autorizare pentru acces local către aplicația pentru telefon, prin e-mail sau printr-o altă metodă.



**NOTĂ:** Această opțiune necesită accesul la rețea al aplicației pentru telefon HP Sure Admin pentru a obține un cod PIN unic.

1. Denumiți cheia în caseta de introducere **Nume cheie**.
2. Introduceți fraza de acces în caseta de introducere **Frază de acces**.



**NOTĂ:** Frază de acces este utilizată pentru a proteja cheia exportată și trebuie introdusă astfel încât utilizatorul aplicației pentru telefon HP Sure Admin să poată importa cheia.

3. Selectați **Conectare Azure AD** și conectați-vă.
4. Selectați numele grupului din caseta derulantă **Nume grup Azure AD**. Pentru a avea acces la cheie, trebuie să fiți membru al grupului.
5. Selectați **Răsfoire** și alegeți locația în care să exportați cheia pe sistem.
6. Selectați **Creare cheie**. Cheia a fost creată cu succes dacă apare o pictogramă de notificare lângă butonul **Creare cheie** cu mesajul **Cheia s-a creat cu succes**.
7. Selectați **Următorul**. Pagina cu rezumatul afișează setările pentru HP Sure Admin pe care le-ați introdus.
8. Selectați **Salvați politica**. Politica se salvează când apare mesajul **Salvare reușită**.
9. Navigați la folderul în care ați salvat cheia și distribuiți-l către utilizatorul aplicației pentru telefon HP Sure Admin, utilizând o metodă disponibilă pentru acel utilizator pe dispozitivul respectiv, cum ar fi e-mailul. Utilizatorul va avea nevoie de fraza de acces pentru a importa cheia. HP recomandă să utilizați mecanisme de distribuire diferite pentru cheie și fraza de acces.



**NOTĂ:** Când trimiteți codul QR, folosiți dimensiunea inițială. Aplicația nu poate citi corect imaginea dacă are o dimensiune mai mică de 800 × 600.

## Creai și trimiteți o cheie către Azure AD Group OneDrive

(recomandat) utilizați această opțiune pentru a evita stocarea cheii de autorizare pentru acces local pe telefon. Când alegeți această opțiune, MIK va stoca cheia de autorizare pentru acces local în folderul OneDrive specificat, care este accesibil numai grupului autorizat. Va trebui ca utilizatorul aplicației pentru telefon HP Sure Admin să se autentifice în Azure AD de fiecare dată când este necesar un cod PIN.

1. Denumiți cheia în caseta de introducere **Nume cheie**.
2. Introduceți fraza de acces în caseta de introducere **Frază de acces**.
3. Selectați **Conectare Azure AD** și conectați-vă.
4. Selectați numele grupului din caseta derulantă **Nume grup Azure AD**.



**NOTĂ:** Pentru a avea acces la cheie, trebuie să fiți membru al grupului.

5. Introduceți numele folderului OneDrive în care doriți să fie salvată cheia în caseta **OneDrive**.

6. Selectați **Răsfoire** și alegeți locația în care să exportați cheia pe sistem.
7. Selectați **Creare cheie**.



---

**NOTĂ:** Cheia a fost adăugată cu succes în folderul OneDrive indicat și exportată în folderul local indicat atunci când apare o pictogramă de notificare lângă butonul **Creare cheie** cu mesajul **Cheia s-a creat cu succes**.

---

8. Selectați **Următorul**. Pagina cu rezumatul afișează setările pentru HP Sure Admin pe care le-ați introdus.
9. Selectați **Salvați politica**. Politica se salvează când apare mesajul **Salvare reușită**.



---

**NOTĂ:** În acest caz, nu este necesar să trimiteți nimic către aplicația pentru telefon HP Sure Admin ca să asigurați accesul acesteia în prealabil. PC-urile vizate sunt selectate pentru a indica locația din OneDrive inclusă în codul QR. Aplicația pentru telefon HP Sure Admin utilizează acest indicator pentru a accesa locația din OneDrive dacă utilizatorul face parte din grupul autorizat și se autentifică cu succes.

---

## 3 Configurarea telefonului

Descărcați aplicația pentru telefon HP Sure Admin din Magazinul Google Play sau din Apple Store.

- Descărcați HP Sure Admin din Google Store pentru telefoanele Android.
- Descărcați HP Sure Admin din Apple Store pentru telefoanele iOS.

### Utilizarea aplicației pentru telefon HP Sure Admin pentru a debloca BIOS-ul

Aplicația mobilă HP Sure Admin înlocuiește utilizarea parolei BIOS-ului pentru accesul local la configurația acestuia cu introducerea unui cod PIN unic, obținut prin scanarea codului QR afișat pe dispozitivul vizat.

Utilizați acești pași pentru a salva cheia local pe telefon într-un scenariu în care cheia este trimisă utilizatorului aplicației pentru telefon. În exemplul următor, cheia este trimisă prin e-mail utilizatorului aplicației pentru telefon HP Sure Admin, iar utilizatorul deschide e-mailul pe telefon.

1. Deschideți e-mailul care conține cheia.
2. Când se afișează pagina **Înscriere**, introduceți fraza de acces în caseta de introducere **Introduceți fraza de acces** și adresa dvs. de e-mail în caseta de introducere **Introduceți adresa de e-mail** ca să decriptați cheia și să o adăugați în aplicația HP Sure Admin. Codul PIN pentru deblocare se afișează pe pagina **Codul dvs. PIN**.



**NOTĂ:** Acest pas salvează cheia pe dispozitivul mobil și finalizează înscrierea. Acum puteți să utilizați aplicația pentru telefon HP Sure Admin pentru a accesa orice dispozitiv la care s-a asigurat accesul prin intermediul acestei chei. Adresa de e-mail este necesară doar dacă administratorul o solicită.

3. Introduceți codul PIN în caseta de introducere **Introduceți codul de răspuns pentru BIOS**.

### Obținerea accesului la configurația BIOS-ului după înscriere

Pentru a obține acces la configurația BIOS-ului pe un dispozitiv vizat după înscriere:

1. Introduceți configurația BIOS-ului la inițializare pe dispozitivul vizat.
2. Selectați **Scanați codul QR** în aplicația pentru telefon și scanați codul QR pe dispozitivul vizat.
3. Dacă se solicită autentificarea utilizatorului, introduceți acreditările.
4. Codul PIN deblocat se afișează pe pagina **Codul dvs. PIN**.
5. Introduceți codul PIN în caseta de introducere **Introduceți codul de răspuns pentru BIOS** de pe dispozitivul vizat.

### Deblocarea BIOS-ului cu Azure AD Group OneDrive

Pentru a utiliza HP Sure Admin ca să deblocați BIOS-ul folosind Azure AD Group OneDrive:



1. Selectați **Scanați codul QR**, apoi scanați codul QR pentru BIOS.



---

**NOTĂ:** Aplicația HP Sure Admin afișează pagina de conectare Azure AD.

---

2. Conectați-vă la contul dvs. Azure.

3. Introduceți PIN-ul în caseta de introducere **Introduceți codul de răspuns pentru BIOS**.



---

**NOTĂ:** Aplicația HP Sure Admin nu salvează cheia la nivel local în acest caz. Aplicația pentru telefon HP Sure Admin trebuie să aibă acces la rețea, iar utilizatorul trebuie să se autentifice de fiecare dată când este necesar un cod PIN unic.

---

## 4 Codurile de eroare HP Sure Admin

Utilizați tabelul din această secțiune pentru a vedea codurile de eroare, tipurile și descrierile acestora pentru HP Sure Admin și KMS Admin Console.

**Tabelul 4-1** Codurile de eroare ale aplicației HP Sure Admin, tipurile și descrierile acestora

Cod de eroare	Tip de eroare	Descriere
100	QRCodeUnknownError	Eroare generală.
101	QRCodeDeserialization	Imposibil de citit codul QR JSON. Fie șirul nu se află într-un fișier JSON valid, fie datele sunt nevalide.
102	QRCodeInvalidImage	Imaginea scanată a codului QR este nevalidă. Imposibil de citit fișierul imagine cu codul QR.
103	QRCodeNoPayload	Imaginea scanată a codului QR este nevalidă. Fișierul imagine nu conține sarcină utilă JSON.
104	QRCodeInvalid	Imposibil de citit codul QR JSON. Fie șirul nu este un JSON valid, fie datele din imaginea QR sunt nevalide.
105	QRCodeInvalidKeyIdHash	Codul hash pentru cheia publică din fișierul JSON cu codul QR nu corespunde codului hash pentru cheia publică din pachetul de înscrisoare (date KeyID).
106	QRCodeTampered	Imaginea scanată a codului QR este falsificată și nevalidă.
107	QRCodeTamperedOrInvalidPassPhrase	Imaginea scanată a codului QR este falsificată și invalidă, sau expresia de acces introdusă este incorectă.

**Tabelul 4-2** Cheia de acces OneTime din erorile OneDrive, tipurile și descrierile acestora

Cod de eroare	Tip de eroare	Descriere
200	OneTimeKeyError	Eroare generală.
201	OneTimeKeyNoUserGroups	Utilizatorul conectat nu aparține niciunui grup AD din organizația dvs.
203	OneTimeKeyInvalidUserGroup	Utilizatorul conectat nu aparține grupului AD căruia i-a fost atribuită această cheie.
204	OneTimeKeyQRFileDoesNotExist	Fișierul cheie OneTime nu există în folderul OneDrive al grupului AD.
205	OneTimeKeyInvalidQRFile	Fișierul cheie OneTime din folderul OneDrive al grupului AD este nevalid.
206	OneTimeKeyInvalidQRpayload	Fișierul cheie OneTime există, dar nu poate citi încărcătura utilă a fișierului.

**Tabelul 4-3** Erori de autorizare Azure AD

Cod de eroare	Tip de eroare	Descriere
300	AzureADUnknownError	Eroare generală.
301	AzureADInvalidDomain	Adresa de e-mail introdusă nu corespunde numelui de domeniu din imaginea cu codul QR.
302	AzureADAccessToken	Eroare la preluarea tokenului de acces din Azure AD. Utilizatorul nu se poate conecta la serviciul Azure AD al organizației sau aplicația nu are permisiunile necesare pentru a se conecta la serviciul Azure AD al organizației. Este posibil, de asemenea, ca utilizatorul să fi anulat autentificarea.
303	AzureADUserProfile	Aplicația HP Sure Admin a fost activată pentru a obține informații despre profilul utilizatorului de la Azure AD al organizației dumneavoastră.
304	AzureADUserPrincipalMismatch	Adresa de e-mail introdusă nu corespunde numelui principal al utilizatorului conectat.
305	AzureADUserInvalidUserGroup	Utilizatorul conectat nu aparține grupului Azure AD căruia i-a fost atribuită această cheie.

**Tabelul 4-4** Erorile Consolei de administrare KMS, tipurile și descrierile acestora

Cod de eroare	Tip de eroare	Descriere
401	KmsUnauthorized	Utilizatorul nu este autorizat să utilizeze serviciul KMS.
402	KmsKeyDoesNotExist	O cheie privată corespunzătoare nu există în seiful de chei KMS. Cheia se află în acest moment într-o stare ștersă, dar recuperabilă, iar numele ei nu poate fi reutilizat în această stare. Cheia poate fi doar recuperată sau ștersă definitiv.
403	KmsKeyDoesNotExistInTableStorage	Cheie nu există în tabelul de stocare.
404	KmsUploadKeyErrorInKeyVault	A apărut o eroare la adăugarea unei chei în seiful de chei.
405	KmsUploadKeyUnauthorized	Utilizatorul nu este autorizat să încarce chei. Utilizatorul nu aparține grupului AD autorizat, cu permisiunea de a apela acest API.
406	KmsInvalidAzureADLogin	Utilizatorul nu este autentificat în Azure Tenant AAD.
407	KmsNoUserGroups	Utilizatorul conectat nu aparține niciunui grup AD din organizația dvs.
408	KmsInvalidUserGroup	Utilizatorul conectat nu aparține grupului AD căruia i-a fost atribuită această cheie.
409	KmsInvalidAccessToken	Token-ul de acces care a fost furnizat în cerere este nevalid.
410	KmsAccessTokenExpired	Tokenul de acces furnizat a expirat.

**Tabelul 4-4** Erorile Consolei de administrare KMS, tipurile și descrierile acestora (Continuare)

Cod de eroare	Tip de eroare	Descriere
411	KmsAccessTokenInvalidTenantId	Tokenul de acces furnizat are o valoare TenantId nevalidă.
412	KmsAccessTokenTenantIdMismatch	TenantId din tokenul de acces furnizat nu se potrivește cu aplicația de funcție TenantId.
413	KmsInvalidKeyId	KeyId-ul este nul sau gol.
414	KmsDeleteKeyUnauthorized	Utilizatorul nu este autorizat să șteargă chei. Utilizatorul nu aparține grupului AD autorizat, cu permisiunea de a apela acest API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Încercarea de a recupera secretul a eșuat și nu a putut fi recuperat. Utilizatorul trebuie să încerce din nou.
416	KmsInvalidGetKeysRequest	Cererea Get Keys este nevalidă.
417	KmsGetKeysUnauthorized	Utilizatorul nu este autorizat să obțină chei. Utilizatorul nu aparține grupului AD autorizat, cu permisiunea de a apela acest API.
418	KmsInvalidRequestPayload	Solicitarea primită de API este nevalidă.
419	KmsRequestRequired	Solicitarea primită nu trebuie să fie goală.
420	KmsKeyNotConcurrent	Cheia de stocare a tabelului a fost actualizată sau modificată de când utilizatorul a preluat ultima dată o copie.