Brugervejledning

HP Sure Recover

Første udgave: februar 2020

Dokumentets bestillingsnummer: L93434-081

Syntaksnøgle til brugerinput

Tekst, som du skal indtaste på en brugergrænseflade, er angivet med en skrifttype med `fast bredde`.

Tabel -1 Syntaksnøgle til brugerinput

Element	Beskrivelse
`Tekst uden parenteser eller krøllede parenteser`	Elementer, der skal indtastes præcist som vist
`<Tekst i vinkelparenteser>`	En pladsholder til en værdi, som du skal angive; Udelad parenteserne
`[Tekst i kantede parenteser]`	Valgfrie elementer; Udelad parenteserne
`{Tekst i krøllede parenteser}`	Et sæt elementer, hvor du kun skal vælge et; Udelad de krøllede parenteser
`|`	Et adskillelsestegn til elementer, hvor du kun skal vælge et; Udelad den lodrette linje
`...`	Elementer, der kan eller skal gentages; Udelad ellipsen

Indholdsfortegnelse

1 Sådan kommer du i gang

HP Sure Recover hjælper dig med at installere operativsystemet sikkert fra netværket med minimal brugerinteraktion. Systemer med HP Sure Recover med indbygget geninstallation af systembillede understøtter også installation fra en lokal lagerenhed.

VIGTIGT: Sikkerhedskopiér dine data, før du bruger HP Sure Recover. Da billedbehandlingsprocessen omformaterer drevet, kan det medføre datatab.

Gendannelsesbilleder, som HP giver mulighed for, indeholder det grundlæggende Windows 10®-installationsprogram. Alternativt kan HP Sure Recover installere optimerede drivere til HP-enheder. HP-gendannelsesbilleder omfatter kun datagendannelsesagenter, der følger med Windows 10, som f.eks. OneDrive. Selskaber kan oprette deres egne brugerdefinerede billeder og tilføje virksomhedsindstillinger, programmer, drivere samt agenter til gendannelse af data.

En gendannelsesagent til et operativsystem udfører de trin, der er nødvendige for at installere gendannelsesbilledet. Gendannelsesagenten fra HP udfører almindelige trin såsom partition, formatering og udpakning af gendannelsesbilledet på destinationsenheden. Da HP-gendannelsesagenten findes på hp.com, skal du have internetadgang for at hente den, medmindre systemet indeholder indbygget geninstallation af systembillede. Virksomheder kan også hoste HP-gendannelsesagenten i deres firewall eller oprette brugerdefinerede gendannelsesagenter til mere komplicerede gendannelsesmiljøer.

Du kan starte HP Sure Recover, når der ikke findes noget operativsystem. Du kan også køre HP Sure Recover efter en tidsplan, f.eks. for at sikre, at malware fjernes. Udfør konfiguration af disse indstillinger ved hjælp af HP Client Security Manager (CSM), Manageability Integration Kit (MIK) eller HP Client Management Script Library.

Udførelse af en netværksgendannelse

BEMÆRK: Hvis du vil udføre en netværksgendannelse, skal du bruge en kabelforbindelse. HP anbefaler, at du sikkerhedskopierer vigtige filer, data, fotos, videoer osv., før du bruger HP Sure Recover, for at undgå tab af data.

1. Opret forbindelse med klientsystemet til det netværk, hvor du kan få adgang til HTTP- eller FTP-distributionspunktet.
2. Genstart klientsystemet, og tryk på F11, når HP-logoet vises.
3. Vælg **Gendan fra netværk**.

Sådan gendanner du ved hjælp af et lokalt drev

Hvis et klientsystem understøtter indbygget geninstallation af systembillede, og indstillingen Planlagt billedoverførsel er aktiveret i den anvendte politik, downloades billedet til klientsystemet på det planlagte tidspunkt. Når billedet er downloadet til klientsystemet, skal du genstarte det for at kopiere billedet til lagerenheden til indbygget geninstallation af systembillede.

Sådan udfører du lokal gendannelse ved hjælp af billedet på lagerenheden til indbygget geninstallation af systembillede:

1. Genstart klientsystemet, og tryk på F11, når HP-logoet vises.
2. Vælg **Gendan fra lokalt drev**.

Systemer med indbygget geninstallation af systembillede skal konfigurere en tidsplan for download og bruge downloadagenten til at søge efter opdateringer. Downloadagenten er inkluderet i HP Sure Recover-plug-in-modulet til HP Client Security Manager og kan også konfigureres i MIK. Du kan se, hvordan du bruger MIK, under https://www.hp.com/go/clientmanagement.

Du kan også oprette en planlagt opgave for at kopiere agenten til SR_AED-partitionen og billedet til SR_IMAGE-partitionen. Du kan derefter bruge HP Client Management Script Library til at sende en servicehændelse, der underretter BIOS'en om, at den bør validere indholdet og kopiere til lagerenheden til indbygget geninstallation af systembillede ved næste genstart.

2 Oprettelse af et virksomhedsbillede

De fleste virksomheder bruger Microsoft Deployment Tools, Windows 10 Assessment and Deployment Kit eller begge dele til at oprette filer, der indeholder et billede i WIM-filformat (Windows Imaging).

Krav

- Den seneste version af Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (eller anden løsning til oprettelse af privat/offentligt RSA-nøglepar)

  Bruges til at oprette RSA-nøglepar, som bruges til at sikre integriteten af det virksomhedsbillede, du opretter og hoster.
- En løsning med hosting på server (f.eks. Microsoft Internet Information Services [IIS])

Oprettelse af billedet

Før du starter billedoprettelsesprocessen, skal du konfigurere arbejdssystemet eller oprette det system, hvor du har installeret de påkrævede værktøjer til forberedelse af behandlingen af billedet, som vist i de følgende trin:

1. Som administrator skal du åbne kommandoprompten `Deployment and Imaging Tools Environment` (installeres med installationsværktøjerne i Windows ADK).
2. Opret et klargøringsområde for dit billede ved hjælp af følgende kommando:

   ```
   mkdir C:\staging
   ```
3. Opret billedet ved hjælp af et af følgende eksempler:

   Eksempel 1: Oprettelse af et billede, der er baseret på Microsoft Windows-installationsbilledet på side 3

   Eksempel 2: Oprettelse af et billede baseret på et referencesystem på side 5

Eksempel 1: Oprettelse af et billede, der er baseret på Microsoft Windows-installationsbilledet

1. Monter eller åbn Microsoft Windows-installationsbilledet (fra en Microsoft ISO eller fra en HP OSDVD).
2. Fra det tilsluttede Windows-installationsbillede skal du kopiere install.wim-filen til klargøringsområdet ved hjælp af følgende kommando:

   ```
   robocopy <M:>\sources C:\staging install.wim
   ```

   BEMÆRK: `<M:>` er det monterede drev. Erstat det med det korrekte drevbogstav.
3. Omdøb install.wim til et billedfilnavn ("my-image" i dette eksempel) ved hjælp af følgende kommando:

   ```
   ren C:\staging\install.wim <my-image>.wim
   ```

(Valgfrit) HP Sure Recover indeholder en funktion til at gendanne en bestemt udgave fra et billede med flere indeks, der er baseret på den Windows-udgave, som oprindeligt var licenseret til HP-destinationssystemet på fabrikken. Denne mekanisme fungerer, hvis indeksene er navngivet korrekt. Hvis Windows-installationsbilledet stammer fra et HP OSDVD-billede, har du sandsynligvis et billede med flere redigeringer. Hvis du ikke vil have, at dette sker, og vil sikre, at en bestemt udgave anvendes til alle dine destinationssystemer, skal du være sikker på, at der kun er ét indeks i installationsbilledet.

4. Kontrollér installationsbilledets indhold ved hjælp af følgende kommando:

```
dism /Get-ImageInfo /ImageFile:C:\staging\<my-image>.wim
```

Følgende viser et eksempel på output fra et installationsbillede, der understøtter fem udgaver (skal matches på basis af BIOS for hvert destinationssystem):

Oplysninger om billede: `my-image.wim`

Indeks: `1`

Navn: `CoreSingleLanguage`

Beskrivelse: `Windows 10-opdatering for maj 2019 - Home Single Language Edition`

Størrelse: `19.512.500.682 bytes`

Indeks: `2`

Navn: `Kerne`

Beskrivelse: `Windows 10-opdatering for maj 2019 - Home Edition`

Størrelse: `19.512.500.682 bytes`

Indeks: `3`

Navn: `Professional`

Beskrivelse: `Windows 10-opdatering for maj 2019 - Professional Update`

Størrelse: `19.758.019.520 bytes`

Indeks: `4`

Navn: `ProfessionalEducation`

Beskrivelse: `Windows 10-opdatering for maj 2019 - Professional Education Edition`

Størrelse: `19.758.019.480 bytes`

Indeks: `5`

Navn: `ProfessionalWorkstation`

Beskrivelse: `Windows 10-opdatering for maj 2019 - Professional Workstation Edition`

Størrelse: `19.758.023.576 bytes`

BEMÆRK: Når der kun er ét indeks, bruges billedet til gendannelse, uanset navnet. Din billedfil kan være større, end den var før sletningerne.

5. Hvis du ikke vil have, at multiredigering udføres, skal du slette alle de indekser, du ikke vil bruge.

   Hvis du kun vil bruge Professional Edition (forudsat at alle destinationssystemer er licenserede), skal du slette indeks 5, 4, 2 og 1 som vist i følgende eksempel. Hver gang du sletter et indeks, tildeles indeksnumrene på ny. Derfor bør du slette fra de højeste til de laveste indeksnumre. Kør `Get-ImageInfo` efter hver sletning for at bekræfte visuelt, hvilket indeks du vil slette bagefter.

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:5
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:4
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:2
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:1
   ```

   Vælg kun ét indeks i udgaven (f.eks. Professional). Når der kun er ét indeks, bruges billedet til gendannelse, uanset navnet. Bemærk, at billedfilen kan være større, end den var før sletningerne, på grund af den måde, som WIM-metadataændringer og indholdsnormalisering fungerer på.

6. (Valgfrit) Benyt nedenstående fremgangsmåde, hvis du vil medtage drivere i virksomhedsgendannelsesbilledet:

   a. Monter dit billede i en tom mappe ved hjælp af følgende kommandoer:

   ```
   mkdir C:\staging\mount
   ```

   ```
   dism /Mount-Wim /WimFile:C:\staging\my-image.wim /MountDir:C:
   \staging\mount /Index:1
   ```

   b. Monter den relevante HP Windows 10-driver-DVD (DRDVD) til det understøttede destinationssystem. Kopiér driverens undermapper fra det monterede drivermedie til klargøringsområdet ved hjælp af følgende kommando:

   ```
   robocopy /E <M:>\SWSETUP\DRV C:\staging\mount\SWSETUP\DRV
   ```

   BEMÆRK: `<M:>` er det monterede drev. Erstat det med det korrekte drevbogstav.

   Du kan medtage yderligere .inf-drivere ved at placere dem i mappen C:\staging\mount\SWSETUP\DRV. Du kan se, hvordan dette indhold behandles af HP Sure Recover, ved hjælp af funktionen `dism /Add-Driver /Recurse` i "Tilføj og fjern drivere til et Windows-offlinebillede" under følgende emne: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Denne funktion understøtter ikke .exe-drivere, der kræver kørsel af et program.

   c. Gem ændringerne, og afmonter dit billede ved hjælp af følgende kommando:

   ```
   dism /Unmount-Wim /MountDir:C:\staging\mount /Commit
   ```

   Den resulterende billedfil er: C:\staging\my-image.wim.

   d. Gå til Opdeling af billedet på side 6.

Eksempel 2: Oprettelse af et billede baseret på et referencesystem

1. Opret USB WinPE-medier, der kan bootes fra.

BEMÆRK: Du kan finde yderligere metoder til at optage billedet i ADK-dokumentationen.

Sørg for, at der er tilstrækkelig plads på USB-drevet til at lagre det optagne billede fra referencesystemet.

2. Opret et billede på et referencesystem.
3. Tag billedet ved at starte referencesystemet med USB WinPE-mediet, og brug derefter DISM.

BEMÆRK: `<U:>` er USB-drevet. Erstat det med det korrekte drevbogstav.

Rediger "my-image"-delen af filnavnet og `<my-image>`-beskrivelsen efter behov.

```
dism /Capture-Image /ImageFile:<U:><\my-image>.wim /CaptureDir:C:\ /
Name:<My Image>
```

4. Kopiér billedet fra USB-drevet til klargøringsområdet på dit arbejdssystem ved hjælp af følgende kommando:

```
robocopy <U:>\ C:\staging <my-image>.wim
```

Du bør have følgende billedfil: C:\staging\my-image.wim.

5. Gå til Opdeling af billedet på side 6.

Opdeling af billedet

HP anbefaler, at du deler billedet i mindre filer, så netværksoverførslen bliver mere stabil, ved hjælp af følgende kommando:

```
dism /Split-Image /ImageFile:C:\staging\<my-image>.wim /SwmFile:C:\staging
\<my-image>.swm /FileSize:64
```

BEMÆRK: Filstørrelsen vises i megabyte. Rediger efter behov.

BEMÆRK: På grund af DISM's opdelte algoritme kan de genererede SWM-filer være enten mindre eller større end den angivne filstørrelse.

Oprettelse af et manifest

Formatér manifestfiler som UTF-8 uden byte-rækkefølgemærke (BOM).

Du kan ændre manifestfilnavnet (custom.mft), der anvendes i følgende procedurer, men du må ikke ændre filtypenavnene .mft og .signa, og filnavnsdelen af manifest- og signaturfilerne skal stemme overens. Du kan f.eks. ændre pardannelsen (custom.mft, custom.sig) til (myimage.mft, myimage.sig).

`mft_version` bruges til at bestemme formatet af billedfilen og skal på nuværende tidspunkt være 1.

`image_version` bruges til at fastslå, om der findes en nyere udgave af billedet, og til at forhindre, at ældre udgaver installeres.

Begge værdier skal være ikke-signerede 16-bit heltal, og linjeseparatoren i manifestet skal være `'\r\n'` `(CR + LF)`.

Generering af et manifest

Da flere filer kan være tilknyttet dit opdelte billede, skal du bruge et powershell-script til at generere et manifest.

I alle resterende trin skal du være i mappen C:\staging.

```
CD /D C:\staging
```

1. Opret et powershell-script ved hjælp af en editor, der kan oprette en tekstfil i UTF-8-format uden BOM, ved hjælp af følgende kommando: `notepad C:\staging\generate-manifest.ps1`

   Opret følgende script:

   ```
   $mftFilename = "custom.mft"
   ```

   `$imageVersion = 1907` (Bemærk: Dette kan være et vilkårligt 16-bit heltal)

   ```
   $header = "mft_version=1, image_version=$imageVersion"
   Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header
   $swmFiles = Get-ChildItem "." -Filter "*.swm"
   $ToNatural = { [regex]::Replace($_, '\d*\....$',
   { $args[0].Value.PadLeft(50) }) }

   $pathToManifest = (Resolve-Path ".").Path

   $total = $swmFiles.count
   $current = 1

   $swmFiles | Sort-Object $ToNatural | ForEach-Object {
       Write-Progress
           -Activity "Generating manifest" `
           -Status "$current of $total ($_)" `
           -PercentComplete ($current / $total * 100)

       $hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName
       $fileHash = $hashObject.Hash.ToLower()
       $filePath = $hashObject.Path.Replace($pathToManifest + '\', '')
       $fileSize = (Get-Item $_.FullName).length
       $manifestContent = "$fileHash $filePath $fileSize"

       Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
   $manifestContent -Append
       $current = $current + 1
   }
   ```

BEMÆRK: Manifester til HP Sure Recover kan ikke omfatte en BOM, så de følgende kommandoer omskriver filen som UTF8 uden BOM.

```
$content = Get-Content $mftFilename

$encoding = New-Object System.Text.UTF8Encoding $False

[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. Gem scriptet.
3. Kør scriptet.

```
powershell .\generate-manifest.ps1
```

Generering af manifestsignatur

Sure Recover validerer agenten og billedet ved hjælp af kryptografiske signaturer. Følgende eksempler bruger et privat/offentligt nøglepar i X.509 PEM-format (.PEM-filtype). Juster kommandoerne efter behov for at bruge binære DER-certifikater (.CER- eller.CRT-filtype), BASE-64-kodede PEM-certifikater (.CER- eller .CRT-filtype) eller PKCS1 PEM-filer (.PEM-filtype). Eksemplet bruger også OpenSSL, som genererer signaturer i big-endian-format. Du kan bruge ethvert hjælpeprogram til at signere manifester, men visse BIOS-versioner understøtter kun signaturer i little-endian-format.

1. Generér en privat 2048-bit RSA-nøgle ved hjælp af følgende kommando. Hvis du har et privat/offentligt 2048-bit RSA-nøglepar i PEM-format, skal du kopiere dem til C:\staging og derefter gå videre til trin 3.

   ```
   openssl genrsa -out my-recovery-private.pem 2048
   ```

2. Generér den offentlige nøgle fra din private nøgle ved hjælp af nedenstående kommando (hvis du har en offentlig nøgle, der svarer til din private nøgle i PEM-format, skal du kopiere den til C:\staging):

   ```
   openssl rsa -in my-recovery-private.pem -pubout -out my-recovery-
   public.pem
   ```

3. Opret en signaturfil (ved brug af SHA256-baseret hash) baseret på din 2048-bit RSA-nøgle fra trin 1 ved hjælp af følgende kommando:

   ```
   openssl dgst -sha256 -sign my-recovery-private.pem -out custom.sig
   custom.mft
   ```

4. Kontrollér signaturfilen ved hjælp af din offentlige nøgle fra forrige trin ved hjælp af følgende kommando:

   ```
   openssl dgst -sha256 -verify my-recovery-public.pem -signature
   custom.sig custom.mft
   ```

BEMÆRK:

- Hvis du kun har brug for at oprette en signaturfil, skal trin 1 og 3 udføres.
- For HP Sure Recover skal som minimum trin 1, 2 og 3 udføres. Du skal bruge den offentlige nøgle fra trin 2 til at klargøre dit destinationssystem.
- Trin 4 er valgfrit, men anbefales, så signaturfilen og manifestfilen valideres korrekt.

Hosting af filerne

Host følgende filer på din server fra mappen C:\staging:

- *.swm
- custom.mft (eller det filnavn, du valgte til manifestfilen)
- custom.sig (eller det tilsvarende filnavn, som du valgte til signaturfilen)

BEMÆRK: Hvis du bruger IIS som din hosting-løsning, skal du konfigurere MIME-posterne, så de omfatter følgende filtypenavne, der alle er konfigureret som "application/octet-stream:"

- .mft
- .sig
- .swm
- .wim

Klargøring af dine destinationssystemer

Du kan oprette dine destinationssystemer vha. HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover eller Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Angiv følgende oplysninger til klargøringen:

1. URL-adressen på manifestfilen, der er hostet i forrige afsnit (http://your_server.domain/path/custom.mft)
2. Den offentlige nøgle, der bruges til at kontrollere den tidligere oprettede signaturfil (f.eks. C:\staging\my-recovery-public.pem).

Fejlfinding

Hvis du får vist en meddelelse om, at den brugerdefinerede gendannelsesproces ikke er sikkerhedsvalideret, skal du kontrollere følgende:

1. Manifestet skal være UTF-8 uden BOM.
2. Kontrollér filernes hashværdier.
3. Sørg for, at systemet blev klargjort med den offentlige nøgle, der svarer til den private nøgle, som bruges til at signere manifestet.
4. IIS-serverens MIME-typer skal være `application/octet-stream`.
5. Filstierne i manifestet skal indeholde hele stien til den øverste mappe med billedet, som det ses på et klientsystem. Denne sti er ikke hele den sti, hvor filerne gemmes på distributionspunktet.

3 Brug af HP Sure Recover-agent i en virksomhedsfirewall

HP Sure Recover-agenten kan hostes på et firmaintranet. Når du har installeret HP Sure Recover SoftPaq, skal du kopiere agentfilerne fra HP Sure Recover-agentmappen fra installationsplaceringen til et HTTP- eller FTP-distributionspunkt. Klargør derefter klientsystemet med URL-adressen på distributionspunktet og den offentlige HP-nøgle med navnet `hpsr_agent_public_key.pem`, som fordeles med HP Sure Recover-agentens SoftPaq.

Installation af HP Sure Recover-agenten

1. Download HP Sure Recover-agenten, og udpak filerne på dit HTTP- eller FTP-distributionspunkt.
2. Angiv de relevante filtilladelser på distributionspunktet.
3. Hvis du bruger Internet Information Services (IIS), skal du oprette application/octet-stream MIME-typer for følgende filformater:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   VIGTIGT: Følgende fremgangsmåde beskriver, hvordan du klargør Sure Recover med SCCM. Du kan finde eksempler på, hvordan du klargør Sure Recover med HP Client Management Script Library, i Arbejde med HP Client Management Script Library (CMSL) på side 12.

4. Start SCCM, gå til **HP Client Security Suite**, og vælg derefter HP Sure Recover-siden.

   BEMÆRK: URL-adressen til distributionspunktet omfatter enten ftp eller http som transportprotokol. Den indeholder også hele stien til den øverste mappe med manifestet for HP Sure Recover-agenten, som det ses på et klientsystem. Denne sti er ikke hele stien til det sted, hvor filerne gemmes på distributionspunktet.

5. I afsnittet **Platformbillede** skal du vælge indstillingen **Virksomhed** for at gendanne et tilpasset OS-billede fra et virksomhedsdistributionspunkt. Indtast URL-adressen fra it-administratoren i feltet **URL-adresse til billedplacering**. Indtast den offentlige nøgle `hpsr_agent_public_key.pem` i feltet **Billedbekræftelse**.

   BEMÆRK: URL-adressen til det brugerdefinerede billede skal indeholde billedmanifestets filnavn.

6. I afsnittet **Gendannelsesagent** skal du vælge indstillingen **Virksomhed** for at benytte en brugerdefineret gendannelsesagent eller HP Recovery-agent fra et virksomhedsdistributionspunkt.

Indtast URL-adressen fra it-administratoren i feltet **URL-adresse til agentens placering**. Indtast den offentlige nøgle `hpsr_agent_public_key.pem` i feltet **Agentbekræftelsesnøgle**.

BEMÆRK: Medtag ikke filnavnet på agentmanifestet i URL-adressen, da BIOS kræver, at den kaldes recovery.mft.

7. Når politikken anvendes på klientsystemet, skal du genstarte den.
8. Under første klargøring vises der en prompt, hvor du kan indtaste en sikkerhedskode på 4 cifre for at fuldføre HP Sure Recover-aktiveringen. Du kan finde flere oplysninger ved at gå til hp.com og søge efter hvidbogen om HP Manageability Integration Kit (MIK) til Microsoft System Center Manager.

Når HP Sure Recover-aktiveringen er gennemført, vises den brugerdefinerede URL, der anvendes af politikken, i menuen med BIOS-indstillinger til HP Sure Recover.

Du kan bekræfte aktiveringen ved at genstarte computeren og trykke på F10, når HP-logoet vises. Vælg **Avanceret**, vælg **HP Sure Recover**, vælg **Gendannelsesagent**, og vælg derefter **URL-adresse**.

4 Arbejde med HP Client Management Script Library (CMSL)

HP Client Management Script Library giver dig mulighed for at administrere HP Sure Recover-indstillinger med PowerShell. Følgende eksempelscript viser, hvordan du klargør, fastslår status, ændrer konfiguration og fjerner klargørelsen af HP Sure Recover.

BEMÆRK: Flere af kommandoerne overskrider denne vejlednings linjelængde, men skal indtastes som en enkelt linje.

```
$ErrorActionPreference = "Stop"

$path = 'C:\test_keys'
$ekpw = ""
$skpw = ""

Get-HPSecurePlatformState

try {
    Write-host 'Provisioning Endorsement Key'
    $p = New-HPSecurePlatformEndorsementKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx"
    $p | Set-HPSecurePLatformPayload

    Start-Sleep -Seconds 3

    Write-host 'Provisioning signing key'
    $p = New-HPSecurePlatformSigningKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx" `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePLatformPayload
```

```
    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image OS `
        -ImageKeyFile "$path\os.pfx" `
        -username test -password test `
        -url "http://www.hp.com/custom/image.mft"
    $p | Set-HPSecurePLatformPayload

    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image agent `
        -ImageKeyFile "$path\re.pfx" `
        -username test -password test `
        -url "http://www.hp.com/pub/pcbios/CPR"
    $p | Set-HPSecurePLatformPayload

 $p = New-HPSureRecoverSchedulePayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -DayOfWeek Sunday,EveryWeek -Hour 13 -Minute 27 -WindowSize 30
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -OSImageFlags NetworkBasedRecovery `
        -AgentFlags DRDVD
    $p | Set-HPSecurePlatformPayload

    Get-HPSureRecoverState -all
    Get-HPSecurePlatformState
}
finally {
```

```
    Write-Host 'Deprovisioning Sure Recover'
    Start-Sleep -Seconds 3
    $p = New-HPSureRecoverDeprovisionPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePlatformPayload

    Start-Sleep -Seconds 3
    Write-host 'Deprovisioning P21'

    $p = New-HPSecurePlatformDeprovisioningPayload `
        -verbose `
        -EndorsementKeyPassword $pw `
        -EndorsementKeyFile "$Path\kek.pfx"
    $p | Set-HPSecurePlatformPayload

    Write-Host 'Final secure platform state:'
    Get-HPSecurePlatformState
}
```

Generering af eksempel på nøgle med OpenSSL

Gem de private nøgler på et sikkert sted. De offentlige nøgler bruges til validering og skal angives under klargøringen. Disse taster skal være 2048 bits i længden og bruge en eksponent, som er 0x10001. Erstat emnet i eksemplerne med oplysninger om din organisation.

Angiv følgende miljøvariabel, før du fortsætter:

```
set OPENSSL_CONF=<path>\openssl.cnf

# Opret et selvsigneret rodnøglecentercertifikat til test
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

# Opret et nøglegodkendelsescertifikat
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

```
openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:


# Opret en kommandosigneringsnøgle

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:


# Opret en billedsigneringsnøgle

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Du kan signere billedmanifestet med denne kommando:

```
openssl dgst -sha256 –sign os.key -out image.sig image.mft


# Opret en agentsigneringsnøgle

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Du kan signere agentmanifestet med denne kommando:

```
openssl dgst -sha256 –sign re.key -out agent.sig agent.mft
```

OpenSSL genererer signaturfiler i big-endian-format, som ikke er kompatibelt med visse BIOS-versioner, så agentens signaturfil-byterækkefølge skal muligvis tilbageføres inden udrulningen. BIOS-versioner, der understøtter big-endian-byterækkefølge, understøtter også little-endian-byterækkefølge.

A Fejlfinding

Partitionering af drev mislykkedes

Fejl ved partitionering af drev kan forekomme, hvis SR_AED- eller SR_IMAGE-partitionen er krypteret med BitLocker. Disse partitioner oprettes normalt med en GPT-attribut, der forhindrer BitLocker i at kryptere dem, men hvis en bruger sletter og genopretter partitionerne eller opretter dem manuelt på et drev til genoprettelse fra bunden, kan den sikrede gendannelsesagent ikke slette dem og afslutter med en fejl ved genpartitionering af drevet. Brugeren skal slette dem manuelt ved at køre diskpart, vælge diskenheden og angive tilsidesættelseskommandoen `del vol` eller lignende.

Firmware-overvågningslog

EFI-variabeloplysningerne er som følger:

- GUID: `{0xec8feb88, 0xb1d1, 0x4f0f, {0xab, 0x9f, 0x86, 0xcd, 0xb5, 0x3e, 0xa4, 0x45}}`
- Navn: `OsRecoveryInfoLog`

Der findes API'er i Windows til læsning af EFI-variabler, eller du kan dumpe variabelt indhold i en fil vha. værktøjet UEFI Shell dmpstore.

Du kan dumpe overvågningsloggen ved hjælp af kommandoen `Get-HPFirmwareAuditLog`, som findes i HP Client Management Script Library.

Windows-hændelseslog

Start- og stophændelser i Sure Recover sendes til BIOS-overvågningsloggen, som du kan få vist i Windows Logbog i Sure Start-log, hvis HP Notifications er installeret. Disse hændelser omfatter dato og klokkeslæt, kilde-ID, hændelses-ID og en hændelsesspecifik kode. F.eks. angiver `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]`, at genoprettelsen mislykkedes, da manifestet ikke kunne godkendes med den hændelsesspecifikke kode c3f 23000, der blev logget kl. 2:26:40 d. 6/27/18.

BEMÆRK: Disse logfiler følger amerikansk datoformat med måned/dato/år.

HP Secure Platform Management (kilde-ID = 84h)

Tabel A-1 HP Secure Platform Management

Hændelses-id	Enhedsantal (alle/DaaS)	Hændelsesantal (alle/DaaS)	Beskrivelse	Bemærkninger
40	256/178	943/552	OS-platformgendannelsesprocessen blev startet af firmwaren.	Platformsgendannelse startet
41	221/147	588/332	OS-platformgendannelsesprocessen er fuldført.	Platformsgendannelse fuldført
42	54/42	252/156	OS-platformgendannelsesprocessen kunne ikke fuldføres.	Platformsgendannelse mislykkedes

Du kan hente firmware-overvågningsloggen ved hjælp af Get-HPFirmwareAuditLog i HP Client Management Script Library, som findes på http://www.hp.com/go/clientmanagement. HP Secure Platform Management-hændelses-ID'erne 40, 41 og 42 returnerer hændelsesspecifikke koder i datafeltet, som angiver resultatet af Sure Recovers operationer. F.eks. angiver følgende logpost, at Sure Recover ikke kunne downloade manifest- eller signaturfilen med fejlen event_id 42 og data: 00:30:f1:c3, som skal fortolkes som dword-værdien 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0
alvorlighedsgrad: Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 42
timestamp_is_exact: 1
tidsstempel: 5/27/2019 2:44:18 PM
beskrivelse: OS-platformgendannelsesprocessen kunne ikke fuldføres.
data: 00:30:f1:c3
```

En vellykket gendannelse vises som event_id = 41 og data: 00:00:00:00, for eksempel:

```
Hændelsesspecifikke koder
Success = 0x00000000
CatalogDownloadFailed = 0xC3F11000
message_number: 0
alvorlighedsgrad: Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 41
timestamp_is_exact: 1
tidsstempel: 5/27/2019 2:55:41 PM
beskrivelse: OS-platformgendannelsesprocessen kunne ikke fuldføres.
data: 00:00:00:00
```

HP Sure Recover bruger følgende hændelsesspecifikke koder.

Tabel A-2 Hændelsesspecifikke koder

Hændelsesbeskrivelse	Hændelseskode
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000

Tabel A-2 Hændelsesspecifikke koder (fortsat)

Hændelsesbeskrivelse	Hændelseskode
AwsDownloadUnattendedFailed	0xC3F16000
UnableToConnectToNetwork	0xC3F17000
CatalogNotAuthenticated	0xC3F21000
FtpHttpDownloadHashFailed	0xC3F22000
ManifestDoesNotAuthenticate	0xC3F23000
CatalogVersionMismatch	0xC3F31000
CatalogLoadFailed	0xC3F32000
OsDvdDidNotResolvedToOneComponent	0xC3F33000
DriversDvdDidNotResolvedToOneComponent	0xC3F34000
ManifestFileEmptyOrInvalid	0xC3F41000
ListedFileInManifestNotFound	0xC3F42000
FailedToInstallDrivers	0xC3F51000
FailedToApplyWimImage	0xC3F52000
FailedToRegisterWimCallback	0xC3F53000
FailedToCreateDismProcess	0xC3F54000
BcdbootFailed	0xC3F55000
NoSuitableDiskFound	0xC3F56000
PartitoningFailed	0xC3F57000
DiskLayoutCreationFailed	0xC3F58000
UnexpectedProblemWithConfigJson	0xC3FF1000
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000