



Användarhandbok för HP Sure Admin

ÖVERSIKT

Med HP Sure Admin kan IT-administratörer hantera känsliga enhetsinställningar för inbyggd programvara på ett säkert sätt med hjälp av certifikat och kryptografi för offentlig nyckel, vid både fjärrhantering och lokal hantering, istället för att använda lösenord.

Rättslig information

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

Apple är ett varumärke som tillhör Apple Inc. och är registrerat i USA och andra länder.

Google Play är ett varumärke som tillhör Google LLC.

Konfidentiell datorprogramvara. Det krävs en giltig licens från HP för att äga, använda eller kopiera programvaran. Överensstämmer med FAR 12.211 och 12.212 och kommersiell datorprogramvara, dokumentation av datorprogramvara samt tekniska data för kommersiella artiklar är licensierade till USA:s regering under HPs standardiserade kommersiella licens.

Informationen i detta dokument kan komma att bli inaktuell utan föregående meddelande. De enda garantier som gäller för HP-produkter och -tjänster beskrivs i de uttryckliga garantier som medföljer produkterna och tjänsterna. Ingenting i detta dokument ska anses utgöra en ytterligare garanti. HP ska inte hållas ansvarigt för tekniska fel, redigeringsfel eller utelämnad information i detta dokument.

Andra utgåvan: oktober 2021

Första utgåvan: December 2019

Dokumentartikelnummer: L83995-102

Innehåll

1 Komma igång	1
Använda HP Sure Admin	1
Inaktivera HP Sure Admin	1
2 Skapa och hantera nycklar	2
Skapa och exportera nycklar	2
Skapa och exportera nyckel med manuell distribution	2
Skapa och exportera nyckel med Azure AD-återkallning	3
Skapa och skicka en nyckel till OneDrive i Azure AD-gruppen	3
3 Telefoninställningar	5
Använda telefonappen HP Sure Admin för att låsa upp BIOS	5
Få tillgång till BIOS-inställningar efter registrering	5
Låsa upp BIOS med Portal Ad Group OneDrive	5
4 HP Sure Admin-felkoder	7

1 Komma igång

Med HP Sure Admin kan IT-administratörer hantera känsliga enhetsinställningar för inbyggd programvara på ett säkert sätt med hjälp av certifikat och kryptografi för offentlig nyckel, vid både fjärrhantering och lokal hantering, istället för att använda lösenord.

HP Sure Admin består av följande delar:

- **Måldator:** De plattformar som har stöd för förbättrat BIOS-autentiseringsläge som hanteras.
- **HP Manageability Integration Kit (MIK):** Plugin-programmet för System Center Configuration Manager (SCCM) eller HP BIOS Configuration Utility (BCU) för fjärrhantering av BIOS-inställningarna.
- **HP Sure Admin Local Access Authenticator:** En telefonapp som ersätter lösenordet för lokal åtkomst till BIOS-inställningarna genom att istället skanna en QR-kod med vilken en engångs-PIN-kod erhålls.

Använda HP Sure Admin


Det här avsnittet beskriver hur du använder HP Sure Admin.

1. Öppna plugin-programmet för HP Sure Admin inuti plugin-programmet för HP Manageability Integration Kit (MIK) för System Configuration Manager (SCCM) eller Enhanced BIOS Configuration Utility (BCU).
2. Hämta telefonappen HP Sure Admin från antingen Google Play™ Store eller Apple App Store®.
3. Skapa ett nyckelpar som används av målenheten och telefonappen HP Sure Admin för att erhålla en engångs-PIN-kod för upplåsning av BIOS.

Inaktivera HP Sure Admin

I det här avsnittet beskrivs alternativen för inaktivering av HP Sure Admin:

- I BIOS F10-inställningen väljer du **Restore Security settings to Factory Defaults (Återställ säkerhetsinställningar till fabriksinställningar)**.

 **OBS!** Det kräver fysisk närvaro då PIN-koden för autentisering för åtkomst till F10-inställningarna tillhandahålls via telefonappen HP Sure Admin.

- Använd BCU-kommandot för att fjärranropa WMI för **återställning av säkerhetsinställningarna till fabriksinställningar**.

 **OBS!** Mer information finns i användarhandboken för HP BIOS Configuration Utility (BCU).

- På sidan MIK Security Provisioning (Säkerhetsprovisionering i MIK) väljer du **Deprovision (Avprovisionera)**.

2 Skapa och hantera nycklar

Slutför säkerhetsprovisioneringen i MIK innan du aktiverar förbättrat BIOS-autentiseringsläge. Förbättrat BIOS-autentiseringsläge måste vara aktiverat för att du ska kunna skapa och exportera nycklar. Så här aktiverar du BIOS-autentiseringsläge:

- ▲ Öppna pluginprogrammet HP Sure Admin och välj **Enhanced BIOS Authentication Mode (Förbättrat BIOS-autentiseringsläge)** för att skapa och exportera nycklar.

Skapa och exportera nycklar

Det finns 3 olika sätt att skapa lokala åtkomstnyckelpar och aktivera telefonappen HP Sure Admin för att komma åt nyckeln.


- [Skapa och exportera nyckel med manuell distribution på sidan 2](#)
- [Skapa och exportera nyckel med Azure AD-återkallning på sidan 3](#)
- [Skapa och skicka en nyckel till OneDrive i Azure AD-gruppen på sidan 3](#)

Skapa och exportera nyckel med manuell distribution


Använd det här alternativet för att exportera behörighetsnyckeln för lokal åtkomst och sedan distribuera den manuellt till telefonappen HP Sure Admin via e-post eller någon annan metod.

 **OBS!** Med det här alternativet krävs inte att telefonappen HP Sure Admin är nätverksansluten för att erhålla en engångs-PIN-kod.

1. Ange ett namn på nyckeln i inmatningsrutan **Key Name (Nyckelnamn)**.
2. Ange lösenordsfrasen i inmatningsrutan **Passphrase (Lösenordsfras)**.

 **OBS!** Lösenordsfrasen används för att skydda den exporterade nyckeln och måste tillhandahållas så att användaren av telefonappen HP Sure Admin kan importera nyckeln.

3. Välj **Browse (Bläddra)** och välj sedan vart du vill exportera sökvägen i systemet.
4. Välj **Create Key (Skapa nyckel)**. Nyckeln skapas när en meddelandeikon visas bredvid knappen **Create Key (Skapa nyckel)** med meddelandet **"Key successfully created" ("Nyckeln har skapats")**.
5. Välj **Next (Nästa)**. På sammanfattningssidan visas inställningarna för HP Sure Admin som du har valt.
6. Välj **Save Policy (Spara princip)**. Principen sparas när meddelandet **Saved successfully (Har sparats)** visas.
7. Navigera till den mapp där du sparade nyckeln och distribuera den till telefonappen HP Sure Admin med en metod som är tillgänglig för användaren på den enheten, t.ex. e-post. Användaren behöver också lösenordsfrasen för att importera nyckeln. HP rekommenderar att du använder olika distributionsmetoder för nyckeln och lösenordfrasen.


 **OBS!** När du skickar QR-koden måste den skickas i ursprunglig storlek. Appen kan inte avläsa bilden på rätt sätt om den är mindre än 800 × 600 i storlek.

Skapa och exportera nyckel med Azure AD-återkallning


Använd det här alternativet för att ansluta nyckeln för lokal åtkomst till en angiven Azure Active Directory-grupp och kräva att telefonappen HP Sure Admin kräver både användarautentisering till Azure Active Directory och bekräftelse på att användaren är medlem i angiven grupp innan en PIN-kod för lokal åtkomst tillhandahålls. För den här metoden krävs även manuell distribution av behörighetsnyckeln för lokal åtkomst till telefonappen via e-post eller någon annan metod.

 **OBS!** För det här alternativet krävs att telefonappen HP Sure Admin har nätverksanslutning för att erhålla en engångs-PIN-kod.

1. Ange ett namn på nyckeln i inmatningsrutan **Key Name (Nyckelnamn)**.
2. Ange lösenordsfrasen i inmatningsrutan **Passphrase (Lösenordsfras)**.

 **OBS!** Lösenordsfrasen används för att skydda den exporterade nyckeln och måste tillhandahållas så att användaren av telefonappen HP Sure Admin kan importera nyckeln.


3. Välj **Azure AD Login (Inloggning för Azure AD)** och logga in.
4. Välj namnet på gruppen i listrutan **Azure AD Group Name (Namn på Azure AD-grupp)**. Du måste vara medlem i gruppen för att få åtkomst till nyckeln.
5. Välj **Browse (Bläddra)** och välj sedan vart du vill exportera sökvägen i systemet.
6. Välj **Create Key (Skapa nyckel)**. Nyckeln skapas när en meddelandeikon visas bredvid knappen **Create Key (Skapa nyckel)** med meddelandet **"Key successfully created" ("Nyckeln har skapats")**.
7. Välj **Next (Nästa)**. På sammanfattningssidan visas inställningarna för HP Sure Admin som du har valt.
8. Välj **Save Policy (Spara princip)**. Principen sparas när meddelandet **Saved successfully (Har sparats)** visas.
9. Navigera till den mapp där du sparade nyckeln och distribuera den till telefonappen HP Sure Admin med en metod som är tillgänglig för användaren på den enheten, t.ex. e-post. Användaren behöver också lösenordsfrasen för att importera nyckeln. HP rekommenderar att du använder olika distributionsmetoder för nyckeln och lösenordfrasen.

 **OBS!** När du skickar QR-koden måste den skickas i ursprunglig storlek. Appen kan inte avläsa bilden på rätt sätt om den är mindre än 800 × 600 i storlek.

Skapa och skicka en nyckel till OneDrive i Azure AD-gruppen

(Rekommenderas) Använd det här alternativet för att undvika att lagra den behörighetsnyckeln för lokal åtkomst på telefonen. När du väljer det här alternativet lagras behörighetsnyckeln för lokal åtkomst i angiven OneDrive-mapp som endast är tillgänglig för den behöriga gruppen. Användaren av telefonappen HP Sure Admin måste verifieras i Azure AD varje gång en PIN-kod behövs.

1. Ange ett namn på nyckeln i inmatningsrutan **Key Name (Nyckelnamn)**.
2. Ange lösenordsfrasen i inmatningsrutan **Passphrase (Lösenordsfras)**.
3. Välj **Azure AD Login (Inloggning för Azure AD)** och logga in.
4. Välj namnet på gruppen i listrutan **Azure AD Group Name (Namn på Azure AD-grupp)**.

 **OBS!** Du måste vara medlem i gruppen för att få åtkomst till nyckeln.

5. Ange namnet på den OneDrive-mapp där du vill att nyckeln ska sparas i inmatningsrutan **OneDrive**.

6. Välj **Browse (Bläddra)** och välj sedan vart du vill exportera sökvägen i systemet.

7. Välj **Create Key (Skapa nyckel)**.



OBS! Din nyckel läggs till i angiven OneDrive-mapp och exporteras till angiven lokal mapp när en meddelandeikon visas bredvid knappen **Create Key (Skapa nyckel)** med meddelandet **Key successfully created (Nyckeln har skapats)**.

8. Välj **Next (Nästa)**. På sammanfattningssidan visas HP Sure Admin-inställningarna som du har angett.

9. Välj **Save Policy (Spara princip)**. Principen sparas när meddelandet **Saved successfully (Har sparats)** visas.



OBS! I det här scenariot behöver du inte skicka något till telefonappen HP Sure Admin för att förprovisionera den. Måldatorerna provisioneras för att peka på OneDrive-platsen som ingår i QR-koden. Telefonappen HP Sure Admin använder den här pekaren för att komma åt OneDrive-platsen om användaren ingår i och verifieras för den behöriga gruppen.

3 Telefoninställningar

Hämta telefonappen HP Sure Admin från antingen Google Play eller Apple Store.

- Hämta HP Sure Admin från Google Store för Android-telefoner.
- Hämta HP Sure Admin från Apple Store för iOS-telefoner.

Använda telefonappen HP Sure Admin för att låsa upp BIOS

Telefonappen HP Sure Admin ersätter användning av BIOS-lösenordet för lokal åtkomst till BIOS-inställningarna genom att tillhandahålla en engångs-PIN-kod genom att skanna QR-koden som visas av målmaskinen.

Följ de här stegen för att spara nyckeln lokalt på telefonen i fall där nyckeln skickas till telefonappens användare. I följande exempel skickas nyckeln till användaren av telefonappen HP Sure Admin och användaren öppnar telefonens e-post.

1. Öppna e-postmeddelandet som innehåller nyckeln.
2. När sidan **Enrollment (Registrering)** visas anger du lösenordsfrasen i inmatningsrutan **Enter passphrase (Ange lösenordsfras)** och din e-postadress i rutan **Enter your email address (Ange din e-postadress)** för att dekryptera nyckeln och lägga till den i programmet HP Sure Admin. PIN-koden för upplåsning visas på sidan **Your PIN (Din PIN-kod)**.



OBS! I det här steget sparas nyckeln i den mobila enheten och registreringen slutförs. Nu kan du använda telefonappen HP Sure Admin för att komma åt en enhet som har provisionerats för att vara tillgänglig via den här nyckeln. En e-postadress krävs endast om administratören kräver det.

3. Ange PIN-koden i inmatningsrutan **BIOS Enter Response Code (Ange svarskod för BIOS)**.

Få tillgång till BIOS-inställningar efter registrering

Så här får du tillgång till BIOS-inställningarna på en måldator efter registrering:

1. Ange BIOS-inställningarna på måldatorn vid start.
2. Välj **Scan QR Code (Skanna QR-kod)** i telefonprogrammet och skanna QR-koden på målmaskinen.
3. Om du uppmanas att ange användarverifiering visar du dina autentiseringsuppgifter.
4. PIN-koden för upplåsning visas på sidan **Your PIN (Din PIN-kod)**.
5. Ange PIN-koden i inmatningsrutan **BIOS Enter Response Code (Ange svarskod för BIOS)** på måldatorn.

Låsa upp BIOS med Portal Ad Group OneDrive

Så här använder du HP Sure Admin för att låsa upp BIOS med OneDrive i Azure AD-gruppen:

1. Välj **Scan QR Code (Skanna QR-kod)** och skanna sedan QR-koden för BIOS.



OBS! Inloggningssidan för Azure AD visas i telefonappen HP Sure Admin.

2. Logga in på ditt Azure-konto.
3. Ange PIN-koden i inmatningsrutan **BIOS Enter Response Code (Ange svars kod för BIOS)**.



OBS! Nyckeln sparas inte lokalt med HP Sure Admin-appen i det här scenariot. Telefonappen HP Sure Admin måste ha nätverksanslutning och användaren måste verifieras varje gång en engångs-PIN-kod behövs.

4 HP Sure Admin-felkoder

I tabellen i det här avsnittet hittar du felkoder, typer och beskrivningar av HP Sure Admin och KMS Admin Console.

Tabell 4-1 HP Sure Admin-appfelkoder, typer och deras beskrivningar

Felkod	Feltyp	Beskrivning
100	QRCodeUnknownError	Allmänt fel.
101	QRCodeDeserialization	Det går inte att läsa QR-kod JSON. Antingen är strängen inte i en giltig JSON-fil eller så är data ogiltiga.
102	QRCodeInvalidImage	Den skannade avbildningen av QR-koden är ogiltig. Det går inte att läsa avbildningsfilen för QR-koden.
103	QRCodeNoPayload	Den skannade avbildningen av QR-koden är ogiltig. Avbildningsfilen har ingen JSON-nyttolast.
104	QRCodeInvalid	Det gick inte att avläsa JSON för QR-koden. Antingen är strängen inte en giltig JSON eller så är data i QR-bilden ogiltiga.
105	QRCodeInvalidKeyldHash	Den offentliga nyckelns hashvärde i JSON för QR-koden stämmer inte överens med registreringspaketets hashvärde för allmän nyckel (KeyID-data).
106	QRCodeTampered	Den skannade avbildningen av QR-koden är manipulerad och ogiltig.
107	QRCodeTamperedOrInvalidPassPhrase	Den skannade avbildningen av QR-koden är manipulerad och ogiltig, eller angivet lösenord är felaktigt.

Tabell 4-2 OneTime-åtkomstnyckel från OneDrive-fel, typer och deras beskrivningar

Felkod	Feltyp	Beskrivning
200	OneTimeKeyError	Allmänt fel.
201	OneTimeKeyNoUserGroups	Den inloggade användaren tillhör inte någon AD-grupp som finns i din organisation.
203	OneTimeKeyInvalidUserGroup	Den inloggade användaren tillhör inte den AD-grupp som tilldelats den här nyckeln.
204	OneTimeKeyQRFileDoesNotExist	OneTime-nyckelfilen finns inte i AD-gruppens OneDrive-mapp.
205	OneTimeKeyInvalidQRFile	OneTime-nyckelfilen i AD-gruppens OneDrive-mapp är ogiltig.
206	OneTimeKeyInvalidQRpayload	OneTime-nyckelfilen finns, men kan inte avläsa filens nyttolast.

Tabell 4-3 Azure AD-autentiseringsfel

Felkod	Feltyp	Beskrivning
300	AzureADUnknownError	Allmänt fel.
301	AzureADInvalidDomain	Angiven e-postadress stämmer inte överens med domännamnet som anges i bilden av QR-koden.
302	AzureADAccessToken	Fel vid erhållande av åtkomsttoken från Azure AD. Antingen kan användaren inte logga in på organisationens Azure AD, eller så har appen inte den behörighet som krävs för att ansluta till organisationens Azure AD. Det kan också vara så att användaren avbröt autentiseringen.
303	AzureADUserProfile	HP Sure Admin-appen aktiverades för att hämta information om användarprofilen från organisationens Azure AD.
304	AzureADUserPrincipalMismatch	Angiven e-postadress stämmer inte överens med den inloggade användarens huvudnamn.
305	AzureADUserInvalidUserGroup	Den inloggade användaren tillhör den tilldelade Azure AD-gruppen som tilldelats den här nyckeln.

Tabell 4-4 KMS Admin Console-fel, typer och deras beskrivningar

Felkod	Feltyp	Beskrivning
401	KmsUnauthorized	Användaren är inte behörig att använda KMS-tjänsten.
402	KmsKeyDoesNotExist	Det finns ingen privat matchande nyckel i KMS-nyckelvalvet. Nyckeln är för närvarande i borttaget men återställningsbart tillstånd och dess namn kan inte återanvändas i det här tillståndet. Nyckeln kan endast återställas eller rensas.
403	KmsKeyDoesNotExistInTableStorage	Nyckeln finns inte i tabellagring.
404	KmsUploadKeyErrorInKeyVault	Ett fel uppstod när en nyckel skulle läggas till i nyckelvalvet.
405	KmsUploadKeyUnauthorized	Användaren är inte behörig att ladda upp nycklar. Användaren tillhör inte den autentiserade AD-grupp som tillåts anropa detta API.
406	KmsInvalidAzureADLogin	Användaren är inte inloggad i Azure Tenant AAD.
407	KmsNoUserGroups	Den inloggade användaren tillhör inte någon AD-grupp i din org.
408	KmsInvalidUserGroup	Den inloggade användaren tillhör inte den AD-grupp som har tilldelats den här nyckeln.
409	KmsInvalidAccessToken	Den åtkomsttoken som angavs i begäran är ogiltig.

Tabell 4-4 KMS Admin Console-fel, typer och deras beskrivningar (fortsättning)

Felkod	Feltyp	Beskrivning
410	KmsAccessTokenExpired	Medföljande accessToken har upphört.
411	KmsAccessTokenInvalidTenantId	Medföljande accessToken har ogiltigt TenantId-värde.
412	KmsAccessTokenTenantIdMismatch	TenantId i medföljande accessToken stämmer inte överens med funktionsappens TenantId.
413	KmsInvalidKeyId	KeyId är ogiltigt eller tomt.
414	KmsDeleteKeyUnauthorized	Användaren är inte behörig att ta bort nycklar. Användaren tillhör inte den autentiserade AD-grupp som tillåts anropa detta API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Försök att återställa hemligheten misslyckades och det gick inte att återställa den. Användaren bör försöka igen.
416	KmsInvalidGetKeysRequest	Begäran om nycklar är ogiltig.
417	KmsGetKeysUnauthorized	Användaren är inte behörig att hämta nycklar. Användaren tillhör inte den autentiserade AD-grupp som tillåts anropa detta API.
418	KmsInvalidRequestPayload	Den begäran som tas emot av API är ogiltig.
419	KmsRequestRequired	Den mottagna begäran får inte vara tom.
420	KmsKeyNotConcurrent	Nyckeln i tabellagringen uppdaterades eller ändrades sedan användaren senast hämtade en kopia.