



Kasutusjuhend

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

Microsoft ja Windows on ettevõtte Microsoft Corporation registreeritud kaubamärgid või kaubamärgid Ameerika Ühendriikides ja/või teistes riikides.

Konfidentsiaalne arvutitarkvara. Omamiseks, kasutamiseks ja kopeerimiseks on nõutav HP kehtiv litsents. Kui olete USA valitsusasutus, siis kooskõlas FAR 12.211 ja 12.212-ga litsentsitakse arvuti äritarkvara, arvuti tarkvaradokumentatsioon ja kaubanduslikeniimetuste tehnilised andmed kehtiva HP ärilitsentsilepingu alusel.

Käesolevas dokumendis sisalduvat teavet võidakse ette teatamata muuta. Ainsad HP toodete ja teenuste garantiid on sätestatud vastavate toodete ja teenustega kaasnevates garantii lühiavaldustes. Käesolevas dokumendis avaldatut ei või mingil juhul tõlgendada täiendava garantii pakkumisena. HP ei vastuta siin leiduda võivate tehniliste või toimetuslike vigade ega väljajätmiste eest.

Esimene versioon: veebruar 2020

Dokumendi number: L93434-E41

## Kasutajasisendi süntaksi võti

Teie poolt kasutajaliidesesse sisestatav tekst on märgitud fikseeritud laiussega kirjatüübis.

**Tabel -1** Kasutajasisendi süntaksi võti

Üksus	Kirjeldus
Sulgudeta või looksulgudeta tekst	Üksused, mis tuleb sisestada täpselt näidatu alusel.
<noolsulgudes tekst>	Kohatäide teie poolt sisestatava väärtuse jaoks; eemaldage sulud.
[nurksulgudes tekst]	Valikulised numbrid; eemaldage sulud.
{looksulgudes tekst}	Üksuste komplekt, millest teil tuleb valida vaid üks; eemaldage looksulud.
	Eraldaja üksuste jaoks, millest teil tuleb valida vaid üks; eemaldage vertikaalriba.
...	Üksused, mis võivad või peavad korduma; eemaldage ellips.



---

# Sisukord

<b>1 Alustamine .....</b>	<b>1</b>
Võrgu taastamise teostamine .....	1
Kohalike draivide taastamise teostamine .....	1
<b>2 Ettevõtte pildi loomine .....</b>	<b>3</b>
Nõuded .....	3
Pildi loomine .....	3
Näide 1. Microsoft Windowsi installi pildil põhineva pildi loomine .....	3
Näide 2. Taustsüsteemi alusel pildi loomine .....	5
Kujutise jagamine .....	6
Manifesti loomine .....	6
Manifesti loomine .....	6
Manifesti signatuuri loomine .....	8
Failide hostimine .....	8
Sihtsüsteemide ettevalmistamine .....	9
Törkeotsing .....	9
<b>3 HP Sure Recover agendi kasutamine ettevõtte tulemüüris .....</b>	<b>10</b>
HP Sure Recover agendi paigaldamine .....	10
<b>4 Töö HP Client Management Scripti Libraryga (CMSL) .....</b>	<b>12</b>
Näidisvõti OpenSSL-i kasutades .....	14
<b>Lisa A Törkeotsing .....</b>	<b>16</b>
Draivi sektsioonimine nurjus .....	16
Püsivara auditi logi .....	16
Windowsi sündmustelogi .....	16
HP Secure Platform Management (Source ID = 84h) .....	16



# 1 Alustamine

HP Sure Recover aitab teil operatsioonisüsteemi turvaliselt installida võrgust minimaalse kasutajapoolse sekkumisega. Süsteemid, millel on HP Sure Recover sisseehitatud taaskujutamisega, toetavad ka installatsiooni kohalikust mäluseadmest.



**NB!** Varundage andmed enne, kui HP Sure Recoverit kasutate. Kuna pildinduse protsess vormindab draivi ümber, toimub andmete kadumine.

HP taastatavad pildid sisaldavad operatsioonisüsteemi Windows 10® installijat. Soovi korral võib HP Sure Recover installida HP seadmete jaoks optimeeritud draivereid. HP taastatavad pildid sisaldavad ainult Windows 10-ga kaasas olevaid andmete taastamise agente, nagu OneDrive. Ettevõtted saavad luua oma kohandatud pildi, et lisada ettevõtte sätteid, rakendused, draiverid ja andmete taastamise agendid.

Operatsioonisüsteemi (OS) taastamise agent teostab taaste-pildi installimiseks vajalikud sammud. HP poolt pakutav taastamise agent teostab ühised samme, nagu sektsioonimine, vormindamine ja taaste-pildi ekstraktimine sihtmärgiks olevasse seadmesse. Kuna HP taastamise agent asub saidil hp.com, on vaja Interneti-ühendust, et seda hankida, kui süsteem ei sisalda sisseehitatud taaskujutamist. Ettevõtted võivad majutada ka HP taastamise agentide oma tulemüüris või luua keerulisemates taastamise keskkondades kohandatud taastamise agendid.

Kui operatsioonisüsteemi ei leita, saate käivitada HP Sure Recover. Saate käivitada ka HP Sure Recover ajastatuna, näiteks tagamaks, et pahavara eemaldatakse. Nende sätete konfigureerimiseks kasutage HP Client Security Manageri (CSM), Manageability Integration Kiti (MIK) või HP Client Management Scripti teeki.

## Võrgu taastamise teostamine



**MÄRKUS.** Võrgu taastamiseks peate kasutama juhtmega ühendust. HP soovib varundada olulised failid, andmed, fotod, videod jne, enne HP Sure Recover kasutamist, et vältida andmete kaotsiminekut.

1. Ühendage klientarvuti võrguga, kus on võimalik kasutada HTTP-või FTP-jaotuspunkti.
2. Taaskäivitage klientarvuti ja kui ilmub HP logo, vajutage klahvi **F11**.
3. Valige **Taasta võrgust**.

## Kohalike draivide taastamise teostamine

Kui klientarvuti toetab sisseehitatud taaspildindamist ja ajastatud pildi allalaadimise suvand on rakendatud poliitikas lubatud, laaditakse pilt määratud ajal klientarvutisse. Pärast seda, kui pilt laaditakse klientsüsteemi, taaskäivitage see, et kopeerida pilt sisseehitatud taaspildindamise mäluseadmesse.

Kohaliku taaste teostamiseks, kasutades sisseehitatud taaspildindamise mäluseadmes olevat pilti, toimige järgmiselt.

1. Taaskäivitage klientarvuti ja kui ilmub HP logo, vajutage klahvi **F11**.
2. Valige **Taasta kohalikust draivist**.

Sisseehitatud taaskujutamisega süsteemid peavad konfigureerima allalaadimise ajakava ja kasutama värskenduste otsimiseks allalaadimise agentide. Allalaadimise agent on lisatud HP Sure Recover HP Client Security Manageri pistikprogrammi ja seda saab konfigureerida ka MIK-is. Juhised MIK-i kasutamiseks leiate peatükist <https://www.hp.com/go/clientmanagement>.

Saate luua ka ajastatud toiming, et kopeerida agent SR\_AED sektsiooni ja pilt SR\_IMAGE sektsiooni. Seejärel saate kasutada HP Client Management Scripti teeki, et saata hooldussündmus, mis teavitaks BIOS-i, et see peaks sisu valideerima ja kopeerima sisseehitatud taaspildindamise mäluseadme järgmisel taaskäivitamisel.



## 2 Ettevõtte pildi loomine

Enamik ettevõtteid kasutab Microsoft Deployment Toolsi, Windows 10 Assessment and Deployment komplekti või mõlemaid, et luua faile, mis sisaldavad pilti Windows Imaging (WIM) failivormingu arhiivis.

### Nõuded

- Windows 10 Assessment and ja Deployment Kit (Windowsi ADK) uusim versioon
- PowerShell
- OpenSSL (või muu lahendus RSA era-/avaliku võtme paari loomiseks)

Kasutage selleks, et luua RSA võtme paar, mida kasutatakse loodava ja hostitava ettevõtte pildi terviklikkuse tagamiseks.

- Serveri hostingu lahendus (nt Microsoft Internet Information Services [IIS])

### Pildi loomine

Enne pildi loomise protsessi alustamist häälestage töösüsteem või ehitage süsteem, kuhu on paigaldatud vajalikud tööriistad, et valmistuda pildi töötlemiseks, nagu on näidatud järgmistes toimingutes.

1. Haldurina avage Deployment and Imaging Tools Environment käsuri (installitakse Windowsi ADK juurutamise tööriistadega).
2. Looge oma pildi jaoks lavastusala, kasutades järgmist käsku.

```
mkdir C:\staging
```

3. Looge pilt, kasutades üht järgmistest näidetest.

[Näide 1. Microsoft Windowsi installi pildil põhineva pildi loomine lk 3](#)

[Näide 2. Taustsüsteemi alusel pildi loomine lk 5](#)

#### Näide 1. Microsoft Windowsi installi pildil põhineva pildi loomine

1. Kinnitage või avage Microsoft Windowsi installi pilt (Microsoft ISO-ist või HP OSDVD-st).
2. Paigaldatud Windowsi installi pildist kopeerige fail install.wim oma lavastusalasse, kasutades järgmist käsku.

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



**MÄRKUS.** <M:> viitab paigaldatud draivile. Asendage õige draivitähga.

3. Nimetage install.wim ümber pildifailiks nimega (selles näites "my-image"), kasutades järgmist käsku.

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

(Valikuline) HP Sure Recover sisaldab funktsiooni, et taastada spetsiaalne väljaanne mitmest indeksiga pildist, mis põhineb tehases HP sihtsüsteemile algselt litsentseeritud Windowsi versioonil. See mehhanism töötab, kui indeksid on õigesti nimetud. Kui teie Windowsi paigaldusjuhend pärineb HP OSDVD pildist, on teil tõenäoliselt ka mitmeversiooniline pilt. Kui te ei soovi sellist käitumist ja soovite

tagada, et ühte kindlat versiooni kasutatakse kõigi teie sihtsüsteemide jaoks, siis peate olema kindel, et installipildil on ainult üks indeks.

#### 4. Kontrollige installipildi sisu järgmise käsu abil.

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

Järgnevalt on esitatud näidisväljund, mis toetab viit versiooni (sobitamiseks vastavalt iga sihtsüsteemi BIOS-iga).

Pildi üksikasjad: my-image.wim

Indeks: 1

Nimi: CoreSingleLanguage

Kirjeldus: Windows 10 May 2019 Update - Home Single Language Edition

Suurus: 19 512 500 682 baiti

Indeks: 2

Nimi: Core

Kirjeldus: Windows 10 May 2019 Update - Home edition

Suurus: 19 512 500 682 baiti

Indeks: 3

Nimi: Professional

Kirjeldus: Windows 10 May 2019 Update- Professional Update

Suurus: 19 758 019 520 baiti

Indeks: 4

Nimi: ProfessionalEducation

Kirjeldus: Windows 10 May 2019 Update - Professional Education edition

Suurus: 19 758 019 480 baiti

Indeks: 5

Nimi: ProfessionalWorkstation

Kirjeldus: Windows 10 May 2019 Update - Professional Workstation edition

Suurus: 19 758 023 576 baiti



**MÄRKUS.** Kui tegemist on ainult ühe indeksiga, kasutatakse pilti taastamiseks, sõltumata selle nimest. Pildifaili maht võib olla suurem kui enne kustutamist.

#### 5. Kui te ei soovi mitmeversioonilist käitumist, kustutage kõik indeksid, mida te ei soovi.

Nagu on näidatud järgmises näites, kui soovite ainult versiooni Professional (eeldades, et kõik sihtsüsteemid on litsentseeritud), kustutage indeks 5, 4, 2 ja 1. Iga kord, kui mõne indeksi kustutate, määratakse indeksi numbrid ümber. Seetõttu peaksite kustutama indeksinumbreid kõrgeimast

madalaimani. Jooksutage `Get-ImageInfo` pärast iga kustutamist, et visuaalselt kinnitada, millise indeksi te järgmisena kustutate.

```
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
```

Valige ainult üks versiooni indeks (näiteks Professional). Kui tegemist on ainult ühe indeksiga, kasutatakse pilti taastamiseks, sõltumata selle nimest. Pange tähele, et pildifaili maht võib olla suurem kui enne kustutamist, WIM metaandmete muudatuste ja sisu normaliseerimise toimimise tõttu.

## 6. (Valikuline) Kui soovite kaasata draiverid ettevõtte taaste-pilti, toimige järgmiselt.

### a. Paigaldage pilt tühja kausta, kasutades järgmisi käske.

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

### b. Paigaldage toetatud sihtsüsteemi jaoks sobiv HP Windows 10 Driver DVD (DRDVD). Kopeerige paigaldatud draiverimeediast draiverite alamkaustad oma lavastusalale, kasutades järgmist käsku.

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



**MÄRKUS.** <M:> viitab paigaldatud draivile. Asendage õige draivitähga.

Võite lisada täiendavad .inf-tüüpi draiverid, pannes need C:\staging\mount\SWSETUP\DRV kausta alla. Kui soovite selgitust selle kohta, kuidas HP Sure Recover seda sisu töötleb utiliidi `dism /Add-Driver /Recurse` funktsiooni abil, vaadake jaotist "Draiverite lisamine ja eemaldamine võrguühenduseta Windowsi pildile" järgmise teema all: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

See funktsioon ei toeta .exe-tüüpi draivereid, mis nõuavad rakenduse käivitamist.

### c. Salvestage muudatused ja eemaldage pilt, kasutades järgmist käsku.

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

Tulemuseks olev pildifail on järgmine: C:\staging\my-image.wim.

### d. Küllastage veebisaiti [Kujutise jagamine lk 6](#).

## Näide 2. Taustsüsteemi alusel pildi loomine

### 1. Looge buuditav USB WinPE andmekandja.



**MÄRKUS.** Pildi jäädvustamise täiendavad meetodid leiate ADK dokumentidest.

Veenduge, et USB-draivil on taustsüsteemist jäädvustatud pildi hoidmiseks piisavalt vaba ruumi.

### 2. Looge taustsüsteemis pilt.

### 3. Jäädvustage pilt, käivitades süsteemi USB WinPE andmekandjaga ja seejärel kasutage DISM-i.

---

 **MÄRKUS.** <U:> viitab USB-draivile. Asendage õige draivitähga.

Redigeerige faili nime "my-image" osa ja <my-image> kirjeldust vastavalt vajadusele.

---

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

4. Kopeerige pilt USB-lt oma töösüsteemis olevasse lavastusalasse, kasutades järgmist käsku.

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

Teil peaks olema järgmine pildifail: C:\staging\my-image.wim.


5. Külastage veebisaiti [Kujutise jagamine lk 6](#).


## Kujutise jagamine

HP soovib teil jagada pildi väiksemateks failideks, et parandada võrgus allalaaditavate failide usaldusväärsust, kasutades järgmist käsku.

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

---

 **MÄRKUS.** FileSize (faili suurus) on näidatud megabaitides. Redigeerige vastavalt vajadusele.

 **MÄRKUS.** DISM-i jagamisalgoritmi olemuse tõttu võivad genereeritud SWM-faili suurused olla kas väiksemad või suuremad kui märgitud faili suurus.

---

## Manifesti loomine

Vormindage MANIFEST-failid UTF-8-na ilma baidi järjestuse märgita (BOM).

Te saate muuta manifesti failinime (custom.mft), mida kasutatakse järgmistes toimingutes, kuid te ei tohi muuta laiendit .mft ja .sig ning manifesti ja signatuurfailide failinime osad peavad ühtima. Näiteks saate muuta paari (custom.mft, custom.sig) paariks (myimage.mft, myimage.sig).

mft\_version kasutatakse pildifaili vormingu tuvastamiseks ja selleks peab praegu olema määratud 1.

image\_version kasutatakse, et teha kindlaks, kas saadaval on pildi uuem versioon, ja takistada vanemate versioonide installimist.

Mõlemad väärtused peavad olema signatuurita 16-bitised täisarvud ja manifesti rea eraldajad peavad olema '\r\n' (CR + LF).

## Manifesti loomine

Kuna teie tükeldatud pildiga võib kaasneda mitu faili, kasutage manifesti loomiseks PowerShell'i skripti.

Kõigil ülejäänud etappidel peate olema kaustas C:\staging.

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

1. Looge PowerShell'i skript, kasutades redaktorit, mille abil saab toota tekstifaili formaadis UTF-8 ilma BOM-ita, kasutades järgmist käsku. notepad C:\staging\generate-manifest.ps1

Looge järgmine skript:

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

```
$imageVersion = 1907 (Märkus. See võib olla mis tahes 16-bitine täisarv)
```

```

$header = "mft_version=1, image_version=$imageVersion"
Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header

$swmFiles = Get-ChildItem "." -Filter "*.swm"

$ToNatural = { [regex]::Replace($_, '\d*\....$',
{ $args[0].Value.PadLeft(50) }) }

$spathToManifest = (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 = $hashObject.Path.Replace($spathToManifest + '\', '')
    $fileSize = (Get-Item $_.FullName).length
    $manifestContent = "$fileHash $filePath $fileSize"

    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
    $manifestContent -Append

    $current = $current + 1
}

```



**MÄRKUS.** HP Sure Recover manifestid ei tohi sisaldada BOM-i, seega järgmised käsud kirjutavad faili UTF8 ilma BOM-ita ümber.

```

$content = Get-Content $mftFilename

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

```

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

2. Salvestage skript.
3. Käivitage skript.

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

## Manifesti signatuuri loomine

Sure Recover valideerib agendi ja pildi krüptograafiliste signatuuride abil. Järgnevad näited kasutavad era-/avaliku võtmega paari X.509 PEM-formaadis (.PEM-laiend). Kohandage käske vastavalt vajadusele, et kasutada DER Binary Certificates (.CER- või .CRT-laiend), alus-64 kodeeritud PEM serte (.CER- või .CRT-laiendiga) või PKCS1 PEM faile (.PEM-laiend). Näites kasutatakse ka OpenSSL-i, mis genereerib signatuure big-endian-formaadis. Võite kasutada mis tahes utiliiti, et signatuurida manifestid, kuid mõned BIOS-i versioonid toetavad ainult signatuure little-endian-formaadis.

1. Genereerige 2048-bitine RSA privaativõti, kasutades järgmist käsku. Kui teil on 2048-bitine RSA privaatne/avalik võtmepaar PEM-formaadis, kopeerige need kausta C:\staging ja seejärel jätkake 3. sammust.  

```
openssl genrsa -out my-recovery-private.pem 2048
```
2. Looge privaativõti (kui teil on avalik võti, mis vastab teie isiklikule võtmele PEMformaadis, kopeerige see kausta C:\staging), kasutades järgmist käsku.  

```
openssl rsa -in my-recovery-private.pem -pubout -out my-recovery-public.pem
```
3. Saate luua signatuurfaili (kasutades sha256-põhiset räsi), mis põhineb teie 2048-bitisel RSA isiklikul võtmel sammust 1, kasutades järgmist käsku.  

```
openssl dgst -sha256 -sign my-recovery-private.pem -out custom.sig custom.mft
```
4. Kontrollige signatuurfaili, kasutades oma avalikku võtit eelmisest sammust, rakendades järgmist käsku.  

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



### MÄRKUS.

- Kui teil on vaja luua ainult signatuurfail, on vajalikud sammud 1 ja 3.
- HP Sure Recover puhul on minimaalsed nõutavad sammud 1, 2 ja 3. Teil on vaja avalikku võtit sammust 2, et pakkuda oma siht-süsteemi.
- Samm 4 on valikuline, kuid seda soovitatakse, et signatuur- ja manifestifail valideeriks õigesti.

## Failide hostimine

Hostige järgmised failid oma serveri kaustast C:\staging:

- \*.swm
- custom.mft (või faili nimi, mille valisite manifestifaili jaoks)
- custom.sig (või sobiva failinime, mille valisite signatuurifaili jaoks)



**MÄRKUS.** Kui kasutate IIS-i hostina, peate konfigureerima oma MIME-kirjed, et lisada järgmised laiendused, mis on kõik konfigureeritud kui "application/octet-stream:"

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

## Sihtsüsteemide ettevalmistamine

Te saate oma sihtsüsteeme ette valmistada, kasutades HP Client Management Scripti teeki, HP Client Manageri (CSM) / Sure Recover või Manageability Integration Kiti (MIK<https://www.hp.com/go/clientmanagement>) ().

Esitage selle ettevalmistamiseks järgmine teave.

1. Eelmises jaotises majutatud manifest-faili URL-aadress ([http://your\\_server.domain/path/custom.mft](http://your_server.domain/path/custom.mft))
2. Avalik võti, mida kasutatakse eelnevalt loodud signatuur failide kontrollimiseks (näiteks C:\staging\my-recovery-public.pem).

## Tõrkeotsing

Kui kuvatakse teade kohandatud taaste kohta, mis ei läbi turvalisuse valideerimist, kontrollige järgmist.


1. Manifest peab olema UTF-8 ilma BOM-ita.
2. Kontrollige failide räsi.
3. Veenduge, et süsteem oleks ette valmistatud avaliku võtmega, mis vastab manifesti signatuurimiseks kasutatavale isiklikule võtmele.
4. IIS-i serveri mime-tüübid peavad olema `application/octet-stream`.
5. Failiteed manifestis peavad sisaldama täielikku teed ülemise kataloogini, mis sisaldab pilti, nagu seda klientsüsteemist näha. See tee, kuhu failid salvestatakse levituspunktist, ei ole täielik tee.

### 3 HP Sure Recover agendi kasutamine ettevõtte tulemüüris


HP Sure Recover agendi saab majutada ettevõtte sisevõrgus. Kui olete HP Sure Recover SoftPaq-i installinud, kopeerige agendi failid HP Sure Recover agendi kataloogist installi asukohast HTTP või FTP levituse punkti. Seejärel varustage klientsüsteemi levituse punkti URL-i ja HP avaliku võtmega nimega `hpsr_agent_public_key.pem`, mis on jaotatud HP Sure Recover agendiga SoftPaq.

#### HP Sure Recover agendi paigaldamine


1. Laadige alla HP Sure Recover agent ja ekstraktige failid oma HTTP- või FTP-levituse punkti.
2. Määrake levituse punktis sobivad failide õigused.
3. Kui kasutate Internet Information Services (IIS), looge application/octet-stream MIME-tüübid järgmiste failivormingute jaoks.
  - .
  - .wim
  - .swm
  - .mft
  - .sig
  - .efi
  - .sdi

 **NB!** Järgnevad sammud kirjeldavad Sure Recoveri ettevalmistust SCCM-iga. Lisateavet selle kohta, kuidas HP Client Management Scripti teegist ette valmistada, leiate jaotisest [Töö HP Client Management Scripti Libraryga \(CMLS\) lk 12](#).


4. Käivitage SCCM, liikuge rakendusse **HP Client Security Suite** ja seejärel valige HP Sure Recover Page.

 **MÄRKUS.** Levituse punkti URL sisaldab kas ftp-d või http-d transpordi protokollina. See sisaldab ka täielikku teed kõige pealmise kataloogini, mis sisaldab HP sure Recover agendi, nagu on näha klientarvutis. See tee, kuhu failid salvestatakse levituspunktist, ei ole täielik tee.

5. Valige jaotisest **Platform Image** suvand **Corporation**, et taastada kohandatud operatsioonisüsteemi pilt ettevõtte levituse punktist. Sisestage IT-halduri antud URL **pildi asukoha URL-i** sisestamise kasti. Sisestage avalik võti väljale `hpsr_agent_public_key.pem`.

 **MÄRKUS.** Kohandatud pildi URL peab sisaldama pildi manifesti failinime.

6. Valige jaotises **Recovery agent** suvand **Corporation**, et kasutada kohandatud taasteagenti või HP taasteagenti ettevõtte levituse punktist. Sisestage IT-halduri antud URL sisestuskasti **Agent Location URL-i**. Sisestage avalik võti `hpsr_agent_public_key.pem` sisestusväljale **Agent Verification Key**.

 **MÄRKUS.** Ärge lisage URL-i aadressile agendi manifesti failinime, kuna BIOS nõuab selle nimeks `recovery.mft`.



7. Pärast poliitika rakendamist klientsüsteemis taaskäivitage see.
8. Algse ettevalmistamise käigus ilmub teade, mis palub sisestada 4-kohaline turvakood, et lõpetada HP Sure Recover aktiveerimine. Lisateavet leiate aadressilt [hp.com](http://hp.com) ja otsige HP Manageability Integration Kiti (MIK) Microsoft System Center Manager valges raamatus.

Kui HP Sure Recover aktiveerimine lõpule jõuab, siis poliitikas sisalduv kohandatud URL kuvatakse pärast seda HP Sure Recover BIOS-i sätete menüüs.

Aktiveerimise õnnestumise kinnitamiseks taaskäivitage arvuti ja kui ilmub HP logo, vajutage klahvi **F10**. Valige **Advanced**, valige **HP Sure Recover**, valige **Recovery agent** ja seejärel valige **URL**.

## 4 Töö HP Client Management Scripti Libraryga (CMSL)

Tarkvara HP Client Management Script Library abil saate hallata HP Sure Recover PowerShelli abil. Järgmises näites olev skript näitab, kuidas HP Sure Recover ette valmistada, määrata olekut, muuta konfiguratsiooni ja ettevalmistamine tühistada.



**MÄRKUS.** Mitu käsku ületavad selle juhendi rea pikkust, kuid tuleb sisestada ühe reana.

```
$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

$sp = New-HPSureRecoverDeprovisionPayload `
    -SigningKeyPassword $skpw `
    -SigningKeyFile "$path\sk.pfx"
$sp | Set-HPSecurePlatformPayload

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

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

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

```

## Näidisvõti OpenSSL-i kasutades

Hoidke privaatsaid võtmeid turvalises kohas. Avalikke võtmeid kasutatakse valideerimiseks ja need peavad olema antud ettevalmistamise ajal. Need võtmed peavad olema 2048 bitti pikad ja kasutama astendajat 0x10001. Vahetage teema näidetes välja teabega oma organisatsiooni kohta.

Seadke enne jätkamist järgmine keskkonnamuutuja.

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

```
# Looge isesigneeritud juur CA setifikaat testimiseks
```

```
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"
```

```
# Looge võtme kinnituse sertifikaat
```

```
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 ja AES Cryptographic Provider" -passout pass:
```

```
# Looge käskluse signeerimise klahv
```

```
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 ja AES Cryptographic Provider" -passout pass:
```

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

```
# Loo pildi signeerimise klahv
```

```
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 ja AES Cryptographic Provider" -passout pass:
```

**Saate selle käsuga pildi manifesti signeerida.**

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

```
# Looge agendi signatuuri võti
```

```
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 ja AES Cryptographic Provider" -passout pass:
```

**Võite selle käsuga agendi manifesti signeerida.**

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

OpenSSL loob signatuuri failid suur-endian vormingus, mis ei ühildu mõne BIOS-i versiooniga, nii et agendi signatuurfailide baitide järjestus võib olla vajalik enne rakendamist tagasi pöörata. BIOS-i versioonid, mis toetavad suur-endian baitide järjestust, toetavad ka endian baitide järjestust.

# A Tõrkeotsing

## Draivi sektsioonimine nurjus

Nurjunud draivi sektsioonimine võib ilmneda juhul, kui SR\_AED või SR\_IMAGE sektsioonimine on krüptitud BitLockeriga. Need sektsioonid on tavaliselt loodud gpt-atribuudiga, mis takistab BitLockeril nende krüptimist, aga kui kasutaja kustutab ja taasloob sektsioonid või loob need käsitsi tühjale metallist draivile, ei saa Sure Recover agent neid kustutada ja väljub draivi ümbersektsioonimisel tõrkega. Kasutaja peab need käsitsi kustutama, käivitades utiliidi Diskpart, valides mahu ja väljastades alistamise käsu `del vol` või muu sarnane.

## Püsivara auditi logi

EFI-muutuja teave on järgmine:

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

API-d on Windowsi jaotises EFI-muutujate lugemiseks olemas või saate kasutada muutuja sisu faili UEFI Shell dmpstore utiliidi abil.

Auditlogi abil saate kasutada HP Client Management Scripti Librarys esitatud käsu `Get-HPFirmwareAuditLog` abil.

## Windowsi sündmustelogi

Veenduge, et Sure Recoveri start- ja stopp-sündmused saadetakse BIOS-i auditilogisse, mida saate vaadata Windows Event Vieweris, kui HP Notifications on installitud. Nende sündmuste hulka kuuluvad kuupäev ja kellaaeg, allika ID, sündmuse ID ja sündmuse konkreetne kood. Näiteks [fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3] viitab, et taastamine nurjus, kuna manifesti ei saanud autentida koos sündmuse konkreetse koodiga c3f 23000, mis oli sisse logitud kell 2:26:40 kuupäeval 6/27/18.



**MÄRKUS.** Need logid järgivad USA kuupäeva formaati kuu/kuupäev/aasta.

## HP Secure Platform Management (Source ID = 84h)

Tabel A-1 HP Secure Platform Management

Sündmuse ID	Seadmete arv (kõik/DaaS)	Sündmuste arv (kõik/DaaS)	Kirjeldus	Märkused
40	256/178	943/552	Platvormi OS-i taastamise protsessi alustas püsivara.	Platvormi taaste käivitus
41	221/147	588/332	Platvormi OS-i taastamise protsess on edukalt lõpule viidud.	Platvormi taaste on lõpule viidud
42	54/42	252/156	Platvormi OS-i taastamise protsessi ei õnnestunud lõpule viia.	Platvormi taaste ebaõnnestus

Saate hankida püsivara auditilogi, kasutades HP Client Management Scripti Librarys olevat Get-HPFirmwareAuditLog, mis on saadaval aadressil <http://www.hp.com/go/clientmanagement>. HP Secure Platform Managementi sündmuse ID-d 40, 41 ja 42 tagastussündmuse spetsiifilised koodid andmeväljal, mis näitavad Sure Recoveri tulemust. Näiteks järgmine logikirje näitab, et Sure Recover ei suutnud laadida alla manifesti või signatuurfaili tõrkega event\_id 42 ja andmetega: 00:30:f1:c3, mida tuleb tõlgendada kui DWORD-väärtus 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0
severity: Teave
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: Platvormi OS-i taastamise protsessi ei õnnestunud lõpule viia.
data: 00:30:f1:c3
```

Edukas taaste on näidatud kui event\_id = 41 ja andmed: 00:00:00:00, näiteks:

```
sündmusespetsiifilised koodid
Success = 0x00000000
CatalogDownloadFailed = 0xC3F11000
message_number: 0
severity: Teave
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: Platvormi OS-i taastamise protsessi ei õnnestunud lõpule viia.
data: 00:00:00:00
```

HP Sure Recover kasutab järgmisi sündmusespetsiifilisi koode.

**Tabel A-2 sündmusespetsiifilised koodid**

Sündmuse kirjeldus	Sündmuse kood
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000

**Tabel A-2 sündmusespetsiifilised koodid (järg)**

Sündmuse kirjeldus	Sündmuse kood
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