Používateľská príručka k nástroju HP Sure Admin

ZHRNUTIE

HP Sure Admin umožňuje správcom IT bezpečne spravovať citlivé nastavenia firmvéru zariadenia pomocou certifikátov a šifrovania verejného kľúča na vzdialené aj lokálne spravovanie nastavení namiesto hesla.

Právne informácie

Druhé vydanie: október 2021

Prvé vydanie: december 2019

Katalógové číslo dokumentu: L83995-232

Obsah

1 Úvodné informácie

HP Sure Admin umožňuje správcom IT bezpečne spravovať citlivé nastavenia firmvéru zariadenia pomocou certifikátov a šifrovania verejného kľúča na vzdialené aj lokálne spravovanie nastavení namiesto hesla.

HP Sure Admin sa skladá z nasledujúcich častí:

- **Cieľový počítač:** Platformy na spravovanie, ktoré podporujú režim rozšíreného overovania v systéme BIOS.
- **HP Manageability Integration Kit (MIK):** Doplnok pre System Center Configuration Manager (SCCM) alebo HP BIOS Configuration Utility (BCU) na vzdialené spravovanie nastavení systému BIOS.
- **HP Sure Admin Local Access Authenticator:** Telefónna aplikácia, ktorá nahrádza heslo a umožňuje lokálny prístup k nastaveniu systému BIOS nasnímaním kódu QR na získanie jednorazového kódu PIN.

Používanie aplikácie HP Sure Admin

Táto časť popisuje postup používania nástroja HP Sure Admin.

1. Otvorte doplnok HP Sure Admin v rámci doplnku HP Manageability Integration Kit (MIK) pre System Center Configuration Manager (SCCM) alebo Enhanced BIOS Configuration Utility (BCU).
2. Prevezmite telefónnu aplikáciu HP Sure Admin z obchodu Google Play™ alebo Apple App Store®.
3. Vytvorte pár kľúčov používaný cieľovým zariadením a telefónnou aplikáciou HP Sure Admin, aby ste získali jednorazový kód PIN na odomknutie systému BIOS.

Zakázanie aplikácie HP Sure Admin

Nižšie sú uvedené možnosti na zakázanie aplikácie HP Sure Admin:

- V nastavení systému BIOS (F10) vyberte možnosť **Restore Security settings to Factory Defaults** (Obnoviť predvolené nastavenia zabezpečenia od výrobcu).

POZNÁMKA: Na prístup k nastaveniam funkcie F10 sa vyžaduje fyzická prítomnosť, a to zadaním overovacieho kódu PIN prostredníctvom telefónnej aplikácie HP Sure Admin.

- Použite príkaz BCU na vzdialené zavolanie rozhrania WMI možnosti **Restore Security settings to Factory Defaults** (Obnoviť predvolené nastavenia zabezpečenia od výrobcu).

POZNÁMKA: Ďalšie informácie nájdete v používateľskej príručke nástroja HP BIOS Configuration Utility (BCU).

- Na stránke poskytnutia zabezpečenia MIK vyberte možnosť **Deprovision** (Zrušiť poskytovanie).

2 Vytvorenie a správa kľúčov

Pred povolením režimu rozšíreného overovania v systéme BIOS dokončite poskytovanie zabezpečenia v rámci MIK. Na vytvorenie a export kľúčov musí byť povolený režim rozšíreného overovania v systéme BIOS. Povolenie režimu overovania v systéme BIOS:

▲ Otvorte doplnok HP Sure Admin a vyberte možnosť **Enhanced BIOS Authentication Mode** (Režim rozšíreného overovania v systéme BIOS) na vytvorenie a export kľúčov.

Vytvorenie a export kľúčov

Existujú 3 rôzne spôsoby, ako vytvoriť páry kľúčov lokálneho prístupu a umožniť mobilnej aplikácii HP Sure Admin prístup ku kľúčom.

- Vytvoriť a exportovať kľúč s manuálnou distribúciou na strane 2
- Vytvorenie a export kľúča pomocou odvolania Azure AD na strane 3
- Vytvorenie a odoslanie kľúča do služby OneDrive skupiny Azure AD na strane 3

Vytvoriť a exportovať kľúč s manuálnou distribúciou

Túto možnosť použite v prípade, že chcete exportovať overovací kľúč lokálneho prístupu a potom ho ručne distribuovať do telefónnej aplikácie HP Sure Admin prostredníctvom e-mailu alebo iného spôsobu.

POZNÁMKA: Táto možnosť nevyžaduje, aby telefónna aplikácia HP Sure Admin mala na získanie jednorazového kódu PIN sieťový prístup.

1. Do vstupného poľa **Key Name** (Názov kľúča) zadajte názov kľúča.
2. Do vstupného poľa **Passphrase** (Prístupová fráza) zadajte prístupovú frázu.

   POZNÁMKA: Prístupová fráza sa používa na ochranu exportovaného kľúča a musí sa poskytnúť, aby používateľ telefónnej aplikácie HP Sure Admin mohol kľúč importovať.

3. Vyberte položku **Browse** (Prehľadávať) a vyberte cestu v systéme, kam chcete exportovať.
4. Vyberte položku **Create Key** (Vytvoriť kľúč). Kľúč je úspešne vytvorený, keď sa vedľa tlačidla **Create Key** (Vytvoriť kľúč) zobrazí ikona oznámení so správou **Key successfully created** (Kľúč úspešne vytvorený).
5. Vyberte položku **Next** (Ďalej). Stránka súhrnu zobrazí nastavenia, ktoré ste zadali v aplikácii HP Sure Admin.
6. Vyberte položku **Save Policy** (Uložiť politiku). Politika sa uloží po zobrazení hlásenia **Saved successfully** (Úspešne uložené).
7. Prejdite do priečinka, do ktorého ste uložili kľúč, a distribuujte ho používateľovi telefónnej aplikácie HP Sure Admin pomocou spôsobu, ktorý je k dispozícii tomuto používateľovi v príslušnom zariadení,

napríklad e-mailom. Tento používateľ tiež bude potrebovať prístupovú frázu, aby mohol importovať kľúč. Spoločnosť HP odporúča používať pre kľúč a prístupovú frázu rôzne distribučné mechanizmy.

POZNÁMKA: Ak odosielate kód QR, odošlite ho s pôvodnou veľkosťou. Aplikácia nedokáže správne načítať obrázok, ak je menší ako 800 × 600.

Vytvorenie a export kľúča pomocou odvolania Azure AD

túto možnosť použite na pripojenie lokálneho prístupového kľúča k zadanej skupine Azure Active Directory a požadovanie, aby pred poskytnutím lokálneho prístupového kódu PIN telefónna aplikácia HP Sure Admin vyžadovala overenie používateľa v službe Azure Active Directory a potvrdila, že používateľ je členom zadanej skupiny. Tento spôsob tiež vyžaduje manuálnu distribúciu overovacieho kľúča lokálneho prístupu do telefónnej aplikácie prostredníctvom e-mailu alebo inak.

POZNÁMKA: Táto možnosť vyžaduje, aby telefónna aplikácia HP Sure Admin mala na získanie jednorazového kódu PIN sieťový prístup.

1. Do vstupného poľa **Key Name** (Názov kľúča) zadajte názov kľúča.
2. Do vstupného poľa **Passphrase** (Prístupová fráza) zadajte prístupovú frázu.

   POZNÁMKA: Prístupová fráza sa používa na ochranu exportovaného kľúča a musí sa poskytnúť, aby používateľ telefónnej aplikácie HP Sure Admin mohol kľúč importovať.

3. Vyberte položku **Azure AD Login** (Prihlásenie do služby Azure AD) a prihláste sa.
4. V rozbaľovacom poli **Azure AD Group Name** (Názov skupiny Azure AD) vyberte názov skupiny. Ak chcete mať prístup ku kľúču, musíte byť členom skupiny.
5. Vyberte položku **Browse** (Prehľadávať) a vyberte cestu v systéme, kam chcete exportovať.
6. Vyberte položku **Create Key** (Vytvoriť kľúč). Kľúč je úspešne vytvorený, keď sa vedľa tlačidla **Create Key** (Vytvoriť kľúč) zobrazí ikona oznámení so správou **Key successfully created** (Kľúč úspešne vytvorený).
7. Vyberte položku **Next** (Ďalej). Stránka súhrnu zobrazí nastavenia, ktoré ste zadali v aplikácii HP Sure Admin.
8. Vyberte položku **Save Policy** (Uložiť politiku). Politika sa uloží po zobrazení hlásenia **Saved successfully** (Úspešne uložené).
9. Prejdite do priečinka, do ktorého ste uložili kľúč, a distribuujte ho používateľovi telefónnej aplikácie HP Sure Admin pomocou spôsobu, ktorý je k dispozícii tomuto používateľovi v príslušnom zariadení, napríklad e-mailom. Tento používateľ tiež bude potrebovať prístupovú frázu, aby mohol importovať kľúč. Spoločnosť HP odporúča používať pre kľúč a prístupovú frázu rôzne distribučné mechanizmy.

   POZNÁMKA: Ak odosielate kód QR, odošlite ho s pôvodnou veľkosťou. Aplikácia nedokáže správne načítať obrázok, ak je menší ako 800 × 600.

Vytvorenie a odoslanie kľúča do služby OneDrive skupiny Azure AD

(odporúča sa) túto možnosť použite v prípade, že chcete zabrániť uloženiu overovacieho kľúča lokálneho prístupu v telefóne. Keď vyberiete túto možnosť, MIK uloží overovací kľúč lokálneho prístupu do určeného priečinka v službe OneDrive, ktorý je prístupný iba oprávnenej skupine. Používateľ telefónnej aplikácie HP Sure Admin sa bude musieť overiť v službe Azure AD, kedykoľvek sa bude vyžadovať kód PIN.

1. Do vstupného poľa **Key Name** (Názov kľúča) zadajte názov kľúča.

2. Do vstupného poľa **Passphrase** (Prístupová fráza) zadajte prístupovú frázu.
3. Vyberte položku **Azure AD Login** (Prihlásenie do služby Azure AD) a prihláste sa.
4. V rozbaľovacom poli Azure AD Group Name (Názov skupiny Azure AD) vyberte názov skupiny.

POZNÁMKA: Ak chcete mať prístup ku kľúču, musíte byť členom skupiny.

5. Do vstupného poľa **OneDrive** zadajte názov priečinka v službe OneDrive, do ktorého chcete kľúč uložiť.
6. Vyberte položku **Browse** (Prehľadávať) a vyberte cestu v systéme, kam chcete exportovať.
7. Vyberte položku **Create Key** (Vytvoriť kľúč).

POZNÁMKA: Kľúč sa úspešne pridá do zadaného priečinka v službe OneDrive a exportuje sa do zadaného lokálneho priečinka, keď sa vedľa tlačidla **Create Key** (Vytvoriť kľúč) zobrazí ikona oznámení so správou **Key successfully created** (Kľúč úspešne vytvorený).

8. Vyberte položku **Next** (Ďalej). Stránka súhrnu zobrazí nastavenia, ktoré ste zadali v aplikácii HP Sure Admin.
9. Vyberte položku **Save Policy** (Uložiť politiku). Politika sa uloží po zobrazení hlásenia **Saved successfully** (Úspešne uložené).

POZNÁMKA: V tomto scenári netreba nič odosielať do telefónnej aplikácie HP Sure Admin na predbežné poskytnutie. Cieľové počítače sú poskytované tak, aby ukazovali na umiestnenie v službe OneDrive, ktoré je súčasťou kódu QR. Telefónna aplikácia HP Sure Admin používa tento ukazovateľ na prístup k umiestneniu v službe OneDrive, ak je používateľ súčasťou oprávnenej skupiny a úspešne sa overí.

3 Nastavenie v telefóne

Prevezmite telefónnu aplikáciu HP Sure Admin z obchodu Google Play alebo Apple Store.

- Pre telefóny so systémom Android prevezmite aplikáciu HP Sure Admin z obchodu spoločnosti Google.
- Pre telefóny so systémom iOS prevezmite aplikáciu HP Sure Admin z obchodu spoločnosti Apple.

Odomknutie systému BIOS pomocou telefónnej aplikácie HP Sure Admin

Mobilná aplikácia HP Sure Admin nahrádza použitie hesla systému BIOS na lokálny prístup k nastaveniu systému BIOS, a to poskytnutím jednorazového kódu PIN, ktorý bol získaný nasnímaním kódu QR zobrazeného cieľovým počítačom.

Tento postup použite na lokálne uloženie kľúča v mobilnom telefóne v situácii, keď je kľúč odoslaný používateľovi telefónnej aplikácie. V nasledujúcom príklade je kľúč odoslaný e-mailom používateľovi mobilnej aplikácie HP Sure Admin a používateľ otvorí e-mail v telefóne.

1. Otvorte e-mail, ktorý obsahuje kľúč.
2. Keď sa zobrazí stránka **Enrollment** (Registrácia), do vstupného poľa **Enter passphrase** (Zadať prístupovú frázu) zadajte prístupovú frázu a do vstupného poľa **Enter your email address** (Zadať e-mailovú adresu) zadajte e-mailovú adresu, aby sa kľúč dešifroval a pridal do aplikácie HP Sure Admin. Na stránke **Your PIN** (Váš kód PIN) sa zobrazí číslo kódu PIN na odomknutie.

   POZNÁMKA: Týmto krokom sa kľúč uloží v mobilnom zariadení a dokončí sa registrácia. V tomto bode môžete použiť telefónnu aplikáciu HP Sure Admin na prístup k ľubovoľnému zariadeniu, ktoré bolo poskytnuté na prístup prostredníctvom tohto kľúča. E-mailová adresa je potrebná iba v prípade, že ju požaduje správca.

3. Do vstupného poľa **BIOS Enter Response Code** (Zadať kód odpovede systému BIOS) zadajte kód PIN.

Získanie prístupu k nastaveniam systému BIOS po zaregistrovaní

Získanie prístupu k nastaveniu systému BIOS v cieľovom počítači po registrácii:

1. Pri spúšťaní cieľového počítača vstúpte do nastavenia systému BIOS.
2. V telefónnej aplikácii vyberte položku **Scan QR Code** (Nasnímať kód QR) a nasnímajte kód QR v cieľovom počítači.
3. Ak sa zobrazí výzva na overenie používateľa, zadajte poverenia.
4. Číslo odomknutého kódu PIN sa zobrazí na stránke **Your PIN** (Váš kód PIN).
5. Do vstupného poľa **Enter Response Code** (Zadať kód odpovede) systému BIOS v cieľovom počítači zadajte kód PIN.

Odomykanie systému BIOS pomocou služby Azure AD Group OneDrive

Použitie aplikácie HP Sure Admin na odomknutie systému BIOS pomocou služby OneDrive skupiny Azure AD:

1. Vyberte položku **Scan QR Code** (Nasnímať kód QR) a nasnímajte kód QR systému BIOS.

POZNÁMKA: V aplikácii HP Sure Admin sa zobrazí prihlasovacia stránka služby Azure AD.

2. Prihláste sa do konta Azure.
3. Do vstupného poľa **BIOS Enter Response Code** (Zadať kód odpovede systému BIOS) zadajte kód PIN.

POZNÁMKA: V tomto scenári aplikácia HP Sure Admin neuloží kľúč lokálne. Telefónna aplikácia HP Sure Admin musí mať sieťový prístup a používateľ sa musí overiť, kedykoľvek sa bude vyžadovať jednorazový kód PIN.

4 Kódy chýb nástroja HP Sure Admin

Pomocou tabuľky v tejto časti nájdete kódy, typy a popis chýb nástroja HP Sure Admin a KMS Admin Console.

Tabuľka 4-1 Kódy, typy a popisy chýb aplikácie HP Sure Admin

Kód chyby	Typ chyby	Opis
100	QRCodeUnknownError	Všeobecná chyba.
101	QRCodeDeserialization	Nie je možné načítať formát JSON kódu QR. Reťazec nemá platný formát JSON alebo údaje sú neplatné.
102	QRCodeInvalidImage	Nasnímaný obrázok kódu QR je neplatný. Nemožno načítať obrazový súbor kódu QR.
103	QRCodeNoPayload	Nasnímaný obrázok kódu QR je neplatný. Obrazový súbor nemá údajovú časť formátu JSON.
104	QRCodeInvalid	Nemožno načítať formát JSON kódu QR. Reťazec nemá platný formát JSON alebo údaje obrázka QR sú neplatné.
105	QRCodeInvalidKeyIdHash	Hodnota hash verejného kľúča vo formáte JSON kódu QR sa nezhoduje s hodnotou hash verejného kľúča registračného balíka (údaje KeyID).
106	QRCodeTampered	Nasnímaný obrázok kódu QR je poškodený a neplatný.
107	QRCodeTamperedOrInvalidPassPhrase	Nasnímaný obrázok kódu QR je poškodený a neplatný alebo zadaná prístupová fráza je nesprávna.

Tabuľka 4-2 Chyby, typy a popisy jednorázového prístupového kľúča z OneDrive

Kód chyby	Typ chyby	Opis
200	OneTimeKeyError	Všeobecná chyba.
201	OneTimeKeyNoUserGroups	Prihlásený používateľ nepatrí do žiadnej skupiny AD vo vašej organizácii.
203	OneTimeKeyInvalidUserGroup	Prihlásený používateľ nepatrí do skupiny AD, ktorej je tento kľúč priradený.
204	OneTimeKeyQRFileDoesNotExist	Súbor jednorazového kľúča neexistuje v priečinku OneDrive skupiny AD.
205	OneTimeKeyInvalidQRFile	Súbor jednorazového kľúča v priečinku OneDrive skupiny AD je neplatný.
206	OneTimeKeyInvalidQRpayload	Súbor jednorazového kľúča existuje, ale nemožno načítať údajovú časť súboru.

Tabuľka 4-3 Chyby autorizácie služby Azure AD

Kód chyby	Typ chyby	Opis
300	AzureADUnknownError	Všeobecná chyba.
301	AzureADInvalidDomain	Zadaná e-mailová adresa sa nezhoduje s názvom domény, ktorý je uvedený na obrázku kódu QR.
302	AzureADAccessToken	Pri získavaní prístupového tokenu zo služby Azure AD sa vyskytla chyba. Používateľ sa nemôže prihlásiť do služby Azure AD vašej organizácie alebo aplikácia nemá požadované povolenia na pripojenie k službe Azure AD vašej organizácie. Mohlo sa tiež stať, že používateľ zrušil overovanie.
303	AzureADUserProfile	Aplikácia HP Sure Admin nemôže získať informácie o profile používateľa zo služby Azure AD vašej organizácie.
304	AzureADUserPrincipalMismatch	Zadaná e-mailová adresa sa nezhoduje s hlavným menom prihláseného používateľa.
305	AzureADUserInvalidUserGroup	Prihlásený používateľ nepatrí do priradenej skupiny Azure AD pre tento kľúč.

Tabuľka 4-4 Chyby, typy a popisy nástroja KMS Admin Console

Kód chyby	Typ chyby	Opis
401	KmsUnauthorized	Používateľ nie je oprávnený používať službu KMS.
402	KmsKeyDoesNotExist	V trezore kľúčov KMS neexistuje zodpovedajúci súkromný kľúč. Kľúč sa momentálne odstraňuje a je možné ho obnoviť, pričom jeho názov nie je možné v tomto stave opätovne použiť. Kľúč možno len obnoviť alebo vyčistiť.
403	KmsKeyDoesNotExistInTableStorage	Kľúč neexistuje v úložisku tabuľky.
404	KmsUploadKeyErrorInKeyVault	Pri pridávaní kľúča do trezoru sa vyskytla chyba.
405	KmsUploadKeyUnauthorized	Používateľ nie je oprávnený nahrávať kľúče. Používateľ nepatrí do autorizovanej skupiny AD, ktorá má povolenie spravovať toto rozhranie API.
406	KmsInvalidAzureADLogin	Používateľ nie je prihlásený do Azure Tenant AAD.
407	Skupiny KmsNoUserGroups	Prihlásený používateľ nepatrí do žiadnej skupiny AD vo vašej organizácii.
408	KmsInvalidUserGroup	Prihlásený používateľ nepatrí do priradenej skupiny AD pre tento kľúč.
409	KmsInvalidAccessToken	Prístupový token, ktorý bol uvedený v požiadavke, je neplatný.
410	KmsAccessTokenExpired	Platnosť poskytnutého AccessToken vypršala.

Tabuľka 4-4 Chyby, typy a popisy nástroja KMS Admin Console (pokračovanie)

Kód chyby	Typ chyby	Opis
411	KmsAccessTokenInvalidTenantId	Poskytnutý AccessToken má neplatnú hodnotu TenantId.
412	KmsAccessTokenTenantIdMismatch	TenantId v poskytnutom AccessToken sa nezhoduje s funkciou aplikácie TenantId.
413	KmsInvalidKeyId	Údaj KeyId je nulový alebo prázdny.
414	KmsDeleteKeyUnauthorized	Používateľ nie je oprávnený odstraňovať kľúče. Používateľ nepatrí do autorizovanej skupiny AD, ktorá má povolenie spravovať toto rozhranie API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Pokus obnoviť tajný údaj zlyhal a nepodarilo sa ho obnoviť. Používateľ by to mal skúsiť znova.
416	KmsInvalidGetKeysRequest	Žiadosť o získanie kľúčov je neplatná.
417	KmsGetKeysUnauthorized	Používateľ nie je oprávnený získavať kľúče. Používateľ nepatrí do autorizovanej skupiny AD, ktorá má povolenie spravovať toto rozhranie API.
418	KmsInvalidRequestPayload	Požiadavka prijatá rozhraním API je neplatná.
419	KmSRequired	Doručená požiadavka nesmie byť prázdna.
420	KmsKeyNotConcurrent	Od posledného prevzatia kópie používateľom bol kľúč v úložisku tabuľky aktualizovaný alebo upravený.