



# Manuel de l'utilisateur

HP Sure Recover

© Copyright 2020 HP Development Company,  
L.P.

Microsoft et Windows sont des marques  
commerciales déposées ou des marques  
commerciales de Microsoft Corporation aux  
États-Unis et/ou dans d'autres pays.

Logiciel d'ordinateur confidentiel. Une licence  
HP est requise pour la possession, l'utilisation  
ou la copie. En accord avec les articles FAR  
12.211 et 12.212, les logiciels informatiques,  
la documentation des logiciels et les  
informations techniques commerciales sont  
concedés au gouvernement américain sous  
licence commerciale du distributeur.

Les informations contenues dans ce document  
peuvent être modifiées sans préavis. Les  
garanties relatives aux produits et aux services  
HP sont décrites dans les déclarations de  
garantie limitée expresse qui les  
accompagnent. Aucun élément du présent  
document ne peut être interprété comme  
constituant une garantie supplémentaire. HP  
ne saurait être tenu pour responsable des  
erreurs ou omissions de nature technique ou  
rédactionnelle qui pourraient subsister dans le  
présent document.

Première édition : février 2020

Numéro de référence du document :  
L93434-051

## Clé de syntaxe du langage d'entrée utilisateur

Le texte que vous devez entrer dans une interface utilisateur est indiqué par `Police à espacement fixe`.

**Tableau -1 Clé de syntaxe du langage d'entrée utilisateur**

Élément	Description
<code>Texte sans crochets ni accolades</code>	Éléments que vous devez saisir exactement comme illustré
<code>&lt;Texte entre chevrons&gt;</code>	Un espace réservé pour une valeur que vous devez fournir ; Omettre les crochets
<code>[Texte entre crochets]</code>	Éléments en option ; Omettre les crochets
<code>{Texte entre accolades}</code>	Un ensemble d'éléments parmi lesquels vous devez en choisir un seul ; Omettre les accolades
<code> </code>	Un séparateur d'éléments parmi lesquels vous devez en choisir un seul ; Omettre la barre verticale
<code>...</code>	Éléments qui peuvent ou doivent être répétés ; Omettre les points de suspension



---

# Sommaire

<b>1 Mise en route .....</b>	<b>1</b>
Exécution d'une récupération réseau .....	1
Exécution d'une récupération du disque local .....	1
<b>2 Création d'une image corporative .....</b>	<b>3</b>
Exigences .....	3
Création de l'image .....	3
Exemple 1 : Création d'une image en fonction de l'image d'installation de Microsoft Windows .....	3
Exemple 2 : Création d'une image basée sur un système de référence .....	6
Fractionnement de l'image .....	6
Création d'un manifeste .....	6
Génération d'un manifeste .....	7
Génération d'une signature manifeste .....	8
Hébergement des fichiers .....	9
Configuration de vos systèmes cibles .....	9
Résolution des problèmes .....	9
<b>3 Utilisation de l'agent HP Sure Recover au sein d'un pare-feu d'entreprise .....</b>	<b>11</b>
Installation de l'agent HP Sure Recover .....	11
<b>4 Utilisation de la bibliothèque de scripts HP Client Management (CML) .....</b>	<b>13</b>
Exemple de génération de clé avec OpenSSL .....	15
<b>Annexe A Résolution des problèmes .....</b>	<b>17</b>
Échec du partitionnement du disque .....	17
Journal d'audit du microprogramme .....	17
Journal d'événements Windows .....	17
HP Secure Platform Management (ID source = 84h) .....	17



# 1 Mise en route

HP Sure Recover vous permet d'installer le système d'exploitation en toute sécurité à partir du réseau avec une interaction minimale de l'utilisateur. Les systèmes dotés de HP Sure Recover avec génération d'images Embedded prennent également en charge l'installation à partir d'un périphérique de stockage local.



**IMPORTANT :** Sauvegardez vos données avant d'utiliser HP Sure Recover. Étant donné que le processus de génération d'images reformate le disque, une perte de données se produit.

Les images de récupération qu'offre HP incluent le programme d'installation de base de Windows 10®. En option, HP Sure Recover peut installer des pilotes optimisés pour les appareils HP. Les images de récupération HP incluent uniquement les agents de récupération des données qui sont inclus avec Windows 10, comme OneDrive. Les entreprises peuvent créer leurs propres images personnalisées pour ajouter des paramètres d'entreprise, des applications, des pilotes et des agents de récupération des données.

Un agent de récupération du système d'exploitation (SE) effectue les étapes nécessaires pour installer l'image de récupération. L'agent de récupération fourni par HP effectue des opérations courantes comme le partitionnement, le formatage et l'extraction de l'image de récupération vers le périphérique cible. Étant donné que l'agent HP Recovery est situé sur hp.com, vous avez besoin d'un accès à Internet pour le récupérer, à moins que le système ne comprenne une génération d'images intégrée. Les sociétés peuvent également héberger l'agent HP Recovery dans leur pare-feu ou créer des agents de récupération personnalisés pour des environnements de récupération plus complexes.

Vous pouvez activer HP Sure Recover lorsqu'aucun système d'exploitation n'est trouvé. Vous pouvez également exécuter HP Sure Recover sur une planification, par exemple pour vous assurer que les logiciels malveillants sont supprimés. Effectuez la configuration de ces paramètres via HP Client Security Manager (CSM), Manageability Integration Kit (MIK) ou la bibliothèque de scripts de HP Client Management.

## Exécution d'une récupération réseau



**REMARQUE :** Pour effectuer une récupération réseau, vous devez utiliser une connexion filaire. HP recommande de sauvegarder les fichiers, données, photos, vidéos, etc. importants avant d'utiliser HP Sure Recover afin d'éviter toute perte de données.

1. Connectez le système client au réseau sur lequel le point de distribution HTTP ou FTP est accessible.
2. Redémarrez le système client, et lorsque le logo HP apparaît, appuyez sur la touche **F11**.
3. Sélectionnez **Restaurer à partir du réseau**.

## Exécution d'une récupération du disque local

Si un système client prend en charge la génération d'images intégrée et que l'option de téléchargement de l'image programmée est activée dans la stratégie appliquée, l'image est alors téléchargée sur le système client à l'heure prévue. Une fois l'image téléchargée sur le système client, redémarrez pour copier l'image sur le périphérique de stockage de génération d'images intégrée.

Pour effectuer une récupération locale à l'aide de l'image sur le périphérique de stockage de génération d'images intégrée :

1. Redémarrez le système client, et lorsque le logo HP apparaît, appuyez sur la touche **F11**.
2. Sélectionnez **Restaurer depuis un disque local**.

Les systèmes dotés de la régénération intégrée doivent configurer une planification de téléchargement et utiliser l'agent de téléchargement pour rechercher des mises à jour. L'agent de téléchargement est inclus dans l'extension HP Sure Recover pour HP Client Security Manager et peut également être configuré dans MIK. Reportez-vous à <https://www.hp.com/go/clientmanagement> pour obtenir les instructions d'utilisation de MIK.

Vous pouvez également créer une tâche planifiée pour copier l'agent sur la partition SR\_AED et l'image sur la partition SR\_IMAGE. Vous pouvez ensuite utiliser la bibliothèque de scripts de HP Client Management pour envoyer un événement de service informant le BIOS afin qu'il valide le contenu et copie sur le périphérique de stockage de génération d'images intégrée lors du prochain redémarrage.



## 2 Création d'une image corporative

La plupart des entreprises utilisent les outils de déploiement Microsoft, le kit d'évaluation et de déploiement de Windows 10 ou les deux, pour produire des fichiers contenant une image dans une archive de format de fichier WIM (Windows Imaging).

### Exigences

- La dernière version du kit de déploiement et d'évaluation Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (ou autre solution pour générer une paire de clés privée/publique RSA)  
Utilisez-le pour générer la paire de clés RSA utilisée pour sécuriser l'intégrité de l'image corporative que vous créez et hébergez.
- Une solution d'hébergement de serveur (par exemple, Microsoft Internet Information Services [IIS])

### Création de l'image

Avant de démarrer le processus de création d'images, configurez le système de travail ou le système de génération où vous avez installé les outils nécessaires pour préparer le traitement de l'image, comme indiqué dans les étapes suivantes :

1. En tant qu'administrateur, ouvrez l'invite de commande `Environnement de déploiement et d'outils de création d'images` (installé avec les outils de déploiement de Windows ADK).
2. Créez une zone de réserve pour votre image, à l'aide de la commande suivante :

```
mkdir C:\staging
```

3. Créez l'image à l'aide de l'un des exemples suivants :

[Exemple 1 : Création d'une image en fonction de l'image d'installation de Microsoft Windows à la page 3](#)

[Exemple 2 : Création d'une image basée sur un système de référence à la page 6](#)

### Exemple 1 : Création d'une image en fonction de l'image d'installation de Microsoft Windows

1. Montez ou ouvrez l'image d'installation de Microsoft Windows (à partir d'un ISO Microsoft ou d'un OSDVD HP).
2. À partir de l'image d'installation Windows montée, copiez le fichier `install.wim` vers votre zone de réserve, à l'aide de la commande suivante :

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



**REMARQUE :** <M:> fait référence au lecteur monté. Remplacez par la lettre de lecteur correcte.

3. Renommez `install.wim` en un nom de fichier image ("`my-image`" pour cet exemple), à l'aide de la commande suivante :

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

En option, HP Sure Recover comprend une fonction qui permet de récupérer une édition spécifique à partir d'une image multi-index, basée sur l'édition Windows qui a été attribuée à l'origine pour le système cible HP en usine. Ce mécanisme fonctionne si les index sont nommés correctement. Si votre image d'installation Windows provient d'une image OSDVD HP, vous avez probablement une image multiédition. Si vous ne souhaitez pas ce comportement et voulez vous assurer qu'une édition spécifique est utilisée pour tous vos systèmes cibles, vous devez être sûr qu'un seul index se trouve dans l'image d'installation.

4. Vérifiez le contenu de l'image d'installation à l'aide de la commande suivante :

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

L'exemple suivant montre la sortie d'exemple d'une image d'installation prenant en charge cinq éditions (à jumeler en fonction du BIOS de chaque système cible) :

Détails pour l'image : `my-image.wim`

Index : 1

Nom : `CoreSingleLanguage`

Description : `Mise à jour Windows 10 mai 2019 - Édition familiale langue unique`

Taille : `19 512 500 682 octets`

Index : 2

Nom : `Noyau`

Description : `Mise à jour Windows 10 mai 2019 - Édition familiale`

Taille : `19 512 500 682 octets`

Index : 3

Nom : `Professionnels`

Description : `Mise à jour Windows 10 mai 2019 - Mise à jour professionnelle`

Taille : `19 758 019 520 octets`

Index : 4

Nom : `Formation professionnelle`

Description : `Mise à jour Windows 10 mai 2019 - Édition formation professionnelle`

Taille : `19 758 019 480 octets`

Index : 5

Nom : `Station de travail professionnelle`

**Description:** Mise à jour Windows 10 mai 2019 – Mise à jour station de travail professionnelle

**Taille:** 19 758 023 576 octets



**REMARQUE :** Lorsqu'il n'y a qu'un seul index, l'image est utilisée pour la récupération, quel que soit le nom. La taille de votre fichier d'image peut être supérieure après les suppressions.

5. Si vous ne souhaitez pas le comportement de la multiédition, supprimez chaque index que vous ne voulez pas.

Comme indiqué dans l'exemple suivant, si vous souhaitez uniquement une édition professionnelle (en supposant que tous les systèmes cibles sont sous licence), supprimez les index 5, 4, 2 et 1. Chaque fois que vous supprimez un index, les numéros d'index sont réaffectés. Par conséquent, vous devez supprimer les numéros d'index des plus hauts vers les plus bas. Exécutez `Get-ImageInfo` après chaque suppression pour confirmer visuellement l'index que vous allez supprimer ensuite.

```
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
```

Choisissez un seul index de l'édition (pour cet exemple, Professionnel). Lorsqu'il n'y a qu'un seul index, l'image est utilisée pour la récupération, quel que soit le nom. Notez que la taille de votre fichier d'image peut être supérieure à celle d'avant les suppressions, en raison de la manière dont les modifications de métadonnées WIM et la normalisation du contenu fonctionnent.

6. En option, si vous souhaitez inclure des pilotes dans l'image de récupération de votre entreprise, procédez comme suit :

- a. Montez votre image dans un dossier vide, à l'aide des commandes suivantes :

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

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

- b. Montez le DVD pilote HP Windows 10 (DRDVD) approprié pour le système cible pris en charge. À partir du support de pilotes monté, copiez les sous-dossiers pilotes vers votre zone de réserve, à l'aide de la commande suivante :

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



**REMARQUE :** <M:> fait référence au lecteur monté. Remplacez par la lettre de lecteur correcte.

Vous pouvez inclure d'autres pilotes .inf-style en les plaçant dans le dossier `C:\staging\mount\SWSETUP\DRV`. Pour obtenir une explication sur la manière dont ce contenu est traité par HP Sure Recover à l'aide de la fonction `dism /Add-Driver /Recurse`, reportez-vous à la section « Ajout et suppression de pilotes à une image Windows hors ligne » dans la rubrique suivante : <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

Cette fonction ne prend pas en charge les pilotes .exe-style qui nécessitent l'exécution d'une application.

- c. Enregistrez les modifications et démontez votre image, à l'aide de la commande suivante :

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

Le fichier d'image résultant est le suivant : C:\staging\my-image.wim.

- d. Ouvrez la page [Fractionnement de l'image à la page 6](#).

## Exemple 2 : Création d'une image basée sur un système de référence

1. Créez un support USB WinPE amorçable.

 **REMARQUE :** Des méthodes supplémentaires pour capturer l'image sont disponibles dans la documentation ADK.

Assurez-vous que le lecteur USB possède suffisamment d'espace libre pour contenir l'image capturée du système de référence.

2. Créez une image sur un système de référence.
3. Capturez l'image en démarrant le système de référence à l'aide du support USB WinPE, puis utilisez DISM.

 **REMARQUE :** <U:> fait référence au lecteur USB. Remplacez par la lettre de lecteur correcte.

Modifiez la partie "my-image" du nom de fichier et la description <my-image>, si nécessaire.

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

4. Copiez l'image de l'USB vers la zone de réserve sur votre système de travail à l'aide de la commande suivante :

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

Vous devez disposer du fichier image suivant : C:\staging\my-image.wim.


5. Ouvrez la page [Fractionnement de l'image à la page 6](#).

## Fractionnement de l'image

HP vous recommande de fractionner l'image en fichiers plus petits afin d'améliorer la fiabilité des téléchargements réseau, à l'aide de la commande suivante :

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

 **REMARQUE :** La taille du fichier est affichée en méga-octets. Modifiez si nécessaire.

 **REMARQUE :** En raison de la nature de l'algorithme de fractionnement DISM, la taille des fichiers SWM générés peut être inférieure ou supérieure à la taille du fichier indiquée.

## Création d'un manifeste

Formatez les fichiers manifeste en tant qu'UTF-8 sans BOM (Byte Order Mark).

Vous pouvez modifier le nom du fichier manifeste (custom.mft) utilisé dans les procédures suivantes, mais vous ne devez pas modifier les extensions .mft et .sig, et la partie du nom de fichier du manifeste et les fichiers de signature doivent correspondre. Par exemple, vous pouvez modifier la paire (custom.mft, custom.sig) en (myimage.mft, myimage.sig).

mft\_version est utilisé pour déterminer le format du fichier image et doit actuellement être défini sur 1.

`image_version` sert à déterminer si une version plus récente de l'image est disponible et à empêcher l'installation d'anciennes versions.

Les deux valeurs doivent être des nombres entiers 16 bits non signés et le séparateur de ligne dans le manifeste doit être `\r\n` (CR + LF).

## Génération d'un manifeste

Dans la mesure où plusieurs fichiers peuvent être associés à votre image fractionnée, utilisez un script PowerShell pour générer un manifeste.

Dans toutes les étapes restantes, vous devez vous trouver dans le dossier `C:\staging`.

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

1. Créez un script PowerShell à l'aide d'un éditeur qui peut produire un fichier texte au format UTF-8 sans BOM, à l'aide de la commande suivante : `notepad C:\staging\generate-manifest.ps1`

Créez le script suivant :

```
$mftFilename = "custom.mft"

$imageVersion = 1907 (Remarque : Il peut s'agir d'un nombre entier 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
}
```

 **REMARQUE :** Les manifestes pour HP Sure Recover ne peuvent pas inclure un BOM, donc les commandes suivantes réécrivent le fichier en UTF8 sans BOM.

```
$content = Get-Content $mftFilename

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

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

2. Enregistrez le script.

3. Exécutez le script.

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

## Génération d'une signature manifeste

Sure Recover valide l'agent et l'image à l'aide de signatures cryptographiques. Les exemples suivants utilisent une paire de clés privée/publique au format X.509 PEM (Extension .PEM). Réglez les commandes selon les besoins pour utiliser les certificats binaires DER (Extension .CER ou .CRT), certificats PEM codés sur la BASE 64 (Extension .CER ou .CRT) ou les fichiers PKCS1 PEM (Extension .PEM). L'exemple utilise également OpenSSL, qui génère des signatures au format big-endian. Vous pouvez utiliser n'importe quel utilitaire pour signer des manifestes, mais certaines versions du BIOS prennent uniquement en charge les signatures au format little-endian.

1. Générez une clé privée RSA 2048 bits à l'aide de la commande suivante. Si vous possédez une paire de clés privée/publique RSA 2048 bits au format PEM, copiez-les sur C:\staging, puis passez à l'étape 3.

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

2. Générez la clé publique à partir de votre clé privée (si vous disposez d'une clé publique correspondant à votre clé privée au format PEM, copiez-la sur C:\staging), à l'aide de la commande suivante :

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

3. Créez un fichier de signature (à l'aide du hachage basé sur sha256) en fonction de votre clé privée RSA 2048 bits de l'étape 1, à l'aide de la commande suivante :

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

4. Vérifiez le fichier de signature à l'aide de votre clé publique de l'étape précédente, à l'aide de la commande suivante :

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

**REMARQUE :**

- Si vous avez besoin de créer un fichier de signature uniquement, les étapes requises sont les 1 et 3.
- Pour HP Sure Recover, les étapes minimales requises sont les 1, 2 et 3. Vous avez besoin de la clé publique de l'étape 2 pour configurer votre système cible.
- L'étape 4 est facultative mais recommandée afin que votre fichier de signature et fichier manifeste se valident correctement.

## Hébergement des fichiers

Hébergez les fichiers suivants sur votre serveur à partir du dossier C:\staging :

- \*.swm
- custom.mft (ou le nom de fichier que vous avez choisi pour le fichier manifeste)
- custom.sig (ou le nom de fichier correspondant que vous avez choisi pour le fichier de signature)



**REMARQUE :** Si vous utilisez IIS comme solution d'hébergement, vous devez configurer vos entrées MIME pour inclure les extensions suivantes, toutes configurées en tant que "application/octet-stream:"

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

## Configuration de vos systèmes cibles

Vous pouvez configurer vos systèmes cibles à l'aide de la bibliothèque de scripts de HP Client Management, de HP Client Security Manager (CSM)/Sure Recover ou du Manageability Integration Kit (MIK) (<https://www.hp.com/go/clientmanagement>).

Fournissez les informations suivantes pour cette configuration :

1. L'adresse URL du fichier manifeste hébergé de la section précédente ([http://your\\_server.domain/path/custom.mft](http://your_server.domain/path/custom.mft))
2. La clé publique utilisée pour vérifier le fichier de signature créé précédemment (par exemple, C:\staging\my-recovery-public.pem).

## Résolution des problèmes

Si vous recevez un message sur la validation de sécurité en cas d'échec du processus de récupération personnalisé, vérifiez les éléments suivants :

1. Le manifeste doit être en UTF-8 sans BOM.
2. Vérifiez les hachages de fichiers.
3. Assurez-vous que le système a été configuré avec la clé publique correspondant à la clé privée utilisée pour signer le manifeste.

4. Les types MIME Server IIS doivent être `application/octet-stream`.
5. Les chemins d'accès au fichier dans le manifeste doivent inclure le chemin d'accès complet au répertoire tout en haut contenant l'image, tel qu'il est vu à partir d'un système client. Ce chemin d'accès n'est pas le chemin d'accès complet où les fichiers sont enregistrés au point de distribution.




### 3 Utilisation de l'agent HP Sure Recover au sein d'un pare-feu d'entreprise

L'agent HP Sure Recover peut être hébergé sur un intranet d'entreprise. Après l'installation du SoftPaq HP Sure Recover, copiez les fichiers de l'agent à partir du répertoire de l'agent HP Sure Recover à partir de l'emplacement d'installation vers un point de distribution HTTP ou FTP. Ensuite, configurez le système client avec l'URL du point de distribution et la clé publique HP nommée `hpsr_agent_public_key.pem`, qui est distribuée avec le SoftPaq de l'agent HP Sure Recover.


#### Installation de l'agent HP Sure Recover

1. Téléchargez l'agent HP Sure Recover et extrayez les fichiers vers le point de distribution HTTP ou FTP.
2. Définissez les permissions de fichiers appropriées sur le point de distribution.
3. Si vous utilisez IIS (Internet Information Services), créez des types MIME application/octet-stream pour les formats de fichiers suivants :

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

 **IMPORTANT :** Les étapes suivantes décrivent la configuration de Sure Recover avec SCCM. Reportez-vous à la section [Utilisation de la bibliothèque de scripts HP Client Management \(CMSL\)](#) à la page 13 pour obtenir des exemples sur la manière de configurer Sure Recover avec la bibliothèque de scripts HP Client Management.

4. Démarrez SCCM, accédez à **HP Client Security Suite**, puis sélectionnez la page HP Sure Recover.

 **REMARQUE :** L'URL du point de distribution comprend soit FTP soit HTTP comme protocole de transport. Il inclut également le chemin d'accès complet au répertoire tout au haut contenant le manifeste pour l'agent HP Sure Recover, tel qu'il est vu à partir d'un système client. Ce chemin d'accès n'est pas le chemin d'accès complet où les fichiers sont enregistrés au point de distribution.

5. Dans la section **Image plate-forme**, sélectionnez l'option **Entreprise** pour restaurer une image du système d'exploitation personnalisée à partir d'un point de distribution d'entreprise. Entrez l'URL fournie par l'administrateur informatique dans la zone de saisie **URL de l'emplacement de l'image**. Entrez la clé publique `hpsr_agent_public_key.pem` dans le champ **Vérification de l'image**.

 **REMARQUE :** L'URL de l'image personnalisée doit inclure le nom du fichier de manifeste de l'image.

6. Dans la section **Agent de récupération**, sélectionnez l'option **Entreprise** pour utiliser un agent de récupération personnalisé ou l'agent HP Recovery à partir d'un point de distribution d'entreprise. Entrez

l'URL fournie par l'administrateur informatique dans la zone de saisie **URL d'emplacement de l'agent**. Entrez la clé publique `hpsr_agent_public_key.pem` dans le champ de saisie **Clé de vérification de l'agent**.



**REMARQUE :** N'incluez pas le nom de fichier du manifeste de l'agent dans l'URL car le BIOS exige qu'il soit nommé `recovery.mft`.

7. Une fois que la stratégie est appliquée au système client, redémarrez-le.
8. Lors de la configuration initiale, une invite apparaît pour vous demander de saisir un code de sécurité à 4 chiffres pour terminer l'activation de HP Sure Recover. Pour plus d'informations, rendez-vous sur [hp.com](http://hp.com) et recherchez le HP Manageability Integration Kit (MIK) pour le livre blanc de Microsoft System Center Manager.

Une fois l'activation de HP Sure Recover terminée avec succès, l'URL personnalisée appliquée par la stratégie est affichée dans le menu des paramètres du BIOS de HP Sure Recover.

Pour confirmer la réussite de l'activation, redémarrez l'ordinateur, puis lorsque le logo HP apparaît, appuyez sur la touche **F10**. Sélectionnez **Avancé**, sélectionnez **HP Sure Recover**, sélectionnez **Agent de récupération**, puis sélectionnez **URL**.

## 4 Utilisation de la bibliothèque de scripts HP Client Management (CMSL)

La bibliothèque de scripts HP Client Management vous permet de gérer les paramètres de HP Sure Recover avec PowerShell. L'exemple de script suivant montre comment configurer, déterminer l'état, modifier la configuration et annuler HP Sure Recover.

 **REMARQUE :** Plusieurs commandes dépassent la longueur de ligne de ce guide mais doivent être saisies comme une seule ligne.

```
$ErrorActionPreference = "Stop"

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

Get-HPSecurePlatformState

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

    Start-Sleep -Seconds 3

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

```

    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image OS `
        -ImageKeyFile "$path\os.pfx" `
        -username test -password test `
        -url "http://www.hp.com/custom/image.mft"
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image agent `
        -ImageKeyFile "$path\re.pfx" `
        -username test -password test `
        -url "http://www.hp.com/pub/pcbios/CPR"
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverSchedulePayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -DayOfWeek Sunday,EveryWeek -Hour 13 -Minute 27 -WindowSize 30
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -OSImageFlags NetworkBasedRecovery `
        -AgentFlags DRDVD
    $p | Set-HPSecurePlatformPayload

    Get-HPSureRecoverState -all
    Get-HPSecurePlatformState
}
finally {

```

```

Write-Host 'Deprovisioning Sure Recover'
Start-Sleep -Seconds 3
$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
}

```

## Exemple de génération de clé avec OpenSSL

Stockez les clés privées dans un endroit sûr. Les clés publiques seront utilisées pour la validation et doivent être fournies lors de la configuration. Ces clés doivent être d'une longueur de 2048 bits et utiliser un exposant de 0x10001. Remplacez le sujet dans les exemples par des informations sur votre entreprise.

Définissez la variable d'environnement suivante avant de continuer :

```

set OPENSSL_CONF=<path>\openssl.cnf

# Créer un certificat d'autorité de certification racine auto-signé pour le test
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"

# Créer un certificat d'endossement de clé
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:

# Créer une commande clé de signature

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:

# Créer une clé de signature d'image

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:

```

**Vous pouvez signer le manifeste d'image avec cette commande :**

```
openssl dgst -sha256 -sign os.key -out image.sig image.mft
```

```

# Créer une clé de signature d'agent

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:

```

**Vous pouvez signer le manifeste de l'agent à l'aide de cette commande :**

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

OpenSSL génère des fichiers de signature au format big-endian, ce qui est incompatible avec certaines versions du BIOS, de sorte que l'ordre des octets du fichier de signature de l'agent doit être inversé avant d'être déployé. Les versions du BIOS prenant en charge l'ordre des octets big-endian prennent également en charge l'ordre des octets little-endian.

# A Résolution des problèmes

## Échec du partitionnement du disque

Un échec de partitionnement du disque peut se produire si la partition SR\_AED ou SR\_IMAGE est cryptée avec Bitlocker. Ces partitions sont normalement créées avec un attribut gpt qui empêche Bitlocker de les chiffrer, mais si un utilisateur supprime et recrée les partitions ou les crée manuellement sur un disque complet, alors l'agent Sure Recover ne peut pas les supprimer et les quitte avec une erreur lors du repartitionnement du disque. L'utilisateur doit les supprimer manuellement en exécutant DiskPart, en sélectionnant le volume et en émettant la commande de remplacement `Suppr vol` ou une commande similaire.

## Journal d'audit du microprogramme

Les informations de variable EFI sont les suivantes :

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

Les API existent sous Windows pour lire les variables EFI ou vous pouvez déverser du contenu de variable dans un fichier à l'aide de l'utilitaire UEFI Shell `dmpstore`.

Vous pouvez vider le journal d'audit à l'aide de la commande `Get-HPFirmwareAuditLog` fournie par la bibliothèque de scripts de HP Client Management.

## Journal d'événements Windows

Les événements de démarrage et d'arrêt de Sure Recover sont envoyés au journal d'audit du BIOS, que vous pouvez afficher dans l'observateur d'événements Windows dans le journal Sure Start si les notifications HP sont installées. Ces événements comprennent la date et l'heure, l'identifiant source, l'identifiant de l'événement et un code spécifique à l'événement. Par exemple, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indique que la récupération a échoué car le manifeste n'a pas pu être authentifié avec le code spécifique à l'événement `c3f 23000` qui a été enregistré à 2:26:40 le 6/27/18.



**REMARQUE :** Ces journaux sont au format de date américain mois/date/année.

## HP Secure Platform Management (ID source = 84h)

Tableau A-1 HP Secure Platform Management

ID de l'événement	Nombre d'appareils (Tous/DaaS)	Nombre d'événements (Tous/DaaS)	Description	Remarques
40	256/178	943/552	Le processus de récupération du système d'exploitation de la plateforme a été démarré par le microprogramme.	Récupération de la plateforme commencée

**Tableau A-1 HP Secure Platform Management (suite)**

ID de l'événement	Nombre d'appareils (Tous/DaaS)	Nombre d'événements (Tous/DaaS)	Description	Remarques
41	221/147	588/332	Le processus de récupération du système d'exploitation de la plate-forme s'est terminé avec succès.	Récupération de la plate-forme terminée
42	54/42	252/156	Le processus de récupération du système d'exploitation de la plateforme n'a pas abouti.	La récupération de la plateforme a échoué

Vous pouvez récupérer le journal d'audit des microprogrammes à l'aide de Get-HPFirmwareAuditLog dans la bibliothèque de script de HP Client Management, disponible à l'adresse <http://www.hp.com/go/clientmanagement>. Les ID d'événement 40, 41 et 42 de HP Secure Platform Management renvoient des codes spécifiques à l'événement dans le champ de données, qui indiquent le résultat des opérations Sure Recover. Par exemple, l'entrée du journal suivante indique que Sure Recover n'a pas pu télécharger le manifeste ou le fichier de signature avec l'erreur event\_id 42 et les données : 00:30:f1:c3, qui doit être interprété comme la valeur 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: Le processus de récupération du système d'exploitation de la
plateforme n'a pas abouti.
data: 00:30:f1:c3
```

Une récupération réussie est indiquée comme event\_id = 41 et data: 00:00:00:00, par exemple :

```
Codes spécifiques à l'événement
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: Le processus de récupération du système d'exploitation de la plateforme n'a pas abouti.

data: 00:00:00:00

HP Sure Recover utilise les codes spécifiques à l'événement suivants.

**Tableau A-2 Codes spécifiques à l'événement**

Description de l'événement	Code d'événement
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