Uporabniški priročnik za HP Sure Admin

POVZETEK

Funkcija HP Sure Admin skrbnikom informacijske tehnologije omogoča varno upravljanje občutljivih nastavitev vdelane programske opreme naprave z uporabo potrdil in šifriranja z javnim ključem namesto z geslom tako za oddaljeno, kot tudi za lokalno upravljanje nastavitev.

Pravne informacije

Druga izdaja: oktober 2021

Prva izdaja: december 2019

Št. dela dokumenta: L83995-BA2

Kazalo

1 Uvod

Funkcija HP Sure Admin skrbnikom informacijske tehnologije omogoča varno upravljanje občutljivih nastavitev vdelane programske opreme naprave z uporabo potrdil in šifriranja z javnim ključem namesto z geslom tako za oddaljeno, kot tudi za lokalno upravljanje nastavitev.

Funkcijo HP Sure Admin sestavljajo:

- **Ciljni računalnik:** platforme za upravljanje, ki podpirajo izboljšan način preverjanja pristnosti BIOS-a.
- **HP Manageability Integration Kit (MIK):** vtičnik za System Center Configuration Manager (SCCM) ali HP BIOS Configuration Utility (BCU) za oddaljeno upravljanje nastavitev BIOS-a.
- **HP Sure Admin Local Access Authenticator:** aplikacija za telefon, ki nadomešča geslo za omogočenje lokalnega dostopa do namestitvenega programa BIOS s skeniranjem kode QR, da se pridobi enkratna koda PIN.

Uporaba funkcije HP Sure Admin

V tem razdelku je opisan postopek uporabe programa HP Sure Admin.

1. Vtičnik HP Sure Admin odprite znotraj vtičnika HP Manageability Integration Kit (MIK) za System Configuration Manager (SCCM) ali Enhanced BIOS Configuration Utility (BCU).
2. Iz trgovine Google Play™ ali Apple App Store® prenesite aplikacijo za telefon HP Sure Admin.
3. Ustvarite par ključev, ki ga uporabita ciljna naprava in aplikacija za telefon HP Sure Admin za pridobitev enkratne kode PIN za odklepanje BIOS-a.

Onemogočenje funkcije HP Sure Admin

Ta razdelek opisuje možnosti, s katerimi lahko onemogočite funkcijo HP Sure Admin:

- Pod nastavitvijo BIOS F10 izberite **Restore Security settings to Factory Defaults** (Obnovi varnostne nastavitve v privzete tovarniške vrednosti).

OPOMBA: Za dostop do nastavitev F10 je potrebna fizična prisotnost z vpisom kode PIN za preverjanje pristnosti prek aplikacije za telefon HP Sure Admin.

- Z ukazom BCU na daljavo pokličite WMI možnosti **Restore Security settings to Factory Defaults** (Obnovi varnostne nastavitve v privzete tovarniške vrednosti).

OPOMBA: Za dodatne informacije glejte Uporabniški vodnik za HP BIOS Configuration Utility (BCU).

- Na strani »MIK Security Provisioning« (Omogočenje varnosti MIK) izberite **Deprovision** (Onemogoči).

2 Ustvarjanje in upravljanje ključev

Preden omogočite izboljšan način preverjanja pristnosti BIOS-a, dokončajte omogočenje varnosti znotraj kompleta MIK. Če želite ustvariti in izvoziti ključe, mora biti izboljšan način preverjanja pristnosti BIOS-a omogočen. Postopek za omogočenje načina preverjanja pristnosti BIOS-a:

▲ Odprite vtičnik HP Sure Admin in izberite **Izboljšan način preverjanja pristnosti BIOS-a**, da ustvarite in izvozite ključe.

Ustvarjanje in izvažanje ključev

Obstajajo 3 različni načini za ustvarjanje parov ključev za lokalni dostop in omogočanje telefonske aplikacije HP Sure Admin za dostop do ključa.

- Ustvarjanje in izvoz ključa z ročno distribucijo na strani 2
- Ustvarjanje in izvoz ključa z Azure AD Revocation: na strani 3
- Ustvarjanje in pošiljanje ključa v OneDrive skupine Azure AD: na strani 3

Ustvarjanje in izvoz ključa z ročno distribucijo

to možnost uporabite, če želite izvoziti pooblastitveni ključ za lokalni dostop, nato pa ga prek e-pošte ali drugega načina ročno poslati v aplikacijo za telefon HP Sure Admin.

OPOMBA: Ta možnost za pridobitev enkratne kode PIN ne zahteva dostopa aplikacije za telefon HP Sure Admin do omrežja.

1. Poimenujte ključ v vnosnem polju **Ime ključa**.
2. Vnesite geslo v vnosno polje **Geslo**.

   OPOMBA: Geslo se uporablja za zaščito izvoženega ključa in ga je treba vnesti, da lahko uporabnik aplikacije za telefon HP Sure Admin uvozi ključ.

3. Izberite **Prebrskaj** in izberite mesto za izvoz poti v sistemu.
4. Izberite **Ustvari ključ**. Vaš ključ je uspešno ustvarjen, ko se zraven gumba **Ustvari ključ** prikaže obvestilna ikona s sporočilom **Ključ je uspešno ustvarjen**.
5. Izberite **Naprej**. Na strani s povzetkom so prikazane vnesene nastavitve za funkcijo HP Sure Admin.
6. Izberite **Shrani pravilnik**. Pravilnik je shranjen, ko se prikaže sporočilo **Uspešno shranjeno**.
7. Pomaknite se v mapo, v katero ste shranili ključ, in ga z načinom, ki je na voljo za tega uporabnika v tej napravi, na primer prek e-pošte, pošljite uporabniku aplikacije za telefon HP Sure Admin. Ta uporabnik bo potreboval geslo tudi za uvoz ključa. HP priporoča, da za ključ in geslo uporabite različna načina pošiljanja.

   OPOMBA: Ko pošiljate kodo QR, jo pošljite v izvirni velikosti. Aplikacija ne more pravilno prebrati slike, če je velikost manjša od 800 × 600.

Ustvarjanje in izvoz ključa z Azure AD Revocation:

to možnost uporabite za povezavo ključa za lokalni dostop z navedeno skupino Azure Active Directory in zahtevo, da aplikacija za telefon Sure Admin zahteva preverjanje pristnosti uporabnika za Azure Active Directory in potrditev, da je uporabnik član navedene skupine, preden se zagotovi koda PIN za lokalni dostop. Ta način zahteva tudi ročno pošiljanje pooblastitvenega ključa za lokalni dostop v aplikacijo za telefon prek e-pošte ali drugega načina.

OPOMBA: Ta možnost zahteva, da ima aplikacija za telefon HP Sure Admin dostop do omrežja, da lahko pridobi enkratno kodo PIN.

1. Poimenujte ključ v vnosnem polju **Ime ključa**.
2. Vnesite geslo v vnosno polje **Geslo**.

   OPOMBA: Geslo se uporablja za zaščito izvoženega ključa in ga je treba vnesti, da lahko uporabnik aplikacije za telefon HP Sure Admin uvozi ključ.

3. Izberite **Prijava v Azure AD** in se prijavite.
4. V spustnem polju **Ime skupine Azure AD** izberite ime skupine. Za dostop do ključa morate biti član skupine.
5. Izberite **Prebrskaj** in izberite mesto za izvoz poti v sistemu.
6. Izberite **Ustvari ključ**. Ključ je uspešno ustvarjen, ko se zraven gumba **Ustvari ključ** prikaže obvestilna ikona s sporočilom **Ključ je uspešno ustvarjen**.
7. Izberite **Naprej**. Na strani s povzetkom so prikazane vnesene nastavitve za funkcijo HP Sure Admin.
8. Izberite **Shrani pravilnik**. Pravilnik je shranjen, ko se prikaže sporočilo **Uspešno shranjeno**.
9. Pomaknite se v mapo, v katero ste shranili ključ, in ga z načinom, ki je na voljo za tega uporabnika v tej napravi, na primer prek e-pošte, pošljite uporabniku aplikacije za telefon HP Sure Admin. Ta uporabnik bo potreboval geslo tudi za uvoz ključa. HP priporoča, da za ključ in geslo uporabite različna načina pošiljanja.

   OPOMBA: Ko pošiljate kodo QR, jo pošljite v izvirni velikosti. Aplikacija ne more pravilno prebrati slike, če je velikost manjša od 800 × 600.

Ustvarjanje in pošiljanje ključa v OneDrive skupine Azure AD:

(priporočeno) to možnost uporabite, da se izognete shranitvi pooblastitvenega ključa za lokalni dostop v telefon. Če izberete to možnost, MIK shrani pooblastitveni ključ za lokalni dostop v navedeni mapi OneDrive, do katere lahko dostopa samo pooblaščena skupina. Uporabnik aplikacije za telefon HP Sure Admin mora opraviti preverjanje pristnosti za Azure AD vsakič, ko je potrebna koda PIN.

1. Poimenujte ključ v vnosnem polju **Ime ključa**.
2. Vnesite geslo v vnosno polje **Geslo**.
3. Izberite **Prijava v Azure AD** in se prijavite.
4. V spustnem polju Ime skupine Azure AD izberite ime skupine.

   OPOMBA: Za dostop do ključa morate biti član skupine.

5. V vnosno polje **OneDrive** vnesite ime mape OneDrive, v katero želite shraniti ključ.

6. Izberite **Prebrskaj** in izberite mesto za izvoz poti v sistemu.

7. Izberite **Ustvari ključ**.

OPOMBA: Ključ je uspešno dodan v navedeno mapo OneDrive in izvožen v navedeno lokalno mapo, ko se zraven gumba **Ustvari ključ** prikaže obvestilna ikona s sporočilom **Ključ je uspešno ustvarjen**.

8. Izberite **Naprej**. Na strani s povzetkom so prikazane vnesene nastavitve za funkcijo HP Sure Admin.

9. Izberite **Shrani pravilnik**. Pravilnik je shranjen, ko se prikaže sporočilo **Uspešno shranjeno**.

OPOMBA: V tem primeru ni treba v aplikacijo za telefon HP Sure Admin poslati ničesar, da jo vnaprej omogočite. Ciljni računalniki so nastavljeni tako, da kažejo na mesto OneDrive, ki je vključeno v kodo QR. Aplikacija za telefon HP Sure Admin uporablja ta kazalec za dostop do mesta OneDrive, če je uporabnik del pooblaščene skupine in uspešno potrdi pristnost.

3 Nastavitev telefona

Iz trgovine Google Play ali Apple Store prenesite aplikacijo za telefon HP Sure Admin.

- Iz Googlove trgovine prenesite aplikacijo HP Sure Admin za telefone Android.
- Iz Applove trgovine prenesite aplikacijo HP Sure Admin za telefone iOS.

Uporaba aplikacije za telefon HP Sure Admin za odklepanje BIOS-a

Mobilna aplikacija HP Sure Admin nadomešča uporabo gesla BIOS-a za lokalni dostop do namestitvenega programa BIOS z zagotovitvijo enkratne kode PIN, pridobljene s skeniranjem kode QR, ki se prikaže v ciljni napravi.

Uporabite te korake za lokalno shranjevanje ključa v telefonu v primeru, ko je ključ poslan uporabniku aplikacije za telefon. V naslednjem primeru je ključ poslan po e-pošti uporabniku telefonske aplikacije HP Sure Admin in uporabnik odpre e-pošto na telefonu.

1. Odprite e-poštno sporočilo, ki vsebuje ključ.
2. Ko se prikaže stran **Včlanitev**, vnesite geslo v vnosno polje **Vnesite geslo** in e-poštni naslov v vnosno polje **Vnesite elektronski naslov**, da boste lahko dešifrirali ključ in ga dodali v aplikacijo HP Sure Admin. Številka PIN za odklepanje je prikazana na strani **Koda PIN**.

   OPOMBA: S tem korakom shranite ključ v mobilno napravo in dokončate včlanitev. Na tej točki lahko z aplikacijo za telefon HP Sure Admin dostopite do katere koli naprave, ki je bila omogočena za dostop prek tega ključa. Elektronski naslov je potreben samo, če ga zahteva skrbnik.

3. Vnesite kodo PIN v vnosno polje **BIOS Vnesite kodo odziva**.

Pridobitev dostopa do nastavitve BIOS-a po vpisu

Postopek za pridobitev dostopa do namestitvenega programa BIOS v ciljnem računalniku po včlanitvi:

1. Pri zagonu v ciljnem računalniku vstopite v namestitveni program BIOS.
2. V aplikaciji za telefon izberite **Skeniraj kodo QR** in skenirajte kodo QR v ciljni napravi.
3. Če se prikaže poziv za preverjanje pristnosti uporabnika, vnesite poverilnice.
4. Na strani **Koda PIN** se prikaže odklenjena številka PIN.
5. Vnesite kodo PIN v vnosno polje **Vnesite kodo odziva BIOS** v ciljni napravi.

Odklepanje BIOS-a s storitvijo Azure AD Group OneDrive

Postopek za uporabo funkcije HP Sure Admin za odklepanje BIOS-a z možnostjo OneDrive skupine Azure AD:

1. Izberite **Skeniraj kodo QR**, nato pa skenirajte kodo QR za BIOS.

   OPOMBA: Aplikacija HP Sure Admin prikaže stran za prijavo v Azure AD.

2. Prijavite se v svoj račun za Azure.

3. Vnesite kodo PIN v vnosno polje **Vnesite kodo odziva**.

OPOMBA: Aplikacija HP Sure Admin v tem primeru ključa ne shrani lokalno. Aplikacija za telefon HP Sure Admin mora imeti dostop do omrežja in uporabnik mora opraviti preverjanje pristnosti vsakič, ko je potrebna enkratna koda PIN.

4 Kode napak HP Sure Admin

V tabeli v tem razdelku si lahko ogledate kode napak, vrste in opise skrbniške konzole HP Sure Admin in KMS.

Tabela 4-1 Kode napak, vrste in opisi aplikacij HP Sure Admin

Koda napake	Vrsta napake	Opis
100	QRCodeUnknownError	Splošna napaka.
101	QRCodeDeserialization	Ni mogoče prebrati QR kode JSON. Niz ni veljavna datoteka json ali pa podatki niso veljavni.
102	QRCodeInvalidImage	Skenirana slika kode QR ni veljavna. Datoteke slike kode QR ni mogoče prebrati.
103	QRCodeNoPayload	Skenirana slika kode QR ni veljavna. Datoteka slike ne vključuje koristne vsebine JSON.
104	QRCodeInvalid	Kode QR JSON ni mogoče prebrati. Niz ni veljaven niz JSON ali pa podatki v sliki QR niso veljavni.
105	QRCodeInvalidKeyIdHash	Razpršitev javnega ključa v nizu JSON kode QR se ne ujema z razpršitvijo javnega ključa paketa za včlanitev (podatki KeyID).
106	QRCodeTampered	Skenirana slika kode QR je spremenjena ni veljavna.
107	QRCodeTamperedOrInvalidPassPhrase	Skenirana QR koda slike je nedovoljena in neveljavna ali pa je vneseno geslo napačno.

Tabela 4-2 Ključ za dostop OneTime iz napak, vrst in opisov storitve OneDrive

Koda napake	Vrsta napake	Opis
200	OneTimeKeyError	Splošna napaka.
201	OneTimeKeyNoUserGroups	Prijavljeni uporabnik ne pripada nobeni skupini AD, ki je v vaši organizaciji.
203	OneTimeKeyInvalidUserGroup	Prijavljeni uporabnik ne pripada skupini AD, ki ji je dodeljen ta ključ.
204	OneTimeKeyQRFileDoesNotExist	Datoteka ključev OneTime ne obstaja v mapi OneDrive skupine AD.
205	OneTimeKeyInvalidQRFile	Datoteka ključev OneTime v mapi OneDrive skupine AD ni veljavna.
206	OneTimeKeyInvalidQRpayload	Datoteka ključev OneTime obstaja, vendar ne more prebrati koristne vsebine.

Tabela 4-3 Napake avtorizacije Azure AD

Koda napake	Vrsta napake	Opis
300	AzureADUnknownError	Splošna napaka.
301	AzureADInvalidDomain	Vneseni elektronski naslov se ne ujema z imenom domene, ki je določen v sliki kode QR.
302	AzureADAccessToken	Napaka pri pridobivanju žetona za dostop iz imenika Azure AD. Uporabnik se ne more prijaviti v imenik Azure AD v vaši organizaciji ali pa aplikacija nima potrebnih dovoljenj za povezavo z imenikom Azure AD vaše organizacije. Lahko se tudi, da je uporabnik preklical avtorizacijo.
303	AzureADUserProfile	Aplikacija HP Sure Admin ni mogla pridobiti informacij o uporabniškem profilu iz imenika Azure AD vaše organizacije.
304	AzureADUserPrincipalMismatch	Vneseni elektronski naslov se ne ujema z glavnim imenom prijavljenega uporabnika.
305	AzureADUserInvalidUserGroup	Prijavljeni uporabnik ne pripada skupini AD Azure, ki ji je dodeljen ta ključ.

Tabela 4-4 Napake, vrste in opisi skrbniške konzole KMS

Koda napake	Vrsta napake	Opis
401	KmsUnauthorized	Uporabnik ni pooblaščen za uporabo storitve KMS.
402	KmsKeyDoesNotExist	Ustrezen zasebni ključ v shrambi ključa KMS ne obstaja. Ključ je trenutno v izbrisanem stanju, vendar ga je mogoče obnoviti, njegovega imena pa v tem stanju ni mogoče ponovno uporabiti. Ključ lahko samo obnovite ali počistite.
403	KmsKeyDoesNotExistInTableStorage	Ključ ne obstaja v pomnilniku tabele.
404	KmsUploadKeyErrorInKeyVault	Pri dodajanju ključa v shrambo ključa je prišlo do napake.
405	KmsUploadKeyUnauthorized	Uporabnik ni pooblaščen za nalaganje ključev. Uporabnik ne pripada pooblaščeni skupini AD, ki lahko pokliče ta API.
406	KmsInvalidAzureADLogin	Uporabnik ni prijavljen v storitvi Azure Tenant AAD.
407	KmsNoUserGroups	Prijavljen uporabnik ne pripada nobeni skupini AD v vaši organizaciji.
408	KmsInvalidUserGroup	Prijavljen uporabnik ne pripada skupini AD, ki ji je dodeljen ta ključ.
409	KmsInvalidAccessToken	Element za dostop, ki ste ga dobili v zahtevi, ni veljaven.
410	KmsAccessTokenExpired	Dodeljen accessToken je potekel.
411	KmsAccessTokenInvalidTenantId	Dodeljen accessToken ima neveljavno vrednost TenantId.

Tabela 4-4 Napake, vrste in opisi skrbniške konzole KMS (Se nadaljuje)

Koda napake	Vrsta napake	Opis
412	KmsAccessTokenTenantIdMismatch	TenantId v priloženem accessToken-u se ne ujema s funkcijsko aplikacijo TenantId.
413	KmsInvalidKeyId	KeyId je ničen ali prazen.
414	KmsDeleteKeyUnauthorized	Uporabnik ni pooblaščen za brisanje ključev. Uporabnik ne pripada pooblaščeni skupini AD, ki lahko pokliče ta API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Poskus obnove skrivnosti je neuspešen in je ni bilo mogoče obnoviti. Uporabnik bi moral poskusiti znova.
416	KmsInvalidGetKeysRequest	Zahteva Get Keys ni veljavna.
417	KmsGetKeysUnauthorized	Uporabnik ni pooblaščen za pridobitev ključev. Uporabnik ne pripada pooblaščeni skupini AD, ki lahko pokliče ta API.
418	KmsInvalidRequestPayload	Zahteva, ki jo je prejel API, je neveljavna.
419	KmsRequestRequired	Prejeti zahtevek ne sme biti prazen.
420	KmsKeyNotConcurrent	Ključ v shrambi tabele je bil posodobljen ali spremenjen od zadnjega uporabniškega kopiranja.