# Vodič za korisnike

## HP Sure Recover

Prvo izdanje: februar 2020.

Broj dela dokumenta: L93434-E31

# Sintaksni ključ za unos korisnika

Tekst koji morate da unesete u korisnički interfejs označen je `fontom fiksne širine`.

**Tabela -1 Sintaksni ključ za unos korisnika**

| Stavka | Opis |
|---|---|
| `Tekst bez zagrade ili vitičaste zagrade` | Stavke morate da otkucate baš onako kao što je prikazano |
| `<tekst unutar ugaone zagrade>` | Čuvar mesta za vrednost koju morate da navedete; izostavite zagrade |
| `[tekst unutar velike zagrade]` | Opcionalne stavke; izostavite zagrade |
| `{tekst unutar vitičaste zagrade}` | Skup stavki od kojih morate odabrati samo jednu; izostavite vitičastu zagradu |
| `\|` | Znak za razdvajanje za stavke od kojih morate odabrati samo jednu; izostavite vertikalnu traku |
| `. . .` | Stavke koje mogu ili moraju da se ponavljaju; izostavite tri tačke |

# Sadržaj

# 1 Prvi koraci

HP Sure Recover vam pomaže da bezbedno instalirate operativni sistem sa mreže uz minimalnu interakciju korisnika. Sistemi koji imaju HP Sure Recover with Embedded Reimaging takođe podržavaju instalaciju sa lokalnog uređaja za skladištenje.

**VAŽNO:** Napravite rezervnu kopiju podataka pre korišćenja tehnologije HP Sure Recover. Pošto proces obrade slika ponovo formatira disk jedinicu, može doći do gubitka podataka.

Slike za oporavak koje HP obezbeđuje obuhvataju osnovni Windows 10® instalacioni program. HP Sure Recover opcionalno može da instalira optimizovane upravljačke programe za HP uređaje. HP slike za oporavak obuhvataju samo agente za oporavak podataka koji su uključeni uz Windows 10, kao što je OneDrive. Korporacije mogu da kreiraju sopstvene slike da bi dodali korporativne postavke, aplikacije, upravljačke programe i agente za oporavak podataka.

Agent za oporavak operativnog sistema (OS) izvršava neophodne korake za instalaciju slike za oporavak. Agent za oporavak koji obezbeđuje HP izvršava uobičajene korake kao što su particionisanje, formatiranje i izdvajanje slike za oporavak na ciljnom uređaju. Pošto se HP agent za oporavak nalazi na sajtu hp.com, potreban vam je pristup internetu da biste ga preuzeli, osim ako sistem ne obuhvata Embedded Reimaging. Korporacije takođe mogu da hostuju HP agent za oporavak u okviru svog zaštitnog zida ili da kreiraju prilagođene agente za oporavak za složenija okruženja za oporavak.

Možete da pokrenete HP Sure Recover kada se ne pronađe nijedan operativni sistem. HP Sure Recover možete da pokrenete i prema planu, na primer, da biste se uverili da je malver uklonjen. Konfigurišite te postavke putem programa HP Client Security Manager (CSM), Manageability Integration Kit (MIK) ili HP Client Management Script Library.

## Izvršavanje oporavka mreže

**NAPOMENA:** Da biste izvršili oporavak mreže, morate da koristite žičnu vezu. HP preporučuje da napravite rezervnu kopiju važnih datoteka, podataka, fotografija, video zapisa itd. pre korišćenja tehnologije HP Sure Recover kako biste izbegli gubitak podataka.

1. Povežite klijentski sistem sa mrežom na kojoj se može pristupiti HTTP ili FTP tački distribucije.
2. Ponovo pokrenite klijentski sistem i kada se pojavi HP logotip, pritisnite f11.
3. Izaberite stavku **Vrati u prethodno stanje sa mreže**.

## Izvršavanje oporavka lokalne disk jedinice

Ako klijentski sistem podržava Embedded Reimaging i ako je opcija planiranog preuzimanja slike omogućena u primenjenim smernicama, slika će u planirano vreme biti preuzeta u klijentski sistem. Kada se slika preuzme u klijentski sistem, ponovo ga pokrenite da biste kopirali sliku na Embedded Reimaging uređaj za skladištenje.

Da biste izvršili lokalni oporavak pomoću slike na Embedded Reimaging uređaju za skladištenje:

1. Ponovo pokrenite klijentski sistem i kada se pojavi HP logotip, pritisnite f11.
2. Izaberite stavku **Vrati u prethodno stanje sa lokalne disk jedinice**.

Sistemi koji imaju Embedded Reimaging moraju da konfigurišu plan preuzimanja i koriste agent za preuzimanje da bi proverili da li postoje ispravke. Agent za preuzimanje je uključen u dodatnu komponentu HP

Sure Recover za HP Client Security Manager, a može se i konfigurisati u MIK-u. Pogledajte https://www.hp.com/go/clientmanagement za uputstva za korišćenje MIK-a.

Takođe možete da kreirate planirani zadatak za kopiranje agenta na SR_AED particiju i kopiranje slike na SR_IMAGE particiju. Zatim možete da koristite HP Client Management Script Library da biste poslali događaj usluge koji obaveštava BIOS da treba da proveri valjanost sadržaja i izvrši kopiranje na Embedded Reimaging uređaj za skladištenje pri sledećem ponovnom pokretanju sistema.

# 2 Kreiranje korporativne slike

Većina preduzeća koristi Microsoft alatke za primenu, Windows 10 komplet za procenu i primenu ili oba da bi proizvele datoteke koje sadrže sliku u okviru Windows Imaging (WIM) arhive formata datoteka.

## Zahtevi

- Najnovija verzija Windows 10 kompleta za procenu i primenu (Windows ADK)
- PowerShell
- OpenSSL (ili drugo rešenje za generisanje RSA para privatnog/javnog ključa)

  Koristite za generisanje RSA para ključeva koji se koristi za zaštitu integriteta korporativne slike koju kreirate i hostujete.
- Server koji hostuje rešenje (na primer, Microsoft Internet Information Services [IIS])

## Kreiranje slike

Pre nego što započnete proces kreiranja slike, podesite radni sistem ili sistem za izgradnju na kom ste instalirali potrebne alatke za pripremanje za obradu slike, kao što je prikazano u sledećim koracima:

1. Kao administrator, otvorite `Deployment and Imaging Tools Environment` komandnu liniju (instalira se uz alatke za primenu kompleta Windows ADK).
2. Kreirajte oblast za pripremanje slike pomoću sledeće komande:

   ```
   mkdir C:\staging
   ```
3. Kreirajte sliku pomoću nekog od sledećih primera:

   Primer 1: Kreiranje slike na osnovu Microsoft Windows slike instalacije na stranici 3

   Primer 2: Kreiranje slike na osnovu referentnog sistema na stranici 5

### Primer 1: Kreiranje slike na osnovu Microsoft Windows slike instalacije

1. Postavite ili otvorite Microsoft Windows sliku instalacije (iz Microsoft ISO ili HP OSDVD slike).
2. Iz postavljene Windows slike instalacije kopirajte datoteku install.wim u oblast za pripremanje pomoću sledeće komande:

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

   **NAPOMENA:** `<M:>` se odnosi na postavljenu disk jedinicu. Zamenite to odgovarajućim slovom disk jedinice.
3. Preimenujte install.wim u ime datoteke slike („my-image“ u ovom primeru) pomoću sledeće komande:

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

   (Opcionalno) HP Sure Recover obuhvata funkciju za oporavak određenog izdanja iz slike sa više indeksa, na osnovu Windows izdanja koje je prvobitno licencirano za HP ciljni sistem u fabrici. Ovaj mehanizam funkcioniše ako su indeksi ispravno imenovani. Ako vaša Windows slika instalacije potiče iz HP OSDVD slike, verovatno imate sliku sa više izdanja. Ako ne želite ovo ponašanje i ne želite da budete sigurni da

će se koristiti jedno konkretno izdanje za sve ciljne sisteme, treba da se uverite da se u slici instalacije nalazi samo jedan indeks.

4. Proverite sadržaj slike instalacije pomoću sledeće komande:

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

Sledi prikaz uzorka izlaza iz slike instalacije koja podržava pet izdanja (koja treba podudariti na osnovu BIOS-a svakog ciljnog sistema):

Detalji za sliku: `my-image.wim`

Indeks: `1`

Ime: `CoreSingleLanguage`

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

Veličina: `19.512.500.682 bajta`

Indeks: `2`

Ime: `Core`

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

Veličina: `19.512.500.682 bajta`

Indeks: `3`

Ime: `Professional`

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

Veličina: `19.758.019.520 bajtova`

Indeks: `4`

Ime: `ProfessionalEducation`

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

Veličina: `19.758.019.480 bajta`

Indeks: `5`

Ime: `ProfessionalWorkstation`

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

Veličina: `19.758.023.576 bajta`

**NAPOMENA:** Kada postoji samo jedan indeks, slika se koristi za oporavak bez obzira na ime. Veličina datoteke slike može biti veća nego pre brisanja.

5. Ako ne želite ponašanje sa više izdanja, izbrišite svaki neželjeni indeks.

Kao što je prikazano u sledećem primeru, ako želite samo Professional edition (pod uslovom da su svi ciljni sistemi licencirani), izbrišite indeks 5, 4, 2 i 1. Svaki put kada izbrišete indeks, brojevi indeksa se

ponovo dodeljuju. Zato treba da ih brišete od najvišeg do najnižeg broja indeksa. Pokrenite `Get-ImageInfo` nakon svakog brisanja da biste potvrdili koji indeks ćete sledeći izbrisati.

```
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
```

Odaberite samo jedan indeks izdanja (u ovom primeru, Professional). Kada postoji samo jedan indeks, slika se koristi za oporavak bez obzira na ime. Imajte u vidu da veličina datoteke slike može biti veća nego pre brisanja zbog načina na koji funkcionišu izmene WIM metapodataka i normalizacija sadržaja.

6. (Opcionalno) Pratite ove korake ako želite da uključite upravljačke programe u korporativnu sliku za oporavak:

   **a.** Postavite sliku u praznu fasciklu pomoću sledećih komandi:

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

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

   **b.** Postavite odgovarajući HP DVD sa Windows 10 upravljačkim programima (DRDVD) za podržani ciljni sistem. Sa postavljenog medijuma sa upravljačkim programima, kopirajte potfascikle sa upravljačkim programima u oblast za pripremanje pomoću sledeće komande:

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

   **NAPOMENA:** `<M:>` se odnosi na postavljenu disk jedinicu. Zamenite to odgovarajućim slovom disk jedinice.

   Možete da uključite dodatne .inf upravljačke programe tako što ćete ih postaviti u okviru fascikle C:\staging\mount\SWSETUP\DRV. Objašnjenje načina na koji HP Sure Recover obrađuje ovaj sadržaj pomoću funkcije `dism /Add-Driver /Recurse` potražite u članku „Dodavanje i uklanjanje upravljačkih programa u vanmrežnoj Windows slici“ u okviru sledeće teme: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ova funkcija ne podržava .exe upravljačke programe koji zahtevaju pokretanje aplikacije.

   **c.** Sačuvajte promene i uklonite sliku pomoću sledeće komande:

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

   Dobijena datoteka slike je: C:\staging\my-image.wim.

   **d.** Posetite Razdeljivanje slike na stranici 6.

## Primer 2: Kreiranje slike na osnovu referentnog sistema

1. Kreirajte USB WinPE medijum sa kog može da se pokrene sistem.

   **NAPOMENA:** Dodatni metodi za hvatanje slike mogu se pronaći u ADK dokumentaciji.

   Uverite se da na USB disku ima dovoljno slobodnog prostora za uhvaćenu sliku iz referentnog sistema.

2. Kreirajte sliku na referentnom sistemu.

3. Uhvatite sliku tako što ćete pokrenuti referentni sistem pomoću USB WinPE medijuma, a zatim koristiti DISM.

**NAPOMENA:** `<U:>` se odnosi na USB disk. Zamenite to odgovarajućim slovom disk jedinice.

Uredite deo imena datoteke „my-image“ i opis `<my-image>` po potrebi.

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

4. Kopirajte sliku sa USB-a u oblast za pripremanje na radnom sistemu pomoću sledeće komande:

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

   Trebalo bi da imate sledeću datoteku slike: C:\staging\my-image.wim.

5. Posetite Razdeljivanje slike na stranici 6.

# Razdeljivanje slike

HP preporučuje da razdelite sliku na manje datoteke da biste poboljšali pouzdanost preuzimanja sa mreže pomoću sledeće komande:

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

**NAPOMENA:** FileSize se prikazuje u megabajtima. Uredite po potrebi.

**NAPOMENA:** Zbog prirode DISM algoritma za razdeljivanje, veličine generisanih SWM datoteka mogu biti manje ili veće od navedene veličine datoteke.

# Kreiranje manifesta

Formatirajte datoteke manifesta kao UTF-8 bez oznake za raspored bajtova (BOM).

Možete da promenite ime datoteke manifesta (custom.mft) koje se koristi u sledećim procedurama, ali ne smete da promenite oznake tipa datoteke .mft i .sig, a deo manifesta koji sadrži ime datoteke i datoteke potpisa se moraju podudarati. Na primer, možete da promenite par (custom.mft, custom.sig) u (myimage.mft, myimage.sig).

`mft_version` se koristi za utvrđivanje formata datoteke slike i trenutno mora da bude postavljen na 1.

`image_version` se koristi da bi se utvrdilo da li je dostupna novija verzija slike i da bi se sprečila instalacija starijih verzija.

Obe vrednosti moraju da budu nepotpisani 16-bitni celi brojevi, a razdelnik redova u manifestu mora da bude „`\r\n`“ (CR + LF).

## Generisanje manifesta

Pošto nekoliko datoteka može biti uključeno uz razdeljenu sliku, koristite PowerShell skriptu za generisanje manifesta.

U svim preostalim koracima morate da se nalazite u fascikli C:\staging.

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

1. Kreirajte PowerShell skriptu pomoću uređivača koji može da proizvede tekstualnu datoteku u formatu UTF-8 bez BOM-a, pomoću sledeće komande: `notepad C:\staging\generate-manifest.ps1`

   Kreirajte sledeću skriptu:

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

```
$imageVersion = 1907 (Napomena: Ovo može da bude bilo koji 16-bitni celi broj)

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

**NAPOMENA:** Manifesti za HP Sure Recover ne mogu da obuhvataju BOM, pa sledeće komande ponovo upisuju datoteku kao UTF8 bez BOM-a.

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
```

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

2. Sačuvajte skriptu.
3. Izvršite skriptu.

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

## Generisanje potpisa manifesta

Sure Recover proverava valjanost agenta i slike pomoću šifrovanih potpisa. Sledeći primeri koriste par privatnog/javnog ključa u X.509 PEM formatu (oznaka tipa datoteke .PEM). Prilagodite komande na odgovarajući način za korišćenje DER binarnih certifikata (oznaka tipa datoteke .CER ili .CRT), BASE-64 kodiranih PEM certifikata (oznaka tipa datoteke .CER ili .CRT) ili PKCS1 PEM datoteka (oznaka tipa datoteke .PEM). Primer takođe koristi OpenSSL, koji generiše potpise u big-endian formatu. Za potpisivanje manifesta možete da koristite bilo koji uslužni program, ali neke verzije BIOS-a podržavaju samo potpise u little-endian formatu.

1. Generišite 2048-bitni RSA privatni ključ pomoću sledeće komande. Ako imate 2048-bitni RSA par privatnog/javnog ključa u pem formatu, kopirajte ih u C:\staging, a zatim pređite na 3. korak.

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

2. Generišite javni ključ od privatnog ključa (ako imate javni ključ koji odgovara privatnom ključu u PEM formatu, kopirajte ga u C:\staging) pomoću sledeće komande:

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

3. Kreirajte datoteku potpisa (koristeći sha256 heš) na osnovu 2048-bitnog RSA privatnog ključa iz 1. koraka, pomoću sledeće komande:

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

4. Verifikujte datoteku potpisa koristeći javni ključ iz prethodnog koraka pomoću sledeće komande:

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

**NAPOMENA:**

- Ako treba da kreirate samo datoteku potpisa, potrebni koraci su 1 i 3.
- Za HP Sure Recover, minimalni potrebni koraci su 1, 2 i 3. Potreban vam je javni ključ iz 2. koraka da biste obezbedili ciljni sistem.
- 4. korak je opcionalan, ali se preporučuje kako bi se ispravno proverila valjanost datoteke potpisa i datoteke manifesta.

# Hostovanje datoteka

Hostujte sledeće datoteke na serveru iz fascikle C:\staging:

- *.swm
- custom.mft (ili ime datoteke koje ste odabrali za datoteku manifesta)
- custom.sig (ili ime datoteke koje se podudara i koje ste odabrali za datoteku potpisa)

**NAPOMENA:** Ako koristite IIS kao rešenje za hostovanje, morate da konfigurišete MIME stavke tako da uključuju sledeće oznake tipa datoteke, sve konfigurisane kao „application/octet-stream:“

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

# Obezbeđivanje ciljnih sistema

Ciljne sisteme možete da obezbedite koristeći HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover ili Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Unesite sledeće informacije za ovo obezbeđivanje:

1. URL adresu datoteke manifesta hostovane u prethodnom odeljku (http://your_server.domain/path/custom.mft)
2. Javni ključ korišćen za verifikaciju datoteke potpisa koja je prethodno kreirana (na primer, C:\staging\my-recovery-public.pem).

# Rešavanje problema

Ako dobijete poruku o tome da nije uspela bezbednosna provera valjanosti prilagođenog procesa oporavka, proverite sledeće:

1. Manifest mora da bude u formatu UTF-8 bez BOM-a.
2. Proverite heševe datoteka.
3. Uverite se da je sistem obezbeđen sa javnim ključem koji odgovara privatnom ključu korišćenom za potpisivanje manifesta.
4. Mime tipovi IIS servera moraju da budu `application/octet-stream`.
5. Putanje datoteka u okviru manifesta moraju da obuhvataju punu putanju do najvišeg direktorijuma koji sadrži sliku, onako kako se vidi iz klijentskog sistema. Ova putanja ne predstavlja punu putanju na kojoj se čuvaju datoteke na tački distribucije.

# 3 Korišćenje HP Sure Recover agenta u okviru korporativnog zaštitnog zida

HP Sure Recover agent može da se hostuje na korporativnom intranetu. Kada instalirate HP Sure Recover SoftPaq, kopirajte datoteke agenta iz direktorijuma HP Sure Recover agenta sa lokacije instalacije na HTTP ili FTP tačku distribucije. Zatim obezbedite klijentski sistem pomoću URL adrese tačke distribucije i HP javnog ključa pod imenom `hpsr_agent_public_key.pem`, koji se distribuira uz SoftPaq HP Sure Recover agenta.

## Instaliranje HP Sure Recover agenta

1. Preuzmite HP Sure Recover agent i izdvojite datoteke na HTTP ili FTP tački distribucije.
2. Postavite odgovarajuće dozvole za datoteku na tačku distribucije.
3. Ako koristite Internet Information Services (IIS), kreirajte application/octet-stream MIME tipove za sledeće formate datoteka:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   **VAŽNO:** Sledeći koraci opisuju obezbeđivanje tehnologije Sure Recover uz SCCM. Za primere načina na koji se obezbeđuje Sure Recover uz HP Client Management Script Library, pogledajte Rad sa programom HP Client Management Script Library (CMSL) na stranici 12.

4. Pokrenite SCCM, idite u **HP Client Security Suite**, a zatim izaberite stranicu HP Sure Recover.

   **NAPOMENA:** URL adresa tačke distribucije obuhvata ftp ili http kao protokol prenosa. Ona takođe obuhvata punu putanju do najvišeg direktorijuma koji sadrži manifest za HP Sure Recover agent, onako kako se vidi iz klijentskog sistema. Ova putanja ne predstavlja punu putanju do mesta na kom se čuvaju datoteke na tački distribucije.

5. U odeljku **Slika platforme** izaberite opciju **Korporacija** da biste vratili prilagođenu sliku operativnog sistema sa korporativne tačke distribucije. Unesite URL adresu koju je obezbedio IT administrator u polje za unos **URL adresa lokacije slike**. Unesite javni ključ `hpsr_agent_public_key.pem` u polje **Verifikacija slike**.

   **NAPOMENA:** Prilagođena URL adresa slike mora da sadrži ime datoteke manifesta slike.

6. U odeljku **Agent za oporavak** izaberite opciju **Korporacija** da biste koristili prilagođeni agent za oporavak ili HP agent za oporavak sa korporativne tačke distribucije. Unesite URL adresu koju je

obezbedio IT administrator u polje za unos **URL adresa lokacije agenta**. Unesite javni ključ `hpsr_agent_public_key.pem` u polje **Ključ za verifikaciju agenta**.

**NAPOMENA:** Nemojte unositi ime datoteke za manifest agenta u URL adresu zato što BIOS zahteva da se on zove recovery.mft.

7. Kada primenite smernice na klijentski sistem, ponovo ga pokrenite.
8. Tokom početnog obezbeđivanja, pojavljuje se odziv da unesete bezbednosni kôd od 4 cifre kako biste dovršili HP Sure Recover aktivaciju. Za više detalja idite na hp.com i pretražite belu knjigu „HP Manageability Integration Kit (MIK) za Microsoft System Center Manager“.

Kada se HP Sure Recover aktivacija uspešno dovrši, prilagođena URL adresa koju su primenile smernice prikazuje se u meniju sa HP Sure Recover BIOS postavkama.

Da biste potvrdili uspešnost aktivacije, ponovo pokrenite računar i kada se pojavi HP logotip, pritisnite f10. Izaberite stavke **Više opcija**, **HP Sure Recover**, **Agent za oporavak**, a zatim stavku **URL**.

# 4 Rad sa programom HP Client Management Script Library (CMSL)

HP Client Management Script Library vam omogućava da upravljate HP Sure Recover postavkama iz programa PowerShell. Sledeći primer skripte pokazuje kako se obezbeđuje HP Sure Recover, kako mu se utvrđuje status, menja konfiguracija i kako se on onemogućava.

**NAPOMENA:** Nekoliko komandi premašuje dužinu reda ovog vodiča, ali se moraju uneti u jednom redu.

```
$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
}
```

## Generisanje uzorka ključa pomoću OpenSSL-a

Uskladištite privatne ključeve na bezbednoj lokaciji. Javni ključevi će se koristiti za proveru valjanosti i moraju se navesti tokom obezbeđivanja. Ovi ključevi moraju da imaju dužinu od 2048 bitova i moraju da koriste eksponent od 0x10001. Zamenite temu u primerima informacijama o vašoj organizaciji.

Postavite sledeću promenljivu okruženja pre nego što nastavite:

```
set OPENSSL_CONF=<path>\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:
```

Manifest slike možete da potpišete pomoću ove komande:

```
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:
```

Manifest agenta možete da potpišete pomoću ove komande:

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

OpenSSL generiše datoteke potpisa u big-endian formatu, koji nije kompatibilan sa nekim BIOS verzijama, pa će raspored bajtova datoteke potpisa agenta možda morati da se obrne pre primene. BIOS verzije koje podržavaju big-endian raspored bajtova podržavaju i little-endian raspored bajtova.

# A Rešavanje problema

## Particionisanje disk jedinice nije uspelo

Do neuspešnog particionisanja disk jedinice može doći ako je SR_AED ili SR_IMAGE particija šifrovana koristeći Bitlocker. Ove particije se obično kreiraju pomoću gpt atributa koji sprečava Bitlocker da ih šifruje, ali ako korisnik izbriše i ponovo kreira particije ili ih kreira ručno na praznoj disk jedinici, Sure Recover agent neće moći da ih izbriše i zatvoriće se uz grešku prilikom ponovnog particionisanja disk jedinice. Korisnik mora ručno da ih izbriše tako što će pokrenuti diskpart, izabrati volumen i izvršiti komandu za zamenu `del vol` ili neku sličnu komandu.

## Evidencija nadzora firmvera

Ovo su informacije o EFI promenljivoj:

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

U okviru operativnog sistema Windows postoje API-ji za čitanje EFI promenljivih, a možete i da prikažete sadržaj promenljive u datoteci pomoću uslužnog programa UEFI Shell dmpstore.

Evidenciju nadzora možete da prikažete pomoću komande `Get-HPFirmwareAuditLog` koju obezbeđuje HP Client Management Script Library.

## Windows evidencija događaja

Sure Recover događaji pokretanja i zaustavljanja šalju se u BIOS evidenciju nadzora, koju možete da prikažete u Windows prikazivaču događaja u Sure Start evidenciji ako je instaliran program HP Notifications. Ovi događaji sadrže datum i vreme, ID izvora, ID događaja i kôd specifičan za događaj. Na primer, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` ukazuje na to da oporavak nije uspeo zato što nije bilo moguće potvrditi identitet manifesta pomoću koda specifičnog za događaj c3f 23000 koji je evidentiran u 2:26:40 dana 27.6.2018.

**NAPOMENA:** Ove evidencije koriste format datuma u SAD – mesec/dan/godina.

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

**Tabela A-1 HP Secure Platform Management**

| ID događaja | Broj uređaja (Svi/DaaS) | Broj događaja (Svi/DaaS) | Opis | Napomene |
|---|---|---|---|---|
| 40 | 256/178 | 943/552 | Firmver je započeo proces oporavka operativnog sistema platforme. | Oporavak platforme je započet |
| 41 | 221/147 | 588/332 | Proces oporavka operativnog sistema platforme je uspešno dovršen. | Oporavak platforme je dovršen |
| 42 | 54/42 | 252/156 | Proces oporavka operativnog sistema platforme nije uspešno dovršen. | Oporavak platforme nije uspeo |

Možete da preuzmete evidenciju nadzora firmvera koristeći Get-HPFirmwareAuditLog u programu HP Client Management Script Library, koji je dostupan na adresi http://www.hp.com/go/clientmanagement. HP Secure Platform Management ID-ovi događaja 40, 41 i 42 vraćaju kodove specifične za događaj u polju podataka, koji ukazuju na rezultat Sure Recover operacija. Na primer, sledeća stavka evidencije ukazuje na to da Sure Recover nije uspeo da preuzme datoteku manifesta ili potpisa uz grešku event_id 42 i podatke: 00:30:f1:c3, što treba tumačiti kao dword vrednost 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
```

Uspešan oporavak je prikazan kao event_id = 41 i podaci: 00:00:00:00, na primer:

```
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 koristi sledeće kodove specifične za događaj.

**Tabela A-2 Kodovi specifični za događaj**

| Opis događaja | Kôd događaja |
|---|---|
| CatalogDownloadFailed | 0xC3F11000 |
| SignatureDownloadFailed | 0xC3F12000 |
| MftOrSigDownloadFailed | 0xC3F13000 |

**Tabela A-2 Kodovi specifični za događaj (nastavljeno)**

| Opis događaja | Kôd događaja |
|---|---|
| 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 |