Vodič za korisnike aplikacije HP Sure Admin

SAŽETAK

HP Sure Admin IT omogućava administratorima bezbedno upravljanje poverljivim postavkama firmvera uređaja pomoću certifikata i kriptografije s javnim ključevima za daljinsko i lokalno upravljanje postavkama umesto korišćenja lozinke.

Pravne informacije

Drugo izdanje: oktobar 2021.

Prvo izdanje: decembar 2019.

Broj dela dokumenta: L83995-E32

Sadržaj

1 Prvi koraci

HP Sure Admin IT omogućava administratorima bezbedno upravljanje poverljivim postavkama firmvera uređaja pomoću certifikata i kriptografije s javnim ključevima za daljinsko i lokalno upravljanje postavkama umesto korišćenja lozinke.

HP Sure Admin se sastoji od sledećih delova:

- **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 mobilne telefone koja zamenjuje upotrebu lozinke za omogućavanje lokalnog pristupa postavkama BIOS-a skeniranjem QR koda radi dobijanja jednokratnog PIN-a.

Korišćenje aplikacije HP Sure Admin

Ovaj odeljak opisuje proces korišćenja aplikacije HP Sure Admin.

1. Otvorite dodatak HP Sure Admin u okviru dodatka HP Manageability Integration Kit (MIK) za System Configuration Manager (SCCM) ili Enhanced BIOS Configuration Utility (BCU).
2. Preuzmite aplikaciju HP Sure Admin za mobilne telefone iz prodavnice Google Play™ ili Apple App Store®.
3. Kreirajte par ključeva koji koriste ciljni uređaj i aplikacija HP Sure Admin za mobilne telefone da biste preuzeli jednokratni PIN za otključavanje BIOS-a.

Onemogućavanje aplikacije HP Sure Admin

Ovaj odeljak opisuje opcije za onemogućavanje aplikacije HP Sure Admin.

- U postavkama BIOS-a dostupnim putem tastera F10 izaberite **Restore Security settings to Factory Defaults** (Vrati postavke bezbednosti na fabričke vrednosti).

NAPOMENA: Za to je potrebna fizička prisutnost radi navođenja PIN-a za proveru identiteta putem telefonske aplikacije HP Sure Admin radi pristupa postavkama dostupnim putem tastera F10.

- Pomoću BCU komande daljinski pozovite WMI **Restore Security settings to Factory Defaults** (Vrati postavke bezbednosti na fabričke vrednosti).

NAPOMENA: Više informacija potražite u vodiču za korisnike za HP BIOS Configuration Utility (BCU).

- Na stranici za bezbednosnu dodelu MIK-a izaberite **Deprovision** (Opozovi dodelu).

2 Kreiranje ključeva i upravljanje njima

Pre omogućavanja režima Enhanced BIOS Authentication Mode dovršite bezbednosnu dodelu u okviru MIK-a. Za kreiranje i izvoz ključeva mora biti omogućen režim Enhanced BIOS Authentication Mode. Da biste omogućili BIOS Authentication Mode:

▲ Otvorite dodatak HP Sure Admin i izaberite **Enhanced BIOS Authentication Mode** za kreiranje i izvoz ključeva.

Kreiranje i izvoz ključeva

Na 3 različita načina možete kreirati parove ključeva za lokalni pristup i telefonskoj aplikaciji HP Sure Admin omogućiti pristup ključu.

- Kreiranje i izvoz ključa pomoću ručne distribucije na stranici 2
- Kreiranje i izvoz ključa uz Azure AD Revocation na stranici 3
- Kreiranje i slanje ključa u Azure AD grupu usluge OneDrive na stranici 3

Kreiranje i izvoz ključa pomoću ručne distribucije

pomoću ove opcije izvezite ključ za autorizaciju za lokalni pristup, a zatim ga ručno pošaljite u aplikaciju HP Sure Admin za mobilne telefone e-poštom ili na neki drugi način.

NAPOMENA: Ova opcija ne zahteva da aplikacija HP Sure Admin za mobilne telefone ima pristup mreži radi dobijanja jednokratnog PIN-a.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite frazu za prolaz u okvir za unos **Passphrase** (Fraza za prolaz).

   NAPOMENA: Fraza za prolaz služi za zaštitu izvezenog ključa i potrebno ga je navesti da bi korisnik aplikacije HP Sure Admin za mobilne telefone mogao da uveze ključ.

3. Izaberite **Browse** (Pregledajte), a zatim odaberite mesto na koje želite da izvezete putanju u sistemu.
4. Izaberite **Create Key** (Kreiraj ključ). Vaš ključ se uspešno kreira kada se ikona obaveštenja pojavi pored dugmeta **Create Key** (Kreiraj ključ) uz poruku **Key successfully created** (Ključ je uspešno kreiran).
5. Izaberite **Dalje**. Stranica sa rezimeom prikazuje HP Sure Admin postavke koje ste uneli.
6. Izaberite **Save Policy** (Sačuvaj smernice). Smernica se čuva kada se pojavi poruka **Saved successfully** (Uspešno sačuvano).
7. Otvorite fasciklu u kojoj ste sačuvali ključ i pošaljite ga u aplikaciju HP Sure Admin za mobilne telefone metodom koja je dostupna tom korisniku na tom uređaju, npr. e-poštom. Pored toga, tom korisniku će biti potrebna fraza za prolaz za uvoz ključa. HP preporučuje korišćenje različitih mehanizama slanja za ključ i frazu za prolaz.

   NAPOMENA: Kada šaljete QR kôd, pošaljite ga u originalnoj veličini. Aplikacija ne može pravilno da pročita sliku ako ima dimenzije manje od 800 × 600.

Kreiranje i izvoz ključa uz Azure AD Revocation

Pomoću ove opcije povežite ključ za lokalni pristup s navedenom grupom usluge Azure Active Directory i naredite aplikaciji HP Sure Admin za mobilne telefone da zatraži proveru identiteta korisnika za Azure Active Directory i proveri da li je korisnik član navedene grupe pre obezbeđivanja PIN-a za lokalni pristup. Za ovaj metod je potrebno i ručno slanje ključa za autorizaciju za lokalni pristup u aplikaciju za mobilne telefone e-poštom ili na neki drugi način.

NAPOMENA: Ova opcija zahteva da aplikacija HP Sure Admin za mobilne telefone ima mrežni pristup radi dobijanja jednokratnog PIN-a.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite frazu za prolaz u okvir za unos **Passphrase** (Fraza za prolaz).

   NAPOMENA: Fraza za prolaz služi za zaštitu izvezenog ključa i potrebno ga je navesti da bi korisnik aplikacije HP Sure Admin za mobilne telefone mogao da uveze ključ.

3. Izaberite **Azure AD Login** (Prijava u Azure AD) i prijavite se.
4. Izaberite naziv grupe iz padajućeg menija **Azure AD Group Name** (Naziv grupe usluge Azure AD). Morate biti član grupe da biste imali pristup ključu.
5. Izaberite **Browse** (Pregledajte), a zatim odaberite mesto na koje želite da izvezete putanju u sistemu.
6. Izaberite **Create Key** (Kreiraj ključ). Vaš ključ se uspešno kreira kada se ikona obaveštenja pojavi pored dugmeta **Create Key** (Kreiraj ključ) uz poruku **Key successfully created** (Ključ je uspešno kreiran).
7. Izaberite **Dalje**. Stranica sa rezimeom prikazuje HP Sure Admin postavke koje ste uneli.
8. Izaberite **Save Policy** (Sačuvaj smernice). Smernica se čuva kada se pojavi poruka **Saved successfully** (Uspešno sačuvano).
9. Otvorite fasciklu u kojoj ste sačuvali ključ i pošaljite ga u aplikaciju HP Sure Admin za mobilne telefone metodom koja je dostupna tom korisniku na tom uređaju, npr. e-poštom. Pored toga, tom korisniku će biti potrebna fraza za prolaz za uvoz ključa. HP preporučuje korišćenje različitih mehanizama slanja za ključ i frazu za prolaz.

   NAPOMENA: Kada šaljete QR kôd, pošaljite ga u originalnoj veličini. Aplikacija ne može pravilno da pročita sliku ako ima dimenzije manje od 800 × 600.

Kreiranje i slanje ključa u Azure AD grupu usluge OneDrive

(Preporučeno) Ovu opciju koristite da biste izbegli skladištenje ključa za autorizaciju za lokalni pristup na telefonu. Kada odaberete ovu opciju, MIK će ključ za autorizaciju za lokalni pristup skladištiti u navedenu fasciklu usluge OneDrive koja je dostupna samo ovlašćenoj grupi. Korisnik aplikacije HP Sure Admin za mobilne telefone će proveriti autentičnost za Azure AD svaki put kada je potreban PIN.

1. Unesite naziv ključa u okvir za unos **Key Name** (Naziv ključa).
2. Unesite frazu za prolaz u okvir za unos **Passphrase** (Fraza za prolaz).
3. Izaberite **Azure AD Login** (Prijava u Azure AD) i prijavite se.
4. Izaberite naziv grupe iz padajućeg menija Azure AD Group Name (Naziv grupe usluge Azure AD).

   NAPOMENA: Morate biti član grupe da biste imali pristup ključu.

5. U okvir za unos **OneDrive** unesite ime OneDrive fascikle u kojoj želite da sačuvate ključ.
6. Izaberite **Browse** (Pregledajte), a zatim odaberite mesto na koje želite da izvezete putanju u sistemu.
7. Izaberite **Create Key** (Kreiraj ključ).

NAPOMENA: Ključ će biti uspešno dodat u navedenu OneDrive fasciklu i izvezen u navedenu lokalnu fasciklu kada se pored dugmeta **Create Key** (Kreiraj ključ) pojavi ikona obaveštenja uz poruku **Key successfully created** (Ključ je uspešno kreiran).

8. Izaberite **Dalje**. Stranica sa rezimeom prikazuje HP Sure Admin postavke koje ste uneli.
9. Izaberite **Save Policy** (Sačuvaj smernice). Smernica se čuva kada se pojavi poruka **Saved successfully** (Uspešno sačuvano).

NAPOMENA: U ovom scenariju nema potrebe za slanjem bilo čega u aplikaciju HP Sure Admin za mobilne telefone radi opozivanja dodele. Odredišni računari se dodeljuju tako da upućuju na OneDrive lokaciju koja je uključena u QR kôd. Aplikacija HP Sure Admin za mobilne telefone koristi taj pokazivač za pristup OneDrive lokaciji ako je korisnik deo autorizovane grupe i ako uspešno potvrdi identitet.

3 Podešavanje telefona

Preuzmite HP Sure Admin aplikaciju za mobilne telefone iz prodavnice Google Play ili Apple store.

- Preuzmite HP Sure Admin iz Google prodavnice za Android telefone.
- Preuzmite HP Sure Admin iz Apple prodavnice za iOS telefone.

Korišćenje aplikacije HP Sure Admin za mobilne telefone za otključavanje BIOS-a

Aplikacija HP Sure Admin za mobilne telefone zamenjuje lozinku za BIOS za lokalni pristup postavkama BIOS-a navođenjem jednokratnog PIN-a dobijenog skeniranjem QR koda prikazanog na ciljnom uređaju.

Pratite ove korake da biste sačuvali ključ lokalno na telefonu u scenariju u kojem je ključ poslat korisniku telefonske aplikacije. U sledećem primeru ključ se e-poštom šalje korisniku telefonske aplikacije HP Sure Admin koji otvara poruku e-pošte na telefonu.

1. Otvorite e-poruku koja sadrži ključ.
2. Kada se prikaže stranica **Enrollment** (Registracija), unesite frazu za prolaz u okvir za unos **Enter passphrase** (Unesite frazu za prolaz) i adresu e-pošte u okvir za unos **Enter your email address** (Unesite adresu e-pošte) da biste dešifrovali ključ i dodali ga u aplikaciju HP Sure Admin. Na stranici **Your PIN** (Vaš PIN) prikazaće se PIN za otključavanje.

   NAPOMENA: Ovaj korak čuva ključ na mobilnom uređaju i dovršava registraciju. Sada možete pomoću aplikacije HP Sure Admin za mobilne telefone pristupiti bilo kojem uređaju koji je dodeljen tako da bude dostupan putem tog ključa. Adresa e-pošte potrebna je samo ako je traži administrator.

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

Ostvarivanje pristupa podešavanju 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. Izaberite **Scan QR Code** (Skeniraj QR kôd) u aplikaciji telefona i skenirajte QR kôd na ciljnom uređaju.
3. Ako bude zatražena provera identiteta korisnika, navedite akreditive.
4. Otključani PIN broj prikazuje se na stranici **Your PIN** (Vaš PIN).
5. Unesite PIN u okvir za unos **BIOS Enter Response Code** (Unesite kôd za odgovor za BIOS) na ciljnom uređaju.

Otključavanje BIOS-a uz Azure AD Group OneDrive

Da biste koristili HP Sure Admin za otključavanje BIOS-a uz Azure AD grupu usluge OneDrive:

1. Izaberite **Scan QR Code** (Skenirajte QR kôd), a zatim skenirajte BIOS QR kôd.

NAPOMENA: Aplikacija HP Sure Admin prikazuje Azure AD stranicu za prijavljivanje.

2. Prijavite se na Azure nalog.
3. Unesite PIN u okvir za unos **BIOS Enter Response Code** (Unesite kôd za odgovor za BIOS).

NAPOMENA: Aplikacija HP Sure Admin ne čuva ključ lokalno u ovom scenariju. Aplikacija HP Sure Admin za mobilne telefone mora imati pristup mreži i korisnik mora da potvrdi identitet svaki put kada je potreban jednokratni PIN.

4 Kodovi grešaka za HP Sure Admin

Koristite tabelu u ovom odeljku da biste videli kodove, tipove i opise grešaka za HP Sure Admin i KMS Admin Console.

Tabela 4-1 Kodovi, tipovi i opisi grešaka u aplikaciji HP Sure Admin

Kôd greške	Tip greške	Opis
100	QRCodeUnknownError	Opšta greška.
101	QRCodeDeserialization	Nije moguće pročitati JSON za QR kôd. Niska nije važeća JSON datoteka ili podaci nisu važeći.
102	QRCodeInvalidImage	Skenirana slika QR koda je nevažeća. Nije moguće pročitati datoteku slike QR koda.
103	QRCodeNoPayload	Skenirana slika QR koda je nevažeća. Datoteka slike ne sadrži korisne podatke JSON-a.
104	QRCodeInvalid	Nije moguće pročitati JSON za QR kôd. Niska nije važeći JSON ili podaci na QR slici nisu važeći.
105	QRCodeInvalidKeyIdHash	Heš znak javnog ključa u JSON-u za QR kôd ne podudara se sa heš znakom javnog ključa paketa za registraciju (podaci ID-a ključa).
106	QRCodeTampered	Skenirana slika QR koda neovlašćeno je izmenjena ili nevažeća.
107	QRCodeTamperedOrInvalidPassPhrase	Skenirana slika QR koda neovlašćeno je izmenjena ili nevažeća ili je uneta fraza za prolaz netačna.

Tabela 4-2 Greške, tipovi i njihovi opisi za OneTime ključ za pristup iz usluge OneDrive

Kôd greške	Tip greške	Opis
200	OneTimeKeyError	Opšta greška.
201	OneTimeKeyNoUserGroups	Prijavljeni korisnik ne pripada nijednoj AD grupi u vašoj organizaciji.
203	OneTimeKeyInvalidUserGroup	Prijavljeni korisnik ne pripada AD grupi kojoj je ovaj ključ dodeljen.
204	OneTimeKeyQRFileDoesNotExist	Datoteka jednokratnog ključa ne postoji u OneDrive fascikli AD grupe.
205	OneTimeKeyInvalidQRFile	Nevažeća je datoteka OneTime ključa u OneDrive fascikli AD grupe.
206	OneTimeKeyInvalidQRpayload	Datoteka OneTime ključa postoji, ali nije moguće pročitati korisne podatke datoteke.

Tabela 4-3 Greške ovlašćenja za Azure AD

Kôd greške	Tip greške	Opis
300	AzureADUnknownError	Opšta greška.
301	AzureADInvalidDomain	Uneta adresa e-pošte se ne podudara sa imenom domena koji je naveden na slici QR koda.
302	AzureADAccessToken	Greška prilikom pribavljanja tokena za pristup iz usluge Azure AD. Korisnik se ne može prijaviti na Azure AD organizacije ili aplikacija nema potrebne dozvole za povezivanje sa uslugom Azure AD organizacije. Moguće je i da je korisnik otkazao potvrdu identiteta.
303	AzureADUserProfile	Aplikacija HP Sure Admin omogućena je da pribavi podatke o korisničkom profilu iz usluge Azure AD organizacije.
304	AzureADUserPrincipalMismatch	Uneta adresa e-pošte ne podudara se s glavnim korisničkim imenom prijavljenog korisnika.
305	AzureADUserInvalidUserGroup	Prijavljeni korisnik ne pripada dodeljenoj grupi usluge Azure AD kojoj je ovaj ključ dodeljen.

Tabela 4-4 Greške, tipovi i njihovi opisi za KMS Admin Console

Kôd greške	Tip greške	Opis
401	KmsUnauthorized	Korisnik nije ovlašćen da koristi KMS uslugu.
402	KmsKeyDoesNotExist	Podudarni privatni ključ ne postoji u KMS trezoru ključeva. Ključ je trenutno izbrisan, ali moguće ga je oporaviti, a njegovo ime ne može ponovo da se koristi dok je u ovom stanju. Ključ samo može da se oporavi ili izbriše.
403	KmsKeyDoesNotExistInTableStorage	Ključ ne postoji u skladištu tabela.
404	KmsUploadKeyErrorInKeyVault	Do greške je došlo pri dodavanju ključa u trezor ključeva.
405	KmsUploadKeyUnauthorized	Korisnik nema ovlašćenje za otpremanje ključeva. Korisnik ne pripada ovlašćenoj AD grupi koja ima dozvolu da poziva ovaj API.
406	KmsInvalidAzureADLogin	Korisnik nije prijavljen na Azure Tenant AAD.
407	KmsNoUserGroups	Prijavljeni korisnik ne pripada nijednoj AD grupi u vašoj organizaciji.
408	KmsInvalidUserGroup	Prijavljeni korisnik ne pripada AD grupi kojoj je ovaj ključ dodeljen.
409	KmsInvalidAccessToken	Token za pristup koji je naveden u zahtevu nije važeći.
410	KmsAccessTokenExpired	Navedeni token za pristup je istekao.

Tabela 4-4 Greške, tipovi i njihovi opisi za KMS Admin Console (nastavljeno)

Kôd greške	Tip greške	Opis
411	KmsAccessTokenInvalidTenantId	Navedeni token za pristup ima nevažeću vrednost za TenantId.
412	KmsAccessTokenTenantIdMismatch	TenantId u navedenom tokenu za pristup ne podudara se sa vrednošću za TenantId aplikacije funkcije.
413	KmsInvalidKeyId	ID ključa je bez vrednosti ili prazan.
414	KmsDeleteKeyUnauthorized	Korisnik nema ovlašćenje za brisanje ključeva. Korisnik ne pripada ovlašćenoj AD grupi koja ima dozvolu da poziva ovaj API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Pokušaj oporavka tajne nije uspeo i nije je bilo moguće oporaviti. Korisnik treba da pokuša ponovo.
416	KmsInvalidGetKeysRequest	Zahtev za dobijanje ključeva nije važeći.
417	KmsGetKeysUnauthorized	Korisnik nema ovlašćenje za dobijanje ključeva. Korisnik ne pripada ovlašćenoj AD grupi koja ima dozvolu da poziva ovaj API.
418	KmsInvalidRequestPayload	Zahtev koji je API primio nije važeći.
419	KmsRequestRequired	Primljeni zahtev ne sme da bude prazan.
420	KmsKeyNotConcurrent	Ključ u skladištu tabela je ažuriran ili izmenjen otkako je korisnik poslednji put preuzeo kopiju.