HP Sure Admin -käyttöopas

YHTEENVETO

HP Sure Adminin avulla IT-järjestelmänvalvojat voivat turvallisesti hallinnoida arkaluonteisia laiteohjelmistoasetuksia käyttämällä varmenteita ja julkiseen avaimeen perustuvaa salausta.

Oikeudelliset tiedot

Luottamuksellinen tietokoneohjelmisto. Ohjelmiston hallintaan, käyttöön ja kopiointiin tarvitaan HP:n voimassa oleva lisenssi. Yhdysvaltojen hallitukselle myönnetään HP:n kaupallinen vakiolisenssi kaupallisiin ohjelmistotuotteisiin, tietokoneohjelmiston dokumentaation ja kaupallisten kohteiden teknisiin tietoihin säädösten FAR 12.211 ja 12.212 mukaan.

Näitä tietoja voidaan muuttaa ilman erillistä ilmoitusta. Ainoat HP:n tuotteita ja palveluja koskevat takuut mainitaan erikseen kyseisten tuotteiden ja palveluiden mukana toimitettavissa takuuehdoissa. Tässä aineistossa olevat tiedot eivät oikeuta lisätakuisiin. HP ei vastaa tässä esiintyvistä mahdollisista teknisistä tai toimituksellisista virheistä tai puutteista.

Toinen painos: lokakuu 2021

Ensimmäinen painos: joulukuu 2019

Asiakirjan osanumero: L83995-352

Sisällysluettelo

1 Aloitusopas

HP Sure Adminin avulla IT-järjestelmänvalvojat voivat turvallisesti hallinnoida arkaluonteisia laiteohjelmistoasetuksia käyttämällä varmenteita ja julkiseen avaimeen perustuvaa salausta.

HP Sure Admin koostuu seuraavista osista:

- **Kohde-PC:** Laajennettua BIOS-todennustilaa tukevat hallinnoitavat alustat.
- **HP Manageability Integration Kit (MIK):** System Center Configuration Manager (SCCM) -laajennus tai HP BIOS Configuration Utility (BCU) BIOS-asetusten etähallintaa varten.
- **HP Sure Admin Local Access Authenticator:** Puhelinsovellus, jonka avulla BIOS-asetusten paikallinen käyttö onnistuu ilman salasanaa. Sovellus antaa kertakäyttöisen PIN-koodin, kun sillä luetaan QRkoodi.

HP Sure Adminin käyttö

Tässä osassa kuvataan HP Sure Adminin käyttöä.

1. Avaa HP Sure Admin -laajennus System Configuration Managerin (SCCM) tai Enhanced BIOS Configuration Utility (BCU) -apuohjelman HP Manageability Integration Kit (MIK) -laajennuksessa.
2. Lataa HP Sure Admin -puhelinsovellus Google Play™ Kaupasta tai Applen App Storesta®.
3. Luo avainpari, jota kohdelaite ja HP Sure Admin -puhelinsovellus käyttävät, jotta saat kertakäyttöisen PIN-koodin BIOSin avaamiseen.

HP Sure Adminin poistaminen käytöstä

Tässä osassa kuvataan HP Sure Adminin käytöstä poiston vaihtoehdot.

- Valitse BIOSin F10-asetuksissa **Restore Security settings to Factory Defaults** (Palauta suojausasetukset tehdasasetuksiin).

HUOMAUTUS: Tämä edellyttää fyysistä läsnäoloa, koska PIN-todentamistunnus F10-asetusten käyttämistä varten annetaan HP Sure Admin -puhelinsovelluksen kautta.

- Tee **Restore Security settings to Factory Defaults** (Palauta suojausasetukset tehdasasetuksiin) -toiminnon WMI-etäkutsu käyttämällä BCU-komentoa.

HUOMAUTUS: Saat lisätietoja HP BIOS Configuration Utility (BCU) -käyttöoppaasta.

- Valitse MIK Security Provisioning -sivulla **Deprovision** (Pura käyttömahdollisuus).

2 Avaimien luonti ja hallinnointi

Suorita suojauksen valmistelu MIK:ssa ennen laajennetun BIOS-todennustilan käyttöönottoa. Laajennetun BIOS-todennustilan on oltava käytössä, jotta avaimia voidaan luoda ja viedä. BIOS-todennustilan ottaminen käyttöön:

▲ Voit luoda ja viedä avaimia avaamalla HP Sure Admin -laajennuksen ja valitsemalla **Enhanced BIOS Authentication Mode** (Laajennettu BIOS-todennustila).

Avainten luonti ja vienti

On kolme erilaista tapaa luoda paikalliset yhteysavainparit sekä ottaa käyttöön HP Sure Admin -puhelinsovellus, jolla avainta käytetään:

- Luo ja vie avain manuaalisella jaolla sivulla 2
- Avaimen luonti ja vienti Azure AD Revocationin avulla sivulla 3
- Avaimen luonti ja lähetys Azure AD Group OneDriveen: sivulla 3

Luo ja vie avain manuaalisella jaolla

Käyttämällä tätä vaihtoehtoa voit viedä paikallisen käyttöoikeusavaimen ja jakaa sen manuaalisesti HP Sure Admin -puhelinsovellukseen sähköpostilla tai muulla tavalla.

HUOMAUTUS: Tämä vaihtoehto ei edellytä HP Sure Admin -puhelinsovelluksen verkkoyhteyttä kertakäyttöisen PIN-koodin saamiseksi.

1. Kirjoita avaimen nimi **Key Name** (Avaimen nimi) -tekstiruutuun.
2. Syötä tunnuslause **Passphrase** (Tunnuslause) -tekstiruutuun.

   HUOMAUTUS: Tunnuslausetta käytetään viedyn avaimen suojaamiseen, ja se tulee antaa, jotta HP Sure Admin -puhelinsovelluksen käyttäjä voi tuoda avaimen.

3. Valitse **Browse** (Selaa) ja valitse, mihin polku viedään järjestelmässä.
4. Valitse **Create Key** (Luo avain). Avaimesi luodaan onnistuneesti, kun **Luo avain** -painikkeen vieressä näkyy ilmoituskuvake **Key successfully created** (Avaimen luonti onnistui).
5. Valitse **Seuraava**. Yhteenvetosivulla näytetään syöttämäsi HP Sure Admin -asetukset.
6. Valitse **Save Policy** (Tallenna käytäntö). Käytäntö on tallennettu, kun viesti **Saved successfully** (Tallennus onnistui) tulee näkyviin.
7. Siirry kansioon, johon tallensit avaimen, ja jaa se HP Sure Admin -puhelinsovellukseen käyttämällä menetelmää, esimerkiksi sähköpostia, joka on kyseisen käyttäjän saatavilla kyseisellä laitteella. Käyttäjä tarvitsee myös tunnuslauseen avaimen tuomiseen. HP suosittelee käyttämään eri jakelumenetelmiä avaimelle ja tunnuslauseelle.

   HUOMAUTUS: Lähetä QR-koodi alkuperäisessä koossaan. Sovellus ei voi lukea kuvaa oikein, jos sen koko on pienempi kuin 800 × 600.

Avaimen luonti ja vienti Azure AD Revocationin avulla

Käyttämällä tätä vaihtoehtoa voit yhdistää paikallisen yhteysavaimen määritettyyn Azure Active Directory -ryhmään ja edellyttää, että HP Sure Admin -puhelinsovellus vaatii sekä käyttäjän todennuksen Azure Active Directoryssa että vahvistuksen siitä, että käyttäjä on määritetyn ryhmän jäsen, ennen paikallisen PIN-käyttöoikeustunnuksen antamista. Tämä menetelmä edellyttää myös paikallisen yhteysavaimen manuaalista jakamista puhelinsovellukseen sähköpostin välityksellä tai muulla tavalla.

HUOMAUTUS: Tämä vaihtoehto edellyttää, että HP Sure Admin -puhelinsovelluksella on verkkoyhteys, jotta se voi saada kertakäyttöisen PIN-koodin.

1. Kirjoita avaimen nimi **Key Name** (Avaimen nimi) -tekstiruutuun.
2. Syötä tunnuslause **Passphrase** (Tunnuslause) -tekstiruutuun.

   HUOMAUTUS: Tunnuslausetta käytetään viedyn avaimen suojaamiseen, ja se tulee antaa, jotta HP Sure Admin -puhelinsovelluksen käyttäjä voi tuoda avaimen.

3. Valitse **Azure AD Login** (Azure AD -kirjautuminen) ja kirjaudu sisään.
4. Valitse ryhmäsi nimi avattavasta **Azure AD Group Name** (Azure AD -ryhmän nimi) luetteloruudusta. Sinun on oltava ryhmän jäsen, jotta voit käyttää avainta.
5. Valitse **Browse** (Selaa) ja valitse, mihin polku viedään järjestelmässä.
6. Valitse **Create Key** (Luo avain). Avaimesi luodaan onnistuneesti, kun **Luo avain** -painikkeen vieressä näkyy ilmoituskuvake **Key successfully created** (Avaimen luonti onnistui).
7. Valitse **Seuraava**. Yhteenvetosivulla näytetään syöttämäsi HP Sure Admin -asetukset.
8. Valitse **Save Policy** (Tallenna käytäntö). Käytäntö on tallennettu, kun viesti **Saved successfully** (Tallennus onnistui) tulee näkyviin.
9. Siirry kansioon, johon tallensit avaimen, ja jaa se HP Sure Admin -puhelinsovellukseen käyttämällä menetelmää, esimerkiksi sähköpostia, joka on kyseisen käyttäjän saatavilla kyseisellä laitteella. Käyttäjä tarvitsee myös tunnuslauseen avaimen tuomiseen. HP suosittelee käyttämään eri jakelumenetelmiä avaimelle ja tunnuslauseelle.

   HUOMAUTUS: Lähetä QR-koodi alkuperäisessä koossaan. Sovellus ei voi lukea kuvaa oikein, jos sen koko on pienempi kuin 800 × 600.

Avaimen luonti ja lähetys Azure AD Group OneDriveen:

(Suositus) Käytä tätä vaihtoehtoa välttääksesi paikallisen yhteysavaimen tallentaminen puhelimeen. Kun valitset tämän vaihtoehdon, MIK tallentaa paikallisen yhteysavaimen määritettyyn OneDrive-kansioon, jota vain valtuutettu ryhmä voi käyttää. HP Sure Admin -puhelinsovelluksen käyttäjän tulee suorittaa Azure AD -todennus aina kun PIN-koodia tarvitaan.

1. Kirjoita avaimen nimi **Key Name** (Avaimen nimi) -tekstiruutuun.
2. Syötä tunnuslause **Passphrase** (Tunnuslause) -tekstiruutuun.
3. Valitse **Azure AD Login** (Azure AD -kirjautuminen) ja kirjaudu sisään.
4. Valitse ryhmäsi nimi avattavasta Azure AD Group Name (Azure AD -ryhmän nimi) luetteloruudusta.

   HUOMAUTUS: Sinun on oltava ryhmän jäsen, jotta voit käyttää avainta.

5. Syötä **OneDrive**-tekstiruutuun sen OneDrive-kansion nimi, johon haluat tallentaa avaimen.
6. Valitse **Browse** (Selaa) ja valitse, mihin polku viedään järjestelmässä.
7. Valitse **Create Key** (Luo avain).

HUOMAUTUS: Avaimesi on lisätty onnistuneesti määritettyyn OneDrive-kansioon ja viety määritettyyn paikalliseen kansioon, kun **Create Key** (Luo avain) -painikkeen vieressä näkyy ilmoituskuvake **Key successfully created** (Avaimen luonti onnistui).

8. Valitse **Seuraava**. Yhteenvetosivulla näytetään syöttämäsi HP Sure Admin -asetukset.
9. Valitse **Save Policy** (Tallenna käytäntö). Käytäntö on tallennettu, kun viesti **Saved successfully** (Tallennus onnistui) tulee näkyviin.

HUOMAUTUS: Tällöin ei ole tarpeen lähettää mitään HP Sure Admin -puhelinsovellukseen esivalmistelua varten. Kohde-PC:t valmistellaan osoittamaan QR-koodiin sisältyvään OneDrive-sijaintiin. HP Sure Admin -puhelinsovellus käyttää tätä osoitinta OneDrive-sijainnin käyttämiseen, jos käyttäjä kuuluu valtuutettuun ryhmään ja suorittaa todennuksen onnistuneesti.

3 Puhelimen asennus

Lataa HP Sure Admin -puhelinsovellus Google Playsta tai Apple Storesta.

- Lataa HP Sure Admin Android-puhelimille Google Storesta.
- Lataa HP Sure Admin iOS-puhelimille Apple Storesta.

HP Sure Admin -puhelinsovelluksen käyttäminen BIOSin lukituksen avaamiseen

HP Sure Admin -mobiilisovellus korvaa BIOS-salasanan käyttämisen BIOS-asetusten paikallisessa käytössä antamalla kertakäyttöisen PIN-koodin, joka saadaan lukemalla kohdekoneen esittämä QR-koodi.

Näiden vaiheiden avulla voit tallentaa avaimen paikallisesti puhelimeen skenaariossa, jossa avain lähetetään puhelinsovelluksen käyttäjälle. Seuraavassa esimerkissä avain lähetetään HP Sure Admin -puhelinsovelluksen käyttäjälle, ja käyttäjä avaa sähköpostin puhelimessa.

1. Avaa avaimen sisältävä sähköpostiviesti.
2. Kun **Enrollment** (Rekisteröinti) -sivu tulee näkyviin, kirjoita tunnuslause **Enter passphrase** (Anna tunnuslause) -tekstiruutuun ja sähköpostisi **Enter your email address** (Anna sähköpostiosoitteesi) -tekstiruutuun avaimen salauksen purkamiseksi. Lisää avain sitten HP Sure Admin -sovellukseen. Lukituksen avaamisen PIN-koodi näytetään **Your PIN** (PIN-koodisi) -sivulla.

   HUOMAUTUS: Tässä vaiheessa avain tallennetaan mobiililaitteelle ja rekisteröinti suoritetaan. Nyt voit HP Sure Admin -puhelinsovelluksen avulla käyttää laitetta, joka on määritetty käytettäväksi kyseisellä avaimella. Sähköpostiosoite on pakollinen vain, jos järjestelmänvalvoja edellyttää sitä.

3. Syötä PIN-koodi **BIOSin Enter Response Code** (Anna vastauskoodi) -tekstiruutuun.

BIOSiin pääsy rekisteröinnin jälkeen

Käyttöoikeuden hankkiminen BIOS-asennukseen kohdekoneella rekisteröinnin jälkeen:

1. Siirry BIOS-asetuksiin käynnistyksen aikana kohdekoneella.
2. Valitse **Scan QR Code** (Lue QR-koodi) puhelinsovelluksessa ja lue QR-koodi kohdekoneella.
3. Jos käyttäjän todennusta pyydetään, anna tunnistetiedot.
4. PIN-koodi, jonka lukitus on avattu, näytetään **Your PIN** (PIN-koodisi) -sivulla.
5. Kirjoita PIN-koodi **BIOS Enter Response Code** (BIOSin Syötä vastauskoodi) -tekstiruutuun kohdekoneella.

BIOSin avaaminen Azure AD Group OneDrivella

HP Sure Adminin käyttäminen BIOSin lukituksen avaamiseen Azure AD -ryhmän OneDriven avulla:

1. Valitse **Scan QR Code** (Lue QR-koodi) ja lue sitten BIOSin QR-koodi.

   HUOMAUTUS: HP Sure Admin -sovellus näyttää Azure AD -kirjautumissivun.

2. Kirjaudu sisään Azure-tiliisi.

3. Syötä PIN-koodi **BIOSin Enter Response Code** (Anna vastauskoodi) -tekstiruutuun.

HUOMAUTUS: HP Sure Admin -sovellus ei tallenna avainta paikallisesti tässä vaihtoehdossa. HP Sure Admin -puhelinsovelluksella on oltava verkkoyhteys, ja käyttäjän tulee suorittaa todennus aina kun kertakäyttöistä PIN-koodia tarvitaan.

4 HP Sure Admin -virhekoodit

Tämän osion taulukossa on lisätietoja HP Sure Admin- ja KMS-hallintakonsolin virhekoodeista, tyypeistä ja niiden kuvauksesta.

Taulukko 4-1 HP Sure Admin -sovelluksen virhekoodit, tyypit ja niiden kuvaukset

Virhekoodi	Virhetyyppi	Kuvaus
100	QRCodeUnknownError	Yleinen virhe.
101	QRCodeDeserialization	QR-koodin JSON-tiedostoa ei voi lukea. Merkkijono ei ole kelvollinen JSON-tiedosto tai tiedot eivät kelpaa.
102	QRCodeInvalidImage	Luettu QR-koodin kuva ei kelpaa. QR-koodin kuvatiedostoa ei voi lukea.
103	QRCodeNoPayload	Luettu QR-koodin kuva ei kelpaa. Kuvatiedostolla ei ole JSON-tietoja.
104	QRCodeInvalid	QR-koodin JSON-tietoja ei voi lukea. Merkkijono ei ole kelvollinen JSON tai QR-kuvan tiedot eivät kelpaa.
105	QRCodeInvalidKeyIdHash	QR-koodin JSON-tietojen julkisen avaimen hajautusarvo ei vastaa rekisteröitymispaketin julkisen avaimen hajautusarvoa (avaimen tunnuksen tiedot).
106	QRCodeTampered	Skannattu QR-koodikuva on peukaloitu ja virheellinen.
107	QRCodeTamperedOrInvalidPassPhrase	Skannattu QR-koodikuva on peukaloitu ja virheellinen, tai syötetty salasana on väärä.

Taulukko 4-2 OneTime-käyttöavain OneDrive-virheistä, -tyypeistä ja niiden kuvauksista

Virhekoodi	Virhetyyppi	Kuvaus
200	OneTimeKeyError	Yleinen virhe.
201	OneTimeKeyNoUserGroups	Kirjautunut käyttäjä ei kuulu mihinkään organisaatioosi kuuluvaan AD-ryhmään.
203	OneTimeKeyInvalidUserGroup	Kirjautunut käyttäjä ei kuulu AD-ryhmään, johon tämä avain on määrätty.
204	OneTimeKeyQRFileDoesNotExist	AD-ryhmän OneDrive-kansiossa ei ole OneTime-avaintiedostoa.
205	OneTimeKeyInvalidQRFile	AD-ryhmän OneDrive-kansiossa oleva OneTime-avaintiedosto ei kelpaa.
206	OneTimeKeyInvalidQRpayload	OneTime-avaintiedosto on olemassa, mutta tiedoston tietoja ei voi lukea.

Taulukko 4-3 Azure AD -valtuusvirheet

Virhekoodi	Virhetyyppi	Kuvaus
300	AzureADUnknownError	Yleinen virhe.
301	AzureADInvalidDomain	Syötetty sähköpostiosoite ei vastaa QR-koodin kuvassa määriteltyä toimialueen nimeä.
302	AzureADAccessToken	Virhe haettaessa käyttöoikeustunnusta Azure AD:stä. Käyttäjä ei voi kirjautua organisaatiosi Azure AD:hen, tai sovelluksella ei ole tarvittavia oikeuksia yhdistää organisaatiosi Azure AD:hen. Voi olla myös, että käyttäjä peruutti todennuksen.
303	AzureADUserProfile	HP Sure Admin -sovellus otettiin käyttöön käyttäjäprofiilitietojen saamiseksi organisaatiosi Azure AD:stä.
304	AzureADUserPrincipalMismatch	Syötetty sähköpostiosoite ei vastaa kirjautuneen käyttäjän päänimeä.
305	AzureADUserInvalidUserGroup	Kirjautunut käyttäjä ei kuulu tämän avaimen määritettyyn Azure AD -ryhmään.

Taulukko 4-4 KMS Admin Consolen virheet, tyypit ja niiden kuvaukset

Virhekoodi	Virhetyyppi	Kuvaus
401	KmsUnauthorized	Käyttäjä ei ole valtuutettu käyttämään KMS-palvelua.
402	KmsKeyDoesNotExist	Vastaavaa yksityistä avainta ei ole KMS-avainholvissa. Avain on tällä hetkellä poistettuna, mutta palautettavassa tilassa eikä sen nimeä voi käyttää uudelleen tässä tilassa. Avain voidaan vain palauttaa tai poistaa.
403	KmsKeyDoesNotExistInTableStorage	Avainta ei ole taulukoissa.
404	KmsUploadKeyErrorInKeyVault	Virhe avaimen lisäämisen aikana avainholviin.
405	KmsUploadKeyUnauthorized	Käyttäjällä ei ole oikeutta ladata avaimia. Käyttäjä ei kuulu valtuutettuun AD-ryhmään, jolla on oikeus tehdä API-kutsu.
406	KmsInvalidAzureADLogin	Käyttäjä ei ole kirjautunut sisään Azure Tenant AAD:hen.
407	KmsNoUserGroups	Kirjautunut käyttäjä ei kuulu mihinkään organisaatiosi AD-ryhmään.
408	KmsInvalidUserGroup	Kirjautunut käyttäjä ei kuulu AD-ryhmään, johon tämä avain on määrätty.
409	KmsInvalidAccessToken	Pyynnössä annettu käyttötunnus on virheellinen.
410	KmsAccessTokenExpired	Annettu accessToken-tunnus on vanhentunut.

Taulukko 4-4 KMS Admin Consolen virheet, tyypit ja niiden kuvaukset (jatkoa)

Virhekoodi	Virhetyyppi	Kuvaus
411	KmsAccessTokenInvalidTenantId	Annetulla accessToken-tunnus sisältää virheellisen TenantId-arvon.
412	KmsAccessTokenTenantIdMismatch	Annetun accessToken-tunnuksen TenantId ei täsmää funktiosovelluksen TenantId-tunnusta.
413	KmsInvalidKeyId	KeyId-tunnus on nolla tai tyhjä.
414	KmsDeleteKeyUnauthorized	Käyttäjällä ei ole oikeutta poistaa avaimia. Käyttäjä ei kuulu valtuutettuun AD-ryhmään, jolla on oikeus tehdä API-kutsu.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Yritys palauttaa salaisuus epäonnistui, eikä sitä voitu palauttaa. Käyttäjän tulee yrittää uudelleen.
416	KmsInvalidGetKeysRequest	Avainten hakupyyntö on virheellinen.
417	KmsGetKeysUnauthorized	Käyttäjällä ei ole oikeutta saada avaimia. Käyttäjä ei kuulu valtuutettuun AD-ryhmään, jolla on oikeus tehdä API-kutsu.
418	KmsInvalidRequestPayload	API:n vastaanottama pyyntö on virheellinen.
419	KmsRequestRequired	Vastaanotettu pyyntö ei voi olla tyhjä.
420	KmsKeyNotConcurrent	Taulukkotaltion avainta päivitettiin tai muokattiin sen jälkeen, kun käyttäjä viimeksi nouti kopion.