



# Uživatelská příručka nástroje HP Sure Admin

## **SOUHRN**

Nástroj HP Sure Admin umožňuje správcům IT bezpečně spravovat citlivá nastavení firmwaru zařízení pomocí certifikátů a kryptografie s veřejným klíčem pro vzdálenou i místní správu nastavení namísto hesla.

## Právní informace

© Copyright 2019, 2021 HP Development Company, L.P.

Apple je ochranná známka společnosti Apple Computer, Inc., registrovaná v USA a dalších zemích.

Google Play je ochrannou známkou společnosti Google LLC.

Důvěryhodný software počítače. K držení, používání nebo kopírování se vyžaduje platná licence od společnosti HP. V souladu s ustanoveními FAR 12.211 a 12.212 jsou komerční počítačový software, počítačová softwarová dokumentace a technické údaje pro komerční položky licencované vládě USA pod standardní obchodní licencí dodavatele.

Informace zde uvedené mohou být bez předchozího upozornění změněny. Veškeré záruky poskytované na produkty a služby společnosti HP jsou popsány ve výslovném prohlášení o záruce přiloženém ke každému výrobku a službě. Žádné informace zde uvedené nelze považovat za rozšíření těchto záruk. Společnost HP nenese odpovědnost za technické nebo redakční chyby, ani za opomenutí vyskytující se v tomto dokumentu.

Druhé vydání: říjen 2021

První vydání: prosinec 2019

Číslo dokumentu: L83995-222

---

# Obsah

<b>1 Začínáme.....</b>	<b>1</b>
Použití aplikace HP Sure Admin .....	1
Zakázání aplikace HP Sure Admin .....	1
<b>2 Vytváření a správa klíčů.....</b>	<b>2</b>
Vytváření a exportování klíčů .....	2
Vytvoření a export klíče s ruční distribucí .....	2
Vytváření a exportování klíče pomocí Azure AD Revocation .....	3
Vytvořte a odešlete klíč do Azure AD Group OneDrive: .....	3
<b>3 Nastavení telefonu.....</b>	<b>5</b>
Použití telefonní aplikace HP Sure Admin k odemknutí systému BIOS .....	5
Získání přístupu k nastavení systému BIOS po registraci .....	5
Odemknutí systému BIOS s Azure AD Group OneDrive .....	5
<b>4 Chybové kódy HP Sure Admin .....</b>	<b>7</b>

# 1 Začínáme

Nástroj HP Sure Admin umožňuje správcům IT bezpečně spravovat citlivá nastavení firmwaru zařízení pomocí certifikátů a kryptografie s veřejným klíčem pro vzdálenou i místní správu nastavení namísto hesla.

Software HP Sure Admin se skládá z následujících částí:

- **Cílový počítač:** Platformy pro správu, které podporují režim Enhanced BIOS Authentication Mode (Rozšířené ověřování systému BIOS).
- **Sada HP Manageability Integration Kit (MIK):** Pro vzdálenou správu nastavení systému BIOS se používá doplněk pro nástroj System Center Configuration Manager (SCCM) nebo nástroj HP BIOS Configuration Utility (BCU).
- **HP Sure Admin Local Access Authenticator:** Telefonní aplikace, která nahrazuje heslo umožňující místní přístup k nastavení systému BIOS tak, že naskenujete kód QR, abyste získali jednorázový kód PIN.

## Použití aplikace HP Sure Admin


Tato část popisuje proces používání nástroje HP Sure Admin.

1. Spustíte nástroj HP Sure Admin, který je součástí sady nástrojů sady HP Manageability Integration Kit (MIK) pro nástroj System Configuration Manager (SCCM) nebo vylepšený Enhanced BIOS Configuration Utility (BCU).
2. Stáhněte si telefonní aplikaci HP Sure Admin v obchodě Google Play™ nebo v obchodě Apple App Store®.
3. Vytvořte dvojici klíčů, kterou používá cílové zařízení a telefonní aplikace HP Sure Admin, abyste získali jednorázový kód PIN pro odemknutí systému BIOS.


## Zakázání aplikace HP Sure Admin

Tato část popisuje možnosti, jak lze deaktivovat aplikaci HP Sure Admin:

- V nastavení systému BIOS F10 vyberte položku **Restore Security settings to Factory Defaults** (Obnovit nastavení zabezpečení na výchozí nastavení výrobce).

 **POZNÁMKA:** To vyžaduje fyzickou přítomnost pomocí autentizačního kódu PIN prostřednictvím telefonní aplikace HP Sure Admin pro přístup k nastavení F10.

- Použijte příkaz BCU pro vzdálené volání WMI z **Restore Security settings to Factory Defaults** (Obnovení nastavení zabezpečení na výchozí nastavení výrobce).

 **POZNÁMKA:** Další informace naleznete v uživatelské příručce nástroje HP BIOS Configuration Utility (BCU).

- Na stránce pro zajišťování zabezpečení MIK vyberte položku **Zrušení zajištění**.

## 2 Vytváření a správa klíčů

Před povolením rozšířeného režimu ověřování systému BIOS dokončete bezpečnostní opatření v rámci MIK. Chcete-li vytvořit a exportovat klíče, musí být povolen režim Enhanced BIOS Authentication Mode (Rozšířené ověřování systému BIOS). Povolení BIOS Authentication Mode (Režim ověřování BIOS):

- ▲ Chcete-li vytvořit a exportovat klíče, otevřete doplněk HP Sure Admin a vyberte možnost **Enhanced BIOS Authentication Mode** (Rozšířený režim ověřování systému BIOS).

### Vytváření a exportování klíčů

Existují tři různé způsoby, jak vytvořit dvojici místních přístupových klíčů a povolit telefonní aplikaci HP Sure Admin přístup ke klíči:

- [Vytvoření a export klíče s ruční distribucí na str. 2](#)
- [Vytváření a exportování klíče pomocí Azure AD Revocation na str. 3](#)
- [Vytvořte a odešlete klíč do Azure AD Group OneDrive: na str. 3](#)

### Vytvoření a export klíče s ruční distribucí

Tuto možnost použijte, chcete-li exportovat autorizační klíč pro místní přístup a poté jej ručně distribuovat do telefonní aplikace HP Sure Admin prostřednictvím e-mailu nebo jiné metody.



**POZNÁMKA:** Tato možnost nevyžaduje přístup k síti pro získání jednorázového kódu PIN pro telefonní aplikaci HP Sure Admin.

1. Zadejte název klíče do pole **Název klíče**.
2. Do pole **Přístupové heslo** zadejte heslo.



**POZNÁMKA:** Přístupové heslo se používá k ochraně exportovaného klíče a musí být zajištěno tak, aby uživatel telefonní aplikace HP Sure Admin mohl importovat tento klíč.

3. Vyberte položku **Procházet** a zvolte, kam chcete exportovat cestu v systému.
4. Vyberte položku **Vytvořit klíč**. Váš klíč se úspěšně vytvořil, když se vedle tlačítka **Vytvořit klíč** se zprávou „Úspěšné vytvoření klíče“ zobrazí ikona potvrzení.
5. Vyberte tlačítko **Další**. Na stránce Souhrn se zobrazí nastavení HP Sure Admin, která jste zadali.
6. Vyberte položku **Uložit pravidlo**. Toto pravidlo se uloží, když se zobrazí zpráva **Úspěšně uloženo**.
7. Přejděte do složky, do které jste klíč uložili, a distribuujte ji do telefonní aplikace HP Sure Admin pomocí metody, která je tomuto uživateli dostupná na tomto zařízení, například e-mailem. Tento uživatel bude také potřebovat přístupové heslo pro import klíče. Společnost HP doporučuje použití různých distribučních mechanismů pro daný klíč a přístupové heslo.



**POZNÁMKA:** Pokud posíláte kód QR, zašlete jej v původní velikosti. Aplikace nemůže správně načíst snímek, pokud je menší než 800 × 600.

## Vytváření a exportování klíče pomocí Azure AD Revocation

Tuto možnost použijte pro připojení místního přístupového klíče k určené skupině Azure Active Directory a vyžaduje, aby telefonní aplikace HP Sure Admin vyžadovala ověření uživatele pro službu Azure Active Directory a potvrzení, že je uživatel členem zadané skupiny, dříve, než je poskytnut kód PIN pro místní přístup. Tato metoda také vyžaduje manuální distribuci autorizačního klíče pro místní přístup k aplikaci telefonu prostřednictvím e-mailu nebo jiné metody.



**POZNÁMKA:** Tato možnost vyžaduje, aby byla telefonní aplikace HP Sure Admin vybavena síťovým přístupem, aby bylo možné získat jednorázový kód PIN.

1. Zadejte název klíče do pole **Název klíče**.
2. Do pole **Přístupové heslo** zadejte heslo.



**POZNÁMKA:** Přístupové heslo se používá k ochraně exportovaného klíče a musí být zajištěno tak, aby uživatel telefonní aplikace HP Sure Admin mohl importovat tento klíč.

3. Vyberte položku **Přihlášení Azure AD** a přihlaste se.
4. Vyberte název skupiny v rozevíracím seznamu **Název skupiny Azure AD**. Chcete-li mít přístup ke klíči, musíte být členem skupiny.
5. Vyberte položku **Procházet** a zvolte, kam chcete exportovat cestu v systému.
6. Vyberte položku **Vytvořit klíč**. Váš klíč se úspěšně vytvořil, když se vedle tlačítka **Vytvořit klíč** se zprávou „Úspěšné vytvoření klíče“ zobrazí ikona potvrzení.
7. Vyberte tlačítko **Další**. Na stránce Souhrn se zobrazí nastavení HP Sure Admin, která jste zadali.
8. Vyberte položku **Uložit pravidlo**. Toto pravidlo se uloží, když se zobrazí zpráva **Úspěšně uloženo**.
9. Přejděte do složky, do které jste klíč uložili, a distribuujte ji do telefonní aplikace HP Sure Admin pomocí metody, která je tomuto uživateli dostupná na tomto zařízení, například e-mailem. Tento uživatel bude také potřebovat přístupové heslo pro import klíče. Společnost HP doporučuje použití různých distribučních mechanismů pro daný klíč a přístupové heslo.



**POZNÁMKA:** Pokud posíláte kód QR, zašlete jej v původní velikosti. Aplikace nemůže správně načíst snímek, pokud je menší než 800 × 600.

## Vytvořte a odešlete klíč do Azure AD Group OneDrive:

(Doporučené) Tuto možnost použijte, chcete-li se vyhnout uložení autorizačního klíče pro místní přístup do telefonu. Když vyberete tuto možnost, MIK uloží autorizační klíč pro místní přístup do zadané složky OneDrive, která je dostupná pouze pro autorizovanou skupinu. Pokaždé, když je vyžadován kód PIN, bude muset uživatel telefonní aplikace HP Sure Admin provést ověření pro službu Azure AD.

1. Zadejte název klíče do pole **Název klíče**.
2. Do pole **Přístupové heslo** zadejte heslo.
3. Vyberte položku **Přihlášení Azure AD** a přihlaste se.
4. Vyberte název skupiny v rozevíracím seznamu **Název skupiny Azure AD**.



**POZNÁMKA:** Chcete-li mít přístup ke klíči, musíte být členem skupiny.

5. Do pole **OneDrive** zadejte název složky OneDrive, kam chcete klíč uložit.

6. Vyberte položku **Procházet** a zvolte, kam chcete exportovat cestu v systému.
7. Vyberte položku **Vytvořit klíč**.



---

**POZNÁMKA:** Váš klíč je úspěšně přidán do zadané složky OneDrive a exportován do zadané místní složky, když se vedle tlačítka **Vytvořit klíč** se zprávou **Úspěšně vytvořený klíč** zobrazí ikona potvrzení.

---

8. Vyberte tlačítko **Další**. Na stránce Souhrn se zobrazí nastavení HP Sure Admin, která jste zadali.
9. Vyberte položku **Uložit pravidlo**. Toto pravidlo se uloží, když se zobrazí zpráva **Úspěšně uloženo**.



---

**POZNÁMKA:** V tomto scénáři není třeba nic posílat do telefonní aplikace HP Sure Admin, aby se předběžně zajistila. Cílové počítače jsou nastaveny tak, aby ukazovaly na umístění OneDrive, které je obsaženo v kódu QR. Telefonní aplikace HP Sure Admin používá tento ukazatel pro přístup k umístění OneDrive, pokud je uživatel součástí autorizované skupiny a úspěšně se ověří.

---

## 3 Nastavení telefonu

Stáhněte si telefonní aplikaci HP Sure Admin z aplikace Google Play nebo Apple Store.

- Stáhněte si aplikaci HP Sure Admin z obchodu Google pro telefony se systémem Android.
- Stáhněte si HP Sure Admin z obchodu Apple pro telefony se systémem iOS.

### Použití telefonní aplikace HP Sure Admin k odemknutí systému BIOS

Mobilní aplikace HP Sure Admin nahrazuje použití hesla systému BIOS pro místní přístup k nástroji nastavení systému BIOS tím, že poskytuje jednorázový kód PIN získaný naskenováním kódu QR předkládaného cílovým zařízením.

Tyto kroky použijte k uložení klíče lokálně v telefonu v situaci, kdy je klíč odeslán uživateli telefonní aplikace. V následujícím příkladu je klíč odeslán e-mailem uživateli telefonní aplikace HP Sure Admin a uživatel otevře e-mail v telefonu.

1. Otevřete e-mailovou zprávu, která obsahuje klíč.
2. Když se zobrazí stránka **Registrace**, zadejte heslo do pole **Zadejte heslo** a svou e-mailovou adresu do pole **Zadejte svou e-mailovou adresu** pro dešifrování klíče a přidejte jej do aplikace HP Sure Admin. Kód PIN pro odemknutí je zobrazen na stránce **Váš kód PIN**.



**POZNÁMKA:** Tento krok uloží klíč do mobilního zařízení a dokončí registraci. V tuto chvíli můžete použít telefonní aplikaci HP Sure Admin pro přístup k jakémukoli zařízení, které bylo nastaveno, aby bylo přístupné pomocí tohoto klíče. E-mailová adresa je vyžadována pouze v případě, že to vyžaduje správce.

3. Zadejte kód PIN do pole **Zadejte kód odpovědi systému BIOS**.

### Získání přístupu k nastavení systému BIOS po registraci

Chcete-li získat přístup k nastavení systému BIOS na cílovém zařízení po registraci:

1. Na cílovém zařízení v průběhu zavádění operačního systému vstupte do systému BIOS.
2. V aplikaci telefonu vyberte možnost **Naskenovat kód QR** a naskenujte kód QR na cílovém zařízení.
3. Pokud budete vyzváni k ověření uživatele, zadejte svá pověření.
4. Odemknutý kód PIN se zobrazí na stránce **Váš kód PIN**.
5. Zadejte kód PIN do pole **BIOS Enter Response Code** (Zadejte kód BIOS odpovědi) na cílovém zařízení.

### Odemknutí systému BIOS s Azure AD Group OneDrive

Chcete-li použít nástroj HP Sure Admin k odemknutí systému BIOS s Azure AD Group OneDrive:

1. Vyberte položku **Skenovat kód QR** a poté naskenujte kód QR systému BIOS.



**POZNÁMKA:** Aplikace HP Sure Admin zobrazí přihlašovací stránku Azure AD.



2. Přihlaste se ke svému účtu Azure.
3. Zadejte kód PIN do pole **Zadejte kód odpovědi systému BIOS**.



---

**POZNÁMKA:** Aplikace HP Sure Admin v tomto scénáři neukládá klíč místně. Telefonní aplikace HP Sure Admin musí mít přístup k síti a uživatel musí být ověřen pokaždé, když je potřeba jednorázový kód PIN.

---

## 4 Chybové kódy HP Sure Admin

V tabulce v této části naleznete chybové kódy, typy a jejich popisy v HP Sure Admin a KMS Admin Console.

**Tabulka 4-1** Chybové kódy, typy a jejich popisy v aplikaci HP Sure Admin

Chybový kód	Typ chyby	Popis
100	QRCodeUnknownError	Obecná chyba.
101	QRCodeDeserialization	Nelze načíst kód QR JSON. Buď řetězec není v platném souboru JSON, nebo jsou data neplatná.
102	QRCodeInvalidImage	Tento snímek kódu QR je neplatný. Nelze načíst soubor obrazu QR kódu.
103	QRCodeNoPayload	Tento snímek kódu QR je neplatný. Soubor snímku nemá datovou část JSON.
104	QRCodeInvalid	Nelze načíst kód QR JSON. Buď řetězec není platným formátem JSON, nebo jsou data ve snímku QR neplatná.
105	QRCodeInvalidKeyldHash	Hash veřejného klíče v kódu QR JSON neodpovídá hashi veřejného klíče zápisového balíčku (údaje KeyID).
106	QRCodeTampered	Kód QR v naskenovaném snímku byl neoprávněně změněn a je neplatný.
107	QRCodeTamperedOrInvalidPassPhrase	Kód QR v naskenovaném snímku byl neoprávněně změněn a je neplatný nebo je zadané heslo nesprávné.

**Tabulka 4-2** Chyby, typy a popisy přístupového klíče OneTime z OneDrive

Chybový kód	Typ chyby	Popis
200	OneTimeKeyError	Obecná chyba.
201	OneTimeKeyNoUserGroups	Přihlášený uživatel nepatří do žádné skupiny AD, která je ve vaší organizaci.
203	OneTimeKeyInvalidUserGroup	Přihlášený uživatel nepatří do skupiny AD, ke které je tento klíč přiřazen.
204	OneTimeKeyQRFileDoesNotExist	Soubor s klíčem OneTime neexistuje ve složce OneDrive pro skupinu AD.
205	OneTimeKeyInvalidQRFile	Soubor s klíčem One Time ve složce OneDrive skupiny AD je neplatný.
206	OneTimeKeyInvalidQRpayload	Soubor s klíčem OneTime existuje, ale nelze číst datovou část souboru.

**Tabulka 4-3 Chyby ověřování Azure AD**

Chybový kód	Typ chyby	Popis
300	AzureADUnknownError	Obecná chyba.
301	AzureADInvalidDomain	Zadaná e-mailová adresa neodpovídá názvu domény, který je uveden ve snímku QR.
302	AzureADAccessToken	Chyba při získávání přístupového tokenu z Azure AD. Buď se uživatel nemůže přihlásit k Azure AD vaší organizace, nebo aplikace nemá požadovaná oprávnění pro připojení k Azure AD vaší organizace. Může se také stát, že uživatel ověřování zrušil.
303	AzureADUserProfile	Aplikace HP Sure Admin byla povolena k získání informací o uživatelském profilu z Azure AD vaší organizace.
304	AzureADUserPrincipalMismatch	Zadaná e-mailová adresa neodpovídá hlavnímu jménu přihlášeného uživatele.
305	AzureADUserInvalidUserGroup	Přihlášený uživatel nepatří do skupiny AD, ke které je tento klíč přiřazen.

**Tabulka 4-4 Chyby, typy a jejich popisy v KMS Admin Console**

Chybový kód	Typ chyby	Popis
401	KmsUnauthorized	Uživatel není oprávněn používat službu KMS.
402	KmsKeyDoesNotExist	V trezoru klíčů KMS neexistuje odpovídající soukromý klíč. Klíč je v současné době ve stavu odstraněný, ale obnovitelný, a jeho název nelze v tomto stavu znovu použít. Klíč lze pouze obnovit nebo vymazat.
403	KmsKeyDoesNotExistInTableStorage	Klíč v úložišti tabulky neexistuje.
404	KmsUploadKeyErrorInKeyVault	Při přidávání klíče do trezoru klíčů došlo k chybě.
405	KmsUploadKeyUnauthorized	Uživatel nemá oprávnění k nahrávání klíčů. Uživatel nepatří do autorizované skupiny AD s povolením volat toto rozhraní API.
406	KmsInvalidAzureADLogin	Uživatel není přihlášen v Azure Tenant AAD.
407	KmsNoUserGroups	Přihlášený uživatel nepatří do žádné skupiny AD ve vaší organizaci.
408	KmsInvalidUserGroup	Přihlášený uživatel nepatří do skupiny AD, ke které je tento klíč přiřazen.
409	KmsInvalidAccessToken	Přístupový token, který byl poskytnut v požadavku, je neplatný.
410	KmsAccessTokenExpired	Platnost poskytnutého přístupového tokenu vypršela.
411	KmsAccessTokenInvalidTenantId	Poskytnutý přístupový token má neplatnou hodnotu TenantId.

**Tabulka 4-4 Chyby, typy a jejich popisy v KMS Admin Console (pokračování)**

Chybový kód	Typ chyby	Popis
412	KmsAccessTokenTenantIdMismatch	TenantId v zadaném přístupovém tokenu se neshoduje s TenantId aplikace funkce.
413	KmsInvalidKeyId	KeyId je nulový nebo prázdný.
414	KmsDeleteKeyUnauthorized	Uživatel není oprávněn mazat klíče. Uživatel nepatří do autorizované skupiny AD s povolením volat toto rozhraní API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Pokus o obnovení tajemství selhal a nepodařilo se jej obnovit. Uživatel by to měl zkusit znovu.
416	KmsInvalidGetKeysRequest	Požadavek na získání klíčů je neplatný.
417	KmsGetKeysUnauthorized	Uživatel nemá oprávnění k získání klíčů. Uživatel nepatří do autorizované skupiny AD s povolením volat toto rozhraní API.
418	KmsInvalidRequestPayload	Požadavek přijatý rozhraním API je neplatný.
419	KmsRequestRequired	Přijatý požadavek nesmí být prázdný.
420	KmsKeyNotConcurrent	Klíč v úložišti tabulky byl aktualizován nebo změněn od posledního načtení kopie uživatelem.