



# Felhasználói útmutató

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

A Microsoft és a Windows a Microsoft Corporation védjegye vagy bejegyzett védjegye az Amerikai Egyesült Államokban és/vagy más országokban.

Bizalmas számítógépes szoftver. A birtokláshoz, használatához vagy másoláshoz érvényes licenc szükséges a HP-től. Az amerikai szövetségi közbeszerzési törvény (FAR) 12.211. és 12.212. cikkelyének megfelelően a kereskedelmi célú szoftverek, a szoftverek dokumentációi, valamint a kereskedelmi célú árucikkkel kapcsolatos műszaki adatok vonatkozásában az Egyesült Államok kormányára a szállító szokásos kereskedelmi licence érvényes.

Az itt szereplő információ előzetes értesítés nélkül változhat. A HP termékeire és szolgáltatásaira vonatkozó kizárólagos jótállás az adott termékhez, illetve szolgáltatáshoz mellékelte, korlátozott jótállásról szóló nyilatkozatban vállalt jótállás. A dokumentumban ismertetettek nem jelentenek semmiféle további jótállást. A HP nem vállal felelősséget az itt található esetleges technikai vagy szerkesztési hibákért és mulasztásokért.

Első kiadás: 2020. február

A dokumentum cikkszám: L93434-211

## Magyarázat a felhasználó által beírandó szintaxishoz

A felhasználói felületen a felhasználó által beírandó szöveg rögzített szélességű betűkészlettel van jelölve.

### -1. táblázat: Magyarázat a felhasználó által beírandó szintaxishoz

Elem	Leírás
Szöveg zárójel vagy kapcsos zárójel nélkül	Pontosan a megadott módon beírandó elemek
<Csúcsos zárójelbe tett szöveg>	A felhasználó által megadandó érték helyőrzője; hagyja el a zárójelet
[Szögletes zárójelbe tett szöveg]	Nem kötelező elemek; hagyja el a zárójelet
{Kapcsos zárójelbe tett szöveg}	Olyan választható elemek, amelyek közül csak egyet választhat; hagyja el a zárójelet
	Elválasztó olyan elemek között, amelyek közül csak egyet választhat; hagyja el a függőleges vonalat
. . .	Elemek, amelyeket lehetséges vagy kötelező ismételni; hagyja el a három pontot



---

# Tartalomjegyzék

<b>1 Első lépések .....</b>	<b>1</b>
Hálózati helyreállítás végrehajtása .....	1
Helyreállítás helyi meghajtóról .....	1
<b>2 Vállalati lemezkép létrehozása .....</b>	<b>3</b>
Előfeltételek .....	3
A lemezkép létrehozása .....	3
1. példa: Lemezkép létrehozása a Microsoft Windows telepítési lemezképe alapján .....	3
2. példa: Lemezkép létrehozása referencia-rendszer alapján .....	5
A lemezkép felosztása .....	6
Jegyzékfájl létrehozása .....	6
Jegyzékfájl létrehozása .....	7
Jegyzékfájl-aláírás létrehozása .....	8
A fájlok tárolása .....	9
A célrendszerek üzembe helyezése .....	9
Hibaelhárítás .....	9
<b>3 A HP Sure Recover-ügynök használata vállalati tűzfalon belül .....</b>	<b>11</b>
A HP Sure Recover-ügynök telepítése .....	11
<b>4 A HP Client Management Script Library (CMSL) használata .....</b>	<b>13</b>
Példakulcs létrehozása az OpenSSL-lel .....	15
<b>A függelék: Hibaelhárítás .....</b>	<b>17</b>
A meghajtó particionálása nem sikerült .....	17
Firmware-naplófájl .....	17
Windows Eseménynapló .....	17
HP Secure Platform Management (forrásazonosító = 84h) .....	17



# 1 Első lépések

A HP Sure Recover segítségével biztonságosan, minimális felhasználói beavatkozással telepítheti az operációs rendszert a hálózatról. A HP Sure Recover with Embedded Reimaging megoldással rendelkező rendszerek helyi tárolóeszköztől is támogatják a telepítést.



**FONTOS:** A HP Sure Recover használata előtt készítsen biztonsági másolatot az adatokról. Mivel a lemezkép-telepítési folyamat újraformázza a meghajtót, adatvesztés fog következni.

A HP által biztosított helyreállítási lemezképek az alapszintű Windows 10®-telepítőprogramot tartalmazzák. A HP Sure Recoverrel azt is megteheti, hogy HP-eszközökhöz optimalizált illesztőprogramokat telepít. A HP helyreállítási lemezképek csak a Windows 10 részét képező adat-helyreállítási ügynököket tartalmazzák, például a OneDrive-ot. A vállalatok létrehozhatják saját egyéni lemezképeiket a vállalati beállítások, alkalmazások, illesztőprogramok és adat-helyreállítási ügynökök hozzáadásához.

A helyreállítási lemezkép telepítéséhez szükséges lépéseket egy operációsrendszer-helyreállítási ügynök hajtja végre. Ez a HP által biztosított ügynök általános lépéseket hajt végre: particionál, formáz, és kicsomagolja a helyreállítási lemezképet a céleszköze. Mivel a HP helyreállítási ügynöke a hp.com webhelyen található, internet-hozzáférésre is szüksége lesz, ha a rendszer nem tartalmaz beágyazott lemezkép-helyreállítást. A vállalatok a saját tűzfalukon belül is üzemeltethetik a HP helyreállítási ügynökét, de egyéni helyreállítási ügynököket is létrehozhatnak a bonyolultabb helyreállítási környezetekhez.

A HP Sure Recover akkor indítható el, ha nem található operációs rendszer. A HP Sure Recover ütemezés szerint is futtatható, például a kártevők eltávolítása érdekében. A kapcsolódó beállításokat a HP Client Security Manager (CSM), a Manageability Integration Kit (MIK) vagy a HP Client Management Script Library segítségével konfigurálhatja.

## Hálózati helyreállítás végrehajtása



**MEGJEGYZÉS:** A hálózati helyreállítást csak vezetékcsatlakozással lehet végrehajtani. A HP azt javasolja, hogy a HP Sure Recover használata előtt készítsen biztonsági másolatot a fontos fájlokról, adatokról, fényképekről, videókról stb., hogy elkerülje az adatvesztést.

1. Csatlakoztassa az ügyfélrendszert ahhoz a hálózathoz, amelyen a HTTP- vagy FTP-terjesztési pont elérhető.
2. Indítsa újra az ügyfélrendszert, és amikor megjelenik a HP embléma, nyomja le az **F11** billentyűt.
3. Válassza a **Restore from network** (Visszaállítás hálózatról) lehetőséget.

## Helyreállítás helyi meghajtóról

Ha az ügyfélrendszer támogatja a beágyazott lemezkép-helyreállítást, és az ütemezett lemezképletöltés engedélyezve lett a vonatkozó szabályzatban, akkor az ügyfélrendszer letölti a lemezképet az ütemezett időpontban. Miután a lemezkép letöltődött az ügyfélrendszerre, indítsa újra a rendszert, hogy átmásolja a lemezképet a beágyazott lemezkép-helyreállítási tárolóeszköze.

Helyi helyreállítás a beágyazott lemezkép-helyreállítási tárolóeszközön található lemezképpel:

1. Indítsa újra az ügyfélrendszert, és amikor megjelenik a HP embléma, nyomja le az **F11** billentyűt.
2. Válassza a **Restore from local drive** (Visszaállítás helyi meghajtóról) lehetőséget.

A beágyazott lemezkép-helyreállítással rendelkező rendszereken konfigurálni kell egy letöltési ütemezést, és a letöltési ügynökkel ellenőriztetni kell, hogy vannak-e elérhető frissítések. A letöltési ügynököt a HP Client Security Manager HP Sure Recover beépülő modulja tartalmazza, és az MIK készletben is konfigurálható. Az MIK használatával kapcsolatban itt talál útmutatást: <https://www.hp.com/go/clientmanagement>.

Ütemezett feladatot is létrehozhat, amellyel az SR\_AED partícióra másolhatja az ügynököt, az SR\_IMAGE partícióra pedig a lemezképet. Ezután a HP Client Management Script Library használatával elküldhet egy szolgáltatási eseményt, amely felszólítja a BIOS-t, hogy érvényesítse a tartalmakat, és másolja őket a beágyazott lemezkép-helyreállítási tárolóeszközre a következő újraindításkor.



## 2 Vállalati lemezkép létrehozása

A vállalatok többsége a Microsoft Deployment Toolst, a Windows 10 Assessment and Deployment Kitet vagy mindkettőt használja lemezképet tartalmazó, a Windows Imaging (WIM) fájlformátumú archívumban megtalálható fájlok létrehozásához.

### Előfeltételek

- A Windows 10 Assessment and Deployment Kit (Windows ADK) legújabb verziója
- PowerShell
- OpenSSL (vagy valamilyen más megoldás a személyes/nyilvános RSA-kulcspár létrehozásához)  
RSA-kulcspár létrehozására szolgál, amellyel a létrehozott és tárolt vállalati lemezkép védelméről lehet gondoskodni.
- Egy kiszolgálóüzemeltetési megoldás (például a Microsoft Internet Information Services, IIS)

### A lemezkép létrehozása

A lemezkép-létrehozási folyamat megkezdése előtt az alábbi lépéseket követve állítsa be azt a munkavégzési vagy összeállítási rendszert, amelyen a lemezkép feldolgozásához szükséges eszközöket telepítette:

1. Nyissa meg rendszergazdaként a Deployment and Imaging Tools Environment parancssorát (a környezet a Windows ADK üzembehelyezési eszközeivel települ).
2. Hozzon létre egy átmeneti területet a lemezkép számára az alábbi paranccsal:

```
mkdir C:\staging
```

3. Hozza létre a lemezképet az alábbi példák valamelyike alapján:

[1. példa: Lemezkép létrehozása a Microsoft Windows telepítési lemezképe alapján 3. oldal](#)

[2. példa: Lemezkép létrehozása referencia-rendszer alapján 5. oldal](#)

#### 1. példa: Lemezkép létrehozása a Microsoft Windows telepítési lemezképe alapján

1. Csatlakoztassa vagy nyissa meg a Microsoft Windows telepítési lemezképét (Microsoft ISO-fájlból vagy HP OSDVD-ről).
2. A csatlakoztatott Windows telepítési lemezképből másolja az install.wim fájlt az átmeneti területre az alábbi paranccsal:

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



**MEGJEGYZÉS:** Az <M:> a csatlakoztatott meghajtó. Cserélje le a megfelelő meghajtó betűjelére.

3. Nevezze át az install.wim fájlt arra a névre, amelynek a lemezképet hívni szeretné (ebben a példában „my-image”) az alábbi paranccsal:

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

(Választható) A HP Sure Recover tartalmaz egy olyan funkciót, amellyel helyre lehet állítani egy adott kiadást egy többindexes lemezképből a Windows azon kiadása alapján, amely eredetileg licencelve lett a HP-célrendszer számára a gyárban. Ez a mechanizmus csak akkor működik, ha az indexek megfelelően lettek elnevezve. Ha a Windows telepítési lemezkép HP OSDVD-lemezképből származik, akkor nagy a valószínűsége, hogy egy többkiadásos lemezképről van szó. Ha nem kívánja használni ezt a funkciót, és gondoskodni szeretne róla, hogy minden célrendszeren egy adott kiadás legyen használatban, meg kell arról győződnie, hogy csak egyetlen index van a telepítési lemezképben.

**4. Ellenőrizze a telepítési lemezkép tartalmát az alábbi paranccsal:**

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

Az alábbiakban egy olyan telepítési lemezkép példakimenete látható, amely öt kiadást támogat (amelyeket az egyes célrendszerek BIOS-a alapján kell egyeztetni):

Lemezkép részletei: `my-image.wim`

Index: 1

Név: `CoreSingleLanguage`

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

Méret: `19,512,500,682 bytes`

Index: 2

Név: `Core`

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

Méret: `19,512,500,682 bytes`

Index: 3

Név: `Professional`

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

Méret: `19.758,019,520 bytes`

Index: 4

Név: `ProfessionalEducation`

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

Méret: `19,758,019,480 bytes`

Index: 5

Név: `ProfessionalWorkstation`

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

Méret: `19,758,023,576 bytes`



**MEGJEGYZÉS:** Ha csak egy index van, a rendszer azt a lemezképet használja a helyreállításhoz a névre való tekintet nélkül. Előfordulhat, hogy a lemezképfájl mérete nagyobb lesz, mint a törlések előtt volt.

5. Ha nem szeretné használni a többkiadásos viselkedést, törölje a nem kívánt indexeket.

Ha csak a Professional kiadást szeretné használni (feltételezve, hogy a célrendszerek mindegyike rendelkezik licenccel), törölje az 5., 4., 2. és 1. indexet, ahogy az alábbi példában is látható. Minden egyes indextörléskor a rendszer ismételten kiosztja az indexszámokat. Ezért a törlést a legmagasabbtól a legalacsonyabb indexszám felé haladva hajtsa végre. Minden törlés után futtassa a `Get-ImageInfo` parancsot, és vizuálisan ellenőrizze, hogy melyik indexet fogja következésként törölni.

```
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
```

Csak a kívánt kiadás indexét válassza ki (ebben a példában ez a Professional). Ha csak egy index van, a rendszer azt a lemezképet használja a helyreállításhoz a névre való tekintet nélkül. Vegye figyelembe, hogy a lemezképfájl mérete esetenként nagyobb lehet, mint a törlések előtt volt, a WIM metaadat-módosításainak és tartalomnormalizálásának a működési módja miatt.

6. (Választható) Ha illesztőprogramokat is hozzá szeretne adni a vállalati helyreállítási lemezképhez, kövesse az alábbi lépéseket:

- a. Csatlakoztassa a lemezképet egy üres mappához az alábbi parancsokkal:

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

- b. Csatlakoztassa a támogatott célrendszer illesztőprogramokat tartalmazó, megfelelő HP Windows 10 Driver DVD-jét (DRDVD). Az illesztőprogramok csatlakoztatott adathordozójáról másolja az illesztőprogramokat tartalmazó almappákat az átmeneti területre az alábbi paranccsal:

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



**MEGJEGYZÉS:** Az <M:> a csatlakoztatott meghajtó. Cserélje le a megfelelő meghajtó betűjelére.

Ha további .inf típusú illesztőprogramokat is hozzá szeretne adni a lemezképhez, helyezze azokat a `C:\staging\mount\SWSETUP\DRV` mappába. Annak ismertetését, hogy a HP Sure Recover hogyan dolgozza fel ezeket a tartalmakat a `dism /Add-Driver /Recurse` paranccsal, a következő cikkben tekintheti át, amely többek között az illesztőprogramok offline Windows-lemezképhez történő hozzáadásával és onnan való eltávolításával foglalkozik: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

Ez a funkció nem támogatja az alkalmazások futtatásához szükséges .exe típusú illesztőprogramokat.

- c. Mentse a módosításokat, és válassza le a lemezképet az alábbi paranccsal:

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

Az eredményül kapott lemezképfájl: `C:\staging\my-image.wim`.

- d. Lépjen a következő lépésre: [A lemezkép felosztása 6. oldal](#).

## 2. példa: Lemezkép létrehozása referencia-rendszer alapján

1. Hozzon létre egy rendszerindításra alkalmas, a WinPE-t tartalmazó USB-adathordozót.



**MEGJEGYZÉS:** A lemezkép rögzítésének további módszerei az ADK dokumentációjában találhatók.

Győződjön meg róla, hogy az USB-meghajtó elegendő szabad területtel rendelkezik a referencia-rendszeren rögzített lemezkép tárolásához.

2. Hozzon létre egy lemezképet egy referencia-rendszeren.
3. Rögzítse a lemezképet úgy, hogy a referencia-rendszert a WinPE-t tartalmazó USB-adathordozóval indítja el, majd használja az alábbi DISM-parancsot.



**MEGJEGYZÉS:** Az <U:> az USB-meghajtóra vonatkozik. Cserélje le a megfelelő meghajtó betűjelére.

Módosítsa a fájlnev „my-image” részét, valamint a <my-image> leírást igény szerint.

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

4. Másolja a lemezképet az USB-meghajtóról a munkavégzési rendszer átmeneti területére az alábbi paranccsal:

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

A következő lemezképfájlt kell kapnia: C:\staging\my-image.wim.

5. Lépjen a következő lépésre: [A lemezkép felosztása 6. oldal.](#)

## A lemezkép felosztása

A HP azt javasolja, hogy a hálózati letöltések megbízhatóságának javítása érdekében ossza fel a lemezképet kisebb fájlokra az alábbi paranccsal:

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



**MEGJEGYZÉS:** A FileSize megabájtban megadott méretet jelöl. Módosítsa az értékét igény szerint.



**MEGJEGYZÉS:** A DISM felosztási algoritmusának jellege miatt előfordulhat, hogy a létrehozott SWM-fájlok mérete kisebb vagy nagyobb lesz a megadott fájlméretnél.

## Jegyzékfájl létrehozása

A jegyzékfájlokat UTF-8 formátumban formázza, bájtrendjelző (Byte Order Mark, BOM) nélkül.

A következő eljárásokban használt jegyzékfájl neve (custom.mft) módosítható, de nem módosíthatja az .mft és az .sig kiterjesztést, a jegyzékfájl és az aláírásfájlok fájlnevrészének pedig meg ugyanannak kell lennie. A custom.mft, custom.sig párt például a myimage.mft, myimage.sig párra módosíthatja.

Az mft\_version a lemezképfájl formátumának a meghatározására szolgál, és jelenleg 1 értékre kell beállítani.

Az image\_version annak megállapítására szolgál, hogy elérhető-e a lemezkép újabb verziója, valamint megakadályozza a régebbi verziók telepítését.

Mindkét értéknek előjel nélküli 16 bites egész számnak kell lennie, a jegyzékfájlban pedig az '\r\n' (CR + LF) karakterláncot kell sorelválasztóként használni.

## Jegyzékfájl létrehozása

Mivel a felosztott lemezkép több fájlt is tartalmazhat, hozzon létre egy jegyzékfájlt egy PowerShell-szkripttel.

A hátralévő lépéseket a C:\staging mappában kell végrehajtani.

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

1. Hozzon létre egy PowerShell-szkriptet az alábbi paranccsal és egy olyan szerkesztővel, amely képes UTF-8 formátumú, bájtrendjelző nélküli szövegfájl létrehozására: `notepad C:\staging\generate-manifest.ps1`

Hozza létre az alábbi szkriptet:

```
$mftFilename = "custom.mft"

$imageVersion = 1907 (Megjegyzés: A szám bármilyen 16 bites egész szám lehet.)

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

```



**MEGJEGYZÉS:** A HP Sure Recover jegyzékfájlja nem tartalmazhat bájtrendjelzőt, így az alábbi parancsok bájtrendjelző nélküli UTF-8 formátumú fájlként írják át a fájlt.

```

$content = Get-Content $mftFilename

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

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

```

2. Mentse a szkriptet.

3. Hajtsa végre a szkriptet.

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

## Jegyzékfájl-aláírás létrehozása

A Sure Recover titkosított aláírással ellenőrzi az ügynököt és a lemezképet. Az alábbi példák egy X.509 PEM formátumú (.PEM kiterjesztésű) személyes/nyilvános kulcspárt használnak. Módosítsa a parancsokat igény szerint, hogy DER bináris tanúsítványokat (.CER vagy .CRT kiterjesztés), BASE-64 kódolású PEM-tanúsítványokat (.CER vagy .CRT kiterjesztés) vagy PKCS1 PEM-fájlokat (.PEM kiterjesztés) használjanak. A példa OpenSSL-t is használ, amely csökkenő bájtrendű formátumban hozza létre az aláírásokat. Bármilyen segédprogrammal aláírhatja a jegyzékfájlokat, de vegye figyelembe, hogy néhány BIOS-verzió csak a növekvő bájtrendű aláírásokat támogatja.

1. Hozzon létre egy 2048 bites személyes RSA-kulcsot az alábbi paranccsal. Ha rendelkezik PEM formátumú, 2048 bites személyes/nyilvános RSA-kulcspárral, másolja a C:\staging mappába, majd ugorjon a 3. lépésre.

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

2. Hozza létre a nyilvános kulcsot a személyes kulcsból az alábbi paranccsal (ha rendelkezik PEM formátumú, a személyes kulcsnak megfelelő nyilvános kulccsal, akkor másolja a C:\staging mappába):

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

3. Hozzon létre egy aláírásfájlt (SHA-256-alapú kivonattal) az 1. lépésben létrehozott 2048 bites személyes RSA-kulcs alapján az alábbi paranccsal:

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

4. Ellenőrizze az aláírásfájlt az előző lépésben létrehozott nyilvános kulcsot használva az alábbi paranccsal:

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



#### MEGJEGYZÉS:

- Ha csak aláírásfájl kell létrehoznia, csak az 1. és a 3. lépést kell végrehajtani.
- A HP Sure Recover esetén legalább az 1., 2. és 3. lépést végre kell hajtani. A 2. lépésben létrehozott nyilvános kulcs a célrendszer üzembe helyezéséhez szükséges.
- A 4. lépés nem kötelező, de ajánlott, hogy az aláírásfájl és a jegyzékfájl ellenőrzése se maradjon el.

## A fájlok tárolása

Az alábbi fájlokat a kiszolgáló C:\staging mappájában tárolja:

- \*.swm
- custom.mft (vagy a jegyzékfájlunk adott fájlnev)
- custom.sig (vagy az aláírásfájlunk adott, a jegyzékfájlunkal egyező fájlnev)



**MEGJEGYZÉS:** Ha tárolási megoldásként az IIS-t használja, a MIME-bejegyzéseket úgy kell konfigurálni, hogy magukban foglalják az alábbi kiterjesztéseket, mindegyiket „application/octet-stream” típusúként konfigurálva:

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

## A célrendszerek üzembe helyezése

A célrendszerek a HP Client Management Script Library, a HP Client Security Manager (CSM)/Sure Recover vagy a Manageability Integration Kit (MIK) (<https://www.hp.com/go/clientmanagement>) használatával helyezhetők üzembe.

Adja meg az alábbi információkat az üzembe helyezéshez:

1. Az előző szakaszban található jegyzékfájl URL-címe ([http://saját\\_kiszolgáló.tartomány/útvonal/custom.mft](http://saját_kiszolgáló.tartomány/útvonal/custom.mft))
2. A korábban létrehozott aláírásfájl ellenőrzésére használt nyilvános kulcs (például: C:\staging\my-recovery-public.pem).

## Hibaelhárítás

Ha olyan üzenetet kap, amely szerint az egyéni helyreállítási folyamat biztonsági ellenőrzése sikertelen volt, ellenőrizze az alábbiakat:

1. A jegyzékfájlunk BOM nélküli UTF-8 formátumú fájlunk kell lennie.
2. Ellenőrizze a fájlkivonatokat.
3. Ellenőrizze, hogy a rendszer üzembe helyezése a jegyzékfájl aláírásához használt személyes kulcsnak megfelelő nyilvános kulccsal történt-e.

4. AZ IIS-kiszolgáló MIME-inek `application/octet-stream` típusúnak kell lenniük.
5. A jegyzékfájlban belüli fájlútvonalaknak a lemezképet tartalmazó legfelső szintű könyvtár teljes elérési útját tartalmazniuk kell, az ügyfélrendszerrel nézve. Ez az elérési út nem annak a helynek a teljes elérési útja, ahol a fájlok mentve lettek a terjesztési ponton.




### 3 A HP Sure Recover-ügynök használata vállalati tűzfalon belül

A HP Sure Recover-ügynök vállalati tűzfalon belül is üzemeltethető. Miután telepítette a HP Sure Recover SoftPac csomagot, másolja az ügynök fájljait a HP Sure Recover-ügynöknek a telepítési helyen található könyvtárból egy HTTP- vagy FTP-terjesztési pontra. Ezután helyezze üzembe az ügyfélrendszert a terjesztési pont URL-címével és a `hpsr_agent_public_key.pem` nevű nyilvános HP-kulccsal, amelynek a terjesztése a HP Sure Recover-ügynök SoftPac csomagjával történik.


#### A HP Sure Recover-ügynök telepítése

1. Töltse le a HP Sure Recover-ügynököt, és bontsa ki a fájlokat a HTTP- vagy FTP-terjesztési pontra.
2. Állítsa be a megfelelő fájlengedélyeket a terjesztési ponton.
3. Ha az Internet Information Services (IIS) megoldást használja, hozzon létre application/octet-stream MIME-típusokat az alábbi fájlformátumokhoz:


- .
- .wim
- .swm
- .mft
- .sig
- .efi
- .sdi

 **FONTOS:** Az alábbi lépések a Sure Recover SCCM használatával történő üzembe helyezését ismertetik. A Sure Recover HP Client Management Script Library használatával történő üzembe helyezésével kapcsolatban lásd: [A HP Client Management Script Library \(CMSL\) használata, 13. oldal](#).

4. Indítsa el az SCCM-et, lépjen a **HP Client Security Suite** (HP Client Security szoftvercsomag) részre, majd válassza a HP Sure Recover oldalt.

 **MEGJEGYZÉS:** A terjesztési pont URL-címe tartalmazza vagy az FTP-t vagy a HTTP-t mint átviteli protokollt. Annak a legfelső szintű könyvtárnak az ügyfélrendszerről látható teljes elérési útvonalát is tartalmazza, amelyen HP Sure Recover-ügynök jegyzékfájlja megtalálható. Ez az elérési út nem annak a helynek a teljes elérési útja, ahol a fájlok mentve lettek a terjesztési ponton.

5. A **Platform Image** (Platform lemezképe) szakaszban válassza a **Corporation** (Vállalat) lehetőséget az operációs rendszer egyéni lemezképének egy vállalati terjesztési pontról való visszaállításához. Adja meg az informatikai rendszergazdától kapott URL-címet az **Image Location URL** (A lemezkép helyének URL-címe) beviteli mezőben. Adja meg a `hpsr_agent_public_key.pem` nyilvános kulcsot az **Image Verification** (Lemezkép ellenőrzése) mezőben.

 **MEGJEGYZÉS:** Az egyéni lemezkép URL-címének tartalmaznia kell a lemezkép jegyzékfájljának a nevét.

6. A **Recovery Agent** (Helyreállítási ügynök) szakaszban válassza a **Corporation** (Vállalat) lehetőséget az egyéni helyreállítási ügynöknek vagy a HP helyreállítási ügynökének egy vállalati terjesztési pontról való használatához. Adja meg az informatikai rendszergazdától kapott URL-címet az **Agent Location URL** (Ügynök helyének URL-címe) mezőben. Adja meg a `hpsr_agent_public_key.pem` nyilvános kulcsot az **Agent Verification Key** (Ügynök ellenőrzési kulcsa) mezőben.



**MEGJEGYZÉS:** Az URL-címbe ne szerepeljen az ügynök jegyzékfájljának a neve, mert a BIOS megköveteli, hogy a név `recovery.mft` legyen.


7. Miután alkalmazta a szabályzatot az ügyfélrendszerre, indítsa újra a rendszert.
8. A kezdeti üzembe helyezés során megjelenik egy, a HP Sure Recover aktiválásához szükséges négyjegyű biztonsági kód megadására felszólító üzenet. További részletekért keresse fel a [hp.com](http://hp.com) webhelyet, és keressen rá a HP Manageability Integration Kit (MIK) for Microsoft System Center Manager megoldással foglalkozó dokumentációra.

A HP Sure Recover sikeres aktiválása után a szabályzat által alkalmazott egyéni URL-cím megjelenik a HP Sure Recover BIOS-beállításainak menüjében.

Ha meg szeretné erősíteni, hogy az aktiválás sikerrel járt, indítsa újra a számítógépet, és amikor megjelenik a HP embléma, nyomja le az **F10** billentyűt. Válassza az **Advanced** (Speciális), a **HP Sure Recover**, a **Recovery Agent** (Helyreállítási ügynök), végül pedig az **URL** lehetőséget.

## 4 A HP Client Management Script Library (CMSL) használata

A HP Client Management Script Library lehetővé teszi a HP Sure Recover beállításainak PowerShell-lel való kezelését. Az alábbi példaszkript bemutatja, hogyan lehet a HP Sure Recover üzembe helyezni, az állapotát meghatározni, a konfigurációját módosítani, valamint kivonni a használatból.

 **MEGJEGYZÉS:** Több parancs is hosszabb annál, hogy ebben az útmutatóban egyetlen sorban kiferjen, de ettől függetlenül egyetlen sorba kell írni őket.

```
$ErrorActionPreference = "Stop"

$spath = 'C:\test_keys'
$ekpw = ""
$skpw = ""

Get-HPSecurePlatformState

try {
    Write-host 'Provisioning Endorsement Key'
    $p = New-HPSecurePlatformEndorsementKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$spath\kek.pfx"
    $p | Set-HPSecurePlatformPayload

    Start-Sleep -Seconds 3

    Write-host 'Provisioning signing key'
    $p = New-HPSecurePlatformSigningKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$spath\kek.pfx" `
        -SigningKeyFile "$spath\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
}

```

## Példakulcs létrehozása az OpenSSL-lel

A személyes kulcsokat tárolja biztonságos helyen. A nyilvános kulcsokat az érvényesítéshez kell használni, és az üzembe helyezés során meg kell adni őket. Ezeknek a kulcsoknak 2048 bit hosszúságúnak kell lenniük, és 0x10001 kitevőt kell használniuk. A példákban szereplő megfelelő adatokat helyettesítse be cégének vagy szervezetének az adataival.

Állítsa be következő környezeti változót, mielőtt folytatná:

```

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:

```

**A lemezkép jegyzékfájlját a következő paranccsal írhatja alá:**

```
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:

```

**Az ügynök jegyzékfájlját a következő paranccsal írhatja alá:**

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

Az OpenSSL az aláírásfájlokat csökkenő bájtrendű formátumban hozza létre, amely néhány BIOS-verzióval nem kompatibilis, ezért előfordulhat, hogy az ügynök aláírásfájljának bájtrendjét meg kell fordítani az üzembe helyezés előtt. Azok a BIOS-verziók, amelyek támogatják a csökkenő bájtrendet, a növekvőt is támogatják.

# A Hibaelhárítás

## A meghajtó particionálása nem sikerült

A meghajtó particionálása akkor bizonyulhat sikertelennek, ha az SR\_AED vagy SR\_IMAGE partíció BitLockerrel van titkosítva. Ezeket a partíciókat általában egy GPT attribútummal hozzák létre, amely megakadályozza, hogy a BitLocker titkosítsa őket, de ha egy felhasználó törli és újra létrehozza a partíciókat, vagy manuálisan hozza létre őket egy operációs rendszer nélküli meghajtón, akkor a Sure Recover ügynök nem tudja törölni őket, és hibajelzéssel kilép, amikor megpróbálja újraparticionálni a meghajtót. A felhasználónak manuálisan kell törölnie a partíciókat a DiskPart futtatásával. Ki kell választania a kötetet, és végére kell hajtania a `del vol` felülírási parancsot vagy valamilyen hasonló műveletet.

## Firmware-naplófájl

Az EFI-változó adatai a következők:

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

Az EFI-változókat API-kkal lehet olvasni a Windowsban, de egy fájlba is kiírhatja a tartalmukat az UEFI Shell dmpstore segédprogrammal.

A naplófájlt a HP Client Management Script Library által biztosított `Get-HPFirmwareAuditLog` paranccsal írhatja ki.

## Windows Eseménynapló

A Sure Recover indítási és leállítási eseményeit a rendszer a BIOS naplófájljába küldi, amelyet a Windows Eseménynaplóban tekinthet meg a Sure Start naplófájljában, amennyiben a HP Notifications telepítve van. A rögzített események tartalmazzák a dátumot és az időpontot, a forrásazonosítót, az eseményazonosítót és egy eseményspecifikus kódot. Az [fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3] például azt jelzi, hogy a helyreállítás nem sikerült, mert a jegyzékfájl nem lehetett hitelesíteni a c3f 23000 eseményspecifikus kóddal, amely a következő napon és időpontban rögzült a naplóban: 6/27/18, 2:26:40.

 **MEGJEGYZÉS:** Ezek a naplók az Amerikai Egyesült Államokban használt hónap/nap/év formátumot követik.

## HP Secure Platform Management (forrásazonosító = 84h)

A-1. táblázat: HP Secure Platform Management

Eseményazonosító	Eszközök száma (összes/DaaS)	Események száma (összes/DaaS)	Leírás	Megjegyzések
40	256/178	943/552	A platform operációs rendszerének helyreállítási folyamatát a firmware megkezdte.	A platform helyreállítása elindult

**A-1. táblázat: HP Secure Platform Management (folytatás)**

Eseményazonosító	Eszközök száma (összes/DaaS)	Események száma (összes/DaaS)	Leírás	Megjegyzések
41	221/147	588/332	A platform operációs rendszerének helyreállítási folyamata sikeresen befejeződött.	A platform helyreállítása befejeződött
42	54/42	252/156	A platform operációs rendszerének helyreállítási folyamata sikertelen.	A platform helyreállítása sikertelen

A firmware-naplófájl a Get-HPFirmwareAuditLog paranccsal kérheti le a HP Client Management Script Libraryben, amely itt érhető el: <http://www.hp.com/go/clientmanagement>. A HP Secure Platform Management 40-es, 41-es és 42-es eseményazonosítói visszaküldik az eseményspecifikus kódokat az adatmezőbe, amely megjeleníti a Sure Recover-műveletek eredményét. Az alábbi naplóbejegyzés például a következőkkel jelzi, hogy a Sure Recovernek nem sikerült letöltenie a jegyzékfájl vagy az aláírásfájl: event\_id 42 és 00:30:f1:c3, amelyet 0xC3F13000 = MftOrSigDownloadFailed DWORD értéként kell értelmezni.

```
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
```

**A sikeres helyreállítást a következők jelzik: event\_id = 41 és 00:00:00:00, például:**

```
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

A HP Sure Recover az alábbi eseményspecifikus kódokat használja.

**A-2. táblázat: Eseményspecifikus kódok**

Esemény leírása	Eseménykód
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