Brugervejledning til HP Sure Admin

OVERSIGT

HP Sure Admin gør det muligt for IT-administratorer at administrere følsomme firmwareindstillinger for enheder på en sikker måde ved hjælp af certifikater og kryptering af offentlige nøgler til både fjernadministration og lokal administration af indstillinger i stedet for en adgangskode.

Juridiske oplysninger

Anden udgave: Oktober 2021

Første udgave: december 2019

Dokumentets bestillingsnummer: L83995-082

Indholdsfortegnelse

1 Sådan kommer du i gang

HP Sure Admin gør det muligt for IT-administratorer at administrere følsomme firmwareindstillinger for enheder på en sikker måde ved hjælp af certifikater og kryptering af offentlige nøgler til både fjernadministration og lokal administration af indstillinger i stedet for en adgangskode.

HP Sure Admin består af følgende dele:

- **Mål-pc:** Platformene, der skal administreres, som understøtter udvidet BIOS-godkendelsestilstand.
- **HP Manageability Integration Kit (MIK):** Plugin-modulet til System Center Configuration Manager (SCCM) eller HP BIOS Configuration Utility (BCU) til fjernadministration af BIOS-indstillingerne.
- **HP Sure Admin Local Access Authenticator:** En telefonapp, der erstatter adgangskoden og gør det muligt at få lokal adgang til BIOS-opsætningen ved at scanne en QR-kode for at få tilsendt en engangspinkode.

Brug af HP Sure Admin

Dette afsnit beskriver processen for brug af HP Sure Admin.

1. Åbn plugin-modulet HP Sure Admin i plugin-modulet HP Manageability Integration Kit (MIK) til System Configuration Manager (SCCM) eller Enhanced BIOS Configuration Utility (BCU).
2. Download HP Sure Admin-telefonappen fra enten Google Play™ Butik eller Apple App Store®.
3. Opret et nøglepar, som skal bruges af målenheden og HP Sure Admin-telefonappen, og få tilsendt en engangspinkode til at låse op for BIOS.

Deaktivering af HP Sure Admin

Dette afsnit beskriver, hvordan HP Sure Admin kan deaktiveres.

- Vælg **Gendan sikkerhedsindstillinger til fabriksstandarder** i BIOS F10-indstillingen.

BEMÆRK: Dette kræver, at du er fysisk til stede, da der sendes en godkendelsespinkode via HP Sure Admin-telefonappen, som bruges til at få adgang til F10-indstillingerne.

- Brug BCU-kommandoen til at kalde WMI til **Gendan sikkerhedsindstillinger til fabriksstandarder** via fjernadgang.

BEMÆRK: Du kan få yderligere oplysninger i brugervejledningen til HP BIOS Configuration Utility (BCU).

- Vælg **Fjern klargøring** på siden MIK-sikkerhedsklargøring.

2 Oprettelse og administration af nøgler

Fuldfør sikkerhedsklargøringen i MIK, før du aktiverer udvidet BIOS-godkendelsestilstand. Udvidet BIOS-godkendelsestilstand skal være aktiveret, før det er muligt at oprette og eksportere nøgler. Sådan aktiveres BIOS-godkendelsestilstand:

▲ Åbn plugin-modulet HP Sure Admin, og vælg **Udvidet BIOS-godkendelsestilstand** for at oprette og eksportere nøgler.

Oprettelse og eksport af nøgler

Der er 3 forskellige måder at oprette lokale adgangsnøglepar og aktivere HP Sure Admin-telefonappen på for at få adgang til nøglen.

- Opret og eksporter nøgle via manuel distribution på side 2
- Sådan oprettes og eksporteres en nøgle med Azure AD-tilbagekaldelse på side 3
- Sådan opretter og sender du en nøgle til Azure AD Group OneDrive på side 3

Opret og eksporter nøgle via manuel distribution

Brug denne indstilling til at eksportere den lokale adgangsgodkendelsesnøgle og derefter distribuere den manuelt til HP Sure Admin-telefonappen via e-mail eller anden metode.

BEMÆRK: Denne valgmulighed kræver ikke, at HP Sure Admin-telefonappen har netværksadgang, for at engangspinkoden kan blive tilsendt.

1. Indtast et navn til nøglen i indtastningsfeltet **Nøglenavn**.
2. Indtast adgangsudtrykket i indtastningsfeltet **Adgangsudtryk**.

   BEMÆRK: Adgangsudtrykket bruges til at beskytte den eksporterede nøgle og skal angives, for at brugeren af HP Sure Admin-telefonappen kan importere nøglen.

3. Vælg **Gennemse**, og vælg, hvor du vil eksportere stien i systemet.
4. Vælg **Opret nøgle**. Din nøgle er oprettet, når der vises et meddelelsesikon ud for knappen **Opret nøgle** efterfulgt af meddelelsen **Nøglen blev oprettet**.
5. Vælg **Næste**. Oversigtssiden viser de HP Sure Admin-indstillinger, du har angivet.
6. Vælg **Gem politik**. Politikken er gemt, når meddelelsen **Lagring gennemført** vises.
7. Åbn mappen, du har gemt nøglen i, og send den til brugeren af HP Sure Admin-telefonappen ved hjælp af en metode, der er tilgængelig for brugeren på den pågældende enhed, f.eks. e-mail. Denne bruger skal desuden bruge adgangsudtrykket til at importere nøglen. HP anbefaler, at du bruger forskellige distributionsmetoder til nøglen og adgangsudtrykket.

   BEMÆRK: Når du sender QR-koden, skal du sende den i den oprindelige størrelse. Appen kan ikke læse billedet korrekt, hvis det er mindre end 800 × 600.

Sådan oprettes og eksporteres en nøgle med Azure AD-tilbagekaldelse

Brug denne indstilling til at knytte den lokale adgangsnøgle til en angiven Azure Active Directory-gruppe og kræve, at HP Sure Admin-telefonappen kræver både brugergodkendelse i Azure Active Directory, samt til at bekræfte, at brugeren er medlem af den angivne gruppe, før der sendes en lokal adgangspinkode. Denne metode kræver også manuel distribution af den lokale adgangsgodkendelsesnøgle til telefonappen via e-mail eller en anden metode.

BEMÆRK: Denne indstilling kræver, at HP Sure Admin-telefonappen har netværksadgang, for at du kan få tilsendt en engangspinkode.

1. Indtast et navn til nøglen i indtastningsfeltet **Nøglenavn**.
2. Indtast adgangsudtrykket i indtastningsfeltet **Adgangsudtryk**.

   BEMÆRK: Adgangsudtrykket bruges til at beskytte den eksporterede nøgle og skal angives, for at brugeren af HP Sure Admin-telefonappen kan importere nøglen.

3. Vælg **Azure AD-login**, og log ind.
4. Vælg dit gruppenavn i rullemenuen **Azure AD-gruppenavn**. Du skal være medlem af gruppen for at få adgang til nøglen.
5. Vælg **Gennemse**, og vælg, hvor du vil eksportere stien i systemet.
6. Vælg **Opret nøgle**. Din nøgle er oprettet, når der vises et meddelelsesikon ud for knappen **Opret nøgle** efterfulgt af meddelelsen **Nøglen blev oprettet**.
7. Vælg **Næste**. Oversigtssiden viser de HP Sure Admin-indstillinger, du har angivet.
8. Vælg **Gem politik**. Politikken er gemt, når meddelelsen **Lagring gennemført** vises.
9. Åbn mappen, du har gemt nøglen i, og send den til brugeren af HP Sure Admin-telefonappen ved hjælp af en metode, der er tilgængelig for brugeren på den pågældende enhed, f.eks. e-mail. Denne bruger skal desuden bruge adgangsudtrykket til at importere nøglen. HP anbefaler, at du bruger forskellige distributionsmetoder til nøglen og adgangsudtrykket.

   BEMÆRK: Når du sender QR-koden, skal du sende den i den oprindelige størrelse. Appen kan ikke læse billedet korrekt, hvis det er mindre end 800 × 600.

Sådan opretter og sender du en nøgle til Azure AD Group OneDrive

(Anbefales) Brug denne indstilling for at undgå at gemme den lokale adgangsgodkendelsesnøgle på telefonen. Når du vælger denne indstilling, gemmer MIK den lokale adgangsgodkendelsesnøgle i den valgte OneDrive-mappe, der kun er tilgængelig for den autoriserede gruppe. Brugeren af HP Sure Admin-telefonappen skal godkendes af Azure AD, hver gang en pinkode er nødvendig.

1. Indtast et navn til nøglen i indtastningsfeltet **Nøglenavn**.
2. Indtast adgangsudtrykket i indtastningsfeltet **Adgangsudtryk**.
3. Vælg **Azure AD-login**, og log ind.
4. Vælg dit gruppenavn i rullemenuen Azure AD-gruppenavn.

   BEMÆRK: Du skal være medlem af gruppen for at få adgang til nøglen.

5. Indtast navnet på den OneDrive-mappe, nøglen skal gemmes i, i indtastningsfeltet **OneDrive**.

6. Vælg **Gennemse**, og vælg, hvor du vil eksportere stien i systemet.

7. Vælg **Opret nøgle**.

BEMÆRK: Din nøgle er blevet føjet til den angivne OneDrive-mappe og eksporteret til den angivne lokale mappe, når der vises et meddelelsesikon ud for knappen **Opret nøgle** efterfulgt af meddelelsen **Nøglen er blevet oprettet**.

8. Vælg **Næste**. Oversigtssiden viser de HP Sure Admin-indstillinger, du har angivet.

9. Vælg **Gem politik**. Politikken er gemt, når meddelelsen **Lagring gennemført** vises.

BEMÆRK: I dette scenario er der ingen grund til at sende noget til HP Sure Admin-telefonappen for at fjerne klargøringen af den. Mål-pc'erne er klargjort til at henvise til den OneDrive-placering, som er inkluderet i QR-koden. HP Sure Admin-telefonappen bruger denne markør til at åbne OneDrive-placeringen, hvis brugeren er medlem af den godkendte gruppe og bliver godkendt.

3 Telefonopsætning

Download HP Sure Admin-telefonappen fra enten Google Play eller Apple Store.

- Download HP Sure Admin fra Google Play Butik, hvis du bruger en Android-telefon.
- Download HP Sure Admin fra Apple Store, hvis du bruger en iOS-telefon.

Brug af HP Sure Admin-telefonappen til at låse BIOS op

HP Sure Admin-mobilappen erstatter BIOS-adgangskoden som mulighed for at få lokal adgang til BIOS-opsætningen. Du modtager en engangspinkode ved at scanne QR-koden, som vises på målcomputeren.

Brug disse trin til at gemme nøglen lokalt på telefonen i et scenarie, hvor nøglen sendes til brugeren af appen. I følgende eksempel sendes nøglen til brugeren af HP Sure Admin-appen, og brugeren åbner e-mailen på telefonen.

1. Åbn den e-mail, der indeholder nøglen.
2. Når siden **Tilmelding** vises, skal du indtaste adgangsudtrykket i indtastningsfeltet **Indtast adgangsudtryk** og din e-mailadresse i feltet **Indtast din e-mailadresse** for at dekryptere nøglen og føje den til HP Sure Admin-appen. Oplåsningspinkoden vises på siden **Din pinkode** .

   BEMÆRK: I dette trin gemmes nøglen på den mobile enhed, og tilmeldingen fuldføres. Herefter kan du bruge HP Sure Admin-telefonappen til at få adgang til alle enheder, der er blevet klargjort, så de kan åbnes ved hjælp af denne nøgle. Der skal kun indtastes en e-mailadresse, hvis administratoren kræver det.

3. Indtast pinkoden i BIOS-indtastningsfeltet **Indtast BIOS-responskode**.

Hentning af adgang til BIOS-opsætning efter tilmelding

Sådan får du adgang til BIOS-opsætningen på en målcomputer efter tilmeldingen:

1. Gå ind i BIOS-opsætningen ved opstart på målcomputeren.
2. Vælg **Scan QR-kode** i telefonappen, og scan QR-koden på målcomputeren.
3. Hvis du bliver bedt om brugergodkendelse, skal du angive dine legitimationsoplysninger.
4. Det oplåste pinnummer vises på siden **Din pinkode** .
5. Indtast pinkoden i BIOS-indtastningsfeltet **Indtast responskode** på målcomputeren.

Oplåsning af BIOS med Installerede AD Group OneDrive

Sådan bruger du HP Sure Admin til at låse BIOS op med Azure AD Group OneDrive:

1. Vælg **Scan QR-kode**, og scan derefter BIOS QR-koden.

   BEMÆRK: HP Sure Admin-appen viser siden Azure AD-login.

2. Log ind på din Azure-konto.

3. Indtast pinkoden i BIOS-indtastningsfeltet **Indtast BIOS-responskode**.

BEMÆRK: HP Sure Admin-appen gemmer ikke nøglen lokalt i dette scenarie. HP Sure Admin-telefonappen skal have netværksadgang, og brugeren skal godkendes, hver gang en engangspinkode er nødvendig.

4 HP Sure Admin-fejlkoder

Brug tabellen i dette afsnit til at se fejlkoder for HP Sure Admin og KMS Admin Console samt typerne og deres beskrivelser.

Tabel 4-1 HP Sure Admin-appens fejlkoder, typer og beskrivelse af dem

Fejlkode	Fejltype	Beskrivelse
100	QRCodeUnknownError	Generel fejl.
101	QRCodeDeserialization	Kan ikke læse QR-kode JSON. Enten er strengen ikke en gyldig JSON-fil, eller også er dataene ugyldige.
102	QRCodeInvalidImage	Det scannede QR-kodebillede er ugyldigt. QR-kodens billedfil kan ikke læses.
103	QRCodeNoPayload	Det scannede QR-kodebillede er ugyldigt. Billedfilen har ikke JSON-nyttedata.
104	QRCodeInvalid	QR-kodens JSON kan ikke læses. Enten er strengen ikke en gyldig JSON, eller også er dataene i QR-billedet ugyldige.
105	QRCodeInvalidKeyIdHash	Den offentlige nøglehash i QR-kodens JSON stemmer ikke overens med tilmeldingspakkens offentlige nøglehash (KeyID-data).
106	QRCodeTampered	Det scannede QR-kodebillede er ændret eller ugyldigt.
107	QRCodeTamperedOrInvalidPassPhrase	QR-kodebilledet er ændret eller ugyldigt, eller det indtastede adgangsudtryk er forkert.

Tabel 4-2 OneTime-adgangstasten fra OneDrives fejl, typer og deres beskrivelser

Fejlkode	Fejltype	Beskrivelse
200	OneTimeKeyError	Generel fejl.
201	OneTimeKeyNoUserGroups	Den bruger, der er logget på, er ikke medlem af en AD-gruppe, som er en del af din organisation.
203	OneTimeKeyInvalidUserGroup	Den bruger, der er logget på, er ikke medlem af den AD-gruppe, som denne nøgle er tildelt til.
204	OneTimeKeyQRFileDoesNotExist	Engangsnøglefilen findes ikke i AD-gruppens OneDrive-mappe.
205	OneTimeKeyInvalidQRFile	Engangsnøglefilen i AD-gruppens OneDrive-mappe er ugyldig.
206	OneTimeKeyInvalidQRpayload	Engangsnøglefilen findes, men kan ikke læse filens nyttedata.

Tabel 4-3 Azure AD Authorization-fejl

Fejlkode	Fejltype	Beskrivelse
300	AzureADUnknownError	Generel fejl.
301	AzureADInvalidDomain	Den angivne e-mailadresse stemmer ikke overens med domænenavnet i QR-kodebilledet.
302	AzureADAccessToken	Fejl ved hentning af adgangstoken fra Azure AD. Enten kan brugeren ikke logge på din organisations Azure AD, eller også har appen ikke de nødvendige tilladelser til at oprette forbindelse til din virksomheds Azure AD. Det kan også være, at brugeren annullerede godkendelse.
303	AzureADUserProfile	HP Sure Admin blev deaktiveret for at hente brugerprofiloplysninger fra din organisations Azure AD.
304	AzureADUserPrincipalMismatch	Den angivne e--mailadresse stemmer ikke overens med brugernavnet på den bruger, der er logget ind.
305	AzureADUserInvalidUserGroup	Den bruger, der er logget på, tilhører ikke den tildelte Azure AD-gruppe, som denne nøgle er tildelt til.

Tabel 4-4 KMS Admin Console-fejl, typer og deres beskrivelser

Fejlkode	Fejltype	Beskrivelse
401	KmsUnauthorized	Brugeren er ikke godkendt til at bruge KMS-tjenesten.
402	KmsKeyDoesNotExist	En matchende, privat nøgle findes ikke i KMS-tasten. Nøglen er i øjeblikket i en slettet, men gendannelig tilstand, og dens navn kan ikke bruges i denne tilstand. Nøglen kan kun gendannes eller renses.
403	KmsKeyDoesNotExistInTableStorage	Nøglen findes ikke i tabellagring.
404	KmsUploadKeyErrorInKeyVault	Der skete en fejl ved tilføjelse af en nøgle til nøglefejl.
405	KmsUploadKeyUnauthorized	Brugeren er ikke godkendt til at overføre nøgler. Brugeren tilhører ikke den godkendte AD-gruppe, som har tilladelse til at kalde op til denne API.
406	KmsInvalidAzureADLogin	Brugeren er ikke logget på Azure Tenant AAD.
407	KmsNoUserGroups	Den bruger, der er logget på, er ikke medlem af en AD-gruppe i din organisation.
408	KmsInvalidUserGroup	Den bruger, der er logget på, er ikke medlem af den AD-gruppe, som denne nøgle er tildelt til.
409	KmsInvalidAccessToken	Det adgangstoken, der blev angivet i anmodningen, er ugyldigt.
410	KmsAccessTokenExpired	Den angivne adgangtoken er udløbet.

Tabel 4-4 KMS Admin Console-fejl, typer og deres beskrivelser (fortsat)

Fejlkode	Fejltype	Beskrivelse
411	KmsAccessTokenInvalidTenantId	Den adgangstoken, der er angivet, har værdien udgyldig TenantId.
412	KmsAccessTokenTenantIdMismatch	Det anvendte TenantId i adgangstoken svarer ikke til funktions-appen TenantId.
413	KmsInvalidKeyId	Nøgle-id er nul eller tomt.
414	KmsDeleteKeyUnauthorized	Brugeren er ikke godkendt til at slette nøgler. Brugeren tilhører ikke den godkendte AD-gruppe, som har tilladelse til at kalde op til denne API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Forsøg på at genoprette den skjulte fejl mislykkedes. Brugeren skal forsøge igen.
416	KmsInvalidGetKeysRequest	Anmodningen om at hente nøgler er ugyldig.
417	KmsGetKeysUnauthorized	Brugeren er ikke godkendt til at hente nøgler. Brugeren tilhører ikke den godkendte AD-gruppe, som har tilladelse til at kalde op til denne API.
418	KmsInvalidRequestPayload	Den anmodning, som blev modtaget af API, er ugyldig.
419	KmsRequestRequired	Den modtagne anmodning må ikke være tom.
420	KmsKeyNotConcurrent	Nøglen i tabellageret blev opdateret eller ændret, siden brugeren sidst hentede en kopi.