



# Ръководство за потребителя за HP Sure Admin

## РЕЗЮМЕ

HP Sure Admin позволява на ИТ администраторите да управляват защитено чувствителни настройки на фърмуера на дадено устройство с помощта на сертификати и шифроване с публични ключове вместо с парола както за отдалечено, така и за локално управление на настройки.

## Правна информация

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

Apple е търговска марка на Apple Computer, Inc., регистрирана в САЩ и други държави.

Google Play е търговска марка на Google LLC.

Конфиденциален софтуер за компютър.  
За притежание, употреба или копиране е нужен валиден лиценз от HP.  
Съгласно FAR 12.211 и 12.212 търговският компютърен софтуер, документацията на компютърния софтуер и техническите данни за търговските артикули са лицензирани пред правителството на САЩ по стандартен търговски лиценз на доставчика.

Информацията, съдържаща се тук, подлежи на промяна без предизвестие. Единствените гаранции, валидни за продуктите и услугите на HP, са изрично описани в гаранционните условия към тези продукти и услуги.  
Нищо от съдържащото се в настоящия документ не трябва да се подразбира като допълнителна гаранция. HP не носи отговорност за технически или редакционни грешки или пропуски, съдържащи се в настоящия документ.

Второ издание: октомври 2021 г.

Първо издание: декември 2019 г.

Номенклатурен номер на документа:  
L83995-262

---

# Съдържание

<b>1 Начални стъпки .....</b>	<b>1</b>
Използване на HP Sure Admin.....	1
Деактивиране на HP Sure Admin .....	1
<b>2 Създаване и управление на ключове .....</b>	<b>2</b>
Създаване и експортиране на ключове.....	2
Създаване и експортиране на ключ с ръчно предоставяне .....	2
За да създадете и експортирате ключ с Azure AD анулиране:.....	3
Създаване и изпращане на ключ до груповия OneDrive на Azure AD .....	3
<b>3 Настройка на телефона .....</b>	<b>5</b>
Използване на приложението за телефон HP Sure Admin за отключване на BIOS .....	5
Получаване на достъп до настройката на BIOS след регистриране.....	5
Отключване на BIOS с групов Azure AD OneDrive .....	6
<b>4 Кодове за грешки на HP Sure Admin .....</b>	<b>7</b>

# 1 Начални стъпки

HP Sure Admin позволява на ИТ администраторите да управляват защитено чувствителни настройки на фърмуера на дадено устройство с помощта на сертификати и шифроване с публични ключове вместо с парола както за отдалечено, така и за локално управление на настройки.

HP Sure Admin се състои от следните части:

- **Целеви компютър:** Платформите за управление, които поддържат Enhanced BIOS Authentication Mode (Разширен режим за удостоверяване на BIOS).
- **HP Manageability Integration Kit (MIK, Комплект за интеграция за управляемост на HP):** Добавката за System Center Configuration Manager (SCCM) или HP BIOS Configuration Utility (BCU) за отдалечено управление на настройките на BIOS.
- **HP Sure Admin Local Access Authenticator:** Приложение за телефон, което замества паролата, за да разреши локален достъп до настройката на BIOS чрез сканиране на QR код, за да се получи еднократен ПИН код.



## Използване на HP Sure Admin

Този раздел описва процеса на използване на HP Sure Admin.

1. Отворете добавката HP Sure Admin в рамките на добавката HP Manageability Integration Kit (MIK) за System Configuration Manager (SCCM) или Enhanced BIOS Configuration Utility (BCU).
2. Изтеглете приложението за телефон HP Sure Admin от Google Play™ Магазин или от Apple App Store®.
3. Създайте двойка ключове, използвани от целевото устройство и приложението за телефон HP Sure Admin, за да получите еднократен ПИН код за отключване на BIOS.

## Деактивиране на HP Sure Admin

Тази секция описва опциите за деактивиране на HP Sure Admin.

- В настройката на BIOS F10 изберете **Restore Security settings to Factory Defaults** (Възстановяване на настройките за защита до фабричните настройки по подразбиране).
- 
-  **ЗАБЕЛЕЖКА:** Това изисква физическо присъствие чрез предоставяне на ПИН код за удостоверяване чрез приложението за телефон HP Sure Admin с цел осъществяване на достъп до настройките на F10.
- 
- Използвайте команда на BCU за отдалечено повикване на WMI от **Restore Security settings to Factory Defaults** (Възстановяване на настройките за защита до фабричните настройки по подразбиране).
- 
-  **ЗАБЕЛЕЖКА:** За повече информация вижте ръководството за потребителя на HP BIOS Configuration Utility (BCU).
- 
- В страницата за осигуряване на защитата на MIK изберете **Deprovision** (Премахване на осигуряване).

## 2 Създаване и управление на ключове

Завършете осигуряването на защитата в рамките на MTK, преди да активирате Enhanced BIOS Authentication Mode (Разширен режим за удостоверяване на BIOS). Enhanced BIOS Authentication Mode (Разширен режим за удостоверяване на BIOS) трябва да бъде активиран, за да можете да създавате и експортирате ключове. За да активирате BIOS Authentication Mode (Режим за удостоверяване на BIOS):

- ▲ Отворете добавката HP Sure Admin и изберете **Enhanced BIOS Authentication Mode** (Разширен режим за удостоверяване на BIOS), за да създадете и експортирате ключове.

### Създаване и експортиране на ключове

Има три различни начина, за да създадете двойки ключове за локален достъп и да активирате приложението за телефон HP Sure Admin, за да осъществите достъп до ключа:

- [Създаване и експортиране на ключ с ръчно предоставяне на страница 2](#)
- [За да създадете и експортирате ключ с Azure AD анулиране: на страница 3](#)
- [Създаване и изпращане на ключ до груповия OneDrive на Azure AD на страница 3](#)

### Създаване и експортиране на ключ с ръчно предоставяне

използвайте тази опция, за да експортирате ключ за удостоверяване за локален достъп, след което ръчно го предоставете на приложението за телефон HP Sure Admin чрез имейл или друг метод.



**ЗАБЕЛЕЖКА:** Тази опция не изисква мрежов достъп за приложението за телефон HP Sure Admin за получаване на еднократен ПИН код.

1. Наименувайте ключа в полето за въвеждане **Key Name** (Наименование на ключ).
2. Въведете фразата за достъп в полето за въвеждане **Passphrase** (Фраза за достъп).



**ЗАБЕЛЕЖКА:** Фразата за достъп се използва за защита на експортирания ключ и трябва да се предостави, за да може потребителят на приложението за телефон HP Sure Admin да импортира ключа.

3. Изберете **Browse** (Преглед) и изберете къде да експортирате пътя в системата.
4. Изберете **Create Key** (Създаване на ключ). Вашият ключ е създаден успешно, когато до бутона **Create Key** (Създаване на ключ) се появи икона за уведомяване със съобщението „**Key successfully created**“ (Ключът е създаден успешно).
5. Изберете **Напред**. Страницата с резюме показва въведените от вас настройки на HP Sure Admin.
6. Изберете **Save Policy** (Записване на правилата). Правилата са записани, когато се появи съобщението **Saved successfully** (Успешно записване).
7. Навигирайте до папката, където сте записали ключа, и го предоставете на потребителя на приложението за телефон HP Sure Admin, като използвате метод, който е наличен за конкретния потребител на конкретното устройство, като например имейл. Този потребител също така ще се

нуждае от фразата за достъп, за да импортира ключа. HP препоръчва да използвате различни механизми за предоставяне на ключа и на фразата за достъп.



**ЗАБЕЛЕЖКА:** Изпращайте QR кода в оригиналния му размер. Приложението не може да прочете изображението правилно, ако размерът му е по-малък от 800 × 600.

## За да създадете и експортирате ключ с Azure AD анулиране:

използвайте тази опция, за да свържете ключа за локален достъп към указана група на Azure Active Directory и да изискате приложението за телефон HP Sure Admin да изисква както удостоверяване на потребителя за Azure Active Directory, така и потвърждение, че потребителят е член на указаната група, преди да се предостави ПИН код за локален достъп. Този метод също така изисква ръчно предоставяне на ключа за удостоверяване за локален достъп до приложението за телефон чрез имейл или друг метод.



**ЗАБЕЛЕЖКА:** Тази опция изисква приложението за телефон HP Sure Admin да има мрежов достъп с цел получаване на еднократен ПИН код.

1. Наименувайте ключа в полето за въвеждане **Key Name** (Наименование на ключ).
2. Въведете фразата за достъп в полето за въвеждане **Passphrase** (Фраза за достъп).



**ЗАБЕЛЕЖКА:** Фразата за достъп се използва за защита на експортирания ключ и трябва да се предостави, за да може потребителят на приложението за телефон HP Sure Admin да импортира ключа.

3. Изберете **Azure AD Login** (Вход в Azure AD) и влезте в системата.
4. Изберете името на групата от падащото меню **Azure AD Group Name** (Име на група в Azure AD). Трябва да сте член на групата, за да имате достъп до ключа.
5. Изберете **Browse** (Преглед) и изберете къде да експортирате пътя в системата.
6. Изберете **Create Key** (Създаване на ключ). Вашият ключ се създава успешно, когато до бутона **Create Key** (Създаване на ключ) се появи икона за уведомяване със съобщението „Key successfully created“ (Ключът е създаден успешно).
7. Изберете **Напред**. Страницата с резюме показва въведените от вас настройки на HP Sure Admin.
8. Изберете **Save Policy** (Записване на правилата). Правилата са записани, когато се появи съобщението **Saved successfully** (Успешно записване).
9. Навигирайте до папката, където сте записали ключа, и го предоставете на потребителя на приложението за телефон HP Sure Admin, като използвате метод, който е наличен за конкретния потребител на конкретното устройство, като например имейл. Този потребител също така ще се нуждае от фразата за достъп, за да импортира ключа. HP препоръчва да използвате различни механизми за предоставяне на ключа и на фразата за достъп.



**ЗАБЕЛЕЖКА:** Изпращайте QR кода в оригиналния му размер. Приложението не може да прочете изображението правилно, ако размерът му е по-малък от 800 × 600.

## Създаване и изпращане на ключ до груповия OneDrive на Azure AD

(препоръчително) използвайте тази опция, за да избегнете съхраняване на ключа за удостоверяване за локален достъп на телефона. Когато изберете тази опция, MİK ще съхрани ключа за удостоверяване за локален достъп в указаната папка на OneDrive, която е достъпна само за упълномощената група.

От потребителя на приложението за телефон HP Sure Admin ще се изисква удостоверяване в Azure AD всеки път, когато е необходим ПИН код.

1. Наименувайте ключа в полето за въвеждане **Key Name** (Наименование на ключ).
2. Въведете фразата за достъп в полето за въвеждане **Passphrase** (Фраза за достъп).
3. Изберете **Azure AD Login** (Вход в Azure AD) и влезте в системата.
4. Изберете името на групата от падащото меню Azure AD Group Name (Име на група в Azure AD).



**ЗАБЕЛЕЖКА:** Трябва да сте член на групата, за да имате достъп до ключа.

5. В полето за въвеждане **OneDrive** въведете името на папката в OneDrive, където искате ключът да бъде записан.
6. Изберете **Browse** (Преглед) и изберете къде да експортирате пътя в системата.
7. Изберете **Create Key** (Създаване на ключ).



**ЗАБЕЛЕЖКА:** Вашият ключ е добавен успешно в указаната папка в OneDrive и е експортиран в указаната локална папка, когато до бутона **Create Key** (Създаване на ключ) се появи икона за уведомяване със съобщението **Key successfully created** (Ключът е създаден успешно).

8. Изберете **Напред**. Страницата с резюме показва въведените от вас настройки на HP Sure Admin.
9. Изберете **Save Policy** (Записване на правилата). Правилата са записани, когато се появи съобщението **Saved successfully** (Успешно записване).



**ЗАБЕЛЕЖКА:** В този случай не е необходимо да изпращате нищо до приложението за телефон HP Sure Admin с цел предварителното им предоставяне. Осигурено е целевите компютри да посочват местоположението на OneDrive, включено в QR кода. Приложението за телефон HP Sure Admin използва този показалец за осъществяване на достъп до местоположението на OneDrive, ако потребителят е част от упълномощената група и успешно се удостовери.

## 3 Настройка на телефона

Изтеглете приложението за телефон HP Sure Admin от Google Play или магазина на Apple.

- Изтеглете HP Sure Admin от магазина на Google за телефони с Android.
- Изтеглете HP Sure Admin от магазина на Apple за телефони с iOS.

### Използване на приложението за телефон HP Sure Admin за отключване на BIOS

Мобилното приложение HP Sure Admin замества използването на паролата на BIOS за локален достъп до настройката на BIOS, като предоставя еднократен ПИН код, получен чрез сканиране на предоставения от целевата машина QR код.

Използвайте тези стъпки, за да запишете ключа локално на телефона в случай, когато ключът се изпраща към приложението за телефон на потребителя. В следния пример ключът се изпраща по имейл на приложението HP Sure Admin на телефона на потребителя и потребителят отваря имейла на телефона.

1. Отворете имейла, който съдържа ключа.
2. Когато се покаже страницата **Enrollment** (Регистриране), въведете фразата за достъп в полето за въвеждане **Enter passphrase** (Въведете фраза за достъп), а имейл адреса си в полето за въвеждане **Enter your email address** (Въведете имейл адрес), за да дешифрирате ключа и да го добавите в приложението HP Sure Admin. ПИН кодът за отключване се показва на страницата **Your PIN** (Вашият ПИН код).



**ЗАБЕЛЕЖКА:** Тази стъпка записва ключа на мобилното устройство и завършва регистрирането. В този момент можете да използвате приложението за телефон HP Sure Admin, за да осъществите достъп до всяко устройство, за което е осигурена достъпност чрез този ключ. Необходим е имейл адрес само ако администраторът го изисква.

3. Въведете ПИН кода в полето за въвеждане **Enter Response Code** (Въведете код за отговор) на BIOS.

### Получаване на достъп до настройката на BIOS след регистриране

За да получите достъп до настройките на BIOS на дадена целева машина след регистриране:

1. Влезте в настройката на BIOS при зареждане на целевата машина.
2. Изберете **Scan QR Code** (Сканиране на QR код) в приложението на телефона и сканирайте QR кода на целевата машина.
3. Ако получите подкана за удостоверяване на потребителя, предоставете идентификационните си данни.
4. Отключеният ПИН код се показва на страницата **Your PIN** (Вашият ПИН код).
5. Въведете ПИН кода в полето за въвеждане **BIOS Enter Response Code** (Въведете код за отговор на BIOS) на целевата машина.



## Отключване на BIOS с групов Azure AD OneDrive

За да използвате HP Sure Admin за отключване на BIOS с груповия OneDrive на Azure AD:

1. Изберете **Scan QR Code** (Сканиране на QR код), след което сканирайте QR кода на BIOS.



---

**ЗАБЕЛЕЖКА:** Приложението HP Sure Admin показва страницата за влизане в Azure AD.

---

2. Влезте в акаунта си в Azure.

3. Въведете ПИН кода в полето за въвеждане **Enter Response Code** (Въведете код за отговор) на BIOS.



---

**ЗАБЕЛЕЖКА:** В този случай приложението HP Sure Admin не записва ключа локално.

Приложението за телефон HP Sure Admin трябва да има мрежов достъп и потребителят трябва да се удостоверява всеки път, когато е необходим еднократен ПИН код.

---

## 4 Кодове за грешки на HP Sure Admin

Използвайте таблицата в този раздел, за да видите кодовете за грешки, типовете и техните описания на HP Sure Admin и KMS Admin Console.

**Таблица 4-1** Кодове за грешки, видове и описанията им за HP Sure Admin

Код на грешка	Тип грешка	Описание
100	QRCodeUnknownError	Обща грешка.
101	QRCodeDeserialization	Не може да се прочете QR код JSON. Низът не е валиден json или данните са невалидни.
102	QRCodeInvalidImage	Сканираното изображение на QR код е невалидно. Файлт с изображение на QR код не може да бъде прочетен.
103	QRCodeNoPayload	Сканираното изображение на QR код е невалидно. Файлт с изображение няма json полезен обем.
104	QRCodeInvalid	Json на QR кода не може да бъде прочетен. Низът не е валиден json или данните в изображението на QR кода са невалидни.
105	QRCodeInvalidKeyldHash	Хешът на публичния ключ в json на QR кода не съвпада с хеша на публичния ключ на пакета за регистриране (KeyID данни).
106	QRCodeTampered	Сканираното изображение на QR код е манипулирано и невалидно.
107	QRCodeTamperedOrInvalidPassPhrase	Сканираното изображение с QR код е манипулирано и невалидно или въведената фраза за достъп е неправилна.

**Таблица 4-2** Клавиш за достъп OneTime от грешки в OneDrive, типове и техните описания

Код на грешка	Тип грешка	Описание
200	OneTimeKeyError	Обща грешка.
201	OneTimeKeyNoUserGroups	Влезият в системата потребител не принадлежи към никоя група в AD във вашата организация.
203	OneTimeKeyInvalidUserGroup	Влезият в системата потребител не принадлежи към възложената група в AD за този ключ.
204	OneTimeKeyQRFileDoesNotExist	Файлт с еднократния ключ не съществува в папката в груповия OneDrive на AD.
205	OneTimeKeyInvalidQRFile	Файлт с еднократния ключ в папката в OneDrive на групата в AD е невалиден.

**Таблица 4-2** Клавиш за достъп OneTime от грешки в OneDrive, типове и техните описания (продължение)

Код на грешка	Тип грешка	Описание
206	OneTimeKeyInvalidQRpayload	Файлът с еднократния ключ съществува, но полезният обем на файла не може да бъде прочетен.

**Таблица 4-3** Грешки при удостоверяване на Azure AD

Код на грешка	Тип грешка	Описание
300	AzureADUnknownError	Обща грешка.
301	AzureADInvalidDomain	Имейл адресът не съвпада с името на домейна в изображението на QR кода.
302	AzureADAccessToken	Грешка при придобиване на маркер за достъп от Azure AD. Потребителят не може да влезе в Azure AD на вашата организация или приложението няма необходимите разрешения за свързване с Azure AD на вашата организация. Също така е възможно потребителят да е отменил удостоверяването.
303	AzureADUserProfile	Приложението HP не може да получи информация за потребителския профил от Azure AD на вашата организация.
304	AzureADUserPrincipalMismatch	Имейл адресът не съвпада с основното име на влезлия в системата потребител.
305	AzureADUserInvalidUserGroup	Влезният в системата потребител не принадлежи към възложената група в Azure AD за този ключ.

**Таблица 4-4** Грешки, типове и описанията им за KMS Admin Console

Код на грешка	Тип грешка	Описание
401	KmsUnauthorized	Потребителят не е упълномощен да използва KMS услугата.
402	KmsKeyDoesNotExist	Подходящ частен ключ не съществува в хранилището за ключове KMS. Ключът в момента е изтрит, но е във възстановимо състояние и името му не може да се използва повторно в това състояние. Ключът може само да се възстанови или изчисти.
403	KmsKeyDoesNotExistInTableStorage	Клавишът не съществува в хранилището на таблицата.
404	KmsUploadKeyErrorInKeyVault	Възникнала е грешка при добавяне на ключ към хранилището за ключове.
405	KmsUploadKeyUnauthorized	Потребителят няма право да качва ключове. Потребителят не е упълномощен от AD Group, който е упълномощен да извиква този API.
406	KmsInvalidAzureADLogin	Потребителят не е влязъл в Azure Tenant AAD.

**Таблица 4–4** Грешки, типове и описанията им за KMS Admin Console (продължение)

Код на грешка	Тип грешка	Описание
407	KmsNoUserGroups	Влезният в системата потребител не принадлежи към никоя група в AD във вашата организация.
408	KmsInvalidUserGroup	Влезният в системата потребител не принадлежи към възложената група в AD за този ключ.
409	KmsInvalidAccessToken	Маркерът за достъп, предоставен в заявката, е невалиден.
410	KmsAccessTokenExpired	Предоставеният маркер за достъп е изтекъл.
411	KmsAccessTokenInvalidTenantId	Предоставеният маркер за достъп има невалидна стойност за TenantId.
412	KmsAccessTokenTenantIdMismatch	TenantId в предоставения маркер за достъп не съответства на функционалното приложение TenantId.
413	KmsInvalidKeyId	Идентификационният код на ключа е нула или е празен.
414	KmsDeleteKeyUnauthorized	Потребителят няма право да изтрива ключове. Потребителят не е упълномощен от AD Group, който е упълномощен да извиква този API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Опитът за възстановяване на тайната е неуспешен и не може да бъде възстановена. Потребителят трябва да опита отново.
416	KmsInvalidGetKeysRequest	Заявката Get Keys е невалидна.
417	KmsGetKeysUnauthorized	Потребителят не е упълномощен да получава ключове. Потребителят не е упълномощен от AD Group, който е упълномощен да извиква този API.
418	KmsInvalidRequestPayload	Заявката, получена от API, е невалидна.
419	KmsRequestRequired	Получената заявка трябва да не е празна.
420	KmsKeyNotConcurrent	Ключът в хранилището на таблицата е актуализиран или променен след последното възстановяване на копие от потребителя.