Användarhandbok

HP Sure Recover

Första utgåvan: Februari 2020

Dokumentartikelnummer: L93434-101

Syntaxnyckel för användarinmatning

Text som du måste ange i ett användargränssnitt indikeras genom `teckensnitt med fast bredd`.

Tabell -1 Syntaxnyckel för användarinmatning

Objekt	Beskrivning
`Text utan parenteser eller klammerparenteser`	Objekt som du måste skriva ut exakt som de visas
`<Text inuti vinkelparenteser>`	En platshållare för ett värde som du måste uppge; utelämna parenteser
`[Text inuti hakparenteser]`	Valfria objekt; utelämna parenteser
`{Text inuti klammerparenteser}`	En uppsättning objekt av vilka du måste du välja endast ett; utelämna klammerparenteser
`|`	En avskiljare för objekt av vilka du måste välja endast ett; utelämna vertikalstreck
`...`	Objekt som kan eller måste upprepas; utelämna ellips

Innehåll

1 Komma igång

HP Sure Recover hjälper dig att på ett säkert sätt installera operativsystemet från nätverket med minimal användarinteraktion. System med HP Sure Recover med inbäddad avbildning stöder även installation från en lokal lagringsenhet.

VIKTIGT: Säkerhetskopiera dina data innan du använder HP Sure Recover. Eftersom avbildningsprocessen omformaterar enheten inträffar dataförlust.

Återställningsavbildningar som HP tillhandahåller inkluderar det grundläggande installationsprogrammet för Windows 10®. Alternativt kan optimerade drivrutiner för HP-enheter installeras med HP Sure Recover. HPs återställningsavbildningar omfattar endast dataåterställningsagenter som ingår i Windows 10, t.ex. OneDrive. Företag kan skapa egna anpassade avbildningar för att lägga till företagsinställningar, program, drivrutiner och dataåterställningsagenter.

En återställningsagent för operativsystem utför de steg som krävs för att installera återställningsavbildningen. HPs återställningsagent utför vanliga steg som partitionering, formatering och extrahering av återställningsavbildningen till målenheten. Eftersom HPs återställningsagent finns på hp.com behöver du tillgång till internet för att hämta den, såvida inte systemet har en inbäddad avbildning. Företag kan också vara värd för HPs återställningsagent inom sin brandvägg eller skapa anpassade återställningsagenter för mer komplicerade återställningsmiljöer.

Du kan initiera HP Sure Recover när det inte finns något operativsystem. Du kan också köra HP Sure Recover enligt ett schema, t.ex. för att säkerställa att skadlig kod tas bort. Konfigurera dessa inställningar med hjälp av HP Client Security Manager (CSM), Management integration Kit (MIK) eller HP Client Management Script Library.

Utföra en nätverksåterställning

OBS! För att kunna återställa nätverket måste du använda en trådbunden anslutning. HP rekommenderar att du säkerhetskopierar viktiga filer, data, foton, videor och så vidare innan du använder HP Sure Recover för att undvika dataförlust.

1. Anslut klientsystemet till nätverket där du kan komma åt HTTP- eller FTP-distributionsplatsen.
2. Starta om klientsystemet och när HP-logotypen visas trycker du på F11.
3. Välj **Återställ från nätverk**.

Utföra en återställning av lokal enhet

Om ett klientsystem har stöd för inbäddad avbildning och nedladdningsalternativet för schemalagd avbildning är aktiverat i den tillämpade principen, hämtas avbildningen till klientsystemet vid den schemalagda tidpunkten. När avbildningen har hämtats till klientsystemet startar du om det så att avbildningen kopieras till lagringsenheten för den inbäddade avbildningen.

Så här utför du lokal återställning med hjälp av avbildningen på lagringsenheten för den inbäddade avbildningen:

1. Starta om klientsystemet och när HP-logotypen visas trycker du på F11.
2. Välj **Återställ från lokal enhet**.

System med inbäddade avbildningar måste konfigurera ett hämtningsschema och använda hämtningsagenten för att söka efter uppdateringar. Hämtningsagenten ingår i plugin-programmet HP Sure Recover för HP Client Security Manager och kan även konfigureras i MIK. Se https://www.hp.com/go/clientmanagement för anvisningar om hur du använder MIK.

Du kan också skapa en schemalagd aktivitet för att kopiera agenten till partitionen SR_AED och avbildningen till partitionen SR_IMAGE. Du kan sedan använda skriptet för HP Client Management Script Library för att skicka en tjänsthändelse som informerar BIOS att den ska validera innehållet och kopiera till lagringsenheten för den inbäddade avbildningen vid nästa omstart.

2 Skapa en företagsavbildning

De flesta företag använder Microsofts distributionsverktyg, Windows 10 Assessment and Deployment Kit, eller båda, för att producera filer som innehåller en avbildning i ett filformatsarkiv i Windows Imaging (WIM).

Krav

- Den senaste versionen av Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (eller någon annan lösning för generering av privata/offentliga RSA-nyckelpar)

  Använd det här alternativet för att generera RSA-nyckelparet som används för att säkra integriteten för den företagsavbildning som du skapar och är värd för.
- En servervärdlösning (t.ex. Microsoft Internet Information Services [IIS])

Skapa avbildningen

Innan du påbörjar processen med att skapa avbildningar konfigurerar du arbetssystemet eller byggsystemet där du har installerat de verktyg som krävs för att förbereda avbildningen för bearbetning, enligt följande steg:

1. Som administratör öppnar du kommandotolken för `Distributions- och avbildningsverktygmiljö` (installeras med distributionsverktygen i Windows ADK).
2. Skapa ett mellanlagringsområde för avbildningen med hjälp av följande kommando:

   ```
   mkdir C:\staging
   ```
3. Skapa avbildningen med något av följande exempel:

   Exempel 1: Skapa en avbildning baserad på installationsavbildningen för Microsoft Windows på sidan 3

   Exempel 2: Skapa en avbildning baserat på ett referenssystem på sidan 5

Exempel 1: Skapa en avbildning baserad på installationsavbildningen för Microsoft Windows

1. Montera eller öppna installationsavbildningen för Microsoft Windows (från en Microsoft ISO eller en HP OSDVD).
2. Kopiera filen install.wim till mellanlagringsområdet med hjälp av följande kommando från den monterade installationsavbildningen för Windows:

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

   OBS! `<M:>` hänvisar till den monterade enheten. Ersätt med korrekt enhetsbokstav.
3. Byt namn på filen install.wim till ett avbildningsfilnamn ("my-image" i det här exemplet) med hjälp av följande kommando:

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

(Tillval) I HP Sure Recover ingår en funktion för att återställa en viss utgåva från en avbildning med flera index, baserad på Windows-utgåvan som ursprungligen licensierats för HP Target-systemet i fabriken. Den här mekanismen fungerar om indexen namnges på rätt sätt. Om din installationsavbildning för Windows kommer från en HP OSDVD-avbildning har du troligtvis en avbildning för flera utgåvor. Om du inte vill använda detta beteende och säkerställa att en viss utgåva används för alla dina målsystem, måste du se till att det endast finns ett index i installationsavbildningen.

4. Kontrollera innehållet i installationsavbildningen med hjälp av följande kommando:

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

   Följande visar exempel på utdata från en installationsavbildning som stöder fem utgåvor (matchas baserat på BIOS för varje målsystem):

   Detaljer för avbildning: `my-image.wim`

   Index: `1`

   Namn: `CoreSingleLanguage`

   Beskrivning: `Windows 10 maj 2019 Uppdatering - Home Single Language Edition`

   Storlek: `19 512 500 682 byte`

   Index: `2`

   Namn: `Kärna`

   Beskrivning: `Windows 10 maj 2019 Uppdatering - Home Edition`

   Storlek: `19 512 500 682 byte`

   Index: `3`

   Namn: `Professional`

   Beskrivning: `Windows 10 maj 2019 Uppdatering - Professional Update`

   Storlek: `19 758 019 520 byte`

   Index: `4`

   Namn: `ProfessionalEducation`

   Beskrivning: `Windows 10 maj 2019 Uppdatering - Professional Education Edition`

   Storlek: `19 758 019 480 byte`

   Index: `5`

   Namn: `ProfessionalWorkstation`

   Beskrivning: `Windows 10 maj 2019 Uppdatering - Professional Workstation Edition`

   Storlek: `19 758 023 576 byte`

OBS! När det endast finns ett index används avbildningen för återställning, oberoende av namnet. Avbildningsfilens storlek kan vara större än före borttagningarna.

5. Ta bort alla index som du inte vill ha om du inte vill använda beteendet för flera utgåvor.

   Om du endast vill ha Professional Edition (förutsatt att alla målsystem är licensierade), enligt följande exempel, tar du bort index 5, 4, 2 och 1. Varje gång du tar bort ett index tilldelas indexnumren på nytt. Du bör därför ta bort från högsta till lägsta indexnummer. Kör `Get-imageinfo` efter varje radering för att visuellt bekräfta vilket index du vill ta bort nästa gång.

   ```
   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
   ```

   Välj endast ett index för utgåvan (i det här exemplet Professional). När det endast finns ett index används avbildningen för återställning, oberoende av namnet. Tänk på att storleken på avbildningsfilen kan vara större än före borttagningarna, på grund av det sätt som ändringar i WIM-metadata och normalisering av innehåll fungerar.

6. (Valfritt) Inkludera drivrutiner i återställningsavbildningen för företaget, enligt följande steg:

   a. Montera avbildningen i en tom mapp med hjälp av följande kommandon:

   ```
   mkdir C:\staging\mount

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

   b. Montera korrekt HP Windows 10-drivrutin DVD (DRDVD) för målsystemet som stöds. Kopiera drivrutinens undermappar till mellanlagringsområdet på de monterade drivrutinsmedierna med hjälp av följande kommando:

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

   OBS! `<M:>` hänvisar till den monterade enheten. Ersätt med korrekt enhetsbokstav.

   Du kan inkludera ytterligare inf-style-drivrutiner genom att placera dem under mappen C:\staging \mount\SWSETUP\DRV. Om du vill veta mer om hur detta innehåll bearbetas av HP Sure Recover med hjälp av funktionen `dism /Add-Driver /Recurse`, se ”Lägg till och ta bort drivrutiner till en frånkopplad Windows-avbildning” i följande avsnitt: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Den här funktionen stöder inte exe-style-drivrutiner som kräver att du kör ett program.

   c. Spara ändringarna och demontera avbildningen med hjälp av följande kommando:

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

   Den resulterande avbildningsfilen är: C:\staging\my-image.wim.

   d. Gå till Dela upp bilden på sidan 6.

Exempel 2: Skapa en avbildning baserat på ett referenssystem

1. Skapa startbara USB WinPE-medier.

OBS! Ytterligare metoder för att ta avbildningen finns i ADK-dokumentationen.

Se till att det finns tillräckligt med ledigt utrymme på USB-enheten för att rymma den tagna avbildningen från referenssystemet.

2. Skapa en avbildning på ett referenssystem.
3. Ta avbildningen genom att starta referenssystemet med hjälp av USB WinPE-mediet och använd sedan DISM.

OBS! `<U:>` hänvisar till USB-enheten. Ersätt med korrekt enhetsbokstav.

Redigera "my-image"-delen av filnamnet och beskrivningen `<my-image>` vid behov.

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

4. Kopiera avbildningen från USB till mellanlagringsområdet på ditt arbetssystem med hjälp av följande kommando:

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

Du bör ha följande avbildningsfil: C:\staging\my-image.wim.

5. Gå till Dela upp bilden på sidan 6.

Dela upp bilden

HP rekommenderar att du delar upp bilden i mindre filer för att förbättra tillförlitligheten i nätverkshämtningar med hjälp av följande kommando:

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

OBS! Storleken visas i megabyte. Redigera vid behov.

OBS! Till följd av funktionen hos den delade algoritmen för DISM kan storleken på de genererade SWM-filerna vara antingen mindre eller större än filstorleken som har angetts.

Skapa ett manifest

Formatera manifestfiler som UTF-8 utan BOM (byte order mark).

Du kan ändra manifestfilnamnet (custom.mf) som används i följande procedurer, men du får inte ändra extensions.mft eller .sig, och filnamnsdelen i manifest- och signaturfilerna måste överensstämma. Du kan till exempel ändra paret (custom.mft, custom.sig) till (myimage.mft, myimage.sig).

`mft_version` används för att avgöra avbildningsfilens format och måste för närvarande vara inställd på 1.

`image_version` används för att avgöra om en nyare version av avbildningen är tillgänglig och för att förhindra att äldre versioner installeras.

Båda värdena måste vara osignerade 16-bitars heltal och radavskiljaren i manifestet måste vara `'\r\n'` (CR + LF).

Generera ett manifest

Eftersom flera filer kan vara inblandade i den delade avbildningen använder du ett PowerShell-skript för att generera ett manifest.

I alla återstående steg måste du vara i mappen C:\staging.

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

1. Skapa ett PowerShell-skript med hjälp av en redigerare som kan producera en textfil i formatet UTF-8 utan BOM, med hjälp av följande kommando: `notepad C:\staging\generate-manifest.ps1`

   Skapa följande skript:

```
$mftFilename = "custom.mft"
$imageVersion = 1907 (Anmärkning: Detta kan vara valfritt 16-bitars 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
}
```

OBS! Manifest för HP Sure Recover kan inte inkludera en BOM, vilket innebär att följande kommandon skriver över filen som UTF8 utan BOM.

```
$content = Get-Content $mftFilename

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

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

2. Spara skriptet.
3. Kör skriptet.

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

Generera manifestsignatur

Med Sure Recover valideras agenten och avbildningen med hjälp av kryptografiska signaturer. Följande exempel använder privata/offentliga nyckelpar i X.509 PEM-format (.PEM-tillägg). Justera kommandona enligt vad som är lämpligt för användning av binära DER-certifikat (.CER- eller.CRT-tillägg), BASE-64-kodade PEM-certifikat (.CER- eller.CRT-tillägg) eller PKCS1, PEM-filer (.PEM-tillägg). I exemplet används även OpenSSL som genererar signaturer i big-endian-format. Du kan använda valfritt verktyg för att signera manifest, men vissa BIOS-versioner har endast stöd för signaturer i little-endian-format.

1. Skapa en 2 048-bitars RSA-nyckel med hjälp av följande kommando. Om du har ett 2 048-bitars privat/offentligt RSA-nyckelpar i PEM-format, kopierar du dem till C:\staging och går sedan vidare till steg 3.

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

2. Generera den offentliga nyckeln från din privata nyckel (om du har en offentlig nyckel som motsvarar din privata nyckel i PEM-format, kopiera den till C:\staging) med hjälp av följande kommando:

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

3. Skapa en signaturfil (med hjälp av SHA256-baserad hash) baserat på din 2 048-bitars privata RSA-nyckel från steg 1, med hjälp av följande kommando:

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

4. Kontrollera signaturfilen med hjälp av din offentliga nyckel från föregående steg med hjälp av följande kommando:

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

OBS!

- Om du bara behöver skapa en signaturfil, är de nödvändiga stegen 1 och 3.
- För HP Sure Recover är minsta nödvändiga steg 1, 2 och 3. Du behöver den offentliga nyckeln från steg 2 för att etablera ditt målsystem.
- Steg 4 är valfritt men rekommenderas så att din signaturfil och manifestfil validerar på korrekt sätt.

Värd för filerna

Var värd för följande filer på servern från mappen C:\staging:

- *.swm
- custom.mft (eller filnamnet du valde för manifestfilen)
- custom.sig (eller det matchande filnamnet som du valde för signaturfilen)

OBS! Om du använder IIS som värdlösning måste du konfigurera dina MIME-poster så att de innehåller följande tillägg, som alla är konfigurerade som "application/octet-stream:"

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

Etablera dina målsystem

Du kan etablera dina målsystem med hjälp av HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover eller Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Ange följande information för den här etableringen:

1. URL-adressen till manifestfilen som finns i föregående avsnitt (http://your_server.domain/path/custom.mft)
2. Den offentliga nyckel som används för att verifiera den tidigare skapade signaturen (till exempel C:\staging\my-recovery-public.pem).

Felsökning

Om du får ett meddelande om att säkerhetsvalideringen för den anpassade återställningsprocessen misslyckas kontrollerar du följande:

1. Manifestet måste vara UTF-8 utan BOM.
2. Kontrollera filhashar.
3. Kontrollera att systemet har etablerats med den offentliga nyckel som motsvarar den privata nyckel som används för att signera manifestet.
4. MIME-typer för IIS-servern måste vara `application/octet-stream`.
5. Filsökvägar inom manifestet måste innehålla den fullständiga sökvägen till den översta katalogen som innehåller avbildningen sett från ett klientsystem. Den här sökvägen är inte den fullständiga sökvägen till distributionsplatsen där filerna sparas.

3 Använda HP Sure Recover-agenten i en företagsbrandvägg

HP Sure Recover-agenten kan finnas på ett företags intranät. När du har installerat HP Sure Recover SoftPaq kopierar du agentfilerna från HP Sure Recover-agentens katalog från installationsplatsen till en HTTP- eller FTP-distributionsplats. Etablera sedan klientsystemet med URL:en till distributionsplatsen och HPs offentliga nyckel med namnet `hpsr_agent_public_key.pem`, som distribueras med SoftPaq för HP Sure Recover-agenten.

Installera HP Sure Recover-agenten

1. Hämta HP Sure Recover-agenten och extrahera filerna till din HTTP-eller FTP-distributionsplats.
2. Ställ in rätt filbehörigheter på distributionsplatsen.
3. Om du använder IIS (Internet Information Services) kan du skapa MIME-typerna application/octet-stream för följande filformat:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

VIKTIGT: Följande steg beskriver etableringen av Sure Recover med SCCM. Exempel på hur du etablerar Sure Recover med HP Client Management Script Library finns i Arbeta med HP Client Management Script Library (CMSL) på sidan 12.

4. Starta SCCM, navigera till **HP Client Security Suite** och välj sedan sidan HP Sure Recover.

OBS! I distributionsplatsens URL ingår antingen ftp eller http som transportprotokoll. Den innehåller även den fullständiga sökvägen till den översta katalogen som innehåller manifestet för HP Sure Recover-agenten sett från ett klientsystem. Den här sökvägen är inte den fullständiga sökvägen till distributionsplatsen där filerna sparas.

5. I avsnittet **Plattformsavbildning** väljer du alternativet **Företag** för att återställa en anpassad operativsystemsavbildning från en företagsdistributionsplats. Ange URL:en som du har fått från IT-administratören i rutan **URL för avbildningsplats** . Ange den offentliga nyckeln `hpsr_agent_public_key.pem` i fältet **Avbildningsverifiering**.

OBS! URL:en för anpassad avbildning måste innehålla avbildningens manifestfilnamn.

6. I avsnittet **Återställningsagent** väljer du alternativet **Företag** för att använda en anpassad återställningsagent eller HPs återställningsagent från en företagsdistributionsplats. Ange URL:en som

du har fått från IT-administratören i rutan **URL för agentplatsen**. Ange den offentliga nyckeln `hpsr_agent_public_key.pem` i fältet **Verifieringsnyckel för agent**.

OBS! Inkludera inte filnamnet för agentens manifest i URL:en eftersom BIOS kräver att det ska heta recovery.mft.

7. När principen har tillämpats på klientsystemet startar du om den.
8. Under den första etableringen visas ett fönster där du uppmanas att ange en fyrsiffrig säkerhetskod för att slutföra aktiveringen av HP Sure Recover. Om du vill ha mer information kan du gå till hp.com och söka efter vitboken HP Manageability Integration Kit (MIK) för Microsoft System Center Manager.

När aktiveringen av HP Sure Recover har slutförts visas den anpassade URL:en som tillämpas av principen i menyn med BIOS-inställningar i HP Sure Recover.

Om du vill bekräfta aktiveringen, startar du om datorn och när HP-logotypen visas trycker du på F10. Välj **Avancerat**, välj **HP Sure Recover**, välj **Återställningsagent**och välj sedan **URL**.

4 Arbeta med HP Client Management Script Library (CMSL)

I HP Client Management Script Library kan du hantera inställningar i HP Sure Recover med PowerShell. Följande exempelskript visar hur du etablerar, fastställer status, ändrar konfiguration och avetablerar HP Sure Recover.

OBS! Flera av kommandona överskrider radlängden i den här handboken men måste anges som en enda rad.

```
$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 av exempelnyckel med hjälp av OpenSSL

Förvara de privata nycklarna på en säker plats. De offentliga nycklarna används för validering och måste tillhandahållas under etableringen. Dessa tangenter måste vara 2 048 bitar långa och använda en exponent för 0x10001. Byt ut ämnet i exemplen med information om din organisation.

Ställ in följande miljövariabel innan du fortsätter:

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

# Skapa ett självsignerat rotcertifikat för testning
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"

# Skapa ett nyckelcertifikat för påskrift
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:


# Skapa en signeringsnyckel för kommando

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:


# Skapa en signeringsnyckel för avbildning

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 signera avbildningsmanifestet med det här kommandot:

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


# Skapa en signeringsnyckel för agent

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 signera agentmanifestet med det här kommandot:

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

OpenSSL genererar signaturer i big endian-format, vilket inte är kompatibelt med vissa BIOS-versioner. Det innebär att agentens byte-ordning för signaturfil kan behöva omvändas innan den distribueras. BIOS-versioner som stöder byte-ordning för big-endian har även stöd för byte-ordning för little-endian.

A Felsökning

Partitionering av enheten misslyckades

Misslyckad enhetspartitionering kan uppstå om partitionen SR_AED eller SR_IMAGE krypteras med BitLocker. De här partitionerna skapas vanligtvis med ett gpt-attribut som hindrar BitLocker från att kryptera dem, men om en användare tar bort och återskapar partitionerna eller skapar dem manuellt på en ”bare metal”-enhet, kan inte Sure Recover-agenten ta bort dem och avslutas med ett fel vid ompartitionering av hårddisken. Användaren måste ta bort dem manuellt genom att köra DiskPart, välja volym och utfärda förbikopplingskommandot `del vol` eller liknande.

Granskningslogg för inbyggd programvara

Information om EFI-variabel är följande:

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

API:er finns i Windows för läsning av EFI-variabler eller så kan du dumpa variabelt innehåll till en fil med hjälp av UEFI Shell dmpstore-verktyget.

Du kan dumpa granskningsloggen med hjälp av kommandot `Get-HPFirmwareAuditLog` som finns i HP Client Management Script Library.

Windows händelselogg

Start- och stopphändelser för Sure Recover skickas till granskningsloggen för BIOS, som du kan visa i Windows händelselogg i Sure Start-loggen om HP Notifications är installerat. Dessa händelser inkluderar datum och tid, käll-ID, händelse-ID och en händelsespecifik kod. T.ex. `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indikerar att återställningen misslyckades eftersom manifestet inte kunde verifieras med händelsekoden c3f 23000 som loggades kl. 2:26:40 den 6/27/18.

OBS! Dessa loggar följer det amerikanska datumformatet månad/datum/år.

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

Tabell A-1 HP Secure Platform Management

Händelse-ID	Enhetsantal (alla/DaaS)	Antal händelser (alla/DaaS)	Beskrivning	Anteckningar
40	256/178	943/552	Återställningsprocessen i plattformens operativsystem startades av den inbyggda programvaran.	Plattformsåterställning har startats

Tabell A-1 HP Secure Platform Management (fortsättning)

Händelse-ID	Enhetsantal (alla/DaaS)	Antal händelser (alla/DaaS)	Beskrivning	Anteckningar
41	221/147	588/332	Återställningsprocessen i plattformens operativsystem har slutförts.	Återställningen av plattformen har slutförts
42	54/42	252/156	Det gick inte att slutföra återställningsprocessen i plattformens operativsystem.	Det gick inte att återställa plattformen

Du kan hämta granskningsloggen för inbyggd programvara med hjälp av Get-HPFirmwareAuditLog i HP Client Management Script Library, som finns på http://www.hp.com/go/clientmanagement. Händelse-ID:n 40, 41 och 42 för HP Secure Platform Management returnerar händelsespecifika koder i datafältet, vilket visar resultatet för Sure Recover-åtgärder. Följande loggpost anger till exempel att du inte kan hämta manifest- eller signaturfilen med felet event_id 42 och data: 00:30:f1:c3, vilket bör tolkas som dword-värdet 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

allvarlighetsgrad: Information

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

tidsstämpel: 2019/05/27 14:44:18

beskrivning: Det gick inte att slutföra återställningsprocessen i
plattformens operativsystem.

data: 00:30:f1:c3
```

En lyckad återställning visas som event_id = 41 och data: 00:00:00:00, t.ex.:

```
Händelsespecifika koder

Success = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

allvarlighetsgrad: Information

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

tidsstämpel: 2019/05/27 14:55:41

beskrivning: Det gick inte att slutföra återställningsprocessen i
plattformens operativsystem.

data: 00:00:00:00
```

HP Sure Recover använder följande händelsespecifika koder.

Tabell A-2 Händelsespecifika koder

Händelsebeskrivning	Händelsekod
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000
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