User Guide

HP Sure Recover

First Edition: February 2020

Document Part Number: L93434-001

User input syntax key

Text that you must enter into a user interface is indicated by `fixed-width font`.

Item	Description
`Text without brackets or braces`	Items you must type exactly as shown
`<Text inside angle brackets>`	A placeholder for a value you must provide; omit the brackets
`[Text inside square brackets]`	Optional items; omit the brackets
`{Text inside braces}`	A set of items from which you must choose only one; omit the braces
`|`	A separator for items from which you must choose only one; omit the vertical bar
`...`	Items that can or must repeat; omit the ellipsis

Table of contents

1 Getting started

HP Sure Recover helps you to securely install the operating system from the network with minimal user interaction. Systems with HP Sure Recover with Embedded Reimaging also support installation from a local storage device.

IMPORTANT: Back up your data before using HP Sure Recover. Because the imaging process reformats the drive, data loss will occur.

Recovery images that HP provides include the basic Windows 10® installer. Optionally, HP Sure Recover can install optimized drivers for HP devices. HP recovery images only include data recovery agents that are included with Windows 10, like OneDrive. Corporations can create their own custom images to add corporate settings, applications, drivers, and data recovery agents.

An operating system (OS) recovery agent performs the steps necessary to install the recovery image. The recovery agent provided by HP performs common steps like partitioning, formatting, and extracting the recovery image to the target device. Because the HP recovery agent is located on hp.com, you need Internet access to retrieve it, unless the system includes embedded reimaging. Corporations can also host the HP recovery agent within their firewall or create custom recovery agents for more complicated recovery environments.

You can initiate HP Sure Recover when no operating system is found. You can also run HP Sure Recover on a schedule, such as to ensure malware is removed. Perform configuration of those settings through HP Client Security Manager (CSM), Manageability Integration Kit (MIK), or the HP Client Management Script Library.

Performing a network recovery

NOTE: To perform a network recovery, you must use a wired connection. HP recommends backing up important files, data, photos, videos, and so on before using HP Sure Recover to avoid loss of data.

1. Connect the client system to the network where the HTTP or FTP distribution point can be accessed.
2. Restart the client system, and when the HP logo appears, press f11.
3. Select **Restore from network**.

Performing a local drive recovery

If a client system supports embedded reimaging and the scheduled image download option is enabled in the applied policy, then the image is downloaded to the client system at the scheduled time. After the image is downloaded to the client system, restart it to copy the image to the Embedded Reimaging storage device.

To perform local recovery using the image on the Embedded Reimaging storage device:

1. Restart the client system, and when the HP logo appears, press f11.
2. Select **Restore from local drive**.

Systems with Embedded Reimaging must configure a download schedule and use the download agent to check for updates. The download agent is included in the HP Sure Recover Plug-in for HP Client Security Manager, and can also be configured in MIK. See https://www.hp.com/go/clientmanagement for the instructions to use MIK.

You can also create a scheduled task to copy the agent to the SR_AED partition and the image to the SR_IMAGE partition. You can then use the HP Client Management Script Library to send a service event informing the BIOS that it should validate the contents and copy to the embedded reimaging storage device on the next reboot.

2 Creating a corporate image

Most companies use the Microsoft Deployment Tools, Windows 10 Assessment and Deployment kit, or both to produce files containing an image within a Windows Imaging (WIM) file format archive.

Requirements

- The latest version of Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (or other solution for generating RSA private/public key pair)

  Use to generate the RSA key pair used to secure the integrity of the corporate image you create and host.
- A server hosting solution (such as Microsoft Internet Information Services [IIS])

Creating the image

Before starting the image creation process, set up the working system or build system where you installed the required tools to prepare for processing the image, as shown in the following steps:

1. As Administrator, open the `Deployment and Imaging Tools Environment` command prompt (installed with the Deployment Tools of Windows ADK).
2. Create a staging area for your image, using the following command:

   ```
   mkdir C:\staging
   ```
3. Create the image using one of the following examples:

   Example 1: Creating an image based on the Microsoft Windows installation image on page 3

   Example 2: Creating an image based on a reference system on page 5

Example 1: Creating an image based on the Microsoft Windows installation image

1. Mount or open the Microsoft Windows installation image (from a Microsoft ISO, or from an HP OSDVD).
2. From the mounted Windows installation image, copy the install.wim file to your staging area, using the following command:

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

   NOTE: `<M:>` refers to the mounted drive. Replace with the correct drive letter.
3. Rename install.wim to an image file name ("my-image" for this example), using the following command:

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

   (Optional) HP Sure Recover includes a feature to recover a specific edition from a multi-index image, based on the Windows edition originally licensed for the HP target system in the factory. This mechanism works if the indexes are named properly. If your Windows installation image comes from an HP OSDVD image, you likely have a multiedition image. If you do not want this behavior and do want to

ensure one specific edition is used for all of your target systems, then you need to be sure that only one index is in the installation image.

4. Check the contents of the installation image using the following command:

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

   The following shows sample output from an installation image that supports five editions (to be matched based on the BIOS of each target system):

   Details for image: `my-image.wim`

   Index: `1`

   Name: `CoreSingleLanguage`

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

   Size: `19,512,500,682 bytes`

   Index: `2`

   Name: `Core`

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

   Size: `19,512,500,682 bytes`

   Index: `3`

   Name: `Professional`

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

   Size: `19.758,019,520 bytes`

   Index: `4`

   Name: `ProfessionalEducation`

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

   Size: `19,758,019,480 bytes`

   Index: `5`

   Name: `ProfessionalWorkstation`

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

   Size: `19,758,023,576 bytes`

   NOTE: When there is only one index, the image is used for recovery, regardless of the name. The size of your image file might be larger than before the deletions.

5. If you do not want the multiedition behavior, delete each index that you do not want.

   As shown in the following example, if you want only Professional edition (assuming all target systems are licensed), delete index 5, 4, 2, and 1. Each time you delete an index, the index numbers are

reassigned. Therefore, you should delete from highest to lowest index numbers. Run `Get-ImageInfo` after each deletion to visually confirm which index you will delete next.

```
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
```

Choose only one index of the edition (for this example, Professional). When there is only one index, the image is used for recovery, regardless of the name. Note that the size of your image file might be larger than before the deletions, because of the way WIM metadata modifications and content normalization work.

6. (Optional) If you want to include drivers in your corporate recovery image, follow these steps:

   a. Mount your image to an empty folder, using the following commands:

   ```
   mkdir C:\staging\mount

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

   b. Mount the appropriate HP Windows 10 Driver DVD (DRDVD) for the supported target system. From the mounted driver media, copy the driver subfolders to your staging area, using the following command:

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

   NOTE: `<M:>` refers to the mounted drive. Replace with the correct drive letter.

   You may include additional .inf-style drivers by placing them under the C:\staging\mount \SWSETUP\DRV folder. For an explanation about how this content is processed by HP Sure Recover using the `dism /Add-Driver /Recurse` function, see “Add and Remove Drivers to an Offline Windows image” in the following topic: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   This feature does not support .exe-style drivers that require running an application.

   c. Save changes and unmount your image, using the following command:

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

   The resulting image file is: C:\staging\my-image.wim.

   d. Go to Splitting the image on page 6.

Example 2: Creating an image based on a reference system

1. Create bootable USB WinPE media.

   NOTE: Additional methods to capture the image can be found in ADK documentation.

   Make sure the USB drive has enough free space to hold the captured image from the reference system.

2. Create an image on a reference system.
3. Capture the image by booting the reference system with the USB WinPE media, and then use DISM.

NOTE: `<U:>` refers to the USB drive. Replace with the correct drive letter.

Edit the “my-image” part of file name, and the `<my-image>` description, as needed.

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

4. Copy the image from USB to the staging area on your working system using the following command:

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

   You should have the following image file: C:\staging\my-image.wim.

5. Go to Splitting the image on page 6.

Splitting the image

HP recommends that you split the image into smaller files to improve reliability of network downloads, using the following command:

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

NOTE: FileSize is shown in megabytes. Edit as necessary.

NOTE: Because of the nature of DISM's split algorithm, the sizes of the generated SWM files might be either smaller or larger than the stated file size.

Creating a manifest

Format manifest files as UTF-8 without Byte Order Mark (BOM).

You can change the manifest file name (custom.mft) used in the following procedures, but you must not change the extensions .mft and .sig, and the file name portion of the manifest and signature files must match. For example, you can change the pair (custom.mft, custom.sig) to (myimage.mft, myimage.sig).

`mft_version` is used to determine the format of the image file and must currently be set to 1.

`image_version` is used to determine if a newer version of the image is available and to prevent older versions from being installed.

Both values must be unsigned 16-bit integers, and the line separator in the manifest must be `'\r\n' (CR + LF)`.

Generating a manifest

Because several files might be involved with your split image, use a powershell script to generate a manifest.

In all remaining steps, you must be in the C:\staging folder.

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

1. Create a powershell script using an editor that can produce a text file in format UTF-8 without BOM, using the following command: `notepad C:\staging\generate-manifest.ps1`

   Create the following script:

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

   ```
   $imageVersion = 1907
   ```
   (Note: This can be any 16-bit integer)

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

NOTE: Manifests for HP Sure Recover cannot include a BOM, so the following commands rewrite the file as UTF8 without BOM.

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

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

2. Save the script.
3. Execute the script.

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

Generating manifest signature

Sure Recover validates the agent and image using cryptographic signatures. The following examples use a private/public key pair in X.509 PEM format (.PEM extension). Adjust the commands as appropriate to use DER binary certificates (.CER or .CRT extension), BASE-64 encoded PEM certificates (.CER or .CRT extension), or PKCS1 PEM files (.PEM extension). The example also uses OpenSSL, which generates signatures in big-endian format. You can use any utility to sign manifests, but some BIOS versions only support signatures in little-endian format.

1. Generate a 2048-bit RSA private key using the following command. If you have a 2048-bit RSA private/public key pair in pem format, copy them to C:\staging, and then skip to step 3.

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

2. Generate the public key from your private key (if you have a public key corresponding to your private key in PEM format, copy it to C:\staging), using the following command:

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

3. Create a signature file (using sha256-based hash) based on your 2048-bit RSA private key from step 1, using the following command:

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

4. Verify the signature file, using your public key from the previous step, using the following command:

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

NOTE:

- If you need to create a signature file only, the required steps are 1 and 3.
- For HP Sure Recover, the minimum required steps are 1, 2, and 3. You need the public key from step 2 to provision your target system.
- Step 4 is optional but recommended so that your signature file and manifest file validate correctly.

Hosting the files

Host the following files on your server from the C:\staging folder:

- *.swm
- custom.mft (or the file name you chose for the manifest file)
- custom.sig (or the matching file name you chose for the signature file)

NOTE: If you use IIS as your hosting solution, you must configure your MIME entries to include the following extensions, all configured as "application/octet-stream:"

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

Provisioning your target systems

You can provision your target systems using the HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover or the Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Provide the following information for this provisioning:

1. The URL address of the manifest file hosted in the previous section (http://your_server.domain/path/custom.mft)
2. The public key used to verify the signature file created previously (for example, C:\staging\my-recovery-public.pem).

Troubleshooting

If you receive a message about the custom recovery process failing security validation, check the following:

1. Manifest must be UTF-8 without BOM.
2. Check file hashes.
3. Ensure that the system was provisioned with the public key corresponding to the private key used to sign the manifest.
4. IIS server mime types must be `application/octet-stream`.
5. File paths within the manifest must include the full path to the topmost directory containing the image as seen from a client system. This path is not the full path where the files are saved at the distribution point.

3 Using the HP Sure Recover Agent Within a Corporate Firewall

The HP Sure Recover agent can be hosted on a corporate intranet. After you install the HP Sure Recover SoftPaq, copy the agent files from the HP Sure Recover agent directory from the installation location to an HTTP or FTP distribution point. Then provision the client system with the URL of the distribution point and the HP public key named `hpsr_agent_public_key.pem`, which is distributed with the HP Sure Recover agent SoftPaq.

Installing the HP Sure Recover agent

1. Download HP Sure Recover agent and extract the files to your HTTP or FTP distribution point.
2. Set the appropriate file permissions on the distribution point.
3. If you are using Internet Information Services (IIS), create application/octet-stream MIME types for the following file formats:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

IMPORTANT: The following steps describe provisioning Sure Recover with SCCM. For examples of how to provision Sure Recover with the HP Client Management Script Library, see Working with the HP Client Management Script Library (CMSL) on page 12.

4. Start SCCM, navigate to **HP Client Security Suite**, and then select the HP Sure Recover page.

NOTE: The distribution point URL includes either ftp or http as the transport protocol. It also includes the full path to the topmost directory containing the manifest for the HP Sure Recover agent as seen from a client system. This path is not the full path to where the files are saved at the distribution point.

5. In the **Platform Image** section, select the **Corporation** option to restore a customized OS image from a corporate distribution point. Enter the URL provided by the IT administrator into the **Image Location URL** entry box. Enter the public key `hpsr_agent_public_key.pem` into the **Image Verification** field.

NOTE: The custom image URL must include the image manifest file name.

6. In the **Recovery Agent** section, select the **Corporation** option to use a custom recovery agent or the HP recovery agent from a corporate distribution point. Enter the URL provided by the IT administrator into the **Agent Location URL** entry box. Enter the public key `hpsr_agent_public_key.pem` into the **Agent Verification Key** entry field.

NOTE: Do not include the file name for the agent manifest in the URL because the BIOS requires it to be named recovery.mft.

7. After the policy is applied to the client system, restart it.
8. During initial provisioning, a prompt appears for you to enter a 4-digit security code to complete HP Sure Recover activation. For more details, go to hp.com and search for the HP Manageability Integration Kit (MIK) for Microsoft System Center Manager white paper.

After the HP Sure Recover activation completes successfully, the custom URL applied by the policy is displayed in the HP Sure Recover BIOS settings menu.

To confirm the activation success, restart the computer, and when the HP logo appears, press f10. Select **Advanced**, select **HP Sure Recover**, select **Recovery Agent**, and then select **URL**.

4 Working with the HP Client Management Script Library (CMSL)

The HP Client Management Script Library allows you to manage HP Sure Recover settings with PowerShell. The following example script demonstrates how to provision, determine status, change configuration, and deprovision HP Sure Recover.

NOTE: Several of the commands exceed the line length of this guide but must be entered as a single line.

```
$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
}
```

Sample key generation using OpenSSL

Store the private keys in a safe location. The public keys will be used for validation and must be provided during provisioning. These keys are required to be 2048 bits in length and use an exponent of 0x10001. Replace the subject in the examples with information about your organization.

Set the following environment variable before proceeding:

```
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:
```

You can sign the image manifest with this command:

```
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:
```

You can sign the agent manifest with this command:

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

OpenSSL generates signature files in big-endian format, which is incompatible with some BIOS versions, so the agent signature file byte order may need to be reversed before being deployed. BIOS versions that support big-endian byte ordering also support little-endian byte ordering.

A Troubleshooting

Drive partitioning failed

Failed drive partitioning can occur if the SR_AED or SR_IMAGE partition is encrypted with Bitlocker. These partitions are normally created with a gpt attribute that prevents Bitlocker from encrypting them, but if a user deletes and recreates the partitions or creates them manually on a bare metal drive, then the Sure Recover agent is unable to delete them and exits with an error when repartitioning the drive. The user must manually delete them by running diskpart, selecting the volume, and issuing the `del vol` override command or similar.

Firmware audit log

EFI variable information is as follows:

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

APIs exist under Windows for reading EFI variables, or you can dump variable content to a file using the UEFI Shell dmpstore utility.

You can dump the audit log using the `Get-HPFirmwareAuditLog` command provided by the HP Client Management Script Library.

Windows event log

Sure Recover start and stop events are sent to the BIOS audit log, which you can view in Windows Event Viewer in the Sure Start log if HP Notifications is installed. These events include the date and time, Source ID, Event ID, and an event specific code. For example, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indicates that recovery failed because the manifest could not be authenticated with the event specific code c3f 23000 that was logged at 2:26:40 on 6/27/18.

NOTE: These logs follow US date format of month/date/year.

HP Secure Platform Management (Source ID = 84h)

Table A-1 HP Secure Platform Management

Event ID	Device count (All/DaaS)	Event count (All/DaaS)	Description	Notes
40	256/178	943/552	The platform OS recovery process was started by the firmware.	Platform recovery started
41	221/147	588/332	The platform OS recovery process has successfully completed.	Platform recovery completed
42	54/42	252/156	The platform OS recovery process failed to complete successfully.	Platform recovery failed

You can retrieve the Firmware Audit Log using Get-HPFirmwareAuditLog in the HP Client Management Script Library, available at http://www.hp.com/go/clientmanagement. HP Secure Platform Management Event ID's 40, 41, and 42 return Event Specific Codes in the data field, which indicate the result of Sure Recover operations. For example, the following log entry indicates Sure Recover failed to download the manifest or signature file with the error event_id 42 and data: 00:30:f1:c3, which should be interpreted as the dword value 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
```

A successful recovery is shown as event_id = 41 and data: 00:00:00:00, for example:

```
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 uses the following Event Specific Codes.

Table A-2 Event Specific Codes

Event Description	Event Code
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