Korisnički priručnik za administratora HP Sure Admin

SAŽETAK

HP Sure Admin IT administratorima omogućuje sigurno upravljanje povjerljivim postavkama firmvera uređaja pomoću certifikata i kriptografije s javnim ključevima za daljinsko i lokalno upravljanje postavkama umjesto korištenja lozinke.

Pravne informacije

Drugo izdanje: listopad 2021.

Prvo izdanje: prosinac 2019.

Šifra dokumenta: L83995-BC2

Sadržaj

1 Početak rada

HP Sure Admin IT administratorima omogućuje sigurno upravljanje povjerljivim postavkama firmvera uređaja pomoću certifikata i kriptografije s javnim ključevima za daljinsko i lokalno upravljanje postavkama umjesto korištenja lozinke.

HP Sure Admin sastoji se od sljedećih dijelova:

- **Ciljni PC:** platforme za upravljanje koje podržavaju Enhanced BIOS Authentication Mode.
- **HP Manageability Integration Kit (MIK):** dodatak za System Center Configuration Manager (SCCM) ili HP BIOS Configuration Utility (BCU) za daljinsko upravljanje postavkama BIOS-a.
- **HP Sure Admin Local Access Authenticator:** aplikacija za mobitel koja zamjenjuje upotrebu lozinke za omogućivanje lokalnog pristupa postavkama BIOS-a skeniranjem QR koda radi dohvaćanja jednokratnog PIN-a.

Korištenje značajke HP Sure Admin

U ovom se odjeljku opisuje postupak upotrebe alata HP Sure Admin.

1. Otvorite dodatak HP Sure Admin unutar dodatka HP Manageability Integration Kit (MIK) za System Configuration Manager (SCCM) ili Enhanced BIOS Configuration Utility (BCU).
2. Preuzmite aplikaciju HP Sure Admin za mobitel sa servisa Google Play™ ili Apple App Store®.
3. Stvorite par ključeva koji koriste ciljni uređaj i aplikacija HP Sure Admin za mobitel da biste dohvatili jednokratni PIN za otključavanje BIOS-a.

Onemogućivanje značajke HP Sure Admin

U ovom se odjeljku opisuju mogućnosti za onemogućivanje značajke HP Sure Admin:

- U postavkama BIOS-a, kojima pristupate pritiskom na F10, odaberite **Restore Security settings to Factory Defaults** (Vrati sigurnosne postavke na tvornički zadane vrijednosti).

NAPOMENA: za to je potrebna fizička prisutnost radi navođenja PIN-a za provjeru autentičnosti putem aplikacije HP Sure Admin radi pristupa postavkama dostupnima putem tipke F10.

- Pomoću naredbe BCU-a daljinski pozovite WMI naredbe **Restore Security settings to Factory Defaults** (Vrati sigurnosne postavke na tvornički zadane vrijednosti).

NAPOMENA: dodatne informacije potražite u korisničkom priručniku za HP BIOS Configuration Utility (BCU).

- Na stranici za sigurnosnu dodjelu MIK-a odaberite **Deprovision** (Poništi dodjelu).

2 Stvaranje ključeva i upravljanje ključevima

Prije omogućivanja načina rada Enhanced BIOS Authentication Mode dovršite sigurnosnu dodjelu unutar MIK-a. Za stvaranje i izvoz ključeva mora biti omogućen način rada Enhanced BIOS Authentication Mode. Da biste omogućili BIOS Authentication Mode:

▲ Otvorite dodatak HP Sure Admin pa odaberite **Enhanced BIOS Authentication Mode** da biste stvorili i izvezli ključeve.

Stvaranje i izvoz ključeva

Postoje tri različita načina za stvaranje parova ključeva za lokalni pristup i aplikaciji HP Sure Admin za mobitel omogućili pristup ključu.

- Stvaranje i izvoz ključa s ručnom distribucijom na stranici 2
- Stvaranje i izvoz ključeva uz Azure AD Revocation na stranici 3
- Stvaranje i slanje ključa na OneDrive grupe servisa Azure AD: na stranici 3

Stvaranje i izvoz ključa s ručnom distribucijom

pomoću te mogućnosti izvezite ključ za autorizaciju za lokalni pristup, a zatim ga ručno pošaljite u aplikaciju HP Sure Admin za mobitel e-poštom ili na neki drugi način.

NAPOMENA: za tu mogućnost aplikacije HP Sure Admin za mobitel ne mora imati pristup mreži radi dohvaćanja jednokratnog PIN-a.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite pristupni izraz u okvir za unos **Passphrase** (Pristupni izraz).

   NAPOMENA: pristupni izraz služi za zaštitu izvezenog ključa potrebno ga je navesti da bi korisnik aplikacije HP Sure Admin za mobitel mogao uvesti ključ.

3. Odaberite **Browse** (Pregledaj), a zatim mjesto na koje želite izvesti put u sustavu.
4. Odaberite **Create Key** (Stvori ključ). ključ je uspješno stvoren kada se ikona obavijesti pojavi pokraj gumba **Create Key** (Stvori ključ) uz poruku **Key successfully created** (Ključ je uspješno stvoren).
5. Odaberite **Dalje**. Na stranici sa sažetkom prikazat će se postavke aplikacije HP Sure Admin koje ste unijeli.
6. Odaberite **Save Policy** (Spremi pravilnik). Pravilnik će biti spremljen kada se prikaže poruka **Saved successfully** (Uspješno spremljeno).
7. Otvorite mapu u koju ste spremili ključ pa ga pošaljite u aplikaciju HP Sure Admin za mobitel metodom koja je dostupna tom korisniku na tom uređaju, npr. e-poštom. Uz to, tom će korisniku biti potreban pristupni izraz za uvoz ključa. HP preporučuje korištenje različitih mehanizama slanja za ključ i pristupni izraz.

   NAPOMENA: prilikom slanja QR koda pošaljite ga u izvornoj veličini. Aplikacija ne može pravilno pročitati sliku ako je manja od 800 × 600.

Stvaranje i izvoz ključeva uz Azure AD Revocation

pomoću te mogućnosti povežite ključ za lokalni pristup s navedenom grupom servisa Azure Active Directory i naredite aplikaciji HP Sure Admin za mobitel da zatraži provjeru autentičnosti korisnika za Azure Active Directory i provjeri je li korisnik član navedene grupe prije davanja PIN-a za lokalni pristup. Za tu je metodu potrebno i ručno slanje ključa za autorizaciju za lokalni pristup u aplikaciju za mobitel e-poštom ili na neki drugi način.

NAPOMENA: za tu mogućnost aplikacija HP Sure Admin za mobitel mora imati pristup mreži radi dohvaćanja jednokratnog PIN-a.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite pristupni izraz u okvir za unos **Passphrase** (Pristupni izraz).

   NAPOMENA: pristupni izraz služi za zaštitu izvezenog ključa potrebno ga je navesti da bi korisnik aplikacije HP Sure Admin za mobitel mogao uvesti ključ.

3. Odaberite **Azure AD Login** (Prijava na Azure AD).
4. Odaberite naziv grupe u okviru s padajućim popisom **Azure AD Group Name** (Naziv grupe servisa Azure AD). da biste imali pristup ključu, morate biti član grupe.
5. Odaberite **Browse** (Pregledaj), a zatim mjesto na koje želite izvesti put u sustavu.
6. Odaberite **Create Key** (Stvori ključ). ključ je uspješno stvoren kada se ikona obavijesti pojavi pokraj gumba **Create Key** (Stvori ključ) uz poruku **Key successfully created** (Ključ je uspješno stvoren).
7. Odaberite **Dalje**. Na stranici sa sažetkom prikazat će se postavke aplikacije HP Sure Admin koje ste unijeli.
8. Odaberite **Save Policy** (Spremi pravilnik). Pravilnik će biti spremljen kada se prikaže poruka **Saved successfully** (Uspješno spremljeno).
9. Otvorite mapu u koju ste spremili ključ pa ga pošaljite u aplikaciju HP Sure Admin za mobitel metodom koja je dostupna tom korisniku na tom uređaju, npr. e-poštom. Uz to, tom će korisniku biti potreban pristupni izraz za uvoz ključa. HP preporučuje korištenje različitih mehanizama slanja za ključ i pristupni izraz.

   NAPOMENA: prilikom slanja QR koda pošaljite ga u izvornoj veličini. Aplikacija ne može pravilno pročitati sliku ako je manja od 800 × 600.

Stvaranje i slanje ključa na OneDrive grupe servisa Azure AD:

(preporučeno) tu mogućnost koristite da biste izbjegli pohranu ključa za autorizaciju za lokalni pristup na mobitel. Kada odaberete tu mogućnost, MIK će ključ za autorizaciju za lokalni pristup pohraniti u navedenu mapu na servisu OneDrive koja je dostupna samo autoriziranoj grupi. Korisnik aplikacije HP Sure Admin za mobitel morat će provjeriti autentičnost za Azure AD svaki put kada je potreban PIN.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite pristupni izraz u okvir za unos **Passphrase** (Pristupni izraz).
3. Odaberite **Azure AD Login** (Prijava na Azure AD) i prijavite se.

4. Odaberite naziv grupe u okviru s padajućim popisom Azure AD Group Name (Naziv grupe servisa Azure AD).

NAPOMENA: da biste imali pristup ključu, morate biti član grupe.

5. U okvir za unos **OneDrive** unesite naziv mape na servisu OneDrive u koju želite spremiti ključ.
6. Odaberite **Browse** (Pregledaj), a zatim mjesto na koje želite izvesti put u sustavu.
7. Odaberite **Create Key** (Stvori ključ).

NAPOMENA: ključ će biti uspješno dodan u navedenu mapu na servisu OneDrive i izvezen u navedenu lokalnu mapu kada se pokraj gumba **Create Key** (Stvori ključ) prikaže ikona obavijesti s porukom **Key successfully created** (Ključ je uspješno stvoren).

8. Odaberite **Dalje**. Na stranici sa sažetkom prikazat će se postavke aplikacije HP Sure Admin koje ste unijeli.
9. Odaberite **Save Policy** (Spremi pravilnik). Pravilnik će biti spremljen kada se prikaže poruka **Saved successfully** (Uspješno spremljeno).

NAPOMENA: U ovom scenariju nema potrebe za slanjem ničega u aplikaciju HP Sure Admin za mobitel radi poništavanja dodjele. Odredišni se PC-jevi dodjeljuju tako da upućuju na mjesto na servisu OneDrive koje je uvršteno u QR kod. Aplikacija HP Sure Admin za mobitel koristi taj pokazivač za pristup mjestu na servisu OneDrive ako je korisnik dio autorizirane grupe i uspješno provjeri autentičnost.

3 Postavljanje mobitela

Preuzmite aplikaciju HP Sure Admin za mobitel sa servisa Google Play ili Apple Store.

- Preuzmite HP Sure Admin sa servisa Google Store za mobitele sa sustavom Android.
- Preuzmite HP Sure Admin sa servisa Apple Store za mobitele sa sustavom iOS.

Otključavanje BIOS-a pomoću aplikacije HP Sure Admin za mobitel

Aplikacija HP Sure Admin za mobitel zamjenjuje lozinku za BIOS za lokalni pristup postavkama BIOS-a navođenjem jednokratnog PIN-a dobivenog skeniranjem QR koda prikazanog na ciljnom uređaju.

Služite se ovim koracima da biste spremili ključ lokalno na mobitel u scenariju u kojem se ključ šalje korisniku mobilne aplikacije. U sljedećem primjeru ključ se šalje e-poštom korisniku mobilne aplikacije HP Sure Admin, a korisnik otvara e-poštu na mobitelu.

1. Otvorite poruku e-pošte s ključem.
2. Kada se prikaže stranica **Enrollment** (Registracija), unesite pristupni izraz u okvir za unos **Enter passphrase** (Unesite pristupni izraz) i adresu e-pošte u okvir za unos **Enter your email address** (Unesite svoju adresu e-pošte) da biste dešifrirali ključ i dodali ga u aplikaciju HP Sure Admin. Na stranici **Your PIN** (Vaš PIN) prikazat će se PIN za otključavanje.

   NAPOMENA: u ovom se koraku ključ sprema na mobilni uređaj i dovršava se registracija. Sada možete pomoću aplikacije HP Sure Admin za mobitel pristupiti bilo kojem uređaju koji je dodijeljen tako da bude dostupan putem tog ključa. Adresa e-pošte potrebna je samo ako je traži administrator.

3. Unesite PIN u okvir za unos **Enter Response Code** (Unesite kod za odgovor) za BIOS.

Dobivanje pristupa za postavljanje BIOS-a nakon registracije

Da biste nakon registracije dobili pristup postavkama BIOS-a na ciljnom uređaju:

1. Na ciljnom uređaju prilikom pokretanja pristupite postavkama BIOS-a.
2. U aplikaciji za mobitel odaberite **Scan QR Code** (Skeniraj QR kod) pa skenirajte QR kod na ciljnom uređaju.
3. Ako za zatraži provjera autentičnosti korisnika, navedite vjerodajnice.
4. Na stranici **Your PIN** (Vaš PIN) prikazat će se otključani PIN.
5. Unesite PIN u okvir za unos **BIOS Enter Response Code** (Unesite kod za odgovor za BIOS) na ciljnom uređaju.

Otključavanje BIOS-a uz Azure AD Group OneDrive

Da biste pomoću aplikacije HP Sure Admin otključali BIOS uz OneDrive grupe servisa Azure AD:

1. Odaberite **Scan QR Code** (Skeniraj QR kod) pa skenirajte QR kod za BIOS.

   NAPOMENA: u aplikaciji HP Sure Admin prikazat će se stranica za prijavu na Azure AD.

2. Prijavite se na račun za Azure.

3. Unesite PIN u okvir za unos **Enter Response Code** (Unesite kod za odgovor) za BIOS.

NAPOMENA: u ovom scenariju aplikacija HP Sure Admin ne sprema ključ lokalno. Aplikacija HP Sure Admin za mobitel mora imati pristup mreži i korisnik mora provjeriti autentičnost svaki put kada je potreban jednokratni PIN.

4 Kodovi pogrešaka za HP Sure Admin

Upotrijebite tablicu u ovom odjeljku da biste vidjeli kodove pogrešaka, vrste i opise HP Sure Admin i KMS Administrator Console.

Tablica 4-1 Kodovi, vrste i opis aplikacije HP Sure Admin

Kôd pogreške	Vrsta pogreške	Opis
100	QRCodeUnknownError	Opća pogreška.
101	QRCodeDeserialization	Nije moguće pročitati format JSON koda QR. Niz nije valjana datoteka JSON ili podatci nisu valjani.
102	QRCodeInvalidImage	Skenirana slika QR koda nije valjana. Nije moguće pročitati datoteku slike QR koda.
103	QRCodeNoPayload	Skenirana slika QR koda nije valjana. Datoteka slike ne sadrži korisne podatke JSON-a.
104	QRCodeInvalid	Nije moguće pročitati JSON koda QR. Niz nije valjan format JSON ili podatci na slici QR nisu valjani.
105	QRCodeInvalidKeyIdHash	Raspršivanje javnog ključa u JSON-u koda QR ne podudara se s raspršivanjem javnog ključa paketa za registraciju (podatci ID-a ključa).
106	QRCodeTampered	Skenirana slika QR koda izmijenjena je ili nije valjana.
107	QRCodeTamperedOrInvalidPassPhrase	Skenirana slika koda QR izmijenjena je i nevažeća ili je uneseni pristupni izraz netočan.

Tablica 4-2 Pristupni ključ za jednokratnu upotrebu s pogrešaka, vrsta i opisa OneDrive

Kôd pogreške	Vrsta pogreške	Opis
200	OneTimeKeyError	Opća pogreška.
201	OneTimeKeyNoUserGroups	Prijavljeni korisnik ne pripada nijednoj grupi servisa AD u ustanovi.
203	OneTimeKeyInvalidUserGroup	Prijavljeni korisnik ne pripada dodijeljenoj grupi servisa AD za ključ.
204	OneTimeKeyQRFileDoesNotExist	U mapi na servisu OneDrive grupe servisa AD nema datoteke ključa za jednokratnu upotrebu.
205	OneTimeKeyInvalidQRFile	Datoteka ključa za jednokratnu upotrebu u mapi na servisu OneDrive grupe servisa AD nije valjana.
206	OneTimeKeyInvalidQRpayload	Datoteka ključa ključa za jednokratnu upotrebu postoji, ali nije moguće pročitati korisne podatke datoteke.

Tablica 4-3 Pogreške odobrenja Azure AD-a

Kôd pogreške	Vrsta pogreške	Opis
300	AzureADUnknownError	Opća pogreška.
301	AzureADInvalidDomain	Unesena adresa e-pošte ne podudara se s nazivom domene na slici koda QR.
302	AzureADAccessToken	Pogreška prilikom dohvaćanja pristupnog tokena sa servisa Azure AD. Korisnik se ne može prijaviti na Azure AD tvrtke ili ustanove ili aplikacija nema potrebne dozvole za povezivanje sa servisom Azure AD tvrtke ili ustanove. Moguće je i da je korisnik otkazao provjeru autentičnosti.
303	AzureADUserProfile	Aplikacija HP Sure Admin ne može dohvatiti podatke o korisničkom profilu sa servisa Azure AD tvrtke ili ustanove.
304	AzureADUserPrincipalMismatch	Unesena adresa e-pošte ne podudara se s korisničkim imenom prijavljenog korisnika.
305	AzureADUserInvalidUserGroup	Prijavljeni korisnik ne pripada dodijeljenoj grupi servisa Azure AD za ključ.

Tablica 4-4 Pogreške, vrste i opis KMS Admin Console

Kôd pogreške	Vrsta pogreške	Opis
401	KmsUnauthorized	Korisnik nije ovlašten za upotrebu usluge KMS.
402	KmsKeyDoesNotExist	Odgovarajući privatni ključ ne postoji u trezoru ključeva usluge KMS. Ključ je trenutačno u izbrisan, ali se može povratiti, a naziv mu se ne može ponovno upotrijebiti u tom stanju. Ključ se može povratiti ili očistiti.
403	KmsKeyDoesNotExistInTableStorage	Ključ ne postoji u tablici za pohranu.
404	KmsUploadKeyErrorInKeyVault	Pogreška u dodavanju ključa u trezor ključeva.
405	KmsUploadKeyUnauthorized	Korisnik nije ovlašten za prijenos ključeva. Korisnik ne pripada ovlaštenoj grupi AD za koju je dopušteno pozivati ovaj API.
406	KmsInvalidAzureADLogin	Korisnik nije prijavljen na Azure Tenant AAD.
407	KmsNoUserGroups	Prijavljeni korisnik ne pripada nijednoj grupi AD u tvrtki ili ustanovi.
408	KmsInvalidUserGroup	Prijavljeni korisnik ne pripada dodijeljenoj grupi AD za ključ.
409	KmsInvalidAccessToken	Pristupni token koji je isporučen u zahtjevu nije valjan.
410	KmsAccessTokenExpired	Pristup je token istekao.
411	KmsAccessTokenInvalidTenantId	Navedeni pristupni token ima nevažeću vrijednost za TenantId.

Tablica 4-4 Pogreške, vrste i opis KMS Admin Console (Nastavak)

Kôd pogreške	Vrsta pogreške	Opis
412	KmsAccessTokenTenantIdMismatch	TenantId u priloženom pristupnom tokenu ne odgovara funkciji aplikacije TenantId.
413	KmsInvalidKeyId	KeyId je ništavan ili prazan.
414	KmsDeleteKeyUnauthorized	Korisnik nije ovlašten za brisanje ključeva. Korisnik ne pripada ovlaštenoj grupi AD za koju je dopušteno pozivati ovaj API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Pokušaj oporavka tajne nije uspio i nije ga moguće oporaviti. Korisnik bi trebao pokušati ponovno.
416	KmsInvalidGetKeysRequest	Zahtjev za preuzimanje ključeva jest nevažeći.
417	KmsGetKeysUnauthorized	Korisnik nije ovlašten za preuzimanje ključeva. Korisnik ne pripada ovlaštenoj grupi AD za koju je dopušteno pozivati ovaj API.
418	KmsInvalidRequestPayload	Zahtjev koji je primio API jest nevažeći.
419	KmsRequestRequired	Primljeni zahtjev ne smije biti prazan.
420	KmsKeyNotConcurrent	Ključ u tablici za pohranu ažuriran je ili izmijenjen od trenutka kada je korisnik zadnji put vratio kopiju.