Ръководство за потребителя

HP Sure Recover

Първо издание: февруари 2020 г.

Номенклатурен номер на документа: L93434-261

Синтактичен ключ на въведените от потребителя данни

Текстът, който трябва да въведете в потребителския интерфейс, е указан от `шрифт с фиксирана ширина`.

Таблица -1 Синтактичен ключ на въведените от потребителя данни

Елемент	Описание
`Текст без скоби`	Елементи, които трябва да въведете точно както е показано
`<Текст в ъглови скоби>`	Контейнер за стойност, която трябва да предоставите; пропуснете скобите
`[Текст в квадратни скоби]`	Допълнителни елементи; пропуснете скобите
`{Текст в кълрави скоби}`	Набор от елементи, от които трябва да изберете само един; пропуснете скобите
`|`	Разделител за елементи, от които трябва да изберете само един; пропуснете вертикалната лента
`...`	Елементи, които може или трябва да се повтарят; пропуснете многоточието

Съдържание

1 Начални стъпки

HP Sure Recover ви помага да инсталирате защитено операционната система от мрежата с минимално взаимодействие с потребителя. Системите с HP Sure Recover с Embedded Reimaging поддържат инсталиране също така и от локално устройство за съхранение.

ВАЖНО: Архивирайте данните си, преди да използвате HP Sure Recover. Тъй като процесът на създаване на образи преформатира устройството, това ще доведе до загуба на данни.

Образите за възстановяване, които HP предоставя, включват основната инсталираща програма на Windows 10®. По желание HP Sure Recover може да инсталира оптимизирани драйвери за устройства на HP. Образите за възстановяване на HP включват само агенти за възстановяване на данни, които са включени в Windows 10, като например OneDrive. Корпорациите могат да създават свои собствени персонализирани образи, за да добавят корпоративни настройки, приложения, драйвери и агенти за възстановяване на данни.

Агентът за възстановяване на операционната система (OS) изпълнява стъпките, необходими за инсталиране на образа за възстановяване. Агентът за възстановяване, предоставен от HP, извършва общи стъпки, като разделяне, форматиране и извличане на образа за възстановяване към целевото устройство. Тъй като агентът за възстановяване на HP се намира на hp.com, ще ви е необходим достъп до интернет, за да го извлечете, освен ако системата не включва Embedded Reimaging. Корпорациите може също така да хостват агента за възстановяване на HP в своята защитна стена или да създават персонализирани агенти за възстановяване за по-сложна среда за възстановяване.

Можете да стартирате HP Sure Recover, когато не е намерена операционна система. Можете също така да стартирате HP Sure Recover по график, като например, за да се уверите, че злонамереният софтуер е премахнат. Извършете конфигурацията на тези настройки чрез HP Client Security Manager (CSM), Manageability Integration Kit (MIK) или HP Client Management Script Library.

Извършване на възстановяване на мрежата

ЗАБЕЛЕЖКА: За да извършите възстановяване на мрежата, трябва да използвате кабелна връзка. HP препоръчва да архивирате важни файлове, данни, снимки, видеоклипове и т. н., преди да използвате HP Sure Recover, за да избегнете загуба на данни.

1. Свържете клиентската система към мрежата, където можете да осъществите достъп до HTTP или FTP точката за разпространение.
2. Рестартирайте клиентската система и когато се появи емблемата на HP, натиснете f11.
3. Изберете **Възстановяване от мрежата**.

Извършване на възстановяване на локално устройство

Ако клиентска система поддържа Embedded Reimaging и функцията за планирано изтегляне на образи е разрешена в приложените правила, тогава образът се изтегля към клиентската система в планирания час. След като образът се изтегли на клиентската система, я рестартирайте, за да копирате образа на устройството за съхранение с Embedded Reimaging.

За да извършите локално възстановяване с помощта на образа от устройството за съхранение с Embedded Reimaging:

1. Рестартирайте клиентската система и когато се появи емблемата на HP, натиснете f11.
2. Изберете **Възстановяване от локално устройство**.

Системите с Embedded Reimaging трябва да конфигурират график за изтегляне и да използват агента за изтегляне, за да проверяват за актуализации. Агентът за изтегляне е включен в добавката HP Sure Recover за HP Client Security Manager и може също така да се конфигурира в MIK. Вижте https://www.hp.com/go/clientmanagement за инструкции за използване на MIK.

Можете също да създадете планирана задача, за да копирате агента в дела SR_AED, а образа – в дела SR_IMAGE. След това можете да използвате HP Client Management Script Library, за да изпратите сервизно събитие, което информира BIOS, че трябва да валидира съдържанието и да копира на устройството за съхранение с Embedded Reimaging при следващото рестартиране.

2 Създаване на корпоративен образ

Повечето компании използват инструментите за разполагане на Microsoft (Microsoft Deployment Tools), комплекта за оценка и разполагане на Windows 10 (Windows 10 Assessment and Deployment kit) или и двете, за да създават файлове, които съдържат образ в архив с файлови формати Windows Imaging (WIM).

Изисквания

- Най-новата версия на комплекта за оценка и разполагане на Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (или друго решение за генериране на RSA двойка частни/публични ключове)

  Използва се за генериране на RSA двойката ключове, използвани за защита на целостта на корпоративния образ, който създавате и хоствате.
- Решение за хостване на сървър (като например Microsoft Internet Information Services [IIS])

Създаване на образа

Преди да стартирате процеса за създаване на образ, настройте работната система или създайте система, в която сте инсталирали необходимите инструменти, за да се подготвите за обработката на образа, както е показано в следните стъпки:

1. Като администратор отворете командния прозорец `Deployment and Imaging Tools Environment` (Среда за инструменти за създаване на образи и разполагане) (инсталиран с инструментите за разполагане на Windows ADK).
2. Създайте област за постановка за вашия образ, като използвате следната команда:

   ```
   mkdir C:\staging
   ```
3. Създайте образа, като използвате един от следните примери:

   Пример 1: Създаване на образ въз основа на инсталационния образ на Microsoft Windows на страница 3

   Пример 2: Създаване на образ въз основа на референтна система на страница 6

Пример 1: Създаване на образ въз основа на инсталационния образ на Microsoft Windows

1. Монтирайте или отворете инсталационния образ на Microsoft Windows (от Microsoft ISO или от HP OSDVD).
2. От монтирания инсталационен образ на Windows копирайте файла install.wim във вашата област за постановка, като използвате следната команда:

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

ЗАБЕЛЕЖКА: `<M:>` се отнася за монтираното устройство. Заменете с правилната буква на дисковото устройство.

3. Преименувайте install.wim в име на файл с образ („my-image“ за този пример), като използвате следната команда:

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

(По избор) HP Sure Recover включва функция за възстановяване на специфично издание от мултииндексен образ въз основа на изданието на Windows, първоначално фабрично лицензирано за целевата система на HP. Този механизъм работи, ако индексите са именувани правилно. Ако вашият инсталационен образ на Windows идва от HP OSDVD образ, вероятно имате образ с много издания. Ако не желаете това поведение и искате да се уверите, че едно конкретно издание се използва за всички ваши целеви системи, трябва да сте сигурни, че в инсталационния образ има само един индекс.

4. Проверете съдържанието на инсталационния образ с помощта на следната команда:

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

По-долу е показан пробен резултат от инсталационен образ, който поддържа пет издания (за съпоставяне на базата на BIOS на всяка целева система):

Подробности за образа: `my-image.wim`

Индекс: `1`

Име: `CoreSingleLanguage`

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

Размер: `19,512,500,682 bytes`

Индекс: `2`

Име: `Core`

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

Размер: `19,512,500,682 bytes`

Индекс: `3`

Име: `Professional`

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

Размер: `19.758,019,520 bytes`

Индекс: `4`

Име: `ProfessionalEducation`

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

Размер: `19,758,019,480 bytes`

Индекс: `5`

Име: `ProfessionalWorkstation`

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

Размер: `19,758,023,576 bytes`

ЗАБЕЛЕЖКА: Когато има само един индекс, образът се използва за възстановяване, независимо от името. Размерът на вашия файл с образ може да е по-голям от преди изтриванията.

5. Ако не искате поведението на много издания, изтрийте всеки индекс, който не желаете.

   Както е показано в следващия пример, ако искате само професионално издание (ако всички целеви системи са лицензирани), изтрийте индекс 5, 4, 2 и 1. Всеки път, когато изтривате даден индекс, номерата на индекса се възлагат повторно. Следователно трябва да изтривате от най-високите към най-ниските номера на индекса. Стартирайте `Get-ImageInfo` след всяко изтриване за визуално потвърждаване на индекса, който ще изтриете след това.

   ```
   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
   ```

   Изберете само един индекс на изданието (за този пример: Professional). Когато има само един индекс, образът се използва за възстановяване, независимо от името. Имайте предвид, че размерът на вашия файл с образ може да бъде по-голям от преди изтриванията поради начина, по който работят промените на WIM метаданните и нормализирането на съдържанието.

6. (По избор) Ако искате да включите драйвери във вашия корпоративен образ за възстановяване, изпълнете следните стъпки:

   а. Монтирайте образа в празна папка, като използвате командите по-долу:

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

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

   б. Монтирайте подходящия HP Windows 10 Driver DVD (DRDVD) диск за поддържаната целева система. От монтирания носител на драйвери копирайте подпапките на драйверите във вашата област за постановка, като използвате следната команда:

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

   ЗАБЕЛЕЖКА: `<M:>` се отнася за монтираното устройство. Заменете с правилната буква на дисковото устройство.

   Можете да включите допълнителни .inf-style драйвери, като ги поставите в папката C:\staging\mount\SWSETUP\DRV. За обяснение относно начина на обработване на това съдържание от HP Sure Recover с помощта на функцията `dism /Add-Driver /Recurse` вижте „Добавяне и премахване на драйвери в офлайн образ на Windows“ в следната тема: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Тази функция не поддържа .exe-style драйвери, които изискват изпълнение на приложение.

   в. Запишете промените и демонтирайте образа, като използвате следната команда:

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

   Полученият файл с образ е: C:\staging\my-image.wim.

   г. Отидете на Разделяне на образа на страница 6.

Пример 2: Създаване на образ въз основа на референтна система

1. Създайте стартов USB WinPE носител.

   ЗАБЕЛЕЖКА: Допълнителни методи за заснемане на образ можете да намерите в документацията на ADK.

   Уверете се, че USB устройството има достатъчно свободно пространство, за да побере снетия образ от референтната система.

2. Създаване на образ на референтна система.
3. Снемете образа, като заредите референтната система с USB WinPE носител, след което използвайте DISM.

   ЗАБЕЛЕЖКА: `<U:>` се отнася за USB устройство. Заменете с правилната буква на дисковото устройство.

   Редактирайте частта „my-image“ от името на файла и описанието `<my-image>`, ако е необходимо.

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

4. Копирайте образа от USB в областта за постановка на вашата работна система, като използвате следната команда:

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

   Трябва да имате следния файл с образ: C:\staging\my-image.wim.

5. Отидете на Разделяне на образа на страница 6.

Разделяне на образа

HP препоръчва да разделите образа на по-малки файлове, за да подобрите надеждността на изтеглянията от мрежата, като използвате следната команда:

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

ЗАБЕЛЕЖКА: Големината на файла се показва в мегабайти. Редактирайте, както е необходимо.

ЗАБЕЛЕЖКА: Поради естеството на алгоритъма за разделяне на DISM размерите на генерираните SWM файлове може да бъдат по-малки или по-големи от заявения размер на файла.

Създаване на манифест

Форматирайте манифестните файлове като UTF-8 без знак за реда на байтовете (BOM).

Можете да промените името на манифестния файл (custom.mft), използван в процедурите по-долу, но не трябва да променяте разширенията .mft и .sig, а частта с името на манифестните файлове и файловете с подписи трябва да съвпада. Можете например да промените двойката (custom.mft, custom.sig) на (myimage.mft, myimage.sig).

`mft_version` се използва за определяне на формата на файла с образа и трябва да е зададено на 1.

`image_version` се използва, за да се определи дали има налична по-нова версия на образа и за да се предотврати инсталирането на по-стари версии.

И двете стойности трябва да са неподписани 16-битови цели числа, а разделителят в манифеста трябва да е `'\r\n' (CR + LF)`.

Генериране на манифест

Тъй като няколко файла може да са включени в разделения образ, използвайте скрипт на PowerShell, за да генерирате манифест.

Във всички останали стъпки трябва да сте в папката C:\staging.

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

1. Създаване на скрипт на PowerShell с помощта на редактор, който може да произведе текстов файл във формат UTF-8 без BOM с помощта на следната команда: `notepad C:\staging\generate-manifest.ps1`

   Създайте следния скрипт:

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

   `$imageVersion = 1907` (Забележка: това може да бъде всяко 16-битово цяло число)

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

}
```

ЗАБЕЛЕЖКА: Манифестите за HP Sure Recover не може да включват BOM, така че командите по-долу презаписват файла като UTF8 без BOM.

```
$content = Get-Content $mftFilename

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

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

2. Запишете скрипта.
3. Изпълнете скрипта.

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

Генериране на подпис на манифест

Sure Recover проверява агента и образа с помощта на криптографски подписи. Следните примери използват двойка частни/публични ключове във формат X.509 PEM (.PEM разширение). Коригирайте командите, както е подходящо, за да използвате DER двоични сертификати (.CER или .CRT разширение), BASE-64 кодирани PEM сертификати (.CER или .CRT разширение) или файлове PKCS1 PEM файлове (.PEM разширение). Примерът също така използва OpenSSL, който генерира подписи във формат big-endian. Можете да използвате която и да е помощна програма за подписване на манифести, но някои версии на BIOS поддържат само подписи във формат little-endian.

1. Генерирайте 2048-битов RSA частен ключ с помощта на командата по-долу. Ако имате 2048-битова двойка RSA частни/публични ключове в pem формат, ги копирайте на C:\staging и след това преминете към стъпка 3.

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

2. Генерирайте публичния ключ от частния ключ (ако имате публичен ключ, съответстващ на вашия частен ключ в PEM формат, го копирайте в C:\staging), като използвате следната команда:

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

3. Създайте файл с подпис (чрез базиран на sha256 хеш) на базата на вашия 2048-битов RSA частен ключ от стъпка 1, като използвате следната команда:

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

4. Проверете файла с подписа, като използвате публичния ключ от предишната стъпка чрез следната команда:

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

ЗАБЕЛЕЖКА:

- Ако трябва да създадете само файл с подписи, задължителните стъпки са 1 и 3.
- За HP Sure Recover минималните задължителни стъпки са 1, 2 и 3. Трябва да имате публичен ключ от стъпка 2, за да обезпечите вашата целева система.
- Стъпка 4 е по избор, но се препоръчва, така че файлът с подпис и манифестният файл да се валидират правилно.

Хостване на файловете

Хоствайте следните файлове от папката C:\staging на вашия сървър:

- *.swm
- custom.mft (или името на файла, което сте избрали за манифестния файл)
- custom.sig (или съответстващото име на файла, което сте избрали за файла с подписа)

ЗАБЕЛЕЖКА: Ако използвате IIS като хостинг решение, трябва да конфигурирате вашите MIME записи да включват следните разширения, всички конфигурирани като „application/octet-stream:“

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

Обезпечаване на вашите целеви системи

Можете да обезпечите вашите целеви системи, като използвате HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover или Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Осигурете следната информация за това обезпечаване:

1. URL адреса на манифестния файл, хостван в предишния раздел (http://your_server.domain/path/custom.mft)
2. Публичния ключ, използван за проверка на създадения по-рано файл с подписи (например C:\staging\my-recovery-public.pem).

Отстраняване на неизправности

Ако получите съобщение, че персонализираният процес на възстановяване е с неуспешна проверка на защитата, проверете следното:

1. Манифестът трябва да е UTF-8 без BOM.
2. Проверете хешовете.
3. Уверете се, че на системата е предоставен публичният ключ, съответстващ на частния ключ, използван за подписване на манифеста.

4. MIME типовете на IIS сървъра трябва да са `application/octet-stream`.
5. Пътищата на файловете в рамките на манифеста трябва да включват пълния път до най-горната директория, съдържаща образа, както се вижда от клиентската система. Този път не е пълният път, когато файловете се записват в точката за разпространение.

3 Използване на агент на HP Sure Recover в корпоративна защитна стена

Агент на HP Sure Recover може да се хоства на корпоративен интранет. След като инсталирате HP Sure Recover SoftPaq, копирайте файловете на агента от директорията на агента на HP Sure Recover от местоположението за инсталиране на HTTP или FTP точка за разпространение. След това обезпечете клиентската система с URL адреса на точката за разпространение и публичния ключ на HP, наречен `hpsr_agent_public_key.pem`, който се предоставя с HP Sure Recover Agent SoftPaq.

Инсталиране на агента на HP Sure Recover

1. Изтеглете агента на HP Sure Recover и разархивирайте файловете във вашата HTTP или FTP точка за разпространение.
2. Задайте подходящите файлови разрешения за точката за разпространение.
3. Ако използвате Internet Information Services (IIS), създайте application/octet-stream MIME типове за следните файлови формати:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   ВАЖНО: Показаните по-долу стъпки описват обезпечаването на Sure Recover с SCCM. За примери за това как да обезпечите Sure Recover с HP Client Management Script Library вижте Работа с HP Client Management Script Library (CMSL) на страница 13.

4. Стартирайте SCCM, навигирайте до **HP client Security Suite**, след което изберете страницата HP Sure Recover.

   ЗАБЕЛЕЖКА: URL адресът на точката за разпространение включва ftp или http като транспортен протокол. Тя също така включва пълния път до най-горната директория, съдържаща манифеста за агента на HP Sure Recover, както се вижда от клиентската система. Този път не е пълният път до мястото, където се записват файловете в точката за разпространение.

5. В раздела **Platform Image** (Образ на платформата) изберете опцията **Corporation** (Корпорация), за да възстановите персонализиран образ на ОС от корпоративна точка за разпространение. Въведете URL адреса, предоставен от ИТ администратора, в полето за въвеждане **Image Location URL** (URL адрес на местоположението на образа). Въведете публичния ключ `hpsr_agent_public_key.pem` в полето **Image Verification** (Проверка на образа).

   ЗАБЕЛЕЖКА: Персонализираният URL адрес на образа трябва да включва името на манифестния файл.

6. В раздела **Recovery Agent** (Агент за възстановяване) изберете опцията **Corporation** (Корпорация), за да използвате персонализиран агент за възстановяване или агент за възстановяване на HP от корпоративна точка за разпространение. Въведете URL адреса, предоставен от ИТ администратора, в полето за въвеждане **Agent Location URL** (URL адрес на местоположението на агента). Въведете публичния ключ `hpsr_agent_public_key.pem` в полето за въвеждане **Agent Verification Key** (Ключ за проверка на агента).

ЗАБЕЛЕЖКА: Не включвайте името на файла за манифеста на агента в URL адреса, защото BIOS изисква да бъде под името recovery.mft.

7. След като правилата се приложат към клиентската система, я рестартирайте.

8. По време на първоначалното обезпечаване се появява подкана да въведете 4-цифрен код за защита, за да завършите активирането на HP Sure Recover. За повече подробности отидете на hp.com и потърсете HP Manageability Integration Kit (MIK) за техническия документ на Microsoft System Center Manager.

След като активирането на HP Sure Recover завърши успешно, персонализираният URL адрес, приложен от правилото, се показва в менюто за настройките на BIOS за HP Sure Recover.

За да потвърдите успешната активация, рестартирайте компютъра и когато се появи емблемата на HP, натиснете f10. Изберете **Advanced** (Разширени), изберете **HP Sure Recover**, изберете **Recovery Agent** (Агент за възстановяване), след което изберете **URL** (URL адрес).

4 Работа с HP Client Management Script Library (CMSL)

HP Client Management Script Library позволява да управлявате настройките на HP Sure Recover с PowerShell. Примерният скрипт по-долу показва как да се обезпечи, да се определи състояние, да се промени конфигурацията и да се премахне обезпечаването на HP Sure Recover.

ЗАБЕЛЕЖКА: Няколко от командите надвишават дължината на линията на това ръководство, но трябва да се въведат като единичен ред.

```
$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
}
```

Примерно генериране на ключ чрез OpenSSL

Съхранявайте частните ключове на безопасно място. Публичните ключове ще се използват за валидиране и трябва да се предоставят по време на обезпечаването. Тези ключове трябва да са с дължина 2048 бита и да използват степенен показател 0x10001. Сменете темата в примерите с информация за вашата организация.

Задайте следната променлива на средата, преди да продължите:

```
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:
```

Можете да подпишете манифеста на образа с тази команда:

```
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:
```

Можете да подпишете манифеста на агента с тази команда:

```
dgst-SHA256 – знак Re. Key-Out Agent. SIG Agent. MFT
```

OpenSSL генерира файлове с подпис във формат big-endian, който е несъвместим с някои версии на BIOS, така че може да се наложи редът на байт на подпис на агента да се обърне, преди да се разположи. Версиите на BIOS, които поддържат реда на байтовете big-endian, също така поддържат и реда на байтовете little-endian.

a Отстраняване на неизправности

Неуспешно разделяне на дисковото устройство

Неуспешно разделяне на дисковото устройство може да възникне, ако дяловете SR_AED или SR_IMAGE са шифровани с Bitlocker. Тези дялове обикновено се създават с gpt атрибут, който предотвратява шифроването на Bitlocker, но ако даден потребител изтрива и пресъздава дяловете или ги създава ръчно на празен метален диск, тогава агентът на Sure Recover не може да ги изтрие и излиза с грешка при повторно разделяне на диска. Потребителят трябва да ги изтрие ръчно, като изпълни diskpart, избере силата на звука и зададе командата за замяна `del vol` или подобна.

Регистър на проверки на фърмуера

Информацията за променливата EFI е както следва:

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

API съществуват под Windows за прочитане на променливи EFI или можете да разтоварите променливото съдържание във файл с помощта на UEFI Shell dmpstore utility.

Можете да разтоварите регистрационния файл за проверка чрез командата `Get-HPFirmwareAuditLog`, предоставена от HP Client Management Script Library.

Регистър на събитията на Windows

Събитията за стартиране и спиране на Sure Recover се изпращат към регистъра за проверки на BIOS, който можете да прегледате в Windows Event Viewer в регистъра на Sure Start, ако HP Notifications е инсталирано. Тези събития включват дата и час, ИД на източник, ИД на събитие и специфичен за събитието код. Например `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` показва, че възстановяването е неуспешно, защото манифестът не може да се удостовери със специфичния за събитието код c3f 23000, който е бил регистриран в 2:26:40 на 6/27/18 (т.е. 27.06.2018 г.).

ЗАБЕЛЕЖКА: Тези регистрационни файлове следват формата за дата на САЩ: месец/дата/година.

HP Secure Platform Management (ИД на източник = 84 ч)

Таблица a-1 HP Secure Platform Management

ИД на събитие	Брой устройства (All/DaaS)	Брой събития (All/DaaS)	Описание	Бележки
40	256/178	943/552	Процесът на възстановяване на платформата на ОС е стартиран от фърмуера.	Възстановяването на платформата е стартирано

Таблица а-1 HP Secure Platform Management (продължение)

ИД на събитие	Брой устройства (All/DaaS)	Брой събития (All/DaaS)	Описание	Бележки
41	221/147	588/332	Процесът на възстановяване на ОС на платформата е завършен успешно.	Възстановяването на платформата е завършено
42	54/42	252/156	Процесът на възстановяване на ОС на платформата не успя да завърши успешно.	Неуспешно възстановяване на платформата

Можете да извлечете регистрационния файл за проверка на фърмуера чрез Get-HPFirmwareAuditLog в HP Client Management Script Library, налична на http://www.hp.com/go/clientmanagement. ИД на събитие 40, 41 и 42 за HP Secure Platform Management връща специфични за събитието кодове, които указват резултата от операциите на Sure Recover. Следният запис в регистър например показва, че Sure Recover не може да изтегли манифеста или файла с подписи с грешката event_id 42 и данни: 00:30:f1:c3, което трябва да се интерпретира като dword стойност 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
```

Успешното възстановяване е показано като event_id = 41 и данни: 00:00:00:00, например:

```
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 използва кодовете за конкретни събития по-долу.

Таблица а-2 Кодове за конкретни събития

Описание на събитието	Код на събитието
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