Rakenduse HP Sure Admin kasutusjuhend

KOKKUVÕTE

Rakendus HP Sure Admin võimaldab administraatoritel turvaliselt hallata tundlike seadmete püsivara sätteid, kasutades selleks serte ja avalikku võtmega krüptograafiat, mis on mõeldud sätete kohalikuks ja eemalt haldamiseks ilma paroolita.

Õiguslik teave

Teine väljaanne: oktoober 2021

Esimene väljaanne: detsember 2019

Dokumendi number: L83995-E42

Sisukord

1 Alustamine

HP Sure Admin võimaldab administraatoritel turvaliselt hallata tundlike seadmete püsivara sätteid, kasutades selleks serte ja avalikku võtmega krüptograafiat, mis on mõeldud sätete kohalikuks ja eemalt haldamiseks ilma paroolita.

HP Sure Admin koosneb järgmistest osadest.

- **Sihtarvuti:** platvormid, mis toetavad täiustatud BIOS-i autentimise režiimi.
- **HP Manageability Integration Kit (MIK):** System Center Configuration Manager (SCCM) või HP BIOS Configuration Utility (BCU) lisandmoodul BIOS-i sätete kaughalduseks.
- **Local Access Authenticator** telefoni rakendus, mis asendab parooli, et lubada kohalik juurdepääs BIOS-i häälestusele QR-koodi skannimise ja ühekordse PIN-koodi saamisega.

Rakenduse HP Sure Admin kasutamine

Selles jaotises kirjeldatakse rakenduse HP Sure Admin kasutamist.

1. Avage rakenduse HP Sure Admin plugin süsteemi seadistushalduri (SCCM) HP Manageability Integration Kit (MIK) või BIOS Configuration Utility (BCU).
2. Laadige alla telefonirakendus HP Sure Admin Google Play™ poest või Apple App Store®-ist.
3. BIOS-i lukuvabastuse ühekordse PIN-koodi loomiseks looge sihtarvuti ja telefonirakenduse HP Sure Admin võtmepaar.

Rakenduse HP Sure Admin keelamine

Järgnevalt on esitatud valikud rakenduse HP Sure Admin keelamiseks.

- Valige BIOS-i F10 sätetes **Turbesätete tehaseväärtuste taastamine**.

MÄRKUS. See nõuab füüsilist kohalolekut, pakkudes autentimise PIN-koodi läbi HP Sure Admin telefonirakenduse, et pääseda juurde F10 sätetele.

- Kasutage BCU käsku suvandi **Turbesätete tehaseväärtuste taastamine** WMI kaugvalimiseks.

MÄRKUS. Lisateavet leiate HP BIOS Configuration Utility (BCU) kasutusjuhendist.

- Valige MIK turbe ettevalmistamise lehel **Eemaldamine**.

2 Võtmete loomine ja haldamine

Enne täiustatud BIOS-i autentimise režiimi lubamist viige MIK-is lõpule turbealane ettevalmistus. Võtmete loomiseks ja eksportimiseks peab täiustatud BIOS-i autentimise režiim olema lubatud. BIOS-i autentimise režiimi lubamiseks toimige järgmiselt.

▲ Võtmete loomiseks ja eksportimiseks avage rakenduse HP Sure Admin plugin ja valige **Täiustatud BIOS-i autentimise režiim**.

Võtmete loomine ja eksportimine

On kolm erinevat võimalust selleks, et luua kohalikud pääsuvõtme paarid ja lubada mobiilirakendusel HP Sure Admin võtmele juurde pääseda.

Käsitsi jaotamise teel võtme loomine ja eksportimine

Kasutage seda suvandit, et eksportida kohaliku juurdepääsu lubamise võti ja seejärel edastada see käsitsi e-posti teel või muul viisil rakendusse HP Sure Admin.

MÄRKUS. See valik ei nõua ühekordse PIN-koodi saamiseks rakendusel HP Sure Admin võrgule juurdepääsu.

1. Sisestage võtme nimi väljale **Võtme nimi**.
2. Sisestage parool väljale **Parool**.

   MÄRKUS. Parooli kasutatakse eksporditud võtme kaitsmiseks ja selle abil saab telefonirakenduse HP Sure Admin kasutaja võtit importida.

3. Valige **Sirvi** ja valige süsteemis eksportimistee.
4. Valige **Loo võti**. Teie võti on loodud, kui teavitusikoon kuvatakse nupu **Loo võti** kõrval koos teatega **Võti edukalt loodud**.
5. Valige **Edasi**. Lehel Kokkuvõte kuvatakse teie sisestatud rakenduse HP Sure Admin sätted.
6. Valige **Salvesta poliitika**. Kui ilmub teade **Edukalt salvestatud**, siis on poliitika salvestatud.
7. Navigeerige kaustani, kuhu salvestasite võtme, seejärel levitage seda mobiilirakenduse HP Sure Admin Phone kasutajale meetodi abil, mis on selle kasutaja jaoks seadmes saadaval (nt e-post). Võtme importimiseks vajab kasutaja ka parooli. HP soovitab võtme ja parooli jaoks kasutada erinevaid edastusmehhanisme.

   MÄRKUS. QR-koodi edastamisel saatke see originaalsuuruses. Rakendus ei saa kujutist õigesti lugeda, kui see on väiksem kui 800 × 600.

Võtme loomine ja eksportimine Azure AD tühistamisega

Kasutage seda suvandit, et ühendada kohalik pääsuvõti määratud Azure aktiivse teegi rühmaga ja märkida, et mobiilirakendus HP Sure Admin nõuaks enne kohaliku juurdepääsu PIN-koodi andmist Azure aktiivse teegiga seoses kasutaja autentimist ja kontrolliks kasutaja kuulumist vastavasse rühma. Selle meetodi kasutamiseks on vajalik ka kohaliku juurdepääsu lubamisvõtme käsitsi edastamine telefonirakendusele e-posti teel või muul viisil.

MÄRKUS. See valik nõuab ühekordse PIN-koodi saamiseks rakendusel HP Sure Admin võrgule juurdepääsu.

1. Sisestage võtme nimi väljale **Võtme nimi**.
2. Sisestage parool väljale **Parool**.

   MÄRKUS. Parooli kasutatakse eksporditud võtme kaitsmiseks ja selle abil saab telefonirakenduse HP Sure Admin kasutaja võtit importida.

3. Valige **Azure AD sisselogimine** ja logige sisse.
4. Valige rühma nimi ripploendist **Azure AD rühma nimi**. Võtmele juurdepääsemiseks peate olema rühma liige.
5. Valige **Sirvi** ja valige süsteemis eksportimistee.
6. Valige **Loo võti**. Teie võti on loodud, kui teavitusikoon kuvatakse nupu **Loo võti** kõrval koos teatega **Võti edukalt loodud**.
7. Valige **Edasi**. Lehel Kokkuvõte kuvatakse teie sisestatud rakenduse HP Sure Admin sätted.
8. Valige **Salvesta poliitika**. Kui ilmub teade **Edukalt salvestatud**, siis on poliitika salvestatud.
9. Navigeerige kaustani, kuhu salvestasite võtme, seejärel levitage seda mobiilirakenduse HP Sure Admin Phone kasutajale meetodi abil, mis on selle kasutaja jaoks seadmes saadaval (nt e-post). Võtme importimiseks vajab kasutaja ka parooli. HP soovitab võtme ja parooli jaoks kasutada erinevaid edastusmehhanisme.

   MÄRKUS. QR-koodi edastamisel saatke see originaalsuuruses. Rakendus ei saa kujutist õigesti lugeda, kui see on väiksem kui 800 × 600.

Võtme loomine ja saatmine Azure AD rühma OneDrive'i

(Soovitatav) Kasutage seda suvandit, et vältida telefonis kohaliku juurdepääsu lubamise võtme talletamist. Kui valite selle suvandi, talletab MIK kohaliku juurdepääsu loavõtme OneDrive'i kausta, mis on saadaval ainult volitatud rühmale. Telefonirakenduse HP Sure Admin kasutaja peab end Azure AD jaoks iga kord autentima, kui nõutakse PIN-koodi.

1. Sisestage võtme nimi väljale **Võtme nimi**.
2. Sisestage parool väljale **Parool**.
3. Valige **Azure AD sisselogimine** ja logige sisse.
4. Valige rühma nimi ripploendist Azure AD rühma nimi.

   MÄRKUS. Võtmele juurdepääsemiseks peate olema rühma liige.

5. Võtme salvestamiseks sisestage **OneDrive'i** väljale OneDrive'i kausta nimi.

6. Valige **Sirvi** ja valige süsteemis eksportimistee.

7. Valige **Loo võti**.

MÄRKUS. Kui nupu **Loo võti** kõrval kuvatakse teavitusikoon koos teatega **Võti edukalt loodud**, siis on võti edukalt lisatud vastavasse OneDrive'i kausta ja eksporditud näidatud kohalikku kausta.

8. Valige **Edasi**. Lehel Kokkuvõte kuvatakse teie sisestatud rakenduse HP Sure Admin sätted.

9. Valige **Salvesta poliitika**. Kui ilmub teade **Edukalt salvestatud**, siis on poliitika salvestatud.

MÄRKUS. Selle stsenaariumi puhul pole ettevalmistamiseks midagi tarvis saata telefonirakendusele HP Sure Admin. Sihtarvutid on ette valmistatud nii, et need osutavad QR-koodis olevale OneDrive'i asukohale. Kui kasutaja on volitatud rühma liige ja autentimine on edukas, siis mobiilirakendus HP Sure Admin kasutab seda OneDrive'i asukohale juurdepääsuks.

3 Telefoni seadistamine

Laadige alla telefonirakendus HP Sure Admin Google Play poest või Apple App Store'ist.

- Laadige Android-telefonidele mõeldud HP Sure Admin alla Google'i poest.
- Laadige iOS-telefonidele mõeldud HP Sure Admin alla Apple App Store'ist.

Telefonirakenduse HP Sure Admin kasutamine BIOS-i avamiseks

Mobiilirakendus HP Sure Admin asendab BIOS-i seadistusele kohalikuks juurdepääsuks BIOS-i parooli, andes sihtarvuti QR-koodi skannimisega ühekordse PIN-koodi.

Kasutage neid samme klahvi kohalikult telefoni salvestamiseks juhul, kui võti saadetakse telefonirakendusse. Järgmises näites saadetakse võti telefonirakenduse HP Sure Admin kasutajale ja kasutaja avab telefonis e-kirja.

1. Avage võtit sisaldav e-kiri.
2. Kui kuvatakse lehekülg **Registreerimine**, siis võtme dekrüptimiseks ja selle lisamiseks rakendusse HP Sure Admin sisestage parool väljale **Sisesta parool** ja oma e-posti aadress väljale **Sisesta e-posti aadress**. **PIN-koodi** leheküljel kuvatakse lukuvabastuse PIN-kood.

   MÄRKUS. Selles etapis salvestatakse võti mobiilseadmesse ja viiakse lõpule registreerimine. Nüüd saate kasutada mobiilirakendust HP Sure Admin, et pääseda juurde seadmetele, mis on selle võtme abil ette valmistatud. E-posti aadress on vajalik ainult siis, kui administraator seda nõuab.

3. Sisestage PIN-kood BIOS-is väljale **Vastuse kood**.

Juurdepääsu saamine BIOS-i häälestusprogrammile pärast registreerimist

Sihtmasina BIOS-i häälestusprogrammile juurdepääs pärast registreerimist

1. Sisenege sihtmasina alglaadimisel selle BIOS-i häälestusprogrammi.
2. Valige telefonirakenduses **Skanni QR-kood** ja skannige QR-kood sihtmasinas.
3. Kui palutakse kasutaja autentimist, siis sisestage oma identimisteave.
4. **PIN-koodi** leheküljel kuvatakse lukuvabastuse PIN-kood.
5. Sisestage PIN-kood sihtmasina BIOS-is sisestusväljale **BIOS-i sisestamise vastuse kood**.

BIOS-i vabastamine rakendusega AD Group OneDrive

Rakenduse HP Sure Admin kasutamine BIOS-i lukuvabastuseks Azure AD rühma OneDrive'iga:

1. Valige **Skanni QR-kood** ja skannige seejärel BIOS-i QR-kood.

   MÄRKUS. Rakendus HP Sure Admin kuvab Azure AD sisselogimislehe.

2. Logige sisse oma Azure'i kontole.

3. Sisestage PIN-kood BIOS-is sisestusväljale **BIOS-i sisestuse vastuse kood**.

MÄRKUS. HP Sure Admin ei salvesta selle stsenaariumi korral kohalikku võtit. Mobiilirakendusel HP Sure Admin peab olema võrgule juurdepääs ja kasutaja peab end autentima iga kord, kui on vajalik ühekordne PIN-kood.

4 Rakenduse HP Sure Admin tõrkekoodid

Kasutage selle jaotise tabelit, et näha HP Sure Admini ja KMS-i halduskonsooli tõrkekoode, tüüpe ja nende kirjeldusi.

Tabel 4-1 Rakenduse HP Sure Admin tõrkekoodid, tüübid ja nende kirjeldused

Tõrkekood	Tõrke tüüp	Kirjeldus
100	QRCodeUnknownError	Üldine tõrge.
101	QRCodeDeserialization	Ei saa lugeda QR-koodi JSON. String pole sobiv JSON või andmed on valed.
102	QRCodeInvalidImage	Skannitud QR-koodi pilt on kehtetu. QR-koodi pildifaili ei õnnestu lugeda.
103	QRCodeNoPayload	Skannitud QR-koodi pilt on kehtetu. Pildifailil pole JSONi tööandmeid.
104	QRCodeInvalid	Ei saa lugeda QR-koodi JSONi. String pole sobiv JSON või QR-kujutise andmed on valed.
105	QRCodeInvalidKeyIdHash	QR-koodi JSONi avaliku võtme räsiandmed ei ühti registreeritud paketi avaliku võtme räsiandmetega (võtme tunnuse andmetega).
106	QRCodeTampered	Skannitud QR-koodi pilt on võltsitud ja see on kehtetu.
107	QRCodeTamperedOrInvalidPassPhrase	Skannitud QR-koodi kujutis on võltsitud ja kehtetu või sisestatud parool on vale.

Tabel 4-2 OneTime'i juurdepääsuklahv OneDrive'i tõrgete, tüüpide ja nende kirjelduste hulgast

Tõrkekood	Tõrke tüüp	Kirjeldus
200	OneTimeKeyError	Üldine tõrge.
201	OneTimeKeyNoUserGroups	Sisselogitud kasutaja ei kuulu teie organisatsioonis ühtegi AD rühma.
203	OneTimeKeyInvalidUserGroup	Sisselogitud kasutaja ei kuulu selle võtme jaoks määratud AD rühma.
204	OneTimeKeyQRFileDoesNotExist	Ühekordse võtme faili pole AD rühma OneDrive'i kaustas.
205	OneTimeKeyInvalidQRFile	AD rühma OneDrive'i kaustas olev ühekordse võtme fail ei sobi.
206	OneTimeKeyInvalidQRpayload	OneTime'i võtme fail on olemas, kuid selle tööandmeid ei saa lugeda.

Tabel 4-3 Azure AD autoriseerimise tõrked

Tõrkekood	Tõrke tüüp	Kirjeldus
300	AzureADUnknownError	Üldine tõrge.
301	AzureADInvalidDomain	Sisestatud e-posti aadress ei ühti QR-koodi pildil oleva domeeninimega.
302	AzureADAccessToken	Tõrge Azure AD juurdepääsuloa hankimisel. Kasutaja ei saa oma organisatsiooni Azure AD-sse sisse logida või rakendusel ei ole teie organisatsiooni Azure AD-ga ühenduse loomiseks vajalikke õigusi. Samuti võis kasutaja tühistada autentimise.
303	AzureADUserProfile	Rakendus HP ei saa teie organisatsiooni Azure AD-st hankida kasutajaprofiili teavet.
304	AzureADUserPrincipalMismatch	E-posti aadress ei vasta sisselogitud kasutaja peamisele nimele.
305	AzureADUserInvalidUserGroup	Sisselogitud kasutaja ei kuulu selle võtme jaoks määratud Azure AD rühma.

Tabel 4-4 KMS-i halduskonsooli tõrked, tüübid ja nende kirjeldused

Tõrkekood	Tõrke tüüp	Kirjeldus
401	KmsUnauthorized	Kasutajal pole lubatud KMS-teenust kasutada.
402	KmsKeyDoesNotExist	KMS-võtme kambris pole sobivat privaatvõtit. Võti on praegu kustutatud, kuid taastatavas olekus ja selle nime ei saa selles olekus uuesti kasutada. Klahvi saab ainult taastada või puhastada.
403	KmsKeyDoesNotExistInTableStorage	Klahve pole tabeli salvestusruumis olemas.
404	KmsUploadKeyErrorInKeyVault	Klahvi lisamisel klahvi kambrisse ilmnes tõrge.
405	KmsUploadKeyUnauthorized	Kasutajal pole õigust klahve üles laadida. Kasutaja ei kuulu volitatud AD Groupi, kellele on lubatud sellele API-le helistada.
406	KmsInvalidAzureADLogin	Kasutaja pole Azure'i rentniku AAD-sse logitud.
407	KmsNoUserGroups	Sisselogitud kasutaja ei kuulu teie organisatsioonis ühtegi AD rühma.
408	KmsInvalidUserGroup	Sisselogitud kasutaja ei kuulu selle võtme jaoks määratud AD rühma.
409	KmsInvalidAccessToken	Taotluses esitatud juurdepääsuluba on kehtetu.
410	KmsAccessTokenExpired	Esitatud accessToken on aegunud.
411	KmsAccessTokenInvalidTenantId	Esitatud accessToken'i väärtus on kehtetu.
412	KmsAccessTokenTenantIdMismatch	Esitatud accessToken'il olev TenantId ei ühti funktsiooni app TenantId-ga.
413	KmsInvalidKeyId	KeyId on null või tühi.

Tabel 4-4 KMS-i halduskonsooli tõrked, tüübid ja nende kirjeldused (järg)

Tõrkekood	Tõrke tüüp	Kirjeldus
414	KmsDeleteKeyUnauthorized	Kasutajal pole õigust klahve kustutada. Kasutaja ei kuulu volitatud AD Groupi, kellele on lubatud sellele API-le helistada.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Saladuse taastamise katse nurjus ja seda ei saanud taastada. Kasutaja peaks uuesti proovima.
416	KmsInvalidGetKeysRequest	Klahvide hankimise taotlus on sobimatu.
417	KmsGetKeysUnauthorized	Kasutajal pole õigust klahve saada. Kasutaja ei kuulu volitatud AD Groupi, kellele on lubatud sellele API-le helistada.
418	KmsInvalidRequestPayload	API saadud taotlus ei sobi.
419	KmsRequestRequired	Saadud taotlus ei tohi olla tühi.
420	KmsKeyNotConcurrent	Tabeli talletusruumi võtit värskendati või muudeti pärast seda, kui kasutaja selle koopia viimati tõi.