Gebruikershandleiding

HP Sure Recover

Eerste editie: februari 2020

Artikelnummer van document: L93434-331

Syntaxissleutel voor gebruikersinvoer

Tekst die u moet invoeren in een gebruikersinterface wordt aangeduid met een `lettertype met een vaste breedte`.

Tabel -1 Syntaxissleutel voor gebruikersinvoer

Item	Beschrijving
`Tekst zonder haakjes of accolades`	Items die u moet typen precies zoals weergegeven
`<Tekst tussen punthaken>`	Een tijdelijke aanduiding voor een waarde die u moet opgeven; laat de haakjes weg
`[Tekst tussen vierkante haken]`	Optionele items; laat de haakjes weg
`{Tekst tussen accolades}`	Een reeks items waaruit u slechts één item moet kiezen; laat de accolades weg
`|`	Een scheidingsteken voor items waaruit u slechts één item moet kiezen; laat de verticale streep weg
`...`	Items die kunnen of moeten worden herhaald; laat de punten weg

Inhoudsopgave

1 Aan de slag

HP Sure Recover helpt u bij het veilig installeren van het besturingssysteem vanaf het netwerk met minimale interactie van de gebruiker. Systemen met HP Sure Recover met Embedded Reimaging bieden ook ondersteuning voor installatie vanaf een lokaal opslagapparaat.

BELANGRIJK: Maak een back-up van uw gegevens voordat u HP Sure Recover gebruikt. Omdat de schijf tijdens het imagingproces opnieuw wordt geformatteerd, treedt er gegevensverlies op.

Herstelimages die door HP worden geleverd, bevatten het basisinstallatieprogramma voor Windows 10®. U kunt HP Sure Recover desgewenst gebruiken om geoptimaliseerde drivers voor HP apparaten te installeren. HP herstelimages bevatten alleen gegevensherstelagenten die worden meegeleverd met Windows 10, zoals OneDrive. Bedrijven kunnen eigen aangepaste images maken om bedrijfsinstellingen, applicaties, drivers en gegevensherstelagenten toe te voegen.

Een herstelagent voor een besturingssysteem (OS) voert de benodigde stappen uit om de herstelimage te installeren. De door HP geleverde herstelagent voert algemene stappen uit, zoals partitioneren, formatteren en uitpakken van de herstelimage naar het doelapparaat. Omdat de HP herstelagent zich op hp.com bevindt, hebt u toegang tot internet nodig om de herstelagent te kunnen downloaden, tenzij het systeem een voorziening voor Embedded Reimaging heeft. Bedrijven kunnen de HP herstelagent ook binnen hun firewall hosten of aangepaste herstelagenten maken voor meer gecompliceerde herstelomgevingen.

U kunt HP Sure Recover activeren wanneer er geen besturingssysteem is gevonden. U kunt HP Sure Recover ook uitvoeren volgens een schema, bijvoorbeeld om ervoor te zorgen dat malware wordt verwijderd. Configureer deze instellingen met HP Client Security Manager (CSM), de Manageability Integration Kit (MIK) of de HP Client Management Script Library.

Netwerkherstel uitvoeren

OPMERKING: Voor het uitvoeren van een netwerkherstel moet u een bekabelde verbinding gebruiken. HP raadt u aan een back-up te maken van belangrijke bestanden, gegevens, foto's, video's, enzovoort voordat u HP Sure Recover gebruikt. Zo wordt gegevensverlies voorkomen.

1. Verbind het clientsysteem met het netwerk voor toegang tot het HTTP-of FTP-distributiepunt.
2. Start het clientsysteem opnieuw op en druk op f11 wanneer het HP logo wordt weergegeven.
3. Selecteer **Herstellen vanaf netwerk**.

Herstel van een lokale schijf uitvoeren

Als een clientsysteem Embedded Reimaging ondersteunt en de optie voor het downloaden van de geplande image is ingeschakeld in het toegepaste beleid, wordt de image op het geplande tijdstip naar het clientsysteem gedownload. Start het clientsysteem na het downloaden opnieuw op om de image naar het opslagapparaat voor Embedded Reimaging te kopiëren.

Ga als volgt te werk om een lokaal herstel uit te voeren met behulp van de image op het opslagapparaat voor Embedded Reimaging:

1. Start het clientsysteem opnieuw op en druk op f11 wanneer het HP logo wordt weergegeven.
2. Selecteer **Herstellen vanaf lokale schijf**.

Systemen met Embedded Reimaging moeten een downloadschema configureren en de downloadagent gebruiken om te controleren op updates. De downloadagent is geïntegreerd in de HP Sure Recover plug-in voor HP Client Security Manager en kan ook worden geconfigureerd in de Manageability Integration Kit (MIK). Zie https://www.hp.com/go/clientmanagement voor instructies voor het gebruik van de MIK.

U kunt ook een geplande taak maken om de agent te kopiëren naar de SR_AED partitie en de image naar de SR_IMAGE partitie. Vervolgens kunt u de HP Client Management Script Library gebruiken om een servicegebeurtenis te verzenden die aangeeft dat het BIOS de inhoud moet valideren en bij de volgende herstart naar het opslagapparaat voor Embedded Reimaging moet kopiëren.

2 Een bedrijfsimage maken

De meeste bedrijven maken gebruik van Microsoft-implementatiehulpprogramma's, de Windows 10 Assessment and Deployment Kit of beide om bestanden met een image te maken in een WIM-bestandsindelingsarchief (Windows Imaging).

Vereisten

- De nieuwste versie van de Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (of een andere oplossing voor het genereren van een privé of openbaar RSA-sleutelpaar

  Gebruik OpenSSL om het RSA-sleutelpaar te genereren en de integriteit te garanderen van de bedrijfsimage die u maakt en host.
- Een oplossing voor serverhosting (zoals Microsoft Internet Information Services [IIS])

De image maken

Voordat u begint met het maken van een image, configureert u het werksysteem of buildsysteem waarin u de benodigde hulpmiddelen hebt geïnstalleerd, zoals in de volgende stappen wordt getoond:

1. Open als beheerder de opdrachtprompt voor de `Deployment and Imaging Tools Environment` (geïnstalleerd met de implementatiehulpprogramma's van de Windows ADK).
2. Maak een klaarzetgebied voor uw image met de volgende opdracht:

   ```
   mkdir C:\staging
   ```
3. Maak de image aan de hand van een van de volgende voorbeelden:

   Voorbeeld 1: een image maken op basis van de Microsoft Windows-installatiekopie op pagina 3

   Voorbeeld 2: een image maken op basis van een referentiesysteem op pagina 5

Voorbeeld 1: een image maken op basis van de Microsoft Windows-installatiekopie

1. Koppel of open de Microsoft Windows-installatiekopie (vanaf een Microsoft ISO of vanaf een HP OSDVD).
2. Kopieer het bestand install.wim van de gekoppelde Windows-installatiekopie naar het klaarzetgebied met de volgende opdracht:

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

   OPMERKING: `<M:>` verwijst naar de gekoppelde schijf. Vervang de letter door de juiste schijfaanduiding.
3. Hernoem install.wim naar een imagebestandsnaam (in dit voorbeeld "my-image") met de volgende opdracht:

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

   (Optioneel) HP Sure Recover bevat een functie voor het herstellen van een specifieke editie uit een image met meerdere indexen, op basis van de Windows-editie die oorspronkelijk is gelicentieerd voor

het HP doelsysteem in de fabrieksinstellingen. Dit mechanisme werkt alleen als de indexen de juiste naam hebben. Als uw Windows-installatiekopie afkomstig is uit een HP OSDVD-image, hebt u waarschijnlijk een image met meerdere versies. Als u dit niet wilt en slechts één specifieke editie wilt gebruiken voor al uw doelsystemen, moet u ervoor zorgen dat de installatiekopie slechts één index bevat.

4. Controleer de inhoud van de installatiekopie met behulp van de volgende opdracht:

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

Hieronder ziet u de voorbeelduitvoer van een installatiekopie die vijf edities ondersteunt (op basis van het BIOS van elk doelsysteem):

Details voor image: `my-image.wim`

Index: `1`

Naam: `CoreSingleLanguage`

Beschrijving: `Windows 10 May 2019 Update - Home Single Language Edition`

Grootte: `19,512,500,682 bytes`

Index: `2`

Naam: `Core`

Beschrijving: `Windows 10 May 2019 Update - Home edition`

Grootte: `19,512,500,682 bytes`

Index: `3`

Naam: `Professional`

Beschrijving: `Windows 10 May 2019 Update- Professional Update`

Grootte: `19.758,019,520 bytes`

Index: `4`

Naam: `ProfessionalEducation`

Beschrijving: `Windows 10 May 2019 Update - Professional Education edition`

Grootte: `19,758,019,480 bytes`

Index: `5`

Naam: `ProfessionalWorkstation`

Beschrijving: `Windows 10 May 2019 Update - Professional Workstation edition`

Grootte: `19,758,023,576 bytes`

OPMERKING: Als er slechts één index is, wordt de image ongeacht de naam gebruikt voor het herstellen. Het imagebestand kan groter zijn dan vóór het verwijderen.

5. Als u slechts één index wilt gebruiken, verwijdert u alle ongewenste indexen.

   Zoals u in het volgende voorbeeld ziet, verwijdert u index 5, 4, 2 en 1 als u alleen de Professional Edition wilt gebruiken (ervan uitgaand dat alle doelsystemen zijn gelicentieerd). Telkens wanneer u een index verwijdert, worden de indexnummers opnieuw toegewezen. Om deze reden moet u de indexnummers van hoog naar laag verwijderen. Voer na elke verwijdering `Get-Imageinfo` uit om visueel te bevestigen welke index u hierna wilt verwijderen.

   ```
   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
   ```

   Kies slechts één index van de editie (in dit voorbeeld Professional). Als er slechts één index is, wordt de image ongeacht de naam gebruikt voor het herstellen. Houd er rekening mee dat het imagebestand groter kan zijn dan vóór het verwijderen. Dit komt door de manier waarop wijzigingen van WIM-metagegevens en normalisatie van inhoud werken.

6. (Optioneel) Als u drivers wilt opnemen in uw bedrijfsimage, voert u de volgende stappen uit:

   a. Koppel uw image aan een lege map met behulp van de volgende opdrachten:

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

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

   b. Koppel de juiste DVD met HP Windows 10-drivers (DRDVD) voor het ondersteunde doelsysteem. Kopieer de driversubmappen vanaf de gekoppelde media naar het klaarzetgebied met behulp van de volgende opdracht:

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

   OPMERKING: `<M:>` verwijst naar de gekoppelde schijf. Vervang de letter door de juiste schijfaanduiding.

   U kunt aanvullende .inf-drivers toevoegen door deze in de map C:\staging\mount\SWSETUP\DRV te plaatsen. Voor een uitleg over de manier waarop deze inhoud wordt verwerkt door HP Sure Recover met de functie `dism /Add-Driver /Recurse`, raadpleegt u “Add and Remove Drivers to an Offline Windows image” in het volgende onderwerp: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Deze functie biedt geen ondersteuning voor .exe-drivers waarvoor een applicatie moet worden uitgevoerd.

   c. Sla uw wijzigingen op en koppel de image los met de volgende opdracht:

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

   Het resulterende imagebestand is: C:\staging\my-image.wim.

   d. Ga naar De image opsplitsen op pagina 6.

Voorbeeld 2: een image maken op basis van een referentiesysteem

1. Maak een opstartbare WinPE USB-drive.

OPMERKING: Aanvullende methoden voor het vastleggen van de image vindt u in de ADK-documentatie.

Zorg ervoor dat de USB-drive voldoende vrije ruimte heeft voor de image uit het referentiesysteem.

2. Maak een image op een referentiesysteem.
3. Leg de image vast door het referentiesysteem op te starten met de WinPE USB-drive en gebruik vervolgens DISM.

OPMERKING: `<U:>` verwijst naar de USB-drive. Vervang de letter door de juiste schijfaanduiding.

Bewerk indien nodig het gedeelte "my-image" in de bestandsnaam en de beschrijving `<my-image>`.

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

4. Kopieer de image van de USB-drive naar het klaarzetgebied in uw werksysteem met de volgende opdracht:

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

U moet het volgende imagebestand hebben: C:\staging\my-image.wim.

5. Ga naar De image opsplitsen op pagina 6.

De image opsplitsen

HP raadt u aan om de image op te splitsen in kleinere bestanden om de betrouwbaarheid van netwerkdownloads te verbeteren. Gebruik hiertoe de volgende opdracht:

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

OPMERKING: De bestandsgrootte wordt weergegeven in megabytes. Bewerk deze waarde indien nodig.

OPMERKING: Vanwege de aard van de splitsingsalgoritme van DISM kunnen de gegenereerde SWM-bestanden kleiner of groter zijn dan de opgegeven bestandsgrootte.

Een manifest maken

Maak manifestbestanden op als UTF-8 zonder BOM (Byte Order Mark).

U kunt de naam wijzigen van het manifestbestand (custom.mft) dat in de volgende procedures wordt gebruikt. De extensies .mft en. sig mogen echter niet worden gewijzigd en het naamgedeelte van het manifest- en handtekeningbestand moet overeenkomen. U kunt bijvoorbeeld het paar (custom.mft, custom.sig) wijzigen naar (myimage.mft, myimage.sig).

`mft_version` wordt gebruikt om de indeling van het imagebestand te bepalen en moet zijn ingesteld op 1.

`image_version` wordt gebruikt om te bepalen of er een nieuwere versie van de image beschikbaar is en om te voorkomen dat er een oude versie wordt geïnstalleerd.

Beide waarden moeten niet-ondertekende 16-bits gehele getallen zijn en het scheidingsteken voor regels in het manifest moet `'\r\n' (CR + LF)` zijn.

Een manifest genereren

Omdat uw opgesplitste image mogelijk meerdere bestanden omvat, gebruikt u een PowerShell-script voor het genereren van een manifest.

In alle resterende stappen moet u zich in de map C:\staging bevinden.

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

1. Maak een PowerShell-script met behulp van een editor die een tekstbestand kan produceren in UTF-8-indeling zonder BOM. Gebruik hiertoe de volgende opdracht: `notepad C:\staging\generate-manifest.ps1`

   Maak het volgende script:

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

   `$imageVersion = 1907` (Opmerking: dit kan een willekeurig 16-bits geheel getal zijn.)

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

}
```

OPMERKING: Manifesten voor HP Sure Recover kunnen geen BOM bevatten. Met de volgende opdrachten wordt het bestand dus herschreven naar UTF-8 zonder BOM.

```
$content = Get-Content $mftFilename

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

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

2. Sla het script op.
3. Voer het script uit.

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

De manifesthandtekening genereren

Sure Recover valideert de agent en image met behulp van cryptografische handtekeningen. In de volgende voorbeelden wordt een privé/openbaar sleutelpaar in X.509 PEM-indeling gebruikt met de extensie .PEM. Pas de opdrachten aan voor het gebruik van binaire DER-certificaten (extensie .CER of .CRT), BASE-64 gecodeerde PEM-certificaten (extensie .CER of .CRT) of PKCS1 PEM-bestanden (extensie .PEM). In het voorbeeld wordt ook gebruikgemaakt van OpenSSL voor het genereren van handtekeningen in big-endian indeling. U kunt elk gewenst hulpprogramma gebruiken om manifesten te ondertekenen. Sommige BIOS-versies ondersteunen echter alleen handtekeningen in little-endian indeling.

1. Genereer een 2048-bits RSA-privésleutel met behulp van de volgende opdracht. Als u een 2048-bits privé/openbaar RSA-sleutelpaar hebt in PEM-indeling, kopieert u ze naar C:\staging en gaat u verder met stap 3.

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

2. Genereer de openbare sleutel op basis van uw privésleutel (als u een openbare sleutel hebt die overeenkomt met uw privésleutel in PEM-indeling, kopieert u deze naar C:\staging) met behulp van de volgende opdracht:

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

3. Maak een handtekeningbestand (met behulp van een sha256-hash) op basis van uw 2048-bits RSA-privésleutel uit stap 1 met behulp van de volgende opdracht:

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

4. Controleer het handtekeningbestand met behulp van de openbare sleutel uit de vorige stap en de volgende opdracht:

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

OPMERKING:

- Als u alleen een handtekeningbestand wilt maken, zijn 1 en 3 de vereiste stappen.
- Voor HP Sure Recover zijn 1,2 en 3 de vereiste stappen. U hebt de openbare sleutel uit stap 2 nodig om uw doelsysteem in te richten.
- Stap 4 is optioneel, maar wordt aanbevolen voor juiste validatie van uw handtekeningbestand en manifestbestand.

De bestanden hosten

Host de volgende bestanden op uw server vanuit de map C:\staging:

- *.swm
- custom.mft (of de bestandsnaam die u voor het manifestbestand kiest)
- custom.sig (of de overeenkomstige bestandsnaam die u voor het handtekeningbestand kiest)

OPMERKING: Als u IIS gebruikt als hostingoplossing, moet u uw MIME-ingangen configureren voor de volgende extensies, die allen zijn geconfigureerd als "application/octet-stream:"

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

Uw doelsystemen inrichten

U kunt uw doelsystemen inrichten met behulp van de HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover of de Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Geef de volgende gegevens op voor het inrichten:

1. Het URL-adres van het manifestbestand dat wordt gehost in de vorige sectie (http://your_server.domain/path/custom.mft)
2. De openbare sleutel voor het verifiëren van het eerder gemaakte handtekeningbestand (bijvoorbeeld C:\staging\my-recovery-public.pem)

Problemen oplossen

Als u een bericht ontvangt dat de beveiligingsvalidatie van het aangepaste herstelproces is mislukt, controleert u het volgende:

1. Het manifestbestand moet de UTF-8-indeling zonder BOM hebben.
2. Controleer de bestand-hashes.
3. Controleer of het systeem is ingericht met de openbare sleutel die overeenkomt met de privésleutel die is gebruikt voor het ondertekenen van het manifestbestand.

4. MIME-typen van de IIS-server moeten `application/octet-stream` zijn.
5. Bestandspaden in het manifestbestand moeten het volledige pad bevatten naar de bovenste directory met de image, zoals gezien vanaf een clientsysteem. Dit pad is niet het volledige pad waar de bestanden worden opgeslagen op het distributiepunt.

3 De HP Sure Recover Agent gebruiken binnen een bedrijfsfirewall

De HP Sure Recover Agent kan worden gehost op een bedrijfsintranet. Nadat u de HP Sure Recover SoftPaq hebt geïnstalleerd, kopieert u de agentbestanden uit de directory van de HP Sure Recover Agent van de installatielocatie naar een HTTP-of FTP-distributiepunt. Richt het clientsysteem vervolgens in met de URL van het distributiepunt en de openbare HP sleutel `hpsr_agent_public_key.pem`, die wordt gedistribueerd met de HP Sure Recover Agent SoftPaq.

De HP Sure Recover Agent installeren

1. Download de HP Sure Recover Agent en pak de bestanden uit naar uw HTTP-of FTP-distributiepunt.
2. Stel de juiste bestandsmachtigingen in voor het distributiepunt.
3. Als u IIS (Internet Information Services) gebruikt, maakt u application/octet-stream MIME-typen voor de volgende bestandsindelingen:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

BELANGRIJK: In de volgende stappen wordt beschreven hoe u HP Sure Recover inricht met SCCM. Zie De HP Client Management Script Library (CMSL) gebruiken op pagina 13 voor voorbeelden van het inrichten van Sure Recover met de HP Client Management Script Library.

4. Start SCCM, navigeer naar **HP Client Security Suite** en selecteer vervolgens de pagina HP Sure Recover.

OPMERKING: De URL van het distributiepunt bevat ftp of http als transportprotocol. De URL bevat ook het volledige pad naar de bovenste directory met het manifestbestand voor de HP Sure Recover Agent, zoals gezien vanaf een clientsysteem. Dit pad is niet het volledige pad waar de bestanden worden opgeslagen op het distributiepunt.

5. Selecteer in de sectie **Platform Image** de optie **Corporation** om een aangepaste OS-image te herstellen vanaf een bedrijfsdistributiepunt. Typ de URL die door de IT-beheerder is geleverd in het invoervak **Image Location URL** . Typ de openbare sleutel `hpsr_agent_public_key.pem` in het veld **Image Verification**.

OPMERKING: De URL van de aangepaste image moet de naam van het manifestbestand van de image bevatten.

6. Selecteer in de sectie **Recovery Agent** de optie **Corporation** om een aangepaste herstelagent of de HP herstelagent te gebruiken vanaf een bedrijfsdistributiepunt. Typ de URL die door de IT-beheerder is

geleverd in het invoervak **Agent Location URL** . Typ de openbare sleutel `hpsr_agent_public_key.pem` in het invoerveld **Agent Verification Key**.

OPMERKING: Gebruik in de URL niet de bestandsnaam voor het agentmanifest. In het BIOS is namelijk de naam recovery.mft vereist.

7. Nadat het beleid is toegepast op het clientsysteem, start u het systeem opnieuw op.
8. Tijdens de initiële inrichting ziet u een prompt waarin u een 4-cijferige beveiligingscode moet invoeren om het activeren van HP Sure Recover te voltooien. Voor meer informatie gaat u naar hp.com en zoekt u de whitepaper 'HP Manageability Integration Kit (MIK) for Microsoft System Center Manager'.

Nadat HP Sure Recover is geactiveerd, wordt de aangepaste URL die door het beleid is toegepast, weergegeven in het BIOS-menu met instellingen voor HP Sure Recover.

Om het voltooien van de activering te bevestigen, start u de computer opnieuw op en drukt u op f10 wanneer u het HP logo ziet. Selecteer **Geavanceerd**, **HP Sure Recover**, **Recovery Agent** en vervolgens **URL**.

4 De HP Client Management Script Library (CMSL) gebruiken

Met de HP Client Management Script Library kunt u de instellingen voor HP Sure Recover beheren met PowerShell. Het volgende voorbeeldscript laat zien hoe u HP Sure Recover kunt inrichten, de status ervan kunt bepalen, de configuratie kunt wijzigen en het inrichten ongedaan kunt maken.

OPMERKING: Enkele opdrachten overschrijden de regellengte van deze handleiding maar moeten worden ingevoerd als één regel.

```
$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
}
```

Voorbeeld van sleutelgeneratie met OpenSSL

Bewaar de privésleutels op een veilige plaats. De openbare sleutels worden gebruikt voor validatie en moeten tijdens het inrichten worden ingevoerd. Deze sleutels moeten 2048 bits lang zijn en een exponent van 0x10001 gebruiken. Vervang het onderwerp in de voorbeelden door de gegevens van uw organisatie.

Stel de volgende omgevingsvariabele in voordat u verdergaat:

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


# Create a self-signed root CA certificate 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"


# Create a key endorsement certificate
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:


# Create a command signing key

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:


# Create an image signing key

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:
```

U kunt het manifestbestand van de image ondertekenen met behulp van de volgende opdracht:

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


# Create an agent signing key

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:
```

U kunt het manifestbestand van de agent ondertekenen met behulp van de volgende opdracht:

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

OpenSSL genereert handtekeningbestanden in big-endian indeling. Deze indeling is niet compatibel met bepaalde BIOS-versies. Om deze reden moet u de bytevolgorde van het handtekeningbestand voor de agent mogelijk omkeren voordat u het kunt implementeren. BIOS-versies die ondersteuning bieden voor de big-endian bytevolgorde, ondersteunen ook de little-endian bytevolgorde.

A Problemen oplossen

Schijfpartitionering is mislukt

Schijfpartitionering kan mislukken als de SR_AED of SR_IMAGE partitie is gecodeerd met Bitlocker. Deze partities worden normaal gesproken gemaakt met een gpt-attribuut dat voorkomt dat Bitlocker de partities codeert. Als een gebruiker de partities echter verwijdert en opnieuw maakt of ze handmatig maakt op een bare metal drive, kan de Sure Recover Agent ze niet verwijderen en treedt er een fout op wanneer de schijf opnieuw wordt gepartitioneerd. De gebruiker moet de partities handmatig verwijderen door diskpart uit te voeren, het volume te selecteren en de overschrijvingsopdracht `del vol` of een soortgelijke opdracht uit te voeren.

Auditlogboek voor de firmware

De informatie voor EFI-variabelen luidt als volgt:

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

Er bestaan API's onder Windows voor het lezen van EFI-variabelen, of u kunt variabele inhoud dumpen naar een bestand met het UEFI Shell-hulpprogramma dmpstore.

U kunt het auditlogboek dumpen met behulp van de opdracht `Get-HPFirmwareAuditLog` die wordt geleverd door de HP Client Management Script Library.

Windows-gebeurtenislogboek

Start-en stopgebeurtenissen van Sure Recover worden verzonden naar het BIOS-auditlogboek dat u kunt bekijken in Windows Logboeken in het Sure Start-logboek als HP Notifications is geïnstalleerd. Deze gebeurtenissen bevatten de datum en tijd, bron-ID, gebeurtenis-ID en een specifieke gebeurteniscode. Voorbeeld: `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` geeft aan dat het herstel is mislukt omdat het manifestbestand niet kon worden geverifieerd met gebeurteniscode c3f 23000 die is geregistreerd op 6/27/18 om 2:26:40.

OPMERKING: In deze logboeken wordt de Amerikaanse datumnotatie maand/dag/jaar gebruikt.

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

Tabel A-1 HP Secure Platform Management

Gebeurtenis-ID	Aantal apparaten (alles/DaaS)	Aantal gebeurtenissen (alles/DaaS)	Beschrijving	Opmerking
40	256/178	943/552	Het herstelproces voor het platform-OS is gestart door de firmware.	Platformherstel is gestart.

Tabel A-1 HP Secure Platform Management (vervolg)

Gebeurtenis-ID	Aantal apparaten (alles/DaaS)	Aantal gebeurtenissen (alles/DaaS)	Beschrijving	Opmerking
41	221/147	588/332	Het herstelproces voor het platform-OS is voltooid.	Platformherstel is voltooid.
42	54/42	252/156	Het herstelproces voor het platform-OS is niet voltooid.	Platformherstel is mislukt.

U kunt het auditlogboek voor de firmware ophalen met Get-HPFirmwareAuditLog in de HP Client Management Script Library, beschikbaar op http://www.hp.com/go/clientmanagement. Met de gebeurtenis-ID's 40, 41 en 42 van HP Secure Platform Management worden specifieke gebeurteniscodes geretourneerd in het gegevensveld. Deze codes geven het resultaat aan van de bewerkingen van Sure Recover. De volgende logboekingang geeft bijvoorbeeld aan dat het downloaden van het manifest- of handtekeningbestand door Sure Recover is mislukt met gebeurtenis-ID 42 met de gegevens 00:30:f1:c3. Deze gegevens moeten worden geïnterpreteerd als de dword-waarde 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

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

Een geslaagde herstelbewerking wordt weergegeven als gebeurtenis-ID 41 met de gegevens 00:00:00:00. Voorbeeld:

```
Event Specific Codes

Success = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

timestamp: 5/27/2019 2:55:41 PM
```

```
description: The platform OS recovery process failed to complete
successfully.
data: 00:00:00:00
```

HP Sure Recover gebruikt de volgende specifieke gebeurteniscodes.

Tabel A-2 Specifieke gebeurteniscodes

Beschrijving gebeurtenis	Gebeurteniscode
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