



HP Sure Recover Administrator Guide

SUMMARY

HP Sure Recover helps you to securely install the operating system with minimal user interaction. Systems with HP Sure Recover with Embedded Reimaging can also include a tamper-resistant, dedicated local storage device that provides additional security, resiliency, and performance enhancements.

Legal information

© Copyright 2020, 2024 HP Development Company, L.P.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Second Edition: September 2024

First Edition: February 2020

Document Part Number: L93434-002

User input syntax key

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

User input syntax key

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

Table of contents

1 Getting started	1
Configuring recovery behavior	1
Configuring recovery image content	2
Performing a network recovery	2
Performing a local drive recovery	2
Disabling HP Sure Recover	3
2 Creating a corporate image	4
Requirements	4
Creating the image	4
Example 1: Creating an image based on the Microsoft Windows installation image	4
Example 2: Creating an image based on a reference system	6
Splitting the image	7
Creating a manifest	7
Generating a manifest	8
Generating a manifest signature	9
Hosting the files	10
Provisioning your target systems	10
Troubleshooting	10
3 Using the HP Sure Recover Agent Within a Corporate Firewall	12
Installing the HP Sure Recover agent	12
4 Working with the HP Client Management Script Library (CMSL)	14
Sample key generation using OpenSSL	15
Appendix A Troubleshooting	18
Drive partitioning failed	18
Firmware audit log	18
Windows event log	18
HP Secure Platform Management (Source ID = 84h)	19
HP Sure Recover download event log	24
Enable Toast notification	24
Index	0

1 Getting started

HP Sure Recover helps you to securely install the operating system with minimal user interaction. Systems with HP Sure Recover with Embedded Reimaging can also include a tamper-resistant, dedicated local storage device that provides additional security, resiliency, and performance enhancements.



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

HP Sure Recover will install the HP Corporate Ready with Office image with default settings that are suitable for most environments, including modern management. It can also be configured to install a clean Windows® 10 or later image with optional optimized drivers, Corporate Ready with or without Office applications, or custom images that include corporate settings, applications, drivers, and data recovery agents. See the *HP Corporate-Ready Whitepaper* for more information.

A 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. Corporations can also host the HP recovery agent locally, in the cloud, or create custom recovery agents for more complicated recovery environments.

Start HP Sure Recover by pressing **F11** while the HP logo is displayed after power-on. It can also start when no operating system is found. Another option is to run HP Sure Recover on a schedule to periodically ensure malware is removed from kiosks. Configure the HP Sure Recover settings through the HP Wolf Security Dashboard, Manageability Integration Kit (MIK), or HP Client Management Script Library (CMSL).

Configuring recovery behavior

Use CMSL, MIK, Wolf Security Console, and other manageability tools to configure recovery agent behavior.



NOTE: Changing settings requires Secure Platform Management configuration first. For examples, go to the following website: [HP Secure Platform Management with the HP Client Management Script Library](#)

For example, CMSL enables or disables image sources by using the New-HPSureRecoverConfigurationPayload -BIOSFlags with the following parameters or bitmasks:

- None = 0
- NetworkBasedRecovery = 1 => Enable network-based recovery
- WiFi = 2 => Enable WiFi
- PartitionRecovery = 4 = Enable partition-based recovery
- SecureStorage = 8 => Enable recovery from secure storage device
- SecureEraseUnit = 16 => Secure Erase Unit before recovery
- RollbackPrevention = 64 => Enforce rollback prevention

Configuring recovery image content

Current shipping operating system and driver details are published in the HP Cloud Recovery Supported Platforms list, although HP Sure Recover does not support all platforms on that list. New image content is provided through the End of Support period up to and including the previous two generations of products and is released on the same cadence as Windows OEM releases.

You can use CMSL, MIK, Wolf Security Console, and other manageability tools to configure image content.

For example, you can use CMSL to specify image content by using the `New-HPSureRecoverConfigurationPayload -AgentFlags` with the following parameters or bitmasks:

- `None = 0 => OEM OS release with in-box drivers`
- `DRDVD = 1 => OEM OS release with optimized drivers`
- `CorporateReadyWithoutOffice = 2 => Corporate Ready without office`
- `CorporateReadyWithOffice = 4 => Corporate Ready with office`
- `InstallManageabilitySuite = 16`
- `InstallSecuritySuite = 32 => Install current components of the HP Wolf Security suite`
- `RollbackPrevention = 64 => Enforce rollback prevention`

Performing a network recovery

HP Sure Recover is available on select HP PCs and requires Windows 10 or later and an open network connection. You must back up important files, data, photos, videos, and so forth before using HP Sure Recover to avoid loss of data. For network-based recovery using Ethernet, you must have an HP Ethernet port or adapter (sold separately). You can use WiFi only on select PCs.

1. Connect the client system to the network.



NOTE: You might need to disable Intel AMT in the BIOS settings to connect the client system to the WiFi. See the *Preboot Wireless Networking on HP Business PCs* technical whitepaper for more information about WiFi configuration.

2. Restart the client system, and when the HP logo appears, press **f11**.
3. Select **Restore from network**.

Performing a local drive recovery

Sure Recover supports two methods of local recovery. Systems with the optional Embedded Reimaging can recover from a dedicated storage device that is isolated from untrusted environments. Partition-Based Recovery is also available on select systems and is only used if the disk size is greater than 192 GB. Because the Partition-Based Recovery partitions are available in untrusted environments, a network recovery is required if the partitions have been tampered with.

Available on select platforms, HP Sure Recover can perform local drive recovery using two methods:

1. **Embedded Reimaging:** The optional embedded storage that is hardware-isolated for secure image storage.
2. **Partition-Based Recovery:** A separate partition that is created within the existing drive to store a copy of the image. Partitions are created on the primary storage device for the recovery agent and image.

Secure Erase cannot be used when Partition-Based Recovery (PBR) is performed, although all partitions are deleted during recovery.

To perform local recovery using the stored image within the device, complete these steps:

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

If the Embedded Reimaging storage device is available, perform local drive recovery from the embedded storage. Otherwise, perform local recovery using Partition-Based Recovery, if available. If the image within either local drive recovery options fails, the system defaults to a network recovery. If both local drive recovery options are unavailable, HP Sure Recover performs the default network recovery.



NOTE: If the system is connected to a network during recovery, the system checks for updates. If an update is found on the network, the update is downloaded, copied to local storage, and used during the recovery. To recover without updating, disconnect from the network before initiating recovery.

Configure a download schedule and use the download agent to check for updates as a background task in Windows. The download agent is included in Cloud Recovery Client and the HP Sure Recover Plug-in for Wolf Security Console. You can also configure the agent in MIK. See <https://www.hp.com/go/clientmanagement> for the instructions to use MIK.

You can create a scheduled task to copy the agent to the SR_AED partition and the image to the SR_IMAGE partition. Before you create the schedule task, download the HP Cloud Recovery Client for Business PCs softpaq and extract `cloudrecovery.exe` from it. Then create a scheduled task with the `CloudRecovery.exe /s /u /c` action and a weekly trigger. If you are using Embedded Reimaging, you can use the HP Client Management Script Library to send a `Invoke-HPSureRecoverTriggerUpdate` command notifying the BIOS to validate the contents and copy to the Embedded Reimaging storage device on the next restart.

Disabling HP Sure Recover

You can enable or disable HP Sure Recover in the BIOS settings or by using the manageability tools. To use Microsoft Windows Recovery for system recovery, you must first disable HP Sure Recover.

1. Turn on the computer, and press **f10** until the HP Computer Setup opens.
2. Use the arrow keys to navigate to the **Advanced** tab.
3. Select **Sure Recover**.
4. Clear the **HP Sure Recover** check box.
5. Navigate to the **Main** tab, and then select **Save Changes** and **Exit**.

2 Creating a corporate image

HP Sure Recover deploys images stored in Windows Imaging (WIM) format, including Split WIM (SWM) files. Split WIM files usually provide more network resilience, and their size can be optimized for the customer's network environment.

Requirements

Before creating a corporate image, be sure to have the requirements listed in this section.

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

Use OpenSSL to generate the RSA key pair used to secure the integrity of the corporate image you create and host.

- A server hosting solution or Azure Blob Service

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 this procedure.

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 4](#)

[Example 2: Creating an image based on a reference system on page 6](#)

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

Use this procedure to create 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 multi-edition image. If you do not want this behavior and do want to ensure that one specific edition is used for all of your target systems, 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, which will be matched based on the BIOS of each target system:

Details for image:my-image.wim

Index: 1

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 the 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 confirm visually which index you 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. 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 or later 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 this page on the Learn / Windows / website: [Add or Remove Packages Offline Using DISM \(in English\)](#)

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

- c. Save the 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 7](#).

Example 2: Creating an image based on a reference system

Use this procedure to create an image based on a reference system.

1. Create bootable USB WinPE media.

 **NOTE:** Additional methods to capture the image can be found in Windows 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.

```
dism /capture-image /imagefile:C:\my-image.wim /capturedir:C: /  
name:"My Custom Image" /description:"Description of my  
image" /compress:max
```

 **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.

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 7](#).

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`

To open a text version of the script example, double-click the following file. Then you can select **OK** to open the file.



NOTE: You might not be able to select this file if you are viewing the PDF within a browser window.

[GenerateManifest.ps1](#)

Create the following script:

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

`$imageVersion = 1907` (Note: This value can be any 16-bit integer, but it must be greater than the previous version. Otherwise, the rollback prevention is disabled.)

```
$header = "mft_version=1, image_version=$imageVersion"
Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header
$swmFiles = Get-ChildItem "." -Filter "*.swm"
$ToNatural = { [regex]::Replace($_, '\d*\....$',
{ $args[0].Value.PadLeft(50) }) }

$spathToManifest = (Resolve-Path ".").Path

$total = $swmFiles.count
$current = 1

$swmFiles | Sort-Object $ToNatural | ForEach-Object {
    Write-Progress
        -Activity "Generating manifest" `
        -Status "$current of $total ($_) " `
        -PercentComplete ($current / $total * 100)

    $hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName
    $fileHash = $hashObject.Hash.ToLower()
    $filePath = $hashObject.Path.Replace($spathToManifest + '\', '')
    $fileSize = (Get-Item $_.FullName).length
    $manifestContent = "$fileHash $filePath $fileSize"

    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
    $manifestContent -Append
```

```
}
    $current = $current + 1
}
```

 **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. Run the script.

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

Generating a manifest signature

HP 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 reverse-formatted order from the format most Windows tools use. You can use any utility to sign manifests, but BIOS versions with that limitation are no longer supported.

To open a text version of the script example, double-click the following file. Then you can select **OK** to open the file.

 **NOTE:** You might not be able to select this file if you are viewing the PDF within a browser window.

[GeneratingManifestSignature.cmd](#)

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
```

- 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 / HTTPS. 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.

You can download the key from <https://support.hp.com>.

Installing the HP Sure Recover agent

Use this procedure to install the HP Sure Recover agent.

1. Download HP Sure Recover agent and extract the files to your HTTP / HTTPS.
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 14](#).

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

 **NOTE:** The distribution point URL includes HTTP or HTTPS 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. Refer to the HP Developers' Blogs for more examples.



NOTE: Several of the commands exceed the line length of this guide but must be entered as a single line. The following script is an example.



IMPORTANT: User names, passwords, and your private keys must never leave your secure PC. Do not distribute them to your clients, and do not depend on the PFX file password. The only part of your certificate that may leave your secure location is the public component of the certificate.

To open a text version of the script example, double-click the following file. Then you can select **OK** to open the file.



NOTE: You might not be able to select this file if you are viewing the PDF within a browser window.

[HPClientManagementScriptLibraryExample.ps1](#)

```
$ErrorActionPreference = "Stop"
$path = 'C:\test_keys'
$ekpw = ""
$skpw = ""
Get-HPSecurePlatformState

try {
    # Provisioning the endorsement key
    Write-host 'Provisioning Endorsement Key'
    $p = New-HPSecurePlatformEndorsementKeyProvisioningPayload
    -EndorsementKeyPassword $ekpw -EndorsementKeyFile "$path\kek.pfx"
    $p | Set-HPSecurePlatformPayload
    Start-Sleep -Seconds 3

    # Provisioning the signing key
    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\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" -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 {
    # Deprovisioning the endorsement key
    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

    # Deprovisioning the signing key
    Write-host 'Deprovisioning P21'
    $p = New-HPSecurePlatformDeprovisioningPayload -verbose
    -EndorsementKeyPassword $pw -EndorsementKeyFile "$Path\kek.pfx"
    $p | Set-HPSecurePlatformPayload

    # Display the final secure platform state
    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.

To open a text version of the script example, double-click the following file. Then you can select **OK** to open the file.



NOTE: You might not be able to select this file if you are viewing the PDF within a browser window.

[KeyGenerationUsingOpenSSL.cmd](#)

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 reverse order from what most Windows tools use, which is incompatible with some BIOS versions, so the agent signature file byte order may need to be reversed before being deployed. BIOS versions with that limitation are no longer supported.

A Troubleshooting

Use this section to troubleshoot issues in HP Sure Recover.

HP Sure Recover uses the HP Cloud Recovery Download Tool in an unattended mode to install the OS. Issues related to OS installation can usually be diagnosed by using the attended mode that is available in the HP Cloud Recovery Download Tool.

Insert a USB drive into the system being recovered to get a detailed log of the recover process. If the recovery is successful, the log will be copied to the `C:\ProgramData\HP\StreamLog\CloudRecovery.exe` folder.

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, the Sure Recover agent might be 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 Firmware 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 p.m. CT on 27 June 2018.



NOTE: These logs follow the US date format of month/date/year. The `event-specific` code is a dword value displayed in `little-endian` order in the last four bytes of each log entry.

HP Secure Platform Management (Source ID = 84h)

You can retrieve the Firmware Audit Log using Get-HPFirmwareAuditLog in the HP Client Management Script Library, available at . HP Secure Platform Management Event IDs 40, 41, and 42 return Event Specific Codes in the data field, which indicate the result of Sure Recover operations.

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

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
```

The BIOS might report the following EFI Event Specific Codes if it is unable to download or start the recovery agent:

Table A-2 EFI Event Specific Codes

Mnemonic	Value	Description
EFI_LOAD_ERROR	1	The image failed to load.
EFI_INVALID_PARAMETER	2	A parameter was incorrect.
EFI_UNSUPPORTED	3	The operation is not supported.
EFI_BAD_BUFFER_SIZE	4	The buffer was not the proper size for the request.
EFI_BUFFER_TOO_SMALL	5	The buffer is not large enough to hold the requested data. The required buffer size is returned in the appropriate parameter when this error occurs.
EFI_NOT_READY	6	There is no data pending upon return.
EFI_DEVICE_ERROR	7	The physical device reported an error while attempting the operation.
EFI_WRITE_PROTECTED	8	The device cannot be written to.
EFI_OUT_OF_RESOURCES	9	A resource has run out.
EFI_VOLUME_CORRUPTED	10	An inconstancy was detected on the file system, causing the operation to fail.
EFI_VOLUME_FULL	11	There is no more space on the file system.
EFI_NO_MEDIA	12	The device does not contain any medium to perform the operation.
EFI_MEDIA_CHANGED	13	The medium in the device has changed since the last access.
EFI_NOT_FOUND	14	The item was not found.
EFI_ACCESS_DENIED	15	Access was denied.
EFI_NO_RESPONSE	16	The server was not found or did not respond to the request.
EFI_NO_MAPPING	17	A mapping to a device does not exist.
EFI_TIMEOUT	18	The timeout time expired.
EFI_NOT_STARTED	19	The protocol has not started.
EFI_ALREADY_STARTED	20	The protocol has already started.

Table A-2 EFI Event Specific Codes (continued)

Mnemonic	Value	Description
EFI_ABORTED	21	The operation was aborted.
EFI_ICMP_ERROR	22	An ICMP error occurred during the network operation.
EFI_TFTP_ERROR	23	A TFTP error occurred during the network operation.
EFI_PROTOCOL_ERROR	24	A protocol error occurred during the network operation.
EFI_INCOMPATIBLE_VERSION	25	The function encountered an internal version that was incompatible with a version requested by the caller.
EFI_SECURITY_VIOLATION	26	The function was not performed due to a security violation.
EFI_CRC_ERROR	27	A CRC error was detected.
EFI_END_OF_MEDIA	28	Beginning or end of media was reached
EFI_END_OF_FILE	31	The end of the file was reached.
EFI_INVALID_LANGUAGE	32	The language specified was invalid.
EFI_COMPROMISED_DATA	33	The security status of the data is unknown or compromised, and the data must be updated or replaced to restore a valid security status.
EFI_HTTP_ERROR	35	An HTTP error occurred during the network operation.

The BIOS might also report the following HP Sure Recover Event Specific Codes:

Table A-3 HP Sure Recover Event Specific Codes

Event Specific Codes
HP_OS_RECOVERY_EMPTY_DOWNLOAD_URL = 0x1
HP_OS_RECOVERY_EMPTY_CONFIG_URL = 0x2
HP_OS_RECOVERY_ERROR_CREATING_RAMDISK = 0x3
HP_OS_RECOVERY_ERROR_DOWNLOADING_FILES = 0x4
HP_OS_RECOVERY_ERROR_BOOTING_SYSTEM = 0x5

Table A-3 HP Sure Recover Event Specific Codes (continued)

Event Specific Codes
HP_OS_RECOVERY_ERROR_DOWNLOAD_URL = 0x6
HP_OS_RECOVERY_ERROR_BAD_MANIFEST_SIG = 0x7
HP_OS_RECOVERY_ERROR_BAD_FILE_HASH = 0x8
HP_OS_RECOVERY_ERROR_SAVING_FILE = 0x9
HP_OS_RECOVERY_ERROR_READING_FILE = 0xA
HP_OS_RECOVERY_ERROR_DOWNLOADING_FILE = 0xB
HP_OS_RECOVERY_ERROR_BAD_FILE_SIZE = 0xC
HP_OS_RECOVERY_ERROR_TIMEOUT_DOWNLOADING_FILE = 0xD
HP_OS_RECOVERY_ERROR_COPYING_FILE = 0xE
HP_OS_RECOVERY_ERROR_NO_VALID_MANIFEST_FOUND = 0xF
HP_OS_RECOVERY_ERROR_NO_RECOVERY_SOURCE = 0x10
HP_OS_RECOVERY_ERROR_LOCAL_RECOVERY_FAILED = 0x11
HP_OS_RECOVERY_ERROR_TOO_MANY_FAILED_DOWNLOADS = 0x12

If the agent starts, it might return the following event-specific codes:

Table A-4 Event-Specific Codes

Event Description	Event Code
AgentFtpHttpDownloadFailed	0xC3F60300
AgentFtpHttpDownloadHashFailed	0xC3F60100
AgentManifestDoesNotAuthenticate	0xC3F6B000
AgentManifestFileEmptyOrInvalid	0xC3F6C000
AgentMftOrSignatureDownloadFailed	0xC3F6A000
AgentSpaceMismatch	0xC3F60900
AwsDownloadFailed	0xC3F15000
AwsDownloadUnattendedFailed	0xC3F16000
BcdbootFailed	0xC3F55000
CatalogDownloadFailed	0xC3F11000
CatalogLoadFailed	0xC3F32000
CatalogNotAuthenticated	0xC3F21000
CatalogVersionMismatch	0xC3F31000
DiskLayoutCreationFailed	0xC3F58000
DownloadAgentShouldNotRun	0xC3F61000
DriversDvdDidNotResolvedToOneComponent	0xC3F34000
FailedToApplyWimImage	0xC3F52000

Table A-4 Event-Specific Codes (continued)

Event Description	Event Code
FailedToCreateDismProcess	0xC3F54000
FailedToCreateServiceEvent	0xC3F67000
FailedToDetectWindowsPE	0xC3FF5000
FailedToInstallDrivers	0xC3F51000
FailedToRegisterWimCallback	0xC3F53000
FtpHttpDownloadFailed	0xC3F14000
FtpHttpDownloadHashFailed	0xC3F22000
ImageFtpHttpDownloadFailed	0xC3F60400
ImageFtpHttpDownloadHashFailed	0xC3F60200
ImageManifestDoesNotAuthenticate	0xC3F6B100
ImageManifestFileEmptyOrInvalid	0xC3F6C100
ImageMftOrSignatureDownloadFailed	0xC3F6A100
ImageSpaceMismatch	0xC3F60800
InvalidAgentUrlConfiguration	0xC3F60700
InvalidCustomImageUrlConfiguration	0xC3F60600
ListedFileInAgentManifestNotFound	0xC3F6D000
ListedFileInImageManifestNotFound	0xC3F6D100
ListedFileInManifestNotFound	0xC3F42000
ManifestDoesNotAuthenticate	0xC3F23000
ManifestFileEmptyOrInvalid	0xC3F41000
MftOrSigDownloadFailed	0xC3F13000
ModelNotResolved	0xC3F36000
NoSuitableDiskFound	0xC3F56000
OsDvdDidNotResolvedToOneComponent	0xC3F33000
OsNotResolved	0xC3F35000
PartitioningFailed	0xC3F57000
RebootRequestFailed	0xC3FF3000
RecoveryAgentPublicKeyNotProvisioned	0xC3F64000
RecoveryAgentUrlNotProvisioned	0xC3F63000
RecoveryImagePublicKeyNotProvisioned	0xC3F60000
RecoveryImageUrlNotProvisioned	0xC3F69000
RegionNotResolved	0xC3F37000
SignatureDownloadFailed	0xC3F12000
SrAedFormatError	0xC3F65000

Table A-4 Event-Specific Codes (continued)

Event Description	Event Code
SrAedManifestCopyFailed	0xC3F66000
SrAedPartitionNotAvailable	0xC3F62000
SrImageCatalogCopyFailed	0xC3F60500
SrImageFormatError	0xC3F6E000
SrImageManifestCopyFailed	0xC3F6F000
SrImagePartitionNotAvailable	0xC3F68000
SureRecoverJsonParsingFailed	0xC3FF2000
UnableToConnectToNetwork	0xC3F17000
UnableToReadConfigFile	0xC3FF4000
UnexpectedProblemWithConfigJson	0xC3FF1000

HP Sure Recover download event log

When HP Sure Recover is running in download mode (`CloudRecovery.exe /u /c`), via command line or through Task Scheduler, it logs download events such as "HP Sure Recover: Download of [HP recovery image | custom image | recovery agent] [started | completed | failed]" in the event viewer at Applications and Services Logs\ HP Sure Recover path.

Enable Toast notification

Install the `HPCloudRecovery.msi` using **CreateDownloadMode** (`msimode=1`) `msiexec.exe /i "<PathToMsi>\HPCloudRecovery.msi" msimode=1`

Determine whether the Task Scheduler event logging is enabled:

1. Open the Event Viewer application.
2. Go to the Applications and Services Logs\Microsoft\Windows\TaskScheduler\Operational path.
3. Right-click **Operational**.
4. Select **Enable Log**.
5. Restart the machine.

The next time the download task is scheduled, a toast notification will be shown at the bottom of the screen.