



Uživatelská příručka

HP Sure Admin

© Copyright 2019 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.

Důvěrný 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 uvedené v této příručce se mohou
změnit bez předchozího upozornění. Jediné
záruky na produkty a služby společnosti HP
jsou výslovně uvedeny v prohlášení o záruce,
které je každému z těchto produktů a služeb
přiloženo. Žádná ze zde uvedených informací
nezakládá další záruky. Společnost HP není
zodpovědná za technické nebo redakční chyby
ani za opomenutí vyskytující se v tomto
dokumentu.

První vydání: prosinec 2019

Číslo dokumentu: L83995-221

Obsah

1 Začínáme	1
Použití aplikace HP Sure Admin	1
Zakázání aplikace HP Sure Admin	1
2 Vytváření a správa klíčů	2
Vytváření a exportování klíčů	2
3 Nastavení telefonu	5
Použití telefonní aplikace HP Sure Admin k odemknutí systému BIOS	5

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:** 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

Proces použití aplikace HP Sure Admin je následující:

1. Spusťte nástroj HP Sure Admin, který je součástí sady nástrojů sady HP Manageability Integration (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

Níže uvádíme 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

Vyberte jeden z následujících modelů, abyste vytvořili dvojici místních přístupových klíčů a povolili telefonní aplikaci HP Sure Admin přístup ke klíči:


- **Vytvořit a exportovat klíč** – 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.

- **Vytvořit a exportovat klíč s 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.

- **Vytvoření a odeslání klíče k 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.


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

Chcete-li vytvořit a exportovat klíč:


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**.

 **POZNÁMKA:** 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**.


 **POZNÁMKA:** 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.

Chcete-li vytvořit a exportovat klíč pomocí Azure AD Revocation:


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**.

 **POZNÁMKA:** 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**.

 **POZNÁMKA:** 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**.

 **POZNÁMKA:** Toto pravidlo se uloží, když se zobrazí zpráva.

9. Přejděte do složky, do které jste klíč uložili, a distribuujte ji pomocí mechanismu, který je uživateli k dispozici v tomto zařízení, například e-mailu. Tento uživatel bude také potřebovat přístupové heslo pro import klíče. Pro klíč a přístupové heslo se doporučuje použít různé distribuční mechanismy.


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

Chcete-li vytvořit a odeslat klíč do Azure AD Group OneDrive:


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**.

 **POZNÁMKA:** Toto pravidlo se uloží, když se zobrazí zpráva **Úspěšně uloženo**.

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.

Registrace klíčů v telefonní aplikaci HP Sure Admin:

Tyto kroky použijte pro uložení klíče místně na telefonu ve scénáři, kde je klíč odeslán uživateli telefonní aplikace. V následujícím příkladu je klíč e-mailem zaslán uživateli telefonní aplikace HP Sure Admin a uživatel otevře e-mailovou zprávu na 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.

 **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.

Kód PIN pro odemknutí je zobrazen na stránce **Váš kód PIN**.

3. Zadejte kód PIN do pole **Enter Response Code** (Zadejte kód odpovědi) systému BIOS.

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.

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 **Enter Response Code** (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.

Tabulka 3-1 Chybové kódy

Chybový kód	Popis
100	Obecná chyba.
101	Nelze přečíst kód QR json. Buď není řetězec platným formátem JSON, nebo jsou data neplatná.
102	Tento snímek kódu QR je neplatný. Nelze načíst soubor obrazu QR kódu.
103	Tento snímek kódu QR je neplatný. Soubor obrazu nemá datovou část JSON.
104	Nelze přečíst kód QR json. Buď řetězec není platným formátem JSON, nebo jsou data v obrázku QR neplatná.
105	Algoritmus hash veřejného klíče v kódu QR json neodpovídá algoritmu hash veřejného klíče balíčku registrace (KeyID data).
200	Obecná chyba.
201	Přihlášený uživatel nepatří do žádné skupiny AD ve vaší organizaci.
203	Přihlášený uživatel nepatří do přiřazené skupiny AD pro tento klíč.
204	Soubor s jednorázovým klíčem neexistuje ve složce OneDrive pro skupinu AD.
205	Soubor s jednorázovým klíčem ve složce OneDrive skupiny AD je neplatný.
206	Soubor s jednorázovým klíčem existuje, ale nelze číst datovou část souboru.
300	Obecná chyba.
301	E-mailová adresa neodpovídá názvu domény v obrázku QR kódu.
302	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.
303	Aplikace BEAM nemůže získat informace o uživatelském profilu z Azure AD vaší organizace.
304	E-mailová adresa neodpovídá hlavnímu jménu přihlášeného uživatele.
305	Přihlášený uživatel nepatří do přiřazené skupiny Azure AD pro tento klíč.