Gebruikershandleiding HP Sure Admin

SAMENVATTING

Met HP Sure Admin kunnen IT-beheerders op een veilige manier de firmware-instellingen van gevoelige apparaten beheren met certificaten en cryptografie voor openbare sleutels voor zowel het externe als het lokale beheer van instellingen in plaats van een wachtwoord.

Juridische informatie

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

Apple is een handelsmerk van Apple Computer Inc., gedeponeerd in de Verenigde Staten en andere landen.

Google Play is een handelsmerk van Google LLC.

Vertrouwelijke computersoftware. Voor het bezit, gebruik of kopiëren hiervan is een geldige licentie van HP vereist. Conform FAR 12.211 en 12.212 worden commerciële computersoftware, computersoftwaredocumentatie en technische gegevens voor commerciële artikelen onder een standaard commerciële licentie van de leverancier aan de Amerikaanse overheid in licentie gegeven.

De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd. De van toepassing zijnde garanties voor producten en diensten van HP zijn vastgelegd in de uitdrukkelijke garantiebepalingen die bij dergelijke producten en diensten worden meegeleverd. Niets in dit document mag als een aanvullende garantie worden opgevat. HP is niet aansprakelijk voor technische fouten, drukfouten of weglatingen in dit document.

Tweede editie: oktober 2021

Eerste editie: december 2019

Artikelnummer van document: L83995-332

Inhoudsopgave

1 Aan de slag

Met HP Sure Admin kunnen IT-beheerders op een veilige manier de firmware-instellingen van gevoelige apparaten beheren met certificaten en cryptografie voor openbare sleutels voor zowel het externe als het lokale beheer van instellingen in plaats van een wachtwoord.

HP Sure Admin bestaat uit de volgende onderdelen:

- **Doel-pc:** De platforms voor beheer die ondersteuning bieden voor Enhanced BIOS-verificatiemodus.
- **HP Manageability Integration Kit (MIK):** De plug-in voor System Center Configuration Manager (SCCM) of HP BIOS Configuration Utility (BCU) voor beheer op afstand van de BIOS-instellingen.
- **HP Sure Admin Local Access Authenticator:** Een telefoonapp die het wachtwoord vervangt om lokale toegang tot de BIOS-Setup in te schakelen door een QR-code te scannen om een eenmalige pincode te verkrijgen.

HP Sure Admin gebruiken

In dit gedeelte wordt de procedure beschreven voor het gebruik van HP Sure Admin.

1. Open HP Sure Admin plug-in in de HP Manageability Integration Kit (MIK) plug-in voor System Configuration Manager (SCCM) of Enhanced BIOS Configuration Utility (BCU).
2. Download de telefoonapp HP Sure Admin in de Google Play™ Store of de Apple App Store®.
3. Maak een sleutelpaar dat wordt gebruikt door het doelapparaat en de telefoonapp HP Sure Admin om de eenmalige pincode te verkrijgen om het BIOS te ontgrendelen.

HP Sure Admin uitschakelen

In dit gedeelte worden de opties beschreven om HP Sure Admin uit te schakelen.

- In BIOS F10-instelling selecteert u **Beveiligingsinstellingen herstellen naar fabrieksinstellingen**.

OPMERKING: Dit vereist fysieke aanwezigheid door verificatiepincode te verstrekken via de telefoonapp HP Sure Admin om de F10-instellingen te openen.

- Gebruik de opdracht BCU om op afstand WMI van **Beveiligingsinstellingen herstellen naar fabrieksinstellingen** op te roepen.

OPMERKING: Raadpleeg de gebruikershandleiding van HP BIOS Configuration Utility (BCU) voor meer informatie.

- Selecteer op de pagina MIK Security Provisioning **Inrichting ongedaan maken**.

2 Sleutels maken en beheren

Voltooi de beveiligingsinrichting in MIK voordat u de Enhanced BIOS-verificatiemodus inschakelt. De Enhanced BIOS-verificatiemodus moet worden ingeschakeld voor het maken en exporteren van sleutels. BIOS-verificatiemodus inschakelen:

▲ Open de HP Sure Admin-plug-in en selecteer **Enhanced BIOS-verificatiemodus** voor het maken en exporteren van sleutels.

Sleutels maken en exporteren

Er zijn drie verschillende manieren voor het maken van lokale toegangssleutelparen en activeer de telefoonapp HP Sure Admin om toegang te krijgen tot de sleutel:

- Sleutel maken en exporteren met handmatige distributie op pagina 2
- Een sleutel maken en exporteren met Azure AD-intrekking op pagina 3
- Een sleutel maken en verzenden naar OneDrive van Azure AD-groep op pagina 3

Sleutel maken en exporteren met handmatige distributie

Gebruik deze optie om de lokale toegangsverificatiesleutel te exporteren en deze vervolgens handmatig te distribueren naar de telefoonapp HP Sure Admin via e-mail of een andere methode.

OPMERKING: Voor deze optie is geen netwerktoegang voor de telefoonapp HP Sure Admin vereist om een eenmalige pincode te verkrijgen.

1. Geef uw sleutel een naam in het invoerveld **Sleutelnaam**.
2. Voer de wachtwoordzin in in het invoerveld **Wachtwoordzin**.

   OPMERKING: De wachtwoordzin wordt gebruikt om de geëxporteerde sleutel te beschermen en moet worden verstrekt voordat de gebruiker van de telefoonapp HP Sure Admin de sleutel kan importeren.

3. Selecteer **Bladeren** en kies waar u het pad in het systeem wilt exporteren.
4. Selecteer **Sleutel maken**. Uw sleutel is gemaakt wanneer er een meldingspictogram verschijnt naast de knop **Sleutel maken** met het bericht **Sleutel is gemaakt**.
5. Selecteer **Volgende**. Op het paginaoverzicht worden de HP Sure Admin instellingen weergegeven die u hebt ingevoerd.
6. Selecteer **Beleid opslaan**. Het beleid wordt opgeslagen wanneer het bericht **Opgeslagen** wordt weergegeven.
7. Ga naar de map waarin u de sleutel hebt opgeslagen en distribueer deze naar de gebruiker van de telefoonapp HP Sure Admin met behulp van een methode die beschikbaar is voor de gebruiker van dat apparaat, zoals e-mail. Deze gebruiker heeft ook de wachtwoordzin nodig om de sleutel te

importeren. HP adviseert om verschillende distributiemechanismen te gebruiken voor de sleutel en de wachtwoordzin.

OPMERKING: Als u de QR-code verzendt, stuurt u deze in de oorspronkelijke grootte. De app kan de afbeelding niet goed lezen als deze kleiner is dan 800 x 600.

Een sleutel maken en exporteren met Azure AD-intrekking

Gebruik deze optie om de lokale toegangssleutel aan een bepaalde Azure Active Directory-groep te verbinden en om de telefoonapp HP Sure Admin te vragen om zowel gebruikersverificatie voor Azure Active Directory te vereisen als om te bevestigen dat de gebruiker deel uitmaakt van de opgegeven groep voordat een lokale toegangspincode wordt verstrekt. Deze methode vereist ook dat de lokale toegangsverificatiesleutel wordt gedistribueerd naar de smartphone-app via e-mail of een andere methode.

OPMERKING: Deze optie vereist dat de telefoonapp HP Sure Admin netwerktoegang heeft om een eenmalige pincode te verkrijgen.

1. Geef uw sleutel een naam in het invoerveld **Sleutelnaam**.
2. Voer de wachtwoordzin in in het invoerveld **Wachtwoordzin**.

   OPMERKING: De wachtwoordzin wordt gebruikt om de geëxporteerde sleutel te beschermen en moet worden verstrekt voordat de gebruiker van de telefoonapp HP Sure Admin de sleutel kan importeren.

3. Selecteer **Azure AD-aanmelding** en meld u aan.
4. Selecteer de naam van uw groep in de vervolgkeuzelijst **Naam van Azure AD-groep**. U moet lid zijn van de groep om toegang te krijgen tot de sleutel.
5. Selecteer **Bladeren** en kies waar u het pad in het systeem wilt exporteren.
6. Selecteer **Sleutel maken**. Uw sleutel is gemaakt wanneer er een meldingspictogram verschijnt naast de knop **Sleutel maken** met het bericht **Sleutel is gemaakt**.
7. Selecteer **Volgende**. Op het paginaoverzicht worden de HP Sure Admin instellingen weergegeven die u hebt ingevoerd.
8. Selecteer **Beleid opslaan**. Het beleid wordt opgeslagen wanneer het bericht **Opgeslagen** wordt weergegeven.
9. Ga naar de map waarin u de sleutel hebt opgeslagen en distribueer deze naar de gebruiker van de telefoonapp HP Sure Admin met behulp van een methode die beschikbaar is voor de gebruiker van dat apparaat, zoals e-mail. Deze gebruiker heeft ook de wachtwoordzin nodig om de sleutel te importeren. HP adviseert om verschillende distributiemechanismen te gebruiken voor de sleutel en de wachtwoordzin.

   OPMERKING: Als u de QR-code verzendt, stuurt u deze in de oorspronkelijke grootte. De app kan de afbeelding niet goed lezen als deze kleiner is dan 800 x 600.

Een sleutel maken en verzenden naar OneDrive van Azure AD-groep

(Aanbevolen) Gebruik deze optie om te voorkomen dat de sleutel voor lokale toegangsverificatie op de telefoon wordt opgeslagen. Wanneer u deze optie kiest, slaat MIK de lokale toegangsverificatiesleutel in de opgegeven OneDrive-map op die alleen toegankelijk is voor de geautoriseerde groep. De gebruiker van de telefoonapp HP Sure Admin moet elke keer dat een pincode nodig is, worden geverifieerd bij Azure AD.

1. Geef uw sleutel een naam in het invoerveld **Sleutelnaam**.

2. Voer de wachtwoordzin in in het invoerveld **Wachtwoordzin**.
3. Selecteer **Azure AD-aanmelding** en meld u aan.
4. Selecteer de naam van uw groep in de vervolgkeuzelijst Naam van Azure AD-groep.

OPMERKING: U moet lid zijn van de groep om toegang te krijgen tot de sleutel.

5. Voer de naam in van de OneDrive-map waarin u de sleutel wilt opslaan in het invoerveld **OneDrive**.
6. Selecteer **Bladeren** en kies waar u het pad in het systeem wilt exporteren.
7. Selecteer **Sleutel maken**.

OPMERKING: Uw sleutel wordt toegevoegd aan de opgegeven OneDrive-map en geëxporteerd naar de opgegeven lokale map wanneer er een meldingspictogram verschijnt naast de knop **Sleutel maken** met het bericht **Sleutel is gemaakt.**

8. Selecteer **Volgende**. Op het paginaoverzicht worden de HP Sure Admin instellingen weergegeven die u hebt ingevoerd.
9. Selecteer **Beleid opslaan**. Het beleid wordt opgeslagen wanneer het bericht **Opgeslagen** wordt weergegeven.

OPMERKING: In dit geval is het niet nodig om iets te verzenden naar de telefoonapp HP Sure Admin om deze in te richten. De doel-pc's zijn ingericht om te verwijzen naar de OneDrive-locatie die is opgenomen in de QR-code. De telefoonapp HP Sure Admin gebruikt deze verwijzing om toegang te krijgen tot de OneDrive-locatie als de gebruiker deel uitmaakt van de gemachtigde groep en wordt geverifieerd.

3 Telefooninstellingen

Download de telefoonapp HP Sure Admin vanuit de Google Play Store of Apple Store.

- Download HP Sure Admin vanuit de Google Play Store voor Android-telefoons.
- Download HP Sure Admin vanuit de Apple Store voor iOS-telefoons.

Telefoonapp HP Sure Admin gebruiken om BIOS te ontgrendelen

De mobiele app HP Sure Admin vervangt het gebruik van het BIOS-wachtwoord voor lokale toegang tot BIOS Setup door een eenmalige pincode te verstrekken door de QR-code te scannen die door de doelcomputer wordt gepresenteerd.

Gebruik deze stappen om de sleutel lokaal op de telefoon op te slaan in een scenario waarin de sleutel naar de gebruiker van de telefoonapp wordt verzonden. In het volgende voorbeeld wordt de sleutel naar de gebruiker van de telefoonapp HP Sure Admin gemaild en opent de gebruiker de e-mail op de telefoon.

1. Open de e-mail die de sleutel bevat.
2. Als de pagina **Registratie** wordt weergegeven, voert u de wachtwoordzin in het invoerveld **Wachtwoordzin invoeren** in en uw e-mailadres in het invoervak **Uw e-mailadres invoeren** om de sleutel te decoderen en toe te voegen aan de HP Sure Admin-applicatie. De ontgrendelingspincode wordt weergegeven op de pagina **Uw pincode**.

   OPMERKING: Met deze stap wordt de sleutel op het mobiele apparaat opgeslagen en wordt de registratie voltooid. Op dit punt kunt u de telefoonapp HP Sure Admin gebruiken om toegang te krijgen tot alle apparaten die via deze registersleutel toegankelijk zijn. Een e-mailadres is alleen vereist als de beheerder dit vereist.

3. Voer de pincode in het invoerveld **BIOS-responscode invoeren** in.

Na registratie toegang krijgen tot BIOS Setup

Na de registratie toegang krijgen tot BIOS Setup op een doelcomputer:

1. Open BIOS Setup bij het opstarten van de doelcomputer.
2. Selecteer **QR-code scannen** in de telefoonapplicatie en scan de QR-code op de doelcomputer.
3. Als u wordt gevraagd om gebruikersverificatie, presenteert u uw referenties.
4. De ontgrendelingspincode wordt weergegeven op de pagina **Uw pincode**.
5. Voer de pincode in het invoerveld **BIOS-responscode invoeren** op de doelcomputer in.

BIOS ontgrendelen met Azure AD Group OneDrive

HP Sure Admin gebruiken om BIOS te ontgrendelen met OneDrive van Azure AD-groep:

1. Selecteer **QR-code scannen** en scan de QR-code van het BIOS.

   OPMERKING: In de app HP Sure Admin wordt de Azure-aanmeldingspagina weergegeven.

2. Meld u aan bij uw Azure-account.
3. Voer de pincode in het invoerveld **BIOS-responscode invoeren** in.

OPMERKING: De HP Sure Admin app slaat de sleutel in dit scenario niet lokaal op. De telefoonapp HP Sure Admin heeft netwerktoegang nodig en de gebruiker moet elke keer dat een eenmalige pincode nodig is, zich authenticeren.

4 HP Sure Admin-foutcodes

Gebruik de tabel in dit gedeelte om de foutcodes, typen en hun beschrijvingen van HP Sure Admin en KMS Admin Console weer te geven.

Tabel 4-1 Foutcodes, typen en hun beschrijvingen van de HP Sure Admin-app

Foutcode	Fouttype	Beschrijving
100	QRCodeUnknownError	Algemene fout.
101	QRCodeDeserialization	Kan de JSON van de QR-code niet lezen. De tekenreeks zitten niet in een geldig JSON-bestand of de gegevens zijn ongeldig.
102	QRCodeInvalidImage	De gescande afbeelding van deze QR-code is ongeldig. Kan het afbeeldingsbestand van de QR-code niet lezen.
103	QRCodeNoPayload	De gescande afbeelding van deze QR-code is ongeldig. Het afbeeldingsbestand bevat geen JSON-payload.
104	QRCodeInvalid	Kan de JSON van de QR-code niet lezen. De tekenreeks is geen geldige JSON of de gegevens in de QR-afbeelding zijn ongeldig.
105	QRCodeInvalidKeyIdHash	De hash van de openbare sleutel in de JSON van de QR-code komt niet overeen met de hash van het registratiepakket van de openbare sleutel (KeyID-gegevens).
106	QRCodeTampered	De gescande afbeelding van deze QR-code is gemanipuleerd en ongeldig.
107	QRCodeTamperedOrInvalidPassPhrase	De gescande afbeelding van deze QR Code is gemanipuleerd en ongeldig, of de ingevoerde wachtwoordzin is onjuist.

Tabel 4-2 OneTime-toegangssleutel van OneDrive-fouten, typen en hun beschrijvingen

Foutcode	Fouttype	Beschrijving
200	OneTimeKeyError	Algemene fout.
201	OneTimeKeyNoUserGroups	De aangemelde gebruiker behoort niet tot een AD-groep die in uw organisatie zit.
203	OneTimeKeyInvalidUserGroup	De aangemelde gebruiker hoort niet bij de AD-groep waar deze sleutel aan is toegewezen.
204	OneTimeKeyQRFileDoesNotExist	Het OneTime-sleutelbestand bestaat niet in de OneDrive-map van de AD-groep.
205	OneTimeKeyInvalidQRFile	Het OneTime-sleutelbestand in de map OneDrive van de AD-groep is ongeldig.
206	OneTimeKeyInvalidQRpayload	Het OneTime-sleutelbestand bestaat maar kan de bestandspayload niet lezen.

Tabel 4-3 Fouten in AD-verificatie Azure

Foutcode	Fouttype	Beschrijving
300	AzureADUnknownError	Algemene fout.
301	AzureADInvalidDomain	Het ingevoerde e-mailadres komt niet overeen met de domeinnaam die is opgegeven in de afbeelding van de QR-code.
302	AzureADAccessToken	Fout bij het verkrijgen van toegangstoken van Azure AD. De gebruiker kan zich niet aanmelden bij de Azure AD van uw organisatie of de app beschikt niet over de vereiste machtigingen om verbinding te maken met de Azure AD van uw organisatie. Het is ook mogelijk dat de gebruiker de verificatie heeft geannuleerd.
303	AzureADUserProfile	De HP Sure Admin-app werd ingeschakeld om gebruikersprofielgegevens te verkrijgen van de Azure AD van uw organisatie.
304	AzureADUserPrincipalMismatch	Het ingevoerde e-mailadres komt niet overeen met de hoofdnaam van de aangemelde gebruiker.
305	AzureADUserInvalidUserGroup	De aangemelde gebruiker hoort niet bij de toegewezen Azure AD-groep waar deze sleutel aan is toegewezen.

Tabel 4-4 KMS Admin Console-fouten, -typen en hun beschrijvingen

Foutcode	Fouttype	Beschrijving
401	KmsUnauthorized	Gebruiker is niet bevoegd om de KMS-service te gebruiken.
402	KmsKeyDoesNotExist	Een overeenkomende persoonlijke sleutel bestaat niet in de KMS-sleutelkluis. De sleutel bevindt zich momenteel in een verwijderde maar herstelbare staat en de naam kan in deze staat niet opnieuw worden gebruikt. De sleutel kan alleen worden hersteld of leeggemaakt.
403	KmsKeyDoesNotExistInTableStorage	Sleutel bestaat niet in tabelopslag.
404	KmsUploadKeyErrorInKeyVault	Er is een fout opgetreden bij het toevoegen van een sleutel aan de sleutelkluis.
405	KmsUploadKeyUnauthorized	De gebruiker is niet gemachtigd om sleutels te uploaden. Gebruiker behoort niet tot de gemachtigde AD-groep die deze API mag aanroepen.
406	KmsInvalidAzureADLogin	Gebruiker is niet aangemeld bij Azure Tenant AAD.
407	KmsNoUserGroups	De aangemelde gebruiker behoort niet tot een AD-groep in uw organisatie.
408	KmsInvalidUserGroup	De aangemelde gebruiker hoort niet bij de AD-groep waar deze sleutel aan is toegewezen.

Tabel 4-4 KMS Admin Console-fouten, -typen en hun beschrijvingen (vervolg)

Foutcode	Fouttype	Beschrijving
409	KmsInvalidAccessToken	Het toegangstoken dat in het verzoek is opgegeven, is ongeldig.
410	KmsAccessTokenExpired	Het opgegeven accessTokenis verlopen.
411	KmsAccessTokenInvalidTenantId	Het opgegeven accessTokenheeft een ongeldige TenantId-waarde.
412	KmsAccessTokenTenantIdMismatch	De TenantId in de opgegeven accessToken komt niet overeen met de functie-app TenantId.
413	KmsInvalidKeyId	De keyId is nul of leeg.
414	KmsDeleteKeyUnauthorized	De gebruiker is niet gemachtigd om sleutels te verwijderen. Gebruiker behoort niet tot de gemachtigde AD-groep die deze API mag aanroepen.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Poging om het geheim te herstellen is mislukt en herstel was niet mogelijk. De gebruiker moet het opnieuw proberen.
416	KmsInvalidGetKeysRequest	Aanvraag om ophalen sleutels is ongeldig.
417	KmsGetKeysUnauthorized	De gebruiker is niet gemachtigd om sleutels op te halen. Gebruiker behoort niet tot de gemachtigde AD-groep die deze API mag aanroepen.
418	KmsInvalidRequestPayload	De aanvraag die de API heeft ontvangen, is ongeldig.
419	KmsRequestRequired	De ontvangen aanvraag mag niet leeg zijn.
420	KmsKeyNotConcurrent	Sleutel in tabelopslag is bijgewerkt of gewijzigd sinds de gebruiker voor het laatst een kopie heeft opgehaald.