Guía del usuario

HP Sure Recover

Primera edición: febrero de 2020

Número de referencia del documento: L93434-E51

Tecla de sintaxis de entrada de usuario

El texto que debe introducir en una interfaz de usuario se indica mediante una `fuente de ancho fijo`.

Tabla -1 Tecla de sintaxis de entrada de usuario

Elemento	Descripción
`Texto sin corchetes o llaves`	Elementos que debe escribir exactamente como se muestra
`<texto dentro de corchetes angulares>`	Un marcador de posición de un valor que usted debe brindar; omitir los corchetes
`[Texto dentro de corchetes cuadrados]`	Elementos opcionales; omitir los corchetes
`{Texto dentro de llaves}`	Un conjunto de elementos de los que debe elegir solo uno; omitir las llaves
`|`	Un separador de elementos de los que debe elegir solo uno; omitir la barra vertical
`...`	Elementos que pueden o deben repetirse; omitir los puntos suspensivos

Tabla de contenido

1 Pasos iniciales

HP Sure Recover lo ayuda a instalar de forma segura el sistema operativo desde la red con una mínima interacción con el usuario. Los sistemas con HP Sure Recover con Embedded Reimaging también admiten la instalación desde un dispositivo de almacenamiento local.

IMPORTANTE: Haga copias de seguridad de sus datos antes de usar HP Sure Recover. Debido a que el proceso de generación de imágenes reformatea la unidad, se perderán los datos.

Las imágenes de recuperación que HP proporciona incluyen el instalador básico de Windows 10®. Opcionalmente, HP Sure Recover puede instalar controladores optimizados para dispositivos HP. Las imágenes de recuperación de HP solo incluyen agentes de recuperación de datos que se incluyen con Windows 10, como OneDrive. Las empresas pueden crear sus propias imágenes personalizadas para agregar configuraciones corporativas, aplicaciones, controladores y agentes de recuperación de datos.

Un agente de recuperación del sistema operativo (SO) realiza los pasos necesarios para instalar la imagen de recuperación. El agente de recuperación proporcionado por HP realiza pasos comunes como el particionamiento, la formatación y la extracción de la imagen de recuperación en el dispositivo de destino. Debido a que el agente de recuperación de HP está ubicado en hp.com, necesita acceder a Internet para recuperarlo, a menos que el sistema incluya Embedded Reimaging. Las empresas también pueden alojar al agente de recuperación de HP dentro de su firewall o crear agentes de recuperación personalizados para entornos de recuperación más complicados.

Puede iniciar HP Sure Recover cuando no se encuentre ningún sistema operativo. También puede ejecutar HP Sure Recover en una programación, por ejemplo, la que se usa para asegurar que se elimine el malware. Realice la configuración de estos valores mediante HP Client Security Manager (CSM), Manageability Integration Kit (MIK) o HP Client Management Script Library.

Realización de una recuperación de red

NOTA: Para realizar una recuperación de red, debe utilizar una conexión cableada. HP recomienda realizar copias de seguridad de datos, fotos, videos y otros archivos importantes antes de usar HP Sure Recover para evitar la pérdida de datos.

1. Conecte el sistema cliente a la red donde se puede acceder al punto de distribución HTTP o FTP.
2. Reinicie el sistema cliente y, cuando aparezca el logotipo de HP, presione F11.
3. Seleccione **Restaurar desde la red**.

Realización de una recuperación de la unidad local

Si un sistema cliente admite Embedded Reimaging y la opción de descarga de imagen programada está activada en la política aplicada, la imagen se descarga en el sistema cliente a la hora programada. Después de que la imagen se descarga en el sistema cliente, reinícielo para copiar la imagen en el dispositivo de almacenamiento con Embedded Reimaging.

Para realizar la recuperación local utilizando la imagen del dispositivo de almacenamiento con Embedded Reimaging:

1. Reinicie el sistema cliente y, cuando aparezca el logotipo de HP, presione F11.
2. Seleccione **Restaurar desde una unidad local**.

Los sistemas con Embedded Reimaging deben configurar una programación de descarga y utilizar el agente de descarga para verificar si hay actualizaciones. El agente de descarga se incluye en el plug-in HP Sure Recover para HP Client Security Manager y también puede configurarse en MIK. Consulte https://www.hp.com/go/clientmanagement para ver las instrucciones de uso de MIK.

También puede crear una tarea programada para copiar el agente en la partición SR_AED y la imagen en la partición SR_IMAGE. A continuación, puede utilizar HP Client Management Script Library para enviar un evento de servicio que informa al BIOS que debe validar el contenido y copiarlo en el dispositivo de almacenamiento con Embedded Reimaging en el siguiente reinicio.

2 Creación de una imagen corporativa

La mayoría de las empresas utilizan las herramientas de implementación de Microsoft, Windows 10 Assessment and Deployment Kit o ambos para producir archivos que contienen una imagen dentro de un archivo de formato Windows Imaging (WIM).

Requisitos

- La última versión de Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (u otra solución para generar el par de claves privadas/públicas de RSA)

  Úselo para generar el par de claves RSA que se requiere para asegurar la integridad de la imagen corporativa que usted crea y aloja.
- Una solución de alojamiento de servidores (como Microsoft Internet Information Services [IIS])

Creación de la imagen

Antes de iniciar el proceso de creación de imagen, configure el sistema de trabajo o el sistema de compilación donde instaló las herramientas necesarias para prepararse para el procesamiento de la imagen, como se muestra en los siguientes pasos:

1. Como Administrador, abra la línea de comando `Deployment and Imaging Tools Environment` (instalada con las herramientas de implementación de Windows ADK).
2. Cree un área de ensayo para su imagen, utilizando el siguiente comando:

   ```
   mkdir C:\staging
   ```
3. Cree la imagen utilizando uno de los siguientes ejemplos:

   Ejemplo 1: Creación de una imagen basada en la imagen de instalación de Microsoft Windows en la página 3

   Ejemplo 2: Creación de una imagen basada en un sistema de referencia en la página 6

Ejemplo 1: Creación de una imagen basada en la imagen de instalación de Microsoft Windows

1. Monte o abra la imagen de instalación de Microsoft Windows (desde una Microsoft ISO o de una HP OSDVD).
2. Desde la imagen de instalación de Windows montada, copie el archivo install.wim en su área de ensayo, utilizando el siguiente comando:

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

NOTA: `<M:>` se refiere a la unidad montada. Sustitúyala por la letra de la unidad correcta.

3. Cambie el nombre de install.wim a un nombre de archivo de imagen ("my-image" para este ejemplo), utilizando el siguiente comando:

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

   (Opcional) HP Sure Recover incluye un recurso para recuperar una edición específica de una imagen con varios índices, basado en la edición de Windows licenciada originalmente para el sistema de destino de HP de fábrica. Este mecanismo funciona si los índices se nombran correctamente. Si su imagen de instalación de Windows proviene de una imagen de HP OSDVD, es probable que tenga una imagen de multiedición. Si no desea este comportamiento y quiere asegurarse de que se utilice una edición específica para todos sus sistemas de destino, debe asegurarse de que solo un índice esté en la imagen de instalación.

4. Compruebe el contenido de la imagen de instalación utilizando el siguiente comando:

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

   A continuación se muestra la salida de ejemplo desde una imagen de instalación que admite cinco ediciones (que se van a emparejar según el BIOS de cada sistema de destino):

   Detalles para la imagen: `my-image.wim`

   Índice: `1`

   Nombre: `CoreSingleLanguage`

   Descripción: `Actualización del 10 de mayo de 2019 de Windows - Home Single Language Edition`

   Tamaño: `19 512 500 682 bytes`

   Índice: `2`

   Nombre: `Core`

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

   Tamaño: `19 512 500 682 bytes`

   Índice: `3`

   Nombre: `Professional`

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

   Tamaño: `19 758 019 520 bytes`

   Índice: `4`

   Nombre: `Professional Education`

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

   Tamaño: `19 758 019 480 bytes`

   Índice: `5`

   Nombre: `ProfessionalWorkstation`

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

Tamaño: `19 758 023 576 bytes`

NOTA: Cuando solo hay un índice, la imagen se utiliza para la recuperación, independientemente del nombre. El tamaño de su archivo de imagen podría ser mayor que antes de las eliminaciones.

5. Si no desea el comportamiento de multiedición, elimine cada índice que no desee.

   Como se muestra en el siguiente ejemplo, si solo desea la edición Professional (asumiendo que todos los sistemas de destino tengan licencia), elimine el índice 5, 4, 2 y 1. Cada vez que elimina un índice, los números de índice se reasignan. Por lo tanto, debe eliminar los números de índice de los más altos a los más bajos. Ejecute `Get-ImageInfo` después de cada eliminación para confirmar visualmente qué índice se eliminará a continuación.

   ```
   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
   ```

   Seleccione solo un índice de la edición (para este ejemplo, Professional). Cuando solo hay un índice, la imagen se utiliza para la recuperación, independientemente del nombre. Tenga en cuenta que el tamaño de su archivo de imagen podría ser mayor que antes de las eliminaciones, debido a la forma en que funcionan las modificaciones de los metadatos de WIM y la normalización de contenido.

6. (Opcional) Si desea incluir controladores en su imagen de recuperación corporativa, siga estos pasos:

   a. Monte su imagen en una carpeta vacía, utilizando los siguientes comandos:

   ```
   mkdir C:\staging\mount

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

   b. Monte el DVD del controlador HP Windows 10 (DRDVD) adecuado para el sistema de destino admitido. Desde el medio del controlador montado, copie las subcarpetas del controlador en su área de ensayo, utilizando el siguiente comando:

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

   NOTA: `<M:>` se refiere a la unidad montada. Sustitúyala por la letra de la unidad correcta.

   Puede incluir controladores adicionales .inf-style colocándolos debajo de la carpeta C:\staging \mount\SWSETUP\DRV. Para obtener una explicación sobre cómo HP Sure Recover procesa este contenido usando la función `dism /Add-Driver /Recurse`, consulte "Agregar y eliminar controladores en una imagen de Windows sin conexión" en el siguiente tema: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Este recurso no admite controladores .exe-style que requieren la ejecución de una aplicación.

   c. Guarde los cambios y desmonte su imagen, utilizando el siguiente comando:

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

   El archivo de imagen resultante es: C:\staging\my-image.wim.

   d. Visite División de la imagen en la página 6.

Ejemplo 2: Creación de una imagen basada en un sistema de referencia

1. Cree medios USB WinPE USB de inicio.

   NOTA: Puede encontrar métodos adicionales para capturar la imagen en la documentación de ADK.

   Asegúrese de que la unidad USB tenga suficiente espacio libre para contener la imagen capturada del sistema de referencia.

2. Cree una imagen en un sistema de referencia.
3. Capture la imagen iniciando el sistema de referencia con el medio USB WinPE y luego use DISM.

   NOTA: `<U:>` hace referencia a la unidad USB. Sustitúyala por la letra de la unidad correcta.

   Edite la parte “my-image” del nombre del archivo, así como la descripción de `<my-image>`, si es necesario.

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

4. Copie la imagen desde USB al área de ensayo de su sistema de trabajo usando el siguiente comando:

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

   Debe tener el siguiente archivo de imagen: C:\staging\my-image.wim.

5. Visite División de la imagen en la página 6.

División de la imagen

HP recomienda que divida la imagen en archivos más pequeños para mejorar la confiabilidad de las descargas de red, utilizando el siguiente comando:

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

NOTA: FileSize se muestra in megabytes. Edite según sea necesario.

NOTA: Debido a la naturaleza del algoritmo de división de DISM, los tamaños de los archivos SWM generados podrían ser más pequeños o más grandes que el tamaño del archivo indicado.

Creación de un manifiesto

Formatee los archivos de manifiesto como UTF-8 sin marca de orden de bytes (BOM, por sus siglas en inglés).

Puede cambiar el nombre del archivo de manifiesto (custom.mft) utilizado en los siguientes procedimientos, pero no debe cambiar las extensiones .mtf y .sig. Además, la parte del nombre de archivo del manifiesto y los archivos de firma deben coincidir. Por ejemplo, puede cambiar el par (custom.mft, custom.sig) por (myimage.mft, myimage.sig).

`mft_version` se utiliza para determinar el formato del archivo de imagen y debe establecerse actualmente como 1.

`image_version` se utiliza para determinar si una versión más reciente de la imagen está disponible y para evitar que se instalen versiones antiguas.

Ambos valores deben ser enteros de 16 bits sin signo, y el separador de línea en el manifiesto debe ser `'\r \n' (CR + LF)`.

Generación de un manifiesto

Debido a que varios archivos pueden estar involucrados con su imagen dividida, use un script de PowerShell para generar un manifiesto.

En todos los pasos restantes, debe estar en la carpeta C:\staging.

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

1. Cree un script de PowerShell usando un editor que pueda producir un archivo de texto en formato UTF-8 sin BOM, usando el siguiente comando: `notepad C:\staging\generate-manifest.ps1`

   Cree el siguiente script:

```
$mftFilename = "custom.mft"
$imageVersion = 1907
```

(Nota: Esto puede ser cualquier entero de 16 bits)

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

NOTA: Los manifiestos de HP Sure Recover no pueden incluir una BOM, por lo que los siguientes comandos reescriben el archivo como UTF8 sin BOM.

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename, $content, $encoding)
```

2. Guarde el script.
3. Ejecute el script.

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

Generación de firma de manifiesto

Sure Recover valida el agente y la imagen utilizando firmas criptográficas. Los siguientes ejemplos utilizan un par de claves privadas/públicas en formato X.509 PEM (extensión .PEM). Ajuste los comandos según corresponda para usar los certificados binarios de DER (extensión .CER o .CRT), certificados PEM codificados BASE-64 (extensión .CER o .CRT), o archivos PEM PKCS1 (extensión .PEM). El ejemplo también utiliza OpenSSL, que genera firmas en formato big-endian. Puede utilizar cualquier utilidad para firmar manifiestos, pero algunas versiones del BIOS solo admiten firmas en formato little-endian.

1. Genere una clave privada RSA de 2048 bits utilizando el siguiente comando. Si tiene un par de claves privadas/públicas RSA de 2048 bits en formato PEM, cópielas en C:\staging y luego vaya al paso 3.

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

2. Genere la clave pública desde su clave privada (si tiene una clave pública que corresponda a su clave privada en formato PEM, cópiela en C:\staging), utilizando el siguiente comando:

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

3. Cree un archivo de firma (usando hash basado en sha256) según su clave privada RSA de 2048 bits del paso 1, utilizando el siguiente comando:

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

4. Verifique el archivo de firma utilizando su clave pública del paso anterior y el siguiente comando:

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

NOTA:

- Si solo necesita crear un archivo de firma, siga los pasos 1 y 3.
- En el caso de HP Sure Recover, los pasos mínimos requeridos son 1, 2 y 3. Necesita la clave pública del paso 2 para aprovisionar su sistema de destino.
- El paso 4 es opcional pero se recomienda para que su archivo de firma y el archivo de manifiesto se validen correctamente.

Alojamiento de los archivos

Aloje los siguientes archivos en su servidor desde la carpeta C:\staging:

- *.swm
- custom.mft (o el nombre de archivo que eligió para el archivo de manifiesto)
- custom.sig (o el nombre de archivo coincidente que eligió para el archivo de firma)

NOTA: Si utiliza IIS como su solución de alojamiento, debe configurar sus entradas MIME para incluir las siguientes extensiones, todas configuradas como "application/octet-stream:"

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

Aprovisionamiento de sus sistemas de destino

Puede suministrar sus sistemas de destino utilizando HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover o el Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Proporcione la siguiente información para este aprovisionamiento:

1. La dirección URL del archivo de manifiesto alojado en la sección anterior (http://your_server.domain/path/custom.mft)
2. La tecla pública utilizada para verificar el archivo de firma creado anteriormente (por ejemplo, C:\staging\my-recovery-public.pem).

Solución de problemas

Si recibe un mensaje de falla en la validación de seguridad del proceso de recuperación personalizado, revise lo siguiente:

1. El manifiesto debe ser UTF-8 sin BOM.
2. Verifique los hashes de archivo.
3. Asegúrese de que el sistema se haya aprovisionado con la clave pública correspondiente a la clave privada utilizada para firmar el manifiesto.
4. Los tipos MIME de servidor IIS deben ser `application/octet-stream`.
5. Las rutas de archivo dentro del manifiesto deben incluir la ruta completa al directorio más completo que contiene la imagen, tal como se ve desde un sistema cliente. Esta ruta no es la ruta completa donde se guardan los archivos en el punto de distribución.

3 Uso del agente HP Sure Recover dentro de un firewall corporativo

El agente de HP Sure Recover se puede alojar en una intranet corporativa. Después de instalar el SoftPaq de HP Sure Recover, copie los archivos del agente del directorio del agente HP Sure Recover desde la ubicación de instalación hasta un punto de distribución HTTP o FTP. A continuación, aprovisione el sistema cliente con la URL del punto de distribución y la clave pública HP denominada `hpsr_agent_public_key.pem`, que se distribuye con SoftPaq del agente HP Sure Recover.

Instalación del agente HP Sure Recover

1. Descargue el agente HP Sure Recover y extraiga los archivos en su punto de distribución HTTP o FTP.
2. Establezca los permisos de archivo apropiados en el punto de distribución.
3. Si está utilizando Internet Information Services (IIS), cree tipos MIME de application/octet-stream para los siguientes formatos de archivo:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

IMPORTANTE: Los siguientes pasos describen el aprovisionamiento de Sure Recover con SCCM. Para ver ejemplos de cómo aprovisionar Sure Recover con HP Client Management Script Library, consulte Trabajar con HP Client Management Script Library (CMSL) en la página 12.

4. Inicie SCCM, desplácese a **HP Client Security Suite** y luego seleccione la página de HP Sure Recover.

NOTA: La URL del punto de distribución incluye ftp o http como protocolo de transporte. También incluye la ruta completa al directorio principal que contiene el manifiesto para el agente de HP Sure Recover, visto desde un sistema cliente. Esta ruta no es la ruta completa donde se guardan los archivos en el punto de distribución.

5. En la sección **Imagen de la plataforma**, seleccione la opción **Corporación** para restaurar una imagen personalizada del SO desde un punto de distribución corporativo. Introduzca la URL proporcionada por el administrador de TI en el cuadro de entrada **URL de la ubicación de la imagen**. Introduzca la clave pública `hpsr_agent_public_key.pem` en el campo **Verificación de imagen**.

NOTA: La URL de la imagen personalizada debe incluir el nombre del archivo de manifiesto de imagen.

6. En la sección **Recovery Agent** (Agente de recuperación), seleccione la opción **Corporation** (Corporación) para usar un agente de recuperación personalizado o el agente de recuperación de HP desde un punto de distribución corporativo. Escriba la URL proporcionada por el administrador de TI en el cuadro de

entrada **URL de ubicación del agente**. Escriba la clave pública `hpsr_agent_public_key.pem` en el campo **Clave de verificación del agente**.

NOTA: No incluya el nombre de archivo del manifiesto del agente en la URL porque el BIOS requiere que se le llame recovery.mft.

7. Después de aplicar la política al sistema cliente, reinícielo.
8. Durante el aprovisionamiento inicial, aparece un mensaje para que introduzca un código de seguridad de 4 dígitos para completar la activación de HP Sure Recover. Para obtener más detalles, vaya a hp.com y busque el informe técnico HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

Después de que la activación de HP Sure Recover concluye satisfactoriamente, la URL personalizada aplicada por la política se mostrará en el menú de configuración del BIOS de HP Sure Recover.

Para confirmar el éxito de la activación, reinicie el equipo y, cuando aparezca el logotipo de HP, presione F10. Seleccione **Advanced** (Avanzado), seleccione **HP Sure Recover**, seleccione **Recovery Agent** (Agente de recuperación) y luego **URL**.

4 Trabajar con HP Client Management Script Library (CMSL)

HP Client Management Script Library le permite administrar las configuraciones de HP Sure Recover con PowerShell. El siguiente script de ejemplo demuestra cómo aprovisionar, determinar el estado, cambiar la configuración y desaprovisionar HP Sure Recover.

NOTA: Varios de los comandos exceden la longitud de línea de esta guía, pero deben introducirse como una sola línea.

```
$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
}
```

Generación de claves de ejemplo usando OpenSSL

Guarde las claves privadas en un lugar seguro. Las claves públicas se usarán para validación y deben proporcionarse durante el aprovisionamiento. Es necesario que estas claves tengan una longitud de 2048 bits y usen un exponente de 0x10001. Sustituya el asunto en los ejemplos con información sobre su organización.

Establezca la siguiente variable de entorno antes de continuar:

```
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:
```

Puede firmar el manifiesto de la imagen con este comando:

```
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:
```

Puede firmar el manifiesto del agente con este comando:

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

OpenSSL genera archivos de forma en formato big-endian, que no es compatible con algunas versiones del BIOS, así que el pedido de bytes de archivo de firma del agente podría tener que revertirse antes de su implementación. Las versiones del BIOS que admiten el pedido de bytes big-endian también admiten el pedido de bytes little-endian.

A Solución de problemas

Se produjo un error en el particionamiento de la unidad

Puede ocurrir una falla en la partición de la unidad si la partición SR_AED o SR_IMAGE está encriptada con BitLocker. Normalmente, estas particiones se crean con un atributo gpt que impide que BitLocker los encripte, pero si un usuario elimina y recrea las particiones o las crea de forma manual en una unidad sin SO, el agente de Sure Recover no puede eliminarlos y sale con un error al reparticionar la unidad. El usuario debe eliminarlos manualmente ejecutando diskpart, seleccionando el volumen y emitiendo el comando de anulación `del vol` o similar.

Registro de auditoría de firmware

La información de la variable EFI es la siguiente:

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

Las API existen en Windows para leer las variables EFI, o puede volcar contenido variable en un archivo utilizando la utilidad UEFI Shell dmpstore.

Puede volcar el registro de auditoría utilizando el comando `Get-HPFirmwareAuditLog` que ofrece HP Client Management Script Library.

Registro de eventos de Windows

Los eventos de inicio y detención de Sure Recover se envían al registro de auditoría del BIOS, que puede ver en el Visor de eventos de Windows, en el registro de Sure Start, si las notificaciones de HP están instaladas. Estos eventos incluyen la fecha y la hora, el ID de origen, el ID de evento y el código de un evento específico. Por ejemplo, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indica que la recuperación falló porque no se pudo autenticar el manifiesto con el código de evento específico c3f 23000 que se registró a las 2:26:40 el 27/6/18.

NOTA: Estos registros siguen el formato de fecha de los EE. UU.: mes/fecha/año.

HP Secure Platform Management (ID de la fuente = 84h)

Tabla A-1 HP Secure Platform Management

ID del evento	Cantidad de dispositivos (Todos/DaaS)	Cantidad de eventos (Todos/DaaS)	Descripción	Notas
40	256/178	943/552	El firmware inició el proceso de recuperación del SO de la plataforma.	Se inició la recuperación de la plataforma

Tabla A-1 HP Secure Platform Management (continuación)

ID del evento	Cantidad de dispositivos (Todos/DaaS)	Cantidad de eventos (Todos/DaaS)	Descripción	Notas
41	221/147	588/332	El proceso de recuperación del SO de la plataforma se ha completado con éxito.	Recuperación de la plataforma completada
42	54/42	252/156	El proceso de recuperación del SO de la plataforma no se completó correctamente.	Error en la recuperación de la plataforma

Puede recuperar el registro de auditoría de firmware utilizando Get-HPFirmwareAuditLog en HP Client Management Script Library disponible en http://www.hp.com/go/clientmanagement. Las ID de evento 40, 41 y 42 de HP Secure Platform Management retornan códigos de evento específicos en el campo de datos, lo que indica el resultado de las operaciones de Sure Recover. Por ejemplo, la siguiente entrada de registro indica que Sure Recover no pudo descargar el manifiesto o el archivo de firma con el error event_id 42 y los datos: 00:30:f1:c3, que debe interpretarse como el valor de dword 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: El proceso de recuperación del SO de la plataforma no se
completó correctamente.

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

Una recuperación exitosa se muestra como event_id = 41 y datos: 00:00:00:00, por ejemplo:

```
Códigos específicos del evento

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: El proceso de recuperación del SO de la plataforma no se
completó correctamente.
```

```
data: 00:00:00:00
```

HP Sure Recover utiliza los siguientes códigos de evento específico.

Tabla A-2 Códigos específicos del evento

Descripción del evento	Código de evento
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