



Brukerhåndbok for HP Sure Admin

SAMMENDRAG

HP Sure Admin gjør det mulig for IT-administratorer å behandle sensitive fastvareinnstillinger for enheter på en sikker måte ved bruk av sertifikater og kryptografi for fellesnøkkel for både ekstern og lokal administrering av innstillingene i stedet for passord.

Juridisk informasjon

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

Apple er et varemerke for Apple Computer, Inc., som er registrert i USA og andre land.

Google Play er et varemerke for Google LLC.

Konfidensiell datamaskinprogramvare. Gyldig lisens fra HP kreves for eierskap, bruk eller kopiering. I samsvar med FAR 12.211 og 12.212 er kommersiell datamaskinprogramvare, dokumentasjon for datamaskinprogramvare og tekniske data for kommersielle elementer lisensiert til de amerikanske myndighetene i henhold til selgers standard kommersielle lisens.

Informasjonen i dette dokumentet kan endres uten varsel. De eneste garantiene for HP-produktene og -tjenestene er uttrykkelig angitt i garantierklæringene som følger med produktene og tjenestene. Ingenting i dette dokumentet skal kunne tolkes som en tilleggsgaranti. HP skal ikke holdes ansvarlig for tekniske eller innholdsmessige feil eller utelatelser i dette dokumentet.

Andre utgave: Oktober 2021

Første utgave: Desember 2019

Dokumentets delenummer: L83995-092

Innhold

1 Komme i gang	1
Bruke HP Sure Admin	1
Deaktivere HP Sure Admin.....	1
2 Opprette og administrere nøkler	2
Opprette og eksportere nøkler	2
Opprett og eksporter nøkkel med manuell distribusjon.....	2
Oppretting og eksportering av nøkkel med Azure AD Revocation	3
Slik oppretter og sender du en nøkkel til Azure AD Group OneDrive	3
3 Telefonoppsett.....	5
Bruke HP Sure Admin-telefonappen for å låse opp BIOS	5
Få tilgang til BIOS-oppsett etter registrering.....	5
Låse opp BIOS med Azure AD Group OneDrive	5
4 HP Sure Admin-feilkoder	7

1 Komme i gang

HP Sure Admin gjør det mulig for IT-administratorer å behandle sensitive fastvareinnstillinger for enheter på en sikker måte ved bruk av sertifikater og kryptografi for fellesnøkkel for både ekstern og lokal administrering av innstillingene i stedet for passord.

HP Sure Admin består av følgende deler:

- **Måldatamaskin:** Plattformene for å administrere støtten forbedret BIOS-godkjenningsmodus.
- **HP Manageability Integration Kit (MIK):** Programtillegget for System Center Configuration Manager (SCCM) eller HP BIOS Configuration Utility (BCU) for ekstern administrering av BIOS-innstillingene.
- **HP Sure Admin Local Access Authenticator:** En telefonapp som erstatter passordet for å aktivere lokal tilgang til BIOS-oppsettet ved å skanne en QR-kode for å få en engangs-PIN-kode.

Bruke HP Sure Admin


Denne delen beskriver prosessen for bruk av HP Sure Admin.

1. Åpne HP Sure Admin-programtillegget i programtillegget HP Manageability Integration Kit (MIK) for System Configuration Manager (SCCM) eller Enhanced BIOS Configuration Utility (BCU).
2. Last ned HP Sure Admin-telefonappen fra enten Google Play™-butikken eller Apple App Store®.
3. Lag et nøkkelpar som skal brukes av målenheten og HP Sure Admin-telefonappen for å få engangs-PIN-kode for å låse opp BIOS.

Deaktivere HP Sure Admin

Denne delen beskriver alternativene for å deaktivere HP Sure Admin.

- I BIOS F10-innstillingen velger du **Gjenopprett sikkerhetsinnstillinger til fabrikkinnstillingene**.

 **MERK:** Dette krever fysisk tilstedeværelse ved å oppgi godkjennings-PIN-kode via HP Sure Admin-telefonappen for å få tilgang til F10-innstillingene.

- Bruk BCU-kommandoen til å ringe eksternt WMI for **Gjenopprett sikkerhetsinnstillinger til fabrikkinnstillingene**.

 **MERK:** Du finner mer informasjon i brukerhåndboken for HP BIOS Configuration Utility (BCU).

- På MIK-siden for sikkerhetsklargjøring velger du **Oppheving av klargjøring**.

2 Opprette og administrere nøkler

Fullfør sikkerhetsklargjøringen i MIK før du aktiverer forbedret BIOS-godkjenningsmodus. Forbedret BIOS-godkjenningsmodus må være aktivert for å kunne opprette og eksportere nøkler. Slik aktiverer du BIOS-godkjenningsmodus:

- ▲ Åpne HP Sure Admin-programtillegget og velg **Forbedret BIOS-godkjenningsmodus** for å opprette og eksportere nøkler.

Opprette og eksportere nøkler

Det finnes tre forskjellige måter å opprette lokale tilgangsnøkkelpar og aktivere HP Sure Admin-telefonappen på for å få tilgang til nøkkelen.

- [Opprett og eksporter nøkkel med manuell distribusjon på side 2](#)
- [Oppretting og eksportering av nøkkel med Azure AD Revocation på side 3](#)
- [Slik oppretter og sender du en nøkkel til Azure AD Group OneDrive på side 3](#)

Opprett og eksporter nøkkel med manuell distribusjon

Bruk dette alternativet for å eksportere den lokale tilgangsgodkjenningsnøkkelen og deretter manuelt distribuere den til HP Sure Admin-telefonappen via e-post eller en annen metode.



MERK: Dette alternativet krever ikke nettverkstilgang til HP Sure Admin-telefonappen for å få en engangs-PIN-kode.

1. Navngi nøkkelen i **Nøkkelnavn**-oppføringsboksen.
2. Skriv inn passordet i **Passord**-oppføringsboksen.



MERK: Passordet brukes til å beskytte den eksporterte nøkkelen og må oppgis slik at brukeren HP Sure Admin-telefonappen kan importere nøkkelen.

3. Velg **Bla gjennom**, og velg hvor du vil eksportere banen i systemet.
4. Velg **Opprett nøkkel**. Nøkkelen er opprettet når et varselikon vises ved siden av **Opprett nøkkel**-knappen, med meldingen «**Key successfully created**» (**Nøkkelen er opprettet**).
5. Velg **Neste**. Sammendragssiden viser innstillingene for HP Sure Admin som du har angitt.
6. Velg **Lagre policy**. Policyen lagres når meldingen **Lagret** vises.
7. Naviger til mappen der du lagret nøkkelen, og send den til brukeren av HP Sure Admin-telefonappen med en metode som er tilgjengelig for brukeren på denne enheten, for eksempel e-post. Denne brukeren vil også trenge passordet for å importere nøkkelen. HP anbefaler at du bruker ulike distribusjonsmetoder for nøkkelen og passordet.



MERK: Når du sender QR-koden, sender du den i opprinnelig størrelse. Appen kan ikke lese bildet på riktig måte hvis det er mindre enn 800 X 600 piksler i størrelse.

Oppretting og eksportering av nøkkel med Azure AD Revocation

Bruk dette alternativet for å koble den lokale tilgangsnøkkelen til en spesifisert Azure Active Directory-gruppe, og krev at HP Sure Admin-telefonappen skal kreve både brukergodkjenning til Azure Active Directory og å bekrefte at brukeren er medlem av den angitte gruppen før det oppgis en lokal tilgangs-PIN-kode. Denne metoden krever også manuell distribusjon av den lokale tilgangsgodkjenningsnøkkelen til telefonappen via e-post eller annen metode.



MERK: Dette alternativet krever at HP Sure Admin-telefonappen har nettverkstilgang for å kunne få en engangs-PIN-kode.

1. Navngi nøkkelen i **Nøkkelnavn**-oppføringsboksen.
2. Skriv inn passordet i **Passord**-oppføringsboksen.



MERK: Passordet brukes til å beskytte den eksporterte nøkkelen og må oppgis slik at brukeren HP Sure Admin-telefonappen kan importere nøkkelen.

3. Velg **Azure AD-pålogging** og logg inn.
4. Velg gruppenavnet ditt i **Azure AD-gruppenavn**-rullegardinlisten. Du må være medlem av gruppen for å ha tilgang til nøkkelen.
5. Velg **Bla gjennom**, og velg hvor du vil eksportere banen i systemet.
6. Velg **Opprett nøkkel**. Nøkkelen opprettes når et varselikon vises ved siden av **Opprett nøkkel**-knappen, med meldingen «Key successfully created» (**Nøkkelen er opprettet**).
7. Velg **Neste**. Sammendragssiden viser innstillingene for HP Sure Admin som du har angitt.
8. Velg **Lagre policy**. Policyen lagres når meldingen **Lagret** vises.
9. Naviger til mappen der du lagret nøkkelen, og send den til brukeren av HP Sure Admin-telefonappen med en metode som er tilgjengelig for brukeren på denne enheten, for eksempel e-post. Denne brukeren vil også trenge passordet for å importere nøkkelen. HP anbefaler at du bruker ulike distribusjonsmetoder for nøkkelen og passordet.



MERK: Når du sender QR-koden, sender du den i opprinnelig størrelse. Appen kan ikke lese bildet på riktig måte hvis det er mindre enn 800 X 600 piksler i størrelse.

Slik oppretter og sender du en nøkkel til Azure AD Group OneDrive

(Anbefales) Bruk dette alternativet for å unngå å lagre den lokale tilgangsgodkjenningsnøkkelen på telefonen. Når du velger dette alternativet, vil MIK lagre den lokale tilgangsgodkjenningsnøkkelen til den angitte OneDrive-mappen som bare er tilgjengelig for den autoriserte gruppen. Det kreves at brukeren av HP Sure Admin-telefonappen får godkjenning til Azure AD hver gang en PIN-kode kreves.

1. Navngi nøkkelen i **Nøkkelnavn**-oppføringsboksen.
2. Skriv inn passordet i **Passord**-oppføringsboksen.
3. Velg **Azure AD-pålogging** og logg inn.
4. Velg gruppenavnet ditt i **Azure AD-gruppenavn**-rullegardinlisten.



MERK: Du må være medlem av gruppen for å ha tilgang til nøkkelen.

5. Skriv inn navnet på OneDrive-mappen der du vil at nøkkelen skal lagres i **OneDrive**-oppføringsboksen.

6. Velg **Bla gjennom**, og velg hvor du vil eksportere banen i systemet.

7. Velg **Opprett nøkkel**.



MERK: Nøkkelen er lagt til i den angitte OneDrive-mappen og eksporteres til den angitte lokale mappen når et varslingsikon vises ved siden av **Opprett nøkkel**-knappen med meldingen **Nøkkelen er opprettet**.

8. Velg **Neste**. Sammendragssiden viser HP Sure Admin-innstillingene du har angitt.

9. Velg **Lagre policy**. Policyen lagres når meldingen **Lagret** vises.



MERK: I dette scenariet er det ikke nødvendig å sende noe til HP Sure Admin-telefonappen for å klargjøre den. Måldatamaskinene er klargjorte for å peke til OneDrive-plasseringen som er inkludert i QR-koden. HP Sure Admin-telefonappen bruker denne pekeren for å få tilgang til OneDrive-plasseringen hvis brukeren er en del av den autoriserte gruppen og godkjennes.

3 Telefonoppsett

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

- Last ned HP Sure Admin fra Google-butikken for Android-telefoner.
- Last ned HP Sure Admin fra Apple Store for iOS-telefoner.

Bruke HP Sure Admin-telefonappen for å låse opp BIOS

HP Sure Admin-mobilappen erstatter bruken av BIOS-passordet for å få lokal tilgang til BIOS-oppsettet ved å gi en engangs-PIN-kode, ved å skanne QR-koden som vises av måldatamaskinen.

Bruk disse trinnene for å lagre nøkkelen lokalt på telefonen i et scenario der nøkkelen sendes til telefonappbrukeren. I dette eksempelet er nøkkelen sendt til HP Sure Admin-telefonappbrukeren, og brukeren åpner e-postmeldingen på telefonen.

1. Åpne e-postmeldingen som inneholder nøkkelen.
2. Når **Registrering**-siden vises, skriver du inn passordet i **Angi passord**-oppføringsboksen og e-postadressen din i **Skriv inn e-postadressen din**-oppføringsboksen for å dekryptere nøkkelen og legge den til i HP Sure Admin-appen. PIN-nummeret for å låse opp vises på **PIN-koden din**-siden.



MERK: Dette trinnet lagrer nøkkelen i mobilenheten og fullfører registreringen. På dette tidspunktet kan du bruke HP Sure Admin-telefonappen for å få tilgang til alle enheter som har blitt klargjort for tilgang med denne nøkkelen. En e-postadresse kreves bare hvis administratoren krever det.

3. Skriv inn PIN-koden i **Angi responskode**-oppføringsboksen i BIOS.

Få tilgang til BIOS-oppsett etter registrering

Slik får du tilgang til BIOS-oppsett på en målmaskin etter registrering:

1. Gå inn i BIOS-oppsett ved oppstart på målmaskinen.
2. Velg **Skann QR-kode** i telefonappen, og skann QR-koden på målmaskinen.
3. Hvis du blir bedt om brukergodkjenning, angir du brukerlegitimasjonen.
4. Det ulåste PIN-nummeret vises på **PIN-koden din**-siden.
5. Skriv inn PIN-koden i **Angi responskoden**-oppføringsboksen i BIOS på målmaskinen.

Låse opp BIOS med Azure AD Group OneDrive

Slik bruker du HP Sure Admin til å låse opp BIOS med Azure AD Group OneDrive:

1. Velg **Skann QR-kode**, og skann deretter BIOS-QR-koden.



MERK: HP Sure Admin-appen viser Azure AD-påloggingssiden.

2. Logg deg på Azure-kontoen din.

3. Skriv inn PIN-koden i **Angi responskode**-oppføringsboksen i BIOS.



MERK: HP Sure Admin-appen lagrer ikke nøkkelen lokalt i dette scenariet. HP Sure Admin-telefonappen må ha nettverkstilgang og brukeren må godkjennes hver gang en engangs-PIN-kode trengs.

4 HP Sure Admin-feilkoder

Bruk tabellen i dette avsnittet for å se feilkodene for HP Sure Admin og KMS Admin Console, typer og beskrivelser.

Tabell 4-1 HP Sure Admin-appfeilkoder, typer og beskrivelser

Feilkode	Feiltype	Beskrivelse
100	QRCodeUnknownError	Generell feil.
101	QRCodeDeserialization	Kan ikke lese QR-kode JSON. Enten er strengen ikke en gyldig JSON-fil, eller dataene er ugyldige.
102	QRCodeInvalidImage	Det skannede QR-kodebildet er ugyldig. Kan ikke lese QR-kodebildefilen.
103	QRCodeNoPayload	Det skannede QR-kodebildet er ugyldig. Bildefilen har ikke JSON-nyttelast.
104	QRCodeInvalid	Kan ikke lese QR-koden i JSON-format. Enten er strengen ikke en gyldig JSON-streng, eller dataene i QR-bildet er ugyldig.
105	QRCodeInvalidKeyldHash	Fellesnøkkelhash-koden i QR-kode JSON samsvarer ikke med fellesnøkkelhash-kode for registreringspakke (KeyID-data).
106	QRCodeTampered	Det skannede QR-kodebildet er manipulert og ugyldig.
107	QRCodeTamperedOrInvalidPassPhrase	Skannet QR-kodebilde er manipulert og ugyldig, eller angitt passord er feil.

Tabell 4-2 OneTime-tilgangstast fra OneDrive-feil, -typer og beskrivelser

Feilkode	Feiltype	Beskrivelse
200	OneTimeKeyError	Generell feil.
201	OneTimeKeyNoUserGroups	Den påloggede brukeren hører ikke til noen av AD-gruppene i organisasjonen.
203	OneTimeKeyInvalidUserGroup	Den påloggede brukeren tilhører ikke AD-gruppen for denne nøkkelen er tilordnet til.
204	OneTimeKeyQRFileDoesNotExist	OneTime-nøkkelfilen finnes ikke i AD-gruppens OneDrive-mappe.
205	OneTimeKeyInvalidQRFile	OneTime-nøkkelfilen i AD-gruppens OneDrive-mappe er ugyldig.
206	OneTimeKeyInvalidQRpayload	OneTime-nøkkelfilen eksisterer, men kan ikke lese filnyttelasten.

Tabell 4-3 Feil i Azure AD-godkjenninger

Feilkode	Feiltype	Beskrivelse
300	AzureADUnknownError	Generell feil.
301	AzureADInvalidDomain	Angitt E-postadresse samsvarer ikke med domenenavnet spesifisert i QR-kodebildet.
302	AzureADAccessToken	Feil under henting av tilgangstoken fra Azure AD. Enten kan ikke brukeren logge seg på organisasjonens Azure AD, eller appen har ikke de nødvendige tillatelsene for å koble seg til organisasjonens Azure AD. Brukeren kan også ha kansellert godkjenningen.
303	AzureADUserProfile	HP Sure Admin-appen ble aktivert for henting av informasjon om brukerprofil fra organisasjonens Azure AD.
304	AzureADUserPrincipalMismatch	Angitt e-postadresse samsvarer ikke med den innloggede brukerens hovednavn.
305	AzureADUserInvalidUserGroup	Den påloggede brukeren tilhører ikke den tilordnede Azure AD-gruppen som denne nøkkelen er tilordnet.

Tabell 4-4 KMS Admin Console-feil, typer og beskrivelser

Feilkode	Feiltype	Beskrivelse
401	KmsUnauthorized	Brukeren er ikke autorisert til å bruke KMS-tjenesten.
402	KmsKeyDoesNotExist	En samsvarende privat nøkkel finnes ikke i KMS-nøkkelhvelvet. Nøkkelen er i en slettet, men gjenopprettelig tilstand, og navnet kan ikke brukes på nytt i denne tilstanden. Nøkkelen kan bare gjenopprettes eller renses.
403	KmsKeyDoesNotExistInTableStorage	Tasten finnes ikke i tabellens lagringsplass.
404	KmsUploadKeyErrorInKeyVault	Det oppstod en feil under tillegging av nøkkel i nøkkelhvelvet.
405	KmsUploadKeyUnauthorized	Brukeren er ikke autorisert til å laste opp nøkler. Brukeren tilhører ikke den autoriserte AD-gruppen som har tillatelse til å kontakte dette API-et.
406	KmsInvalidAzureADLogin	Brukeren er ikke logget på Azure Tenant AAD.
407	KmsNoUserGroups	Den påloggede brukeren hører ikke til en AD-gruppe i organisasjonen.
408	KmsInvalidUserGroup	Den påloggede brukeren tilhører ikke AD-gruppen denne nøkkelen er tilordnet.
409	KmsInvalidAccessToken	Tilgangstoken som ble oppgitt i forespørselen, er ugyldig.
410	KmsAccessTokenExpired	Angitt accessToken har utløpt.
411	KmsAccessTokenInvalidTenantId	accessToken har ugyldig TenantId-verdi.

Tabell 4-4 KMS Admin Console-feil, typer og beskrivelser (forts.)

Feilkode	Feiltype	Beskrivelse
412	KmsAccessTokenTenantIdMismatch	TenantId i angitt accessToken samsvarer ikke med funksjonsappen TenantId.
413	KmsInvalidKeyId	KeyId er null eller tom.
414	KmsDeleteKeyUnauthorized	Brukeren er ikke autorisert til å slette nøkler. Brukeren tilhører ikke den autoriserte AD-gruppen som har tillatelse til å kontakte dette API-et.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Forsøk på å gjenopprette hemmeligheten mislyktes, og den kunne ikke gjenopprettes. Brukeren bør prøve igjen.
416	KmsInvalidGetKeysRequest	Hent nøkler-forespørselen er ugyldig.
417	KmsGetKeysUnauthorized	Brukeren er ikke autorisert til å hente nøkler. Brukeren tilhører ikke den autoriserte AD-gruppen som har tillatelse til å kontakte dette API-et.
418	KmsInvalidRequestPayload	Forespørsel mottatt av API er ugyldig.
419	KmsRequestRequired	Mottatt forespørsel må ikke være tom.
420	KmsKeyNotConcurrent	Nøkkelen i tabellagringen er oppdatert eller endret siden sist brukeren hentet en kopi.