Brukerhåndbok

HP Sure Recover

Første utgave: Februar 2020

Dokumentets delenummer: L93434-091

Syntaksnøkkel for brukerinndata

Tekst som du må oppgi i et brukergrensesnitt er indikert med `skrifttype med fast tegnavstand`.

Tabell -1 Syntaksnøkkel for brukerinndata

Ikon	Beskrivelse
`Tekst uten parenteser eller klammeparenteser`	Elementer du må skrive inn nøyaktig som vist
`<Tekst i vinkelparenteser>`	En plassholder for en verdi du må angi, utelat parentesene
`[Tekst i firkantparenteser]`	Valgfrie elementer, utelat parentesene
`{Tekst i klammeparenteser}`	Et sett med elementer som du må velge bare én fra, utelat klammeparentesene
`|`	Et skilletegn for elementer som du må velge bare én fra, utelat den vertikale linjen
`. . .`	Elementer som kan eller må gjentas, utelat ellipsen

Innhold

1 Komme i gang

HP Sure Recover hjelper deg med å installere operativsystemet fra nettverket med minimalt brukermedvirkning på en sikker måte. Systemer med HP Sure Recover med innebygd gjenoppbygging støtter også installasjon fra en lokal lagringsenhet.

VIKTIG: Ta sikkerhetskopi av data før du bruker HP Sure Recover. Fordi gjenopprettingsprosessen formaterer stasjonen på nytt, vil datatap forekomme.

Gjenopprettingsbilder som HP tilbyr inkluderer det grunnleggende Windows 10®-installasjonsprogrammet. Hvis du ønsker det, kan HP Sure Recover installere optimaliserte drivere for HP-enheter. HP-gjenopprettingsbilder inkluderer bare datagjenopprettingsagenter som følger med Windows 10, som OneDrive. Selskaper kan lage egendefinerte bilder for å legge til bedriftsinnstillinger, -programmer, -drivere og datagjenopprettingsagenter.

En gjenopprettingsagent for operativsystem (OS) utfører trinnene som er nødvendige for å installere gjenopprettingsbildet. Gjenopprettingsagenten som er levert av HP utfører vanlige trinn som å partisjonere, formatere og trekke ut gjenopprettingsbildet til målenheten. Fordi HP-gjenopprettingsagenten er plassert på hp.com, trenger du Internett-tilgang for å hente den, med mindre systemet har innebygd gjenoppbygging. Selskaper kan også være vert for HP-gjenopprettingsagent inne i brannmuren eller lage tilpassede gjenopprettingsagenter for mer kompliserte gjenopprettingsmiljøer.

Du kan starte HP Sure Recover når du ikke finner noe operativsystem. Du kan også kjøre HP Sure Recover på en tidsplan, som for eksempel for å sikre at skadelig programvare fjernes. Utfør konfigurering av disse innstillingene via HP Client Security Manager (CSM), Manageability Integration Kit (MIK) eller HP Client Management Script Library.

Utføre en nettverksgjenoppretting

MERK: Hvis du skal utføre en nettverksgjenoppretting, må du bruke en kablet tilkobling. HP anbefaler at du sikkerhetskopierer viktige filer, data, bilder, videoer og så videre før du bruker HP Sure Recover for å unngå tap av data.

1. Koble klientsystemet til nettverket der du får tilgang til HTTP- eller FTP-distribusjonspunktet.
2. Start klientsystemet på nytt, og når HP-logoen vises, trykker du på f11.
3. Velg **Gjenopprett fra nettverk**.

Utføre en gjenoppretting av en lokal stasjon

Hvis et klientsystem støtter innebygd gjenoppbygging, og det planlagte alternativet for nedlasting av bilde er aktivert i gjeldende retningslinjer, lastes bildet ned til klientsystemet på det angitte tidspunktet. Når bildet lastes ned til klientsystemet, må du starte det på nytt for å kopiere bildet til den innebygde lagringsenheten for gjenoppbygging.

Slik utfører du lokal gjenoppretting ved å bruke bildet på den innebygde lagringsenheten for gjenoppbygging:

1. Start klientsystemet på nytt, og når HP-logoen vises, trykker du på f11.
2. Velg **Gjenopprett fra lokal stasjon**.

Systemer med innebygd gjenoppbygging må konfigurere en tidsplan for nedlasting og bruke nedlastingsagenten til å se etter oppdateringer. Nedlastingsagenten er inkludert i programtillegget HP Sure Recover for HP Client Security Manager, og kan også konfigureres i MIK. Se https://www.hp.com/go/clientmanagement for å få veiledning om hvordan du bruker MIK.

Du kan også opprette en planlagt oppgave for å kopiere agenten til SR_AED-partisjonen og bildet til SR_IMAGE-partisjonen. Du kan deretter bruke HP Client Management Script Library til å sende en servicehendelse som informerer BIOS om at den skal validere innholdet og kopiere til den innebygde lagringsenheten for gjenoppbygging ved neste omstart.

2 Lage et bedriftsbilde

De fleste firmaer bruker Microsoft Deployment Tools, Windows 10 Assessment and Deployment Kit eller begge deler til å produsere filer som inneholder et bilde i et filformatarkiv for Windows Imaging (WIM).

Systemkrav

- Den nyeste versjonen av Windows 10 Assessment and Deployment Kit (Windows-ADK)
- PowerShell
- OpenSSL (eller annen løsning for å generere RSA privat/offentlig nøkkelpar)

  Brukes til å generere RSA-nøkkelparet som brukes til å sikre integriteten til bedriftsbildet du oppretter og er vert for.
- En serververtskapsløsning (for eksempel Microsoft Internet Information Services [IIS])

Lage bildet

Før du starter prosessen med å lage bildet, må du sette opp et fungerende system eller bygge system der du installerte de nødvendige verktøyene for å klargjøre for behandling av bildet, som vist på følgende måte:

1. Som administrator åpner du ledeteksten `Deployment and Imaging Tools Environment` (Distribusjon og miljø for bildeverktøy) (installeres med Deployment Tools of Windows ADK).
2. Opprett et klargjøringsområde for bildet, ved å bruke følgende kommando:

   ```
   mkdir C:\staging
   ```
3. Lag profilen med ett av disse eksemplene:

   Eksempel 1: Lage et bilde basert på installasjonsbildet for Microsoft Windows på side 3

   Eksempel 2: Lage et bilde basert på et referansesystem på side 5

Eksempel 1: Lage et bilde basert på installasjonsbildet for Microsoft Windows

1. Monter eller åpne installasjonsbildet for Microsoft Windows (fra en Microsoft ISO eller fra en HP-OSDVD).
2. Fra det monterte Windows-installasjonsbildet kopierer du install.wim-filen til klargjøringsområdet, ved å bruke følgende kommando:

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

   MERK: `<M:>` refererer til den monterte stasjonen. Bytt ut med riktig stasjonsbokstav.
3. Endre navnet install. wim til et bildefilnavn («mitt-bilde» for dette eksempelet), ved å bruke følgende kommando:

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

   (Valgfri) HP Sure Recover inkluderer en funksjon for å gjenopprette en bestemt utgave fra et bilde med flere indekser, basert på Windows-versjonen som opprinnelig var lisensiert for HP-målsystemet i fabrikken. Denne mekanismen fungerer hvis indeksene navngis riktig. Hvis Windows-installasjonsbildet kommer fra et HP OSDVD-bilde, har du sannsynligvis et bilde med flere utgaver. Hvis du ikke vil at dette

skal skje, og ønsker å sikre én bestemt utgave brukes for alle målsystemene, må du sørge for at det bare er én indeks er i installasjonsbildet.

4. Sjekk innholdet i installasjonsbildet ved hjelp av følgende kommando:

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

Følgende viser eksempelresultat fra en installasjonsbilde som støtter fem utgaver (for å samsvare basert på BIOS-en for hvert målsystem):

Detaljer for bilde: `my-image.wim`

Indeks: `1`

Navn: `CoreSingleLanguage`

Beskrivelse: `Windows 10-oppdatering mai 2019 - Hjemmeutgave med ett språk`

Størrelse: `19 512 500 682 byte`

Indeks: `2`

Navn: `Core`

Beskrivelse: `Windows 10-oppdatering mai 2019 - Hjemmeutgave`

Størrelse: `19 512 500 682 byte`

Indeks: `3`

Navn: `Professional`

Beskrivelse: `Windows 10-oppdatering mai 2019 - Professional-oppdatering`

Størrelse: `19.758, 019520 byte`

Indeks: `4`

Navn: `ProfessionalEducation`

Beskrivelse: `Windows 10-oppdatering mai 2019 - Professional Education-utgave`

Størrelse: `19 758 019 480 byte`

Indeks: `5`

Navn: `ProfessionalWorkstation`

Beskrivelse: `Windows 10-oppdatering mai 2019 - Professional Workstation-utgave`

Størrelse: `19 758 023 576 byte`

MERK: Når det bare er én indeks, brukes bildet til gjenoppretting, uansett navn. Størrelsen på bildefilen kan være større enn før slettingene.

5. Hvis du ikke vil ha atferden som flere utgave skaper, sletter du hver indeks du ikke vil ha.

   Som vist i følgende eksempel, hvis du bare vil ha Professional-utgave (forutsatt at alle målsystemer er lisensiert), sletter du indeks 5, 4, 2 og 1. Hver gang du sletter en indeks, tilordnes indeksnumrene på nytt. Derfor bør du slette fra høyeste til laveste indeksnummer. Kjør `Get-ImageInfo` (få bildeinfo) etter hver sletting for å visuelt bekrefte hvilken indeks du nå vil slette.

   ```
   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
   ```

   Velg bare én indeks for utgaven (for dette eksempelet, Professional). Når det bare er én indeks, brukes bildet til gjenoppretting, uansett navn. Vær oppmerksom på at størrelsen på bildefilen kan være større enn før slettingene, på grunn av måten modifikasjoner og innholdsnormalisering av WIM-metadata fungerer.

6. (Valgfri) Hvis du vil inkludere drivere i bedriftens gjenopprettingsbilde, følger du denne fremgangsmåten:

   a. Monter bildet i en tom mappe, ved hjelp av følgende kommandoer:

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

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

   b. Monter riktig HP Windows 10-driver-DVD (DRDVD) for det støttede målsystemet. Fra de monterte drivermediene kopierer du undermappene for driveren til klargjøringsområdet, ved hjelp av følgende kommando:

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

   MERK: `<M:>` refererer til den monterte stasjonen. Bytt ut med riktig stasjonsbokstav.

   Du kan inkludere ytterligere drivere i .inf-stil ved å plassere dem under C:\staging\mount \SWSETUP\DRV-mappen. Hvis du vil ha en forklaring på hvordan dette innholdet behandles av HP Sure Recover ved hjelp av `dism /Add-Driver /Recurse`-funksjonen, kan du se «Legge til og fjerne drivere til et Windows-bilde frakoblet nett» i følgende emne: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Denne funksjonen støtter ikke drivere i .exe-stil som krever kjøring av et program.

   c. Lagre endringer og demonter bildet, ved hjelp følgende kommando:

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

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

   d. Gå til Splitte bildet på side 6.

Eksempel 2: Lage et bilde basert på et referansesystem

1. Opprett oppstartbare USB WinPE-medier.

MERK: Flere metoder for å ta bildet finner du i ADK-dokumentasjon.

Sørg for at USB-stasjonen har nok ledig plass til å lagre bildet tatt av referansesystemet.

2. Lag et bilde på et referansesystem.
3. Ta bildet ved å starte referansesystemet med USB WinPE-mediet, og deretter bruke DISM.

MERK: `<U:>` refererer til USB-stasjonen. Bytt ut med riktig stasjonsbokstav.

Rediger «my-image»-delen av filnavnet og `<my-image>`-beskrivelsen etter behov.

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

4. Kopier bildet fra USB til klargjøringsområdet på arbeidssystemet ved hjelp av følgende kommando:

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

Du bør ha følgende bildefil: C:\staging\my-image.wim.

5. Gå til Splitte bildet på side 6.

Splitte bildet

HP anbefaler at du deler bildet i mindre filer for å forbedre påliteligheten til nettverksnedlastinger, ved hjelp av følgende kommando:

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

MERK: FileSize vises i megabyte. Rediger etter behov.

MERK: På grunn av innholdet i DISMs dele-algoritme, kan størrelsen på de genererte SWM-filene være enten mindre eller større enn den angitte filstørrelsen.

Lage et manifest

Formater manifest-filer som UTF-8 uten Byte Order Mark (BOM).

Du kan endre navnet på manifest-filen (custom.mft) som brukes i de følgende prosedyrene, men du må ikke endre utvidelsene .mtf og .sig, og filnavndelen av manifest- og signaturfilene må samsvare. Du kan for eksempel endre paret (custom.mft, custom.sig) til (myimage.mft, myimage.sig).

`mft_version` brukes til å bestemme formatet til bildefilen og må i øyeblikket være satt til 1.

`image_version` brukes til å finne ut om en nyere versjon av bildet er tilgjengelig og hindre at eldre versjoner blir installert.

Begge verdier må være usignerte 16-bit heltall, og linjeavstanden i manifestet må være `'\r\n' (CR + LF)`.

Generere et manifest

Fordi flere filer kan være involvert i det delte bildet, kan du bruke et powershell-skript til å generere et manifest.

I alle gjenværende trinn må du være i C:\staging-mappen.

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

1. Lag et powershell-skript ved hjelp av et redigeringsprogram som kan gi en tekstfil i formatet UTF-8 uten BOM, ved hjelp av følgende kommando: `notepad C:\staging\generate-manifest.ps1`

   Opprett følgende skript:

   `$mftFilename = "custom.mft"`

   `$imageVersion = 1907` (Merk: Dette kan være et hvilket som helst 16-bit heltall)

```
$header = "mft_version=1, image_version=$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

}
```

MERK: Manifester for HP Sure Recover kan ikke inkludere en BOM, slik at de følgende kommandoene omskriver filen som UTF8 uten BOM.

```
$content = Get-Content $mftFilename
```

```
$encoding = New-Object System.Text.UTF8Encoding $False
[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. Lagre skriptet.
3. Kjør skriptet.

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

Generere manifestsignatur

Sure Recover validerer agent og bilde ved hjelp av kryptografiske signaturer. De følgende eksemplene bruker et privat/offentlig nøkkelpar i X.509 PEM-format (.PEM-utvidelse). Juster kommandoene etter behov for å bruke DER binære sertifikater (.CER eller .CRT-utvidelser), BASE-64 kodet PEM-sertifikater (.CER eller .CRT-utvidelser) eller PKCS1 PEM-filer (.PEM-utvidelse). Eksempelet bruker også OpenSSL, som genererer signaturer i big-endian-format. Du kan bruke et hvilket som helst verktøy til å signere manifester, men noen BIOS-versjoner støtter bare signaturer i little-endian-format.

1. Generer en 2048-bit RSA privat nøkkel ved hjelp av følgende kommando. Hvis du har et 2048-bit RSA privat/offentlig nøkkelpar i pem-format, kopier dem til C:\staging, og hopp deretter til trinn 3.

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

2. Generer den offentlige nøkkelen fra den private nøkkelen (hvis du har en offentlig nøkkel som samsvarer med den private nøkkelen i PEM-format, kopier den til C:\staging), ved å bruke følgende kommando:

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

3. Opprett en signaturfil (ved å bruke sha256-basert avtrykk) basert på din 2048-bit RSA private nøkkel fra trinn 1, ved hjelp av følgende kommando:

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

4. Bekreft signaturfilen ved å bruke den offentlige nøkkelen fra forrige trinn, ved hjelp av følgende kommando:

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

MERK:

- Hvis du bare må opprette en signaturfil, er de nødvendige trinnene 1 og 3.
- For HP Sure Recover, er de nødvendige trinnene minimum 1, 2 og 3. Du trenger den offentlige nøkkelen fra trinn 2 for å levere målsystemet.
- Trinn 4 er valgfritt, men anbefales slik at signaturfilen og manifestfilen validerer på riktig måte.

Vert for filene

Vær vert for følgende filer på serveren fra C:\staging-mappen:

- *.swm
- custom.mft (eller filnavnet du valgte for manifestfilen)
- custom.sig (eller det samsvarende filnavnet du valgte for signaturfilen)

MERK: Hvis du bruker IIS som vertsløsning, må du konfigurere MIME-oppføringene til å inkludere følgende utvidelser, alle konfigurert som «application/octet-stream:»

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

Levere målsystemene

Du kan levere målsystemene ved hjelp av HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover eller Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Oppgi følgende informasjon for denne leveringen:

1. URL-adressen til manifestfilen som er lagret i forrige avsnitt (http://your_server.domain/path/custom.mft)
2. Den offentlige nøkkelen som brukes til å bekrefte signaturfilen som ble opprettet tidligere (for eksempel C:\staging\my-recovery-public.pem).

Feilsøking

Hvis du mottar en melding om at den tilpassede gjenopprettingsprosessen ikke består sikkerhetsvalideringen, sjekk følgende:

1. Manifestet må være UTF-8 uten BOM.
2. Kontroller filavtrykkene.
3. Kontroller at systemet ble levert med den offentlige nøkkelen som samsvarer med den private nøkkelen som brukes til å signere manifestet.
4. MIME-typene for IIS-server må være `application/octet-stream`.
5. Filbaner i manifestet må inkludere den fullstendige banen til den øverste katalogen som inneholder bildet sett fra et klientsystem. Denne banen er ikke den fullstendige banen der filene lagres i distribusjonspunktet.

3 Bruke HP Sure Recover Agent i en bedriftsbrannmur

HP Sure Recover-agenten kan ligge på et bedriftsintranett. Når du har installert HP Sure Recover SoftPaq, kopierer du agentfilene fra HP Sure Recover-agentkatalog fra installasjonsstedet til et HTTP- eller FTP-distribusjonspunkt. Lever deretter klientsystemet med URL-en for distribusjonspunktet, og den offentlige HP-nøkkelen som heter `hpsr_agent_public_key.pem`, som er distribuert med HP Sure Recover agent-SoftPaq.

Installere HP Sure Recover-agent

1. Last ned HP Sure Recover-agent og pakk ut filene til HTTP- eller FTP-distribusjonspunktet.
2. Angi de nødvendige filtillatelsene på distribusjonspunktet.
3. Hvis du bruker Internet Information Services (IIS), må du lage MIME-typer av typen application/octet-stream for følgende filformater:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   VIKTIG: De følgende trinnene beskriver levering av Sure Recover med SCCM. Se Arbeide med HP Client Management Script Library (CMSL) på side 12for å få eksempler på hvordan du levere Sure Recover med HP Client Management Script Library.

4. Start SCCM, Naviger til **HP Client Security Suite**, og velg deretter siden HP Sure Recover.

   MERK: URL-adressen for distribusjonspunktet inkluderer enten ftp eller http som transportprotokoll. Den inkluderer også den fullstendige banen til den øverste katalogen som inneholder manifestet for HP Sure Recover-agenten sett fra et klientsystem. Denne banen er ikke den fullstendige banen til der filene lagres på distribusjonsstedet.

5. I delen **Platform Image** (plattformbilde) velger du alternativet **Corporation** (bedrift) for å gjenopprette et tilpasset OS-bilde fra et distribusjonspunkt for bedriften. Skriv inn URL-en som er levert av IT-administratoren, i tekstboksen **Image Location URL** (URL for bildeplassering). Skriv inn den offentlige nøkkelen `hpsr_agent_public_key.pem` i feltet **Image Verifcation** (bildekontroll).

   MERK: URL-en for egendefinert bilde må inneholde filnavnet til bildemanifestet.

6. I delen **Recovery Agent** (gjenopprettingsagent) velger du alternativet **Corporation** (bedrift) for å bruke en egendefinert gjenopprettingsagent eller HP-gjenopprettingsagenten fra et distribusjonspunkt for bedriften. Skriv inn URL-en som er levert av IT-administratoren, i boksen **Agent Location URL** (URL-

adresse for agentplassering). Skriv inn den offentlige nøkkelen `hpsr_agent_public_key.pem` i feltet **Agent Verification Key** (verifiseringsnøkkel for agent).

MERK: Ikke ta med filnavnet til agentmanifestet i URL-en fordi BIOS krever at det kalles recovery.mft.

7. Når policyen er brukt på klientsystemet, starter du det på nytt.
8. Ved første levering vises en melding der du kan skrive inn en firesifret sikkerhetskode for å fullføre HP Sure Recover-aktiveringen. Hvis du vil ha mer informasjon, går du til hp.com og søker etter den tekniske artikkelen HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

Etter at aktiveringen av HP Sure Recover er fullført, vises den egendefinerte URL-en som brukes av policyen, i innstillingsmenyen for HP Sure Recover BIOS.

For å bekrefte at aktiveringen var vellykket, start datamaskinen på nytt, og trykk på F10 når HP-logoen vises. Velg **Advanced** (Avansert), velg **HP Sure Recover**, velg **Recovery Agent** (gjenopprettingsagent), og velg deretter **URL**.

4 Arbeide med HP Client Management Script Library (CMSL)

Ved hjelp av HP Client Management Script Library kan du administrere innstillingene for HP Sure Recover med PowerShell. Følgende eksempelskript viser hvordan du leverer, bestemmer status, endrer konfigurasjon og leverer HP Sure Recover.

MERK: Flere av kommandoene overskrider linjelengden i denne håndboken, men må angis som én 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
}
```

Eksempel på nøkkelgenerering ved hjelp av OpenSSL

Oppbevar de private nøklene på et trygt sted. De offentlige nøklene vil bli brukt for validering, og må angis under levering. Disse nøklene må være 2048 bits i lengde og bruke en eksponent for 0x10001. Bytt ut emnet i eksemplene med informasjon om din organisasjon.

Angi følgende miljøvariabel før du fortsetter:

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

# Opprett et selvsignert root CA-sertifikat for testing
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"

# Opprett et endossementssertifikat for nøkler
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:


# Opprett en nøkkel for kommandosignering

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:


# Opprett en nøkkel for bildesignering

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 bilde manifestet med denne kommandoen:

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


# Opprett en nøkkel for agentsignering

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 kommandoen:

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

OpenSSL genererer signaturfiler i big-endian-format, som er uforenlig med noen BIOS-versjoner, slik at byterekkefølgen på agentsignaturfilen må reverseres før de kan distribueres. BIOS-versjoner som støtter big-endian-byterekkefølge, støtter også little-endian-byterekkefølge.

A Feilsøking

Partisjonering mislyktes

Mislykket stasjonspartisjonering kan oppstå hvis SR_AED eller SR_IMAGE-partisjonen er kryptert med Bitlocker. Disse partisjonene er vanligvis laget med en gpt-attributt som hindrer Bitlocker fra å kryptere dem, men hvis en bruker sletter og gjenoppretter partisjonene eller oppretter dem manuelt på en bare-metal-stasjon, kan ikke Sure Recover-agenten slette dem og avslutter med en feil når du partisjonerer stasjonen på nytt. Brukeren må manuelt slette dem ved å kjøre DiskPart, velge volum og sende overstyringskommandoen `del vol` (slett vol.) eller lignende.

Revisjonslogg for fastvare

Informasjon om EFI-variabelen er som følger:

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

APIer finnes under Windows for lesing av EFI-variabler, eller du kan dumpe variabelinnhold til en fil med UEFI Shell dmpstore-verktøyet.

Du kan dumpe revisjonsloggen med kommandoen `Get-HPFirmwareAuditLog` fra HP Client Management Script Library.

Hendelsesloggen i Windows

Start- og stopphendelser for Sure Recover sendes til BIOS-revisjonslogg, som du kan se i Windows Event Viewer i Sure Start-loggen hvis HP-varsler er installert. Disse hendelsene inkluderer dato og klokkeslett, kilde-ID, hendelses-ID og en hendelsesspesifikk kode. `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indikerer for eksempel at gjenopprettingen mislyktes fordi manifestet ikke kunne godkjennes med den hendelsesspesifikke koden c3f 23000 som ble logget kl. 2:26:40 den 27/6/18.

MERK: Disse loggene følger amerikansk datoformat av måned/dato/år.

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

Tabell A-1 HP Secure Platform Management

Hendelses-ID	Enhetsantall (alle/DaaS)	Hendelsesantall (alle/DaaS)	Beskrivelse	Merknader
40	256/178	943/552	Gjenopprettingsprosessen for Platform OS ble startet av fastvaren.	Plattformgjenoppretting startet
41	221/147	588/332	Gjenopprettingsprosessen for Platform OS er fullført.	Opprettelse av plattform fullført
42	54/42	252/156	Gjenopprettingsprosessen for Platform OS ble ikke fullført.	Plattformgjenoppretting mislyktes

Du kan hente revisjonsloggen for fastvare med Get-HPFirmwareAuditLog i HP Client Management Script Library, som er tilgjengelig på http://www.hp.com/go/clientmanagement. HP Secure Platform Management-hendelses-ID-er 40, 41 og 42 returnerer hendelsesspesifikke koder i datafeltet, som angir resultatet av at Sure Recover-operasjoner. Følgende loggoppføring viser for eksempel at Sure Recover ikke kan laste ned manifest- eller signaturfilen med feilen event_id 42 og data: 00:30:F1:c3, som skal tolkes som dword-verdien 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0
alvorlighetsgrad Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 42
timestamp_is_exact: 1
tidsangivelse: 27/5/2019 14:44:18
beskrivelse: Gjenopprettingsprosessen for Platform OS ble ikke fullført.
data: 00:30:f1:c3
```

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

```
Hendelsesspesifikke koder
Suksess = 0x00000000
CatalogDownloadFailed = 0xC3F11000
message_number: 0
alvorlighetsgrad Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 41
timestamp_is_exact: 1
tidsangivelse: 27/5/2019 14.55.41
beskrivelse: Gjenopprettingsprosessen for Platform OS ble ikke fullført.
data: 00:00:00:00
```

HP Sure Recover bruker følgende hendelsesspesifikke koder.

Tabell A-2 Hendelsesspesifikke koder

Beskrivelse av hendelse	Hendelseskode
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000

Tabell A-2 Hendelsesspesifikke koder (forts.)

Beskrivelse av hendelse	Hendelseskode
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