



HP Sure administratora lietotāja rokasgrāmata

KOPSAVILKUMS

HP Sure Admin nodrošina IT administratoriem iespēju droši pārvaldīt sensitīvus ierīces programmaparatūras iestatījumus, paroles vietā izmantojot sertifikātus un publiskā koda kriptogrāfiju gan attāļajai, gan lokālajai iestatījumu pārvaldībai.

Juridiskā informācija

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

Apple ir Apple Computer, Inc. preču zīme, kas reģistrēta ASV un citās valstīs.

Google Play ir Google LLC preču zīme.

Konfidenciāla datorprogrammatūra. Piekļuvei, lietošanai un kopēšanai nepieciešama derīga licence no HP. Saskaņā ar FAR 12.211 un 12.212 komerciālās datorprogrammatūras, datorprogrammatūras dokumentācijas un tehnisko datu komerciāliem objektiem licence ir piešķirta ASV valdībai ar atbilstošu piegādātāju standarta komerciālo licenci.

Šeit iekļautā informācija var tikt mainīta bez iepriekšēja brīdinājuma. Vienīgās HP produktu un pakalpojumu garantijas ir izklāstītas šiem produktiem un pakalpojumiem pievienotajos garantijas paziņojumos. Nekas no šeit minētā nav interpretējams kā papildu garantija. Uzņēmums HP neuzņemas atbildību par šeit atrodamajām tehniskajām un drukas kļūdām vai izlaidumiem.

Otrais izdevums: 2021. gada oktobris

Pirmais izdevums: 2019. gada decembris

Dokumenta daļas numurs: L83995-E12

Saturs

1 Darba sākšana.....	1
HP Sure Admin lietošana	1
HP Sure Admin atspējošana	1
2 Atslēgu izveide un pārvaldība.....	2
Atslēgu izveide un eksportēšana	2
Izveidot un eksportēt atslēgu ar manuālu nosūtīšanu	2
Atslēgas izveidošana un eksportēšana ar Azure AD atsaukšanu	3
Izveidojiet un nosūtiet atslēgu uz Azure AD grupas OneDrive	3
3 Tālrūpa iestatīšana	5
HP Sure Admin tālrūpa lietojumprogrammas izmantošana BIOS atbloķēšanai	5
Piekļuves saņemšana BIOS iestatīšanai pēc reģistrācijas	5
BIOS atbloķēšana, izmantojot Azure AD grupas OneDrive	5
4 HP Sure Admin kļūdu kodi.....	7

1 Darba sākšana

HP Sure Admin nodrošina IT administratoriem iespēju droši pārvaldīt sensitīvus ierīces programmaparatūras iestatījumus, paroles vietā izmantojot sertifikātus un publiskā koda kriptogrāfiju gan attāļajai, gan lokālajai iestatījumu pārvaldībai.

HP Sure Admin veido tālāk norādītie elementi.

- **Mērķa dators:** pārvaldāmās platformas, kas atbalsta Enhanced BIOS Authentication Mode (uzlaboto BIOS autentifikācijas režīmu).
- **HP Manageability Integration Kit (MIK):** spraudnis System Center Configuration Manager (SCCM) vai HP BIOS Configuration Utility (BCU), lai attālināti pārvaldītu BIOS iestatījumus.
- **HP Sure Admin Local Access Authenticator:** tālruņa lietojumprogramma, kas aizstāj paroli, lai iespējotu lokālu piekļuvi BIOS iestatīšanai, skenējot QR kodu, lai iegūtu vienreizēju PIN.

HP Sure Admin lietošana


Šajā sadaļā ir aprakstīts HP Sure Admin lietošanas process.

1. Atveriet HP Sure Admin spraudni HP Manageability Integration Kit (MIK) spraudnī sistēmas konfigurācijas pārvaldniekam (SCCM) vai Enhanced BIOS Configuration Utility (BCU) (uzlabotā BIOS konfigurācijas utilīta).
2. Lejupielādējiet HP Sure Admin tālruņa lietojumprogrammu no Google Play™ veikala vai Apple App Store®.
3. Izveidojiet atslēgu pāri, ko izmanto mērķa ierīce un HP Sure Admin tālruņa lietojumprogramma, lai iegūtu vienreizēju PIN kodu BIOS atbloķēšanai.

HP Sure Admin atspējošana

Šajā sadaļā ir aprakstītas opcijas HP Sure Admin atspējošanai.

- BIOS F10 iestatījumā atlasiet **Restore Security settings to Factory Defaults** (Atjaunot drošības iestatījumus uz rūpnīcas noklusējumiem).

 **PIEZĪME.** Tam nepieciešama fiziska klātbūtne, nodrošinot autentifikācijas PIN kodu ar HP Sure Admin tālruņa lietojumprogrammas starpniecību, lai piekļūtu F10 iestatījumiem.

- Izmantojiet BCU komandu, lai attālināti izsauktu **Restore Security settings to Factory Defaults** (Atjaunot drošības iestatījumus uz rūpnīcas noklusējumiem) WMI.

 **PIEZĪME.** Papildinformāciju skatiet HP BIOS Configuration Utility (BCU) lietotāja rokasgrāmatā.

- MIK drošības nodrošinājuma lapā atlasiet **Nodrošinājuma atcelšana**.

2 Atslēgu izveide un pārvaldība

Pirms Enhanced BIOS Authentication Mode (uzlabotā BIOS autentifikācijas režīma) iespējošanas pabeidziet drošības nodrošināšanu MIK. Lai izveidotu un eksportētu atslēgas, jābūt iespējamam Enhanced BIOS Authentication Mode (uzlabotajam BIOS autentifikācijas režīmam). Lai iespējotu BIOS Authentication Mode (BIOS autentifikācijas režīmu):

- ▲ atveriet HP Sure Admin spraudni un atlasiet **Enhanced BIOS Authentication Mode** (uzlaboto BIOS autentifikācijas režīmu), lai izveidotu un eksportētu atslēgas.


Atslēgu izveide un eksportēšana

Ir 3 veidi, kādos ir iespējams izveidot lokālas piekļuves atslēgu pārus un iespējot HP Sure Admin tālruņa lietojumprogrammu, tādējādi piekļūstot atslēgai.


- [Izveidot un eksportēt atslēgu ar manuālu nosūtīšanu 2. lpp.](#)
- [Atslēgas izveidošana un eksportēšana ar Azure AD atsaukšanu 3. lpp.](#)
- [Izveidojiet un nosūtiet atslēgu uz Azure AD grupas OneDrive 3. lpp.](#)

Izveidot un eksportēt atslēgu ar manuālu nosūtīšanu


Izmantojiet šo opciju, lai eksportētu lokālās piekļuves autorizācijas atslēgu, un pēc tam manuāli nosūtiet to uz HP Sure Admin tālruņa lietojumprogrammu, izmantojot e-pastu vai citu metodi.

 **PIEZĪME.** Šai opcijai nav nepieciešama HP Sure Admin tālruņa lietojumprogrammas tīkla piekļuve, lai iegūtu vienreizēju PIN kodu.

1. Piešķiriet atslēgai nosaukumu ievades lodziņā **Atslēgas nosaukums**.
2. Ievadiet ieejas frāzi ievades lodziņā **Ieejas frāze**.

 **PIEZĪME.** Ieejas frāze tiek izmantota, lai aizsargātu eksportēto atslēgu, un tā ir jānodrošina, lai HP Sure Admin tālruņa lietojumprogrammas lietotājs varētu importēt atslēgu.

3. Atlasiet **Pārlūkot** un izvēlieties ceļa eksportēšanas vietu sistēmā.
4. Atlasiet **Izveidot atslēgu**. Jūsu atslēga ir veiksmīgi izveidota, kad paziņojuma ikona tiek parādīta blakus pogai **Izveidot atslēgu** ar ziņojumu **“Atslēga veiksmīgi izveidota”**.
5. Atlasiet **Tālāk**. Kopsavilkuma lapā ir redzami jūsu ievadītie HP Sure Admin iestatījumi.
6. Atlasiet **Saglabāt politiku**. Politika ir saglabāta, kad parādās ziņojums **Veiksmīgi saglabāts**.
7. Atveriet mapi, kurā saglabājat atslēgu, un nosūtiet to HP Sure Admin tālruņa lietojumprogrammas lietotājam, izmantojot metodi, kas lietotājam ir pieejama konkrētajā ierīcē, piemēram, e-pastā. Šim lietotājam arī būs nepieciešama ieejas frāze, lai importētu atslēgu. HP iesaka izmantot dažādus izplatīšanas mehānismus atslēgai un ieejas frāzei.

 **PIEZĪME.** Sūtot QR kodu, nosūtiet to oriģinālajā izmērā. Lietojumprogramma nevar pareizi nolasīt attēlu, ja tā izmērs ir mazāks par 800 × 600.

Atslēgas izveidošana un eksportēšana ar Azure AD atsaukšanu

Izmantojiet šo opciju, lai pievienotu lokālo piekļuves atslēgu norādītajai Azure Active Directory grupai un liktu HP Sure Admin tālruņa lietojumprogrammai pieprasīt lietotāja autentifikāciju Azure Active Directory un apstiprināt, ka lietotājs ir konkrētās grupas dalībnieks, pirms tiek nodrošināts lokālās piekļuves PIN kods. Šī metode nosaka to, ka lokālās piekļuves autorizācijas atslēga ir manuāli jānosūta uz tālruņa lietojumprogrammu, izmantojot e-pastu vai citu metodi.



PIEZĪME. Šī opcija nosaka to, ka HP Sure Admin tālruņa lietojumprogrammai ir jābūt piekļuvei tīklam, lai iegūtu vienreizēju PIN kodu.

1. Piešķiriet atslēgai nosaukumu ievades lodziņā **Atslēgas nosaukums**.
2. Ievadiet ieejas frāzi ievades lodziņā **leejas frāze**.



PIEZĪME. Ieejas frāze tiek izmantota, lai aizsargātu eksportēto atslēgu, un tā ir jānodrošina, lai HP Sure Admin tālruņa lietojumprogrammas lietotājs varētu importēt atslēgu.

3. Atlasiet **Pieteikšanās Azure AD** un piesakieties.
4. Nolaizamajā lodziņā **Azure AD grupas nosaukums** atlasiet savas grupas nosaukumu. Lai piekļūtu atslēgai, jums ir jābūt grupas dalībniekam.
5. Atlasiet **Pārlūkot** un izvēlieties ceļa eksportēšanas vietu sistēmā.
6. Atlasiet **Izveidot atslēgu**. Jūsu atslēga ir veiksmīgi izveidota, kad paziņojuma ikona tiek parādīta blakus pogai **Izveidot atslēgu** ar ziņojumu **"Atslēga veiksmīgi izveidota"**.
7. Atlasiet **Tālāk**. Kopsavilkuma lapā ir redzami jūsu ievadītie HP Sure Admin iestatījumi.
8. Atlasiet **Saglabāt politiku**. Politika ir saglabāta, kad parādās ziņojums **Veiksmīgi saglabāts**.
9. Atveriet mapi, kurā saglabājat atslēgu, un nosūtiet to HP Sure Admin tālruņa lietojumprogrammas lietotājam, izmantojot metodi, kas lietotājam ir pieejama konkrētajā ierīcē, piemēram, e-pastā. Šim lietotājam arī būs nepieciešama ieejas frāze, lai importētu atslēgu. HP iesaka izmantot dažādus izplatīšanas mehānismus atslēgai un ieejas frāzei.



PIEZĪME. Sūtot QR kodu, nosūtiet to oriģinālajā izmērā. Lietojumprogramma nevar pareizi nolasīt attēlu, ja tā izmērs ir mazāks par 800 × 600.

Izveidojiet un nosūtiet atslēgu uz Azure AD grupas OneDrive

(Ieteicams) izmantojiet šo opciju, lai lokālās piekļuves autorizācijas atslēga netiktu saglabāta tālrunī. Izvēloties šo opciju, MIK saglabā lokālās piekļuves autorizācijas atslēgu norādītajā OneDrive mapē, kas ir pieejama tikai pilnvarotajai grupai. HP Sure Admin tālruņa lietojumprogrammas lietotājam būs jāveic autentifikācija Azure AD katru reizi, kad būs jāievada PIN kods.

1. Piešķiriet atslēgai nosaukumu ievades lodziņā **Atslēgas nosaukums**.
2. Ievadiet ieejas frāzi ievades lodziņā **leejas frāze**.
3. Atlasiet **Pieteikšanās Azure AD** un piesakieties.
4. Nolaizamajā lodziņā **Azure AD grupas nosaukums** atlasiet savas grupas nosaukumu.



PIEZĪME. Lai piekļūtu atslēgai, jums ir jābūt grupas dalībniekam.

5. **OneDrive** ievades lodziņā ievadiet tās OneDrive mapes nosaukumu, kurā vēlaties saglabāt atslēgu.

6. Atlasiet **Pārlūkot** un izvēlieties ceļa eksportēšanas vietu sistēmā.
7. Atlasiet **Izveidot atslēgu**.



PIEZĪME. Jūsu atslēga ir veiksmīgi pievienota norādītajai OneDrive mapei un eksportēta uz norādīto lokālo mapi, kad paziņojuma ikona tiek parādīta blakus pogai **Izveidot atslēgu** ar ziņojumu **Atslēga veiksmīgi izveidota**.

8. Atlasiet **Tālāk**. Kopsavilkuma lapā ir redzami jūsu ievadītie HP Sure Admin iestatījumi.
9. Atlasiet **Saglabāt politiku**. Politika ir saglabāta, kad parādās ziņojums **Veiksmīgi saglabāts**.



PIEZĪME. Šajā gadījumā nekas nav jāsūta uz HP Sure Admin tālruņa lietojumprogrammu, lai to iepriekš nodrošinātu. Mērķa datori tiek nodrošināti, lai norādītu uz OneDrive atrašanās vietu, kas ir iekļauta QR kodā. HP Sure Admin tālruņa lietojumprogramma izmanto šo rādītāju, lai piekļūtu OneDrive atrašanās vietai, ja lietotājs ir pilnvarotās grupas dalībnieks un veic veiksmīgu autentificēšanu.

3 Tālruņa iestatīšana

Lejupielādējiet HP Sure Admin tālruņa lietojumprogrammu no Google Play vai Apple Store.

- Lejupielādējiet Android tālruņiem paredzēto HP Sure Admin no Google Store.
- Lejupielādējiet iOS tālruņiem paredzēto HP Sure Admin.

HP Sure Admin tālruņa lietojumprogrammas izmantošana BIOS atbloķēšanai

HP Sure Admin mobilā lietojumprogramma aizstāj BIOS paroles lietošanu, lai lokāli piekļūtu BIOS iestatīšanai, nodrošinot vienreizēju PIN kodu, kas iegūts, skenējot mērķa ierīces norādīto QR kodu.

Veiciet šīs darbības, lai lokāli saglabātu atslēgu lokāli tālrunī situācijā, kurā atslēga tiek nosūtīta tālruņa lietojumprogrammas lietotājam. Šajā piemērā taustiņš tiek nosūtīts uz HP Sure Admin tālruņa lietojumprogrammas lietotāju un lietotājs tālrunī atver e-pasta ziņojumu.

1. Atveriet e-pasta ziņu, kurā ir ietverta atslēga.
2. Kad tiek parādīta lapa **Reģistrācija**, ievadiet ieejas frāzi ievades lodziņā **ievadiet ieejas frāzi** un ievadiet savu e-pasta adresi ievades lodziņā **ievadiet savu e-pasta adresi**, lai atšifrētu atslēgu un pievienotu to HP Sure Admin lietojumprogrammai. Atbloķēšanas PIN kods tiek parādīts lapā **Jūsu PIN kods**.



PIEZĪME. Veicot šo darbību, atslēga tiek saglabāta mobilajā ierīcē, un tiek pabeigta reģistrācija. Šajā brīdī varat izmantot HP Sure Admin tālruņa lietojumprogrammu, lai piekļūtu jebkurai ierīcei, kurai ir nodrošināta piekļuve, izmantojot šo atslēgu. E-pasta adrese ir nepieciešama tikai tad, ja to pieprasa administrators.

3. Ievadiet PIN kodu BIOS ievades lodziņā **Enter Response Code** (ievadiet atbildes kodu).

Piekļuves saņemšana BIOS iestatīšanai pēc reģistrācijas

Lai pēc reģistrācijas piekļūtu BIOS iestatīšanai mērķa ierīcē, veiciet tālāk norādītās darbības.

1. Atveriet BIOS iestatīšanas sadaļu mērķa ierīcē, kad tā tiek sāknēta.
2. Tālruņa lietojumprogrammā atlasiet **Skenēt QR kodu** un skenējiet QR kodu mērķa ierīcē.
3. Ja tiek prasīta lietotāja autentifikācija, norādiet savus akreditācijas datus.
4. Atbloķētais PIN kods tiek parādīts lapā **Jūsu PIN kods**.
5. Ievadiet PIN kodu ievades lodziņā **BIOS Enter Response Code** (BIOS atbildes koda ievadīšana) mērķa ierīcē.

BIOS atbloķēšana, izmantojot Azure AD grupas OneDrive

Lai izmantotu HP Sure Admin BIOS atbloķēšanai ar Azure AD grupas OneDrive, veiciet tālāk norādītās darbības.

1. Atlasiet **Skenēt QR kodu** un pēc tam skenējiet BIOS QR kodu.



PIEZĪME. HP Sure Admin lietojumprogramma parāda Azure AD pieteikšanās lapu.

2. Piesakieties savā Azure kontā.
3. Ievadiet PIN kodu BIOS ievades lodziņā **Enter Response Code** (ievadiet atbildes kodu).



PIEZĪME. Šajā gadījumā HP Sure Admin lietojumprogramma nesaglabā atslēgu lokāli. HP Sure Admin tālruņa lietojumprogrammai ir jābūt piekļuvei tīklam, un lietotājam katru reizi ir jāveic autentifikācija, kad ir nepieciešams vienreizējs PIN kods.

4 HP Sure Admin kļūdu kodi

Izmantojiet šīs sadaļas tabulu, lai skatītu HP Sure Admin un KMS administratora konsoles kļūdu kodus, veidus un to aprakstus.

4-1. tabula. HP Sure Admin lietojumprogrammas kļūdu kodi, veidi un to apraksti

Kļūdas kods	Kļūdas veids	Apraksts
100	QRCodeUnknownError	Vispārīga kļūda.
101	QRCodeDeserialization	Nevar nolasīt QR kodu JSON formātā. Virkne nav derīgā JSON formātā vai dati nav derīgi.
102	QRCodeInvalidImage	Noskenētais QR koda attēls nav derīgs. Nevar nolasīt QR koda attēla failu.
103	QRCodeNoPayload	Noskenētais QR koda attēls nav derīgs. Attēla failam nav JSON lietderīgās slodzes.
104	QRCodeInvalid	Nevar nolasīt QR kodu JSON formātā. Virkne nav derīgā JSON formātā vai dati QR attēlā nav derīgi.
105	QRCodeInvalidKeyIdHash	Publiskā koda jaucējkode QR kodā JSON formātā neatbilst reģistrācijas pakotnes publiskā koda jaucējkodam (KeyId dati).
106	QRCodeTampered	Noskenētais QR koda attēls ir pārveidots un nav derīgs.
107	QRCodeTamperedOrInvalidPassPhrase	Skenēta QR kod attēls ir ticis pārveidots un nav derīgs, vai ievadītā ieejas frāze ir nepareiza.

4-2. tabula. OneTime piekļuves atslēga no OneDrive kļūdām, veidiem un to aprakstiem

Kļūdas kods	Kļūdas veids	Apraksts
200	OneTimeKeyError	Vispārīga kļūda.
201	OneTimeKeyNoUserGroups	Pieteicies lietotājs nepieder nevienai jūsu organizācijas AD grupai.
203	OneTimeKeyInvalidUserGroup	Pieteicies lietotājs nepieder šai atslēgai piešķirtajai AD grupai.
204	OneTimeKeyQRFileDoesNotExist	OneTime atslēgas fails nepastāv AD grupas OneDrive mapē.
205	OneTimeKeyInvalidQRfails	OneTime atslēgas fails AD grupas OneDrive mapē nav derīgs.
206	OneTimeKeyInvalidQRpayload	OneTime atslēgas fails pastāv, bet nevar nolasīt faila lietderīgo slodzi.

4-3. tabula. Azure AD autorizācijas kļūdas

Kļūdas kods	Kļūdas veids	Apraksts
300	AzureADUnknownError	Vispārīga kļūda.
301	AzureADInvalidDomain	E-pasta adrese neatbilst domēna nosaukumam, kas norādīts QR koda attēlā.
302	AzureADAccessToken	Kļūda, iegūstot piekļuves pilnvaru no Azure AD. Lietotājs nevar pieteikties jūsu organizācijas Azure AD vai lietojumprogrammai nav nepieciešamo atļauju, lai izveidotu savienojumu ar jūsu organizācijas Azure AD. Pastāv iespēja, ka lietotājs ir atcēlis autentifikāciju.
303	AzureADUserProfails	Lietojumprogramma HP Sure Admin nevar iegūt lietotāja profila informāciju no organizācijas Azure AD.
304	AzureADUserPrincipalMismatch	Ievadītā e-pasta adrese neatbilst pieteiktā lietotāja pamatnosaukumam.
305	AzureADUserInvalidUserGroup	Pieteicies lietotājs nepieder šai atslēgai piešķirtajai Azure AD grupai.

4-4. tabula. KMS administratora konsoles kļūdas, veidi un to apraksti

Kļūdas kods	Kļūdas veids	Apraksts
401	KmsUnhorized (Nehorizēts)	Lietotājs nav pilnvarots izmantot KMS pakalpojumu.
402	KmsKeyDoesNotExist	KMS atslēgas glabātavā atbilstoša privātā atslēga nepastāv. Atslēga pašlaik ir dzēstā, bet atjaunojamā stāvoklī, un šajā stāvoklī atslēgu nevar atkārtoti izmantot. Atslēgu iespējams tikai atjaunot vai iztīrīt
403	KmsKeyDoesNotExistInTableStorage	Atslēga tabulas krātuvē nepastāv.
404	KmsUploadKeyErrorInKeyVault	Pievienojot atslēgu atslēgu akreditācijas datu komplektā, radās kļūda.
405	KmsUploadKeyUnauthorized	Lietotājs nav pilnvarots augšupielādēt atslēgas. Lietotājs nepieder pilnvarotai AD grupai, kurai ir atļauts sazināties ar šo API.
406	KmsInvalidAzureADLogin	Lietotājs nav pierakstījies Azure nomnieka AAD.
407	KmsNoUserGroups	Pieteicies lietotājs nepieder nevienai jūsu org. AD grupai.
408	KmsInvalidUserGroup	Pieteicies lietotājs nepieder šai atslēgai piešķirtajai AD grupai. =
409	KmsInvalidAccessToken	Pieprasījumā nodrošinātā piekļuves pilnvara nav derīga.
410 g	KmsAccessTokenExpired	Nodrošinātās piekļuves pilnvaras termiņš ir beidzies.
411	KmsAccessTokenInvalidTenantId	Nodrošinātā piekļuves pilnvarai ir nederīga TenantId parametra vērtība.

4-4. tabula. KMS administratora konsoles kļūdas, veidi un to apraksti (turpinājums)

Kļūdas kods	Kļūdas veids	Apraksts
412	KmsAccessTokenTenantIdMismatch	Nodrošinātajā piekļuves pilnvarā TenantId parametri nesakrīt ar funkcijas lietojumprogrammas TenantId parametriem.
413	KmsInvalidKeyId	KeyId ir nulle vai tukšs.
414	KmsDeleteKeyUnauthorized	Lietotājam nav pilnvaras taustiņu dzēšanai. Lietotājs nepieder pilnvarotai AD grupai, kurai ir atļauts sazināties ar šo API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Mēģinājums atgūt noslēpumu neizdevās, un tas netika atņemts. Lietotājam jāmēģina vēlreiz
416	KmsInvalidGetKeysRequest	Atslēgas saņemšanas pieprasījums nav derīgs.
417	KmsGetKeysUnauthorized	Lietotājs nav pilnvarots iegūt atslēgas. Lietotājs nepieder pilnvarotai AD grupai, kurai ir atļauts sazināties ar šo API.
418	KmsInvalidRequestPayload	API saņemtais pieprasījums nav derīgs.
419	KmsRequestRequired	Saņemtais pieprasījums nedrīkst būt tukšs.
420 W	KmsKeyNotConcurrent	Atslēga tabulas krātuvē tika atjaunināta vai pārveidota, kopš pēdējās reizes, kad lietotājs izguva tās kopiju.