



Manual do Utilizador

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

Microsoft e Windows são marcas comerciais ou marcas comerciais registadas da Microsoft Corporation nos Estados Unidos e/ou noutros países.

Software informático confidencial. Licença válida da HP necessária para posse, utilização ou cópia. De acordo com a FAR 12.211 e 12.212, o Software Informático Comercial, a Documentação do Software Informático e os Dados Técnicos de Itens Comerciais são licenciados ao Governo dos EUA segundo a licença comercial padrão do fornecedor.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. As únicas garantias que cobrem os produtos e serviços da HP são estabelecidas exclusivamente na documentação de garantia que os acompanha. Neste documento, nenhuma declaração deverá ser interpretada como a constituição de garantia adicional. A HP não se responsabiliza por erros técnicos e editoriais ou omissões neste documento.

Primeira edição: fevereiro de 2020

Número de publicação do documento:
L93434-131

Chave de sintaxe de entrada do utilizador

O texto que tem de introduzir numa interface de utilizador é indicado por um tipo de letra de largura fixa.

Tabela -1 Chave de sintaxe de entrada do utilizador


Item	Descrição
Texto sem parênteses ou chavetas	Itens que tem de digitar exatamente como mostrado
<Texto no interior de parênteses angulares>	Um marcador de posição para um valor que tem de fornecer; omitir os parênteses
[Texto no interior de parênteses retos]	Itens opcionais; omitir os parênteses
{Texto no interior de chavetas}	Um conjunto de itens dos quais tem de escolher apenas um; omitir as chavetas
	Um separador para os itens dos quais tem de escolher apenas um; omitir a barra vertical
...	Os itens que podem ou devem ser repetidos; omitir as reticências

Índice

1 Introdução	1
Executar uma recuperação de rede	1
Realizar a recuperação de uma unidade local	1
2 Criar uma imagem da empresa	3
Requisitos	3
Criar a imagem	3
Exemplo 1: Criar uma imagem com base na imagem de instalação do Microsoft Windows	3
Exemplo 2: Criação de uma imagem baseada num sistema de referência	5
Dividir a imagem	6
Criar um manifesto	6
Gerar um manifesto	7
Gerar a assinatura do manifesto	8
Alojar os ficheiros	9
Aprovisionar os sistemas de destino	9
Deteção e resolução de problemas	9
3 Utilizar o agente HP Sure Recover dentro de um firewall da empresa	10
Instalar o agente HP Sure Recover	10
4 Trabalhar com a HP Client Management Script Library (CMSL)	12
Gerar chave de exemplo utilizando o OpenSSL	14
Apêndice A Deteção e resolução de problemas	16
Falha de criação de partições da unidade	16
Registo de auditoria de firmware	16
Registo de eventos do Windows	16
HP Secure Platform Management (ID de origem = 84h)	16

1 Introdução

O HP Sure Recover ajuda-o a instalar com segurança o sistema operativo a partir da rede com uma interação mínima por parte do utilizador. Os sistemas com o HP Sure Recover com Recriação de imagem incorporada também suportam a instalação a partir de um dispositivo de armazenamento local.


 **IMPORTANTE:** Realize uma cópia de segurança dos seus dados antes de usar o HP Sure Recover. Como o processamento de imagem reformata a unidade, ocorrerá a perda de dados.

As imagens de recuperação fornecidas pela HP incluem o instalador básico do Windows 10®. Opcionalmente, o HP Sure Recover pode instalar controladores otimizados para dispositivos HP. As imagens de recuperação HP só incluem agentes de recuperação de dados incluídos no Windows 10, como o OneDrive. As empresas podem criar as suas próprias imagens personalizadas para adicionar configurações, aplicações, controladores e agentes de recuperação de dados empresariais.

Um agente de recuperação do sistema operativo (SO) executa os passos necessários para instalar a imagem de recuperação. O agente de recuperação fornecido pela HP executa os passos comuns, como a criação de partições, a formatação e a extração da imagem de recuperação para o dispositivo de destino. Como o agente de recuperação HP está localizado em hp.com, tem de ter acesso à Internet para o recuperar, a menos que o sistema inclua a recriação de imagem incorporada. As empresas também podem alojar o agente de recuperação HP na firewall ou criar agentes de recuperação personalizados para ambientes de recuperação mais complicados.

Pode iniciar o HP Sure Recover quando não for encontrado nenhum sistema operativo. Também pode agendar a execução do HP Sure Recover para garantir, por exemplo, que o malware é removido. Realize a configuração dessas definições através do HP Client Security Manager (CSM), do Manageability Integration Kit (MIK) ou da HP Client Management Script Library.

Executar uma recuperação de rede

 **NOTA:** Para realizar uma recuperação de rede, tem de utilizar uma ligação com fios. A HP recomenda fazer cópias de segurança de ficheiros, dados, fotos e vídeos importantes, entre outros, antes de utilizar o HP Sure Recover para evitar a perda de dados.

1. Ligue o sistema cliente à rede na qual o ponto de distribuição HTTP ou FTP pode ser acedido.
2. Reinicie o sistema cliente e, quando o logótipo da HP for apresentado, carregue em [F11](#).
3. Selecione **Recuperar a partir da rede**.

Realizar a recuperação de uma unidade local

Se um sistema cliente oferecer suporte à recriação de imagem e a opção de transferência de imagem programada estiver ativada na política aplicada, a imagem será transferida para o sistema cliente no horário programado. Depois de a imagem ser transferida para o sistema cliente, reinicie-o para copiar a imagem para o dispositivo de armazenamento de Recriação de imagem incorporada.

Para realizar a recuperação local utilizando a imagem no dispositivo de armazenamento de recriação de imagem incorporada:

1. Reinicie o sistema cliente e, quando o logótipo da HP for apresentado, carregue em [F11](#).
2. Selecione **Recuperar a partir da unidade local**.

Os sistemas com recriação de imagem incorporada devem agendar a configuração da transferência e utilizar o agente de transferência para verificar se há atualizações. O agente de transferência está incluído no plug-in do HP Sure Recover para o HP Client Security Manager e também pode ser configurado no MIK. Consulte <https://www.hp.com/go/clientmanagement> para obter instruções para utilização do MIK.

Também pode criar uma tarefa agendada para copiar o agente para a partição SR_AED e a imagem para a partição SR_IMAGE. Pode então utilizar a HP Client Management Script Library para enviar um evento de serviço informando o BIOS de que deve validar os conteúdos e copiá-los para o dispositivo de armazenamento de recriação de imagem incorporada na reinicialização seguinte.

2 Criar uma imagem da empresa

A maioria das empresas utiliza as ferramentas de implementação Microsoft, o Windows 10 Assessment and Deployment Kit, ou ambos, para produzir ficheiros contendo uma imagem num arquivo de formato de ficheiro Windows Imaging (WIM).

Requisitos

- A versão mais recente do kit Windows 10 Assessment and Deployment (Windows ADK)
- PowerShell
- OpenSSL (ou outra solução para gerar o par de chaves RSA privadas/públicas)
Utilizado para gerar o par de chaves RSA usado para proteger a integridade da imagem da empresa que cria e aloja.
- Uma solução de alojamento do servidor (como o Microsoft Internet Information Services [IIS])

Criar a imagem

Antes de iniciar o processo de criação de imagem, configure o sistema de trabalho ou o sistema de compilação onde instalou as ferramentas necessárias para preparar o processamento da imagem, conforme mostrado nos passos a seguir:

1. Como Administrador, abra a linha de comandos `Deployment and Imaging Tools Environment` (instalado com as ferramentas de implantação do Windows ADK).
2. Crie uma área de transição para a imagem, utilizando o seguinte comando:

```
mkdir C:\staging
```

3. Crie a imagem utilizando um dos seguintes exemplos:

[Exemplo 1: Criar uma imagem com base na imagem de instalação do Microsoft Windows na página 3](#)

[Exemplo 2: Criação de uma imagem baseada num sistema de referência na página 5](#)

Exemplo 1: Criar uma imagem com base na imagem de instalação do Microsoft Windows

1. Montar ou abrir a imagem de instalação do Microsoft Windows (a partir de um ISO Microsoft ou de um OSDVD HP).
2. A partir da imagem de instalação montada do Windows, copie o ficheiro `install.wim` para a área de transição, utilizando o seguinte comando:

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



NOTA: <M:> refere-se à unidade montada. Substitua pela letra da unidade correta.

3. Renomeie o `install.wim` para um nome de ficheiro de imagem ("my-image", neste exemplo), utilizando o seguinte comando:

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

(Opcional) O HP Sure Recover inclui uma funcionalidade para recuperar uma edição específica de uma imagem multi-índices, com base na edição do Windows originalmente licenciada para o sistema de destino HP na fábrica. Este mecanismo funciona se os índices forem nomeados adequadamente. Se a imagem de instalação do Windows for proveniente de uma imagem do OSDVD HP, é provável que tenha uma imagem de multiedições. Se não pretender este comportamento e quiser garantir que é utilizada uma edição específica para todos os seus sistemas de destino, então tem de ter a certeza de que tem apenas um índice na imagem de instalação.

4. Verifique o conteúdo da imagem de instalação utilizando o seguinte comando:

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

A seguir apresentamos um exemplo de uma imagem de instalação que suporta cinco edições (a corresponder com base no BIOS de cada sistema de destino):

Detalhes da imagem: my-image.wim

Índice: 1

Nome: CoreSingleLanguage

Descrição: Atualização do Windows 10, maio de 2019 - Home Single Language Edition

Tamanho: 19.512.500.682 bytes

Índice: 2

Nome: Core

Descrição: Atualização do Windows 10, maio de 2019 - Home Edition

Tamanho: 19.512.500.682 bytes

Índice: 3

Nome: Professional

Descrição: Atualização do Windows 10, maio de 2019 - Professional

Tamanho: 19.758.019.520 bytes

Índice: 4

Nome: ProfessionalEducation

Descrição: Atualização do Windows 10, maio de 2019 - Professional Education Edition

Tamanho: 19.758.019.480 bytes

Índice: 5

Nome: ProfessionalWorkstation

Descrição: Atualização do Windows 10, maio de 2019 - Professional Workstation Edition

Tamanho: 19.758.023.576 bytes



NOTA: Quando há apenas um índice, a imagem é utilizada para recuperação, independentemente do nome. O tamanho do ficheiro de imagem pode ser maior do que antes das eliminações.

5. Se não pretender o comportamento de multiedição, elimine cada índice que não quer.

Conforme mostrado no exemplo a seguir, se pretender apenas a Professional Edition (assumindo que todos os sistemas de destino são licenciados), elimine o índice 5, 4, 2 e 1. Cada vez que eliminar um índice, os números de índice são reatribuídos. Portanto, deve eliminar dos números de índice mais altos para os mais baixos. Execute `Get-ImageInfo` após cada eliminação para confirmar visualmente qual o índice que vai eliminar a seguir.

```
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
```

Escolha apenas um índice da edição (para este exemplo, Professional). Quando há apenas um índice, a imagem é utilizada para recuperação, independentemente do nome. Tenha em conta que o tamanho do ficheiro de imagem pode ser maior do que antes das eliminações, devido à forma como as modificações de metadados e a normalização de conteúdos do WIM funciona.

6. (Opcional) Se quiser incluir controladores na sua imagem de recuperação da empresa, siga estes passos:

- a. Monte a sua imagem numa pasta vazia, utilizando os seguintes comandos:

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

- b. Monte o DVD HP de controladores do Windows 10 (DRDVD) adequado para o sistema de destino suportado. No suporte de dados do controlador montado, copie as subpastas do controlador para a área de transição, utilizando o seguinte comando:

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



NOTA: <M:> refere-se à unidade montada. Substitua pela letra da unidade correta.

Pode incluir controladores adicionais .inf-style colocando-os na pasta `C:\staging\mount\SWSETUP\DRV`. Para obter uma explicação sobre como este conteúdo é processado pelo HP Sure Recover utilizando a função `dism /Add-driver /Recurse`, consulte "Adicionar e remover controladores para uma imagem do Windows offline" no tópico seguinte:

<https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

Esta funcionalidade não suporta controladores .exe-style que exigem a execução de uma aplicação.

- c. Guarde as alterações e desmonte a imagem utilizando o seguinte comando:

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

O ficheiro de imagem resultante é: `C:\staging\my-image.wim`.

- d. Vá a [Dividir a imagem na página 6](#).

Exemplo 2: Criação de uma imagem baseada num sistema de referência

1. Criar um suporte de dados inicializável USB WinPE.

 **NOTA:** Pode encontrar métodos adicionais para capturar a imagem na documentação do ADK.

Certifique-se de que a unidade USB tem espaço livre suficiente para manter a imagem capturada do sistema de referência.

2. Crie uma imagem num sistema de referência.
3. Capture a imagem inicializando o sistema de referência com o suporte de dados USB WinPE e, em seguida, utilize o DISM.

 **NOTA:** <U:> refere-se à unidade USB. Substitua pela letra da unidade correta.

Edite a parte "my-image" no nome do ficheiro e a descrição de <my-image>, conforme necessário.

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

4. Copie a imagem do USB para a área de transição no seu sistema de trabalho utilizando o seguinte comando:

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

Deve ter o seguinte ficheiro de imagem: C:\staging\my-image.wim.


5. Vá a [Dividir a imagem na página 6](#).

Dividir a imagem

A HP recomenda que divida a imagem em ficheiros mais pequenos para melhorar a fiabilidade das transferências da rede, utilizando o seguinte comando:

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

 **NOTA:** O tamanho do ficheiro é apresentado em megabytes. Edite conforme necessário.

 **NOTA:** Devido à natureza do algoritmo de divisão do DISM, os tamanhos dos ficheiros SWM gerados podem ser menores ou maiores do que o tamanho do ficheiro declarado.

Criar um manifesto

Formate os ficheiros de manifesto como UTF-8 sem BOM (Byte Order Mark).

Pode alterar o nome do ficheiro de manifesto (custom.mtf) utilizado nos procedimentos a seguir, mas não pode alterar as extensões .mft e .sig, e a parte do nome de ficheiro do manifesto e ficheiros de assinatura deve corresponder. Por exemplo, pode mudar o par (custom.mft, custom.sig) para (myimage.mft, myimage.sig).

mft_version é utilizado para determinar o formato do ficheiro de imagem e deve ser definido para 1.

image_version é utilizado para determinar se uma versão mais recente da imagem está disponível e para evitar que versões anteriores sejam instaladas.

Ambos os valores devem ser números inteiros não assinalados de 16 bits, e o separador de linha no manifesto deve ser '\r\n' (CR + LF).

Gerar um manifesto

Como vários ficheiros podem estar envolvidos com a imagem dividida, utilize um script PowerShell para gerar um manifesto.

Em todos os passos restantes, tem de estar na pasta C:\staging.

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

1. Crie um script PowerShell utilizando um editor que pode produzir um ficheiro de texto no formato UTF-8 sem BOM, utilizando o seguinte comando: `notepad C:\staging\generate-manifest.ps1`

Crie o script seguinte:

```
$mftFilename = "custom.mft"

$imageVersion = 1907 (Nota: pode ser qualquer número inteiro de 16 bits)

$header = "mft_version=1, image_version=$imageVersion"
Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header

$swmFiles = Get-ChildItem "." -Filter "*.swm"

$ToNatural = { [regex]::Replace($_, '\d*\....$',
{ $args[0].Value.PadLeft(50) }) }

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


$total = $swmFiles.count
$current = 1

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

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

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

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

 **NOTA:** os manifestos para o HP Sure Recover não podem incluir um BOM, portanto, os seguintes comandos reescrevem o ficheiro como UTF8 sem BOM.

```
$content = Get-Content $mftFilename

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

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

2. Guarde o script.
3. Execute o script.

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

Gerar a assinatura do manifesto

O Sure Recover valida o agente e a imagem utilizando assinaturas criptográficas. Os exemplos a seguir utilizam um par de chaves privada/pública no formato X.509 PEM (extensão .PEM). Ajuste os comandos conforme adequado para utilizarem certificados binários DER (extensão .CER ou .CRT), certificados PEM codificados BASE-64 (extensão .CER ou .CRT) ou ficheiros PEM PKCS1 (extensão .PEM). O exemplo também utiliza OpenSSL, que gera assinaturas no formato big-endian. Pode utilizar qualquer utilitário para assinar manifestos, mas algumas versões do BIOS só aceitam assinaturas no formato little-endian.

1. Gere uma chave privada RSA de 2048 bits utilizando o comando seguinte. Se tiver um par de chaves privada/pública RSA de 2048 bits no formato PEM, copie-o para C:\staging e, em seguida, passe para o passo 3.

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

2. Gere a chave pública a partir da chave privada (se tiver uma chave pública correspondente à chave privada em formato PEM, copie-a para C:\staging), utilizando o seguinte comando:

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

3. Crie um ficheiro de assinatura (utilizando o hash de base SHA256) com base na sua chave privada RSA de 2048 bits do passo 1, utilizando o seguinte comando:

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

4. Verifique o ficheiro de assinatura utilizando a chave pública do passo anterior, utilizando o seguinte comando:

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

 **NOTA:**

- Se precisar de criar um ficheiro apenas de assinatura, os passos necessários são o 1 e o 3.
- Para o HP Sure Recover, os passos mínimos necessários são o 1, o 2 e o 3. Vai precisar da chave pública do passo 2 para aprovisionar o sistema de destino.
- O passo 4 é opcional, mas recomendado, para que o ficheiro de assinatura e o ficheiro de manifesto sejam validados corretamente.

Alojar os ficheiros

Aloje os seguintes ficheiros no servidor a partir da pasta C:\staging:

- *.swm
- custom.mft (ou o nome de ficheiro que escolheu para o ficheiro de manifesto)
- custom.sig (ou o nome de ficheiro correspondente que escolheu para o ficheiro de assinatura)



NOTA: Se utilizar o IIS como solução de alojamento, será necessário configurar as entradas MIME para incluir as seguintes extensões, todas configuradas como "application/octet-stream:"

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

Aprovisionar os sistemas de destino

Pode aprovisionar os sistemas de destino utilizando a HP Client Management Script Library, o HP Client Security Manager (CSM)/Sure Recover ou o Manageability Integration Kit (MIK) (<https://www.hp.com/go/clientmanagement>).

Indique as seguintes informações para este aprovisionamento:

1. O endereço de URL do ficheiro de manifesto alojado na secção anterior (http://your_server.domain/path/custom.mft)
2. A chave pública utilizada para verificar o ficheiro de assinatura criado anteriormente (por exemplo, C:\staging\my-recovery-public.pem).

Deteção e resolução de problemas

Se receber uma mensagem referente a uma falha de validação de segurança do processo de recuperação personalizado, verifique o seguinte:

1. O manifesto tem de ser UTF-8 sem BOM.
2. Verifique os hashes do ficheiro.
3. Certifique-se de que o sistema foi aprovisionado com a chave pública correspondente à chave privada utilizada para assinar o manifesto.
4. Os tipos MIME do servidor IIS devem ser `application/octet-stream`.
5. Os caminhos de ficheiro no manifesto têm de incluir o caminho completo para o diretório superior que contém a imagem, como vista pelo sistema cliente. Este caminho não é o caminho completo onde os ficheiros são guardados no ponto de distribuição.

3 Utilizar o agente HP Sure Recover dentro de um firewall da empresa

O agente HP Sure Recover pode ser alojado numa intranet de empresa. Depois de instalar o SoftPaq HP Sure Recover, copie os ficheiros de agente do diretório do agente HP Sure Recover a partir do local de instalação para um ponto de distribuição HTTP ou FTP. Em seguida, aprovisione o sistema cliente com o URL do ponto de distribuição e a chave pública HP denominada `hpsr_agent_public_key.pem`, que é distribuída com o SoftPaq do agente HP Sure Recover.

Instalar o agente HP Sure Recover

1. Transfira o agente HP Sure Recover e extraia os ficheiros para o ponto de distribuição HTTP ou FTP.
2. Defina as permissões adequadas do ficheiro no ponto de distribuição.
3. Se estiver a utilizar IIS (Internet Information Services), crie tipos MIME application/octet-stream para os seguintes formatos de ficheiro:

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



IMPORTANTE: Os passos a seguir descrevem o aprovisionamento do Sure Recover com SCCM. Para obter exemplos sobre como aprovisionar o Sure Recover com a HP Client Management Script Library, consulte [Trabalhar com a HP Client Management Script Library \(CMSL\) na página 12](#).

4. Inicie o SCCM, navegue até **HP Client Security Suite** e, em seguida, selecione a página HP Sure Recover.



NOTA: O URL do ponto de distribuição inclui ftp ou http como protocolo de transporte. Também inclui o caminho completo para o diretório superior que contém o manifesto para o agente HP Sure Recover, como visto a partir de um sistema cliente. Este caminho não é o caminho completo onde os ficheiros são guardados no ponto de distribuição.

5. Na secção **Imagem da plataforma**, selecione a opção **Empresa** para restaurar uma imagem do SO personalizada a partir de um ponto de distribuição de empresa. Introduza o URL fornecido pelo administrador de TI na caixa de entrada **URL do local da imagem**. Introduza a chave pública `hpsr_agent_public_key.pem` no campo **Verificação da imagem**.



NOTA: O URL da imagem personalizada tem de incluir o nome do ficheiro de manifesto de imagem.

6. Na secção **Agente de recuperação**, selecione a opção **Empresa** para usar um agente de recuperação personalizado ou o agente de recuperação HP a partir de um ponto de distribuição da empresa. Insira o

URL fornecido pelo administrador de TI na caixa de entrada **URL da localização do agente**. Insira a chave pública `hpsr_agent_public_key.pem` no campo de entrada da **Chave de verificação do agente**.



NOTA: Não inclua o nome do ficheiro do manifesto do agente no URL porque o BIOS exige que tenha o nome `recovery.mft`.

7. Após a política ser aplicada ao sistema cliente, reinicie-o.
8. Durante o provisionamento inicial, aparece um pedido para introdução de um código de segurança de 4 dígitos para concluir a ativação do HP Sure Recover. Para obter mais detalhes, acesse hp.com e procure a documentação referente ao kit HP Manageability Integration Kit (MIK) para o Microsoft System Center Manager.

Depois de a ativação do HP Sure Recover estar concluída com êxito, o URL personalizado aplicado pela política é apresentado no menu de definições do BIOS do HP Sure Recover.

Para confirmar o sucesso de ativação, reinicie o computador e, quando o logótipo da HP aparecer, prima **F10**. Selecione **Avançadas**, selecione **HP Sure Recover**, selecione **Agente de recuperação** e, em seguida, selecione o **URL**.

4 Trabalhar com a HP Client Management Script Library (CMSL)

A HP Client Management Script Library permite-lhe gerir as definições do HP Sure Recover com PowerShell. O script de exemplo a seguir demonstra como aprovisionar, determinar o estado, alterar a configuração e desaprovisionar o HP Sure Recover.



NOTA: Muitos dos comandos excedem o comprimento da linha deste guia, mas devem ser inseridos como uma única linha.

```
$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
}

```

Gerar chave de exemplo utilizando o OpenSSL

Guarde as chaves privadas num local seguro. As chaves públicas serão utilizadas para validação e têm de ser fornecidas durante o aprovisionamento. É necessário que estas chaves tenham 2048 bits de comprimento e utilizem um expoente de 0x10001. Substitua o assunto nos exemplos com informações sobre a sua empresa.

Defina a seguinte variável de ambiente antes de continuar:

```
set OPENSSL_CONF=<path>\openssl.cnf
```

```
# Create a self-signed root CA certificate for testing
```

```
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
```

```
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

```
# Create a key endorsement certificate
```

```
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
```

```
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

```
openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Create a command signing key

```
openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:
```

Create an image signing key

```
openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Pode assinar o manifesto de imagem com o seguinte comando:

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

Create an agent signing key

```
openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Pode assinar o manifesto de agente com o seguinte comando:

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

O OpenSSL gera ficheiros de assinatura em formato big-endian, que é incompatível com algumas versões do BIOS, pelo que a ordem de byte do ficheiro de assinatura do agente pode precisar de ser invertida antes de ser implementada. As versões do BIOS que suportam a ordem de byte big-endian também suportam a ordem de byte little-endian.

A Detecção e resolução de problemas

Falha de criação de partições da unidade

Pode ocorrer uma falha de criação de partições da unidade se a partição SR_AED ou SR_IMAGE estiver encriptada com Bitlocker. Estas partições são normalmente criadas com um atributo GPT que impede que o Bitlocker as encripte, mas se um utilizador eliminar e recriar as partições, ou se as criar manualmente numa unidade bare-metal, então o agente Sure Recover não consegue eliminá-las e acaba com um erro quando volta a criar as partições da unidade. O utilizador tem de as eliminar manualmente executando o `diskpart`, seleccionando o volume e emitindo o comando de substituição `del vol` ou semelhante.

Registo de auditoria de firmware

As informações de variável EFI são as seguintes:


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

Existem APIs no Windows para a leitura de variáveis EFI, ou pode capturar o conteúdo das variáveis num ficheiro utilizando o utilitário UEFI Shell `dumpstore`.

Pode capturar o registo de auditoria utilizando o comando `Get-HPFirmwareAuditLog` fornecido pela HP Client Management Script Library.

Registo de eventos do Windows

Os eventos de início e paragem do Sure Recover são enviados para o registo de auditoria do BIOS. Pode vê-los no Visualizador de Eventos do Windows, no registo Sure Start, se o HP Notifications estiver instalado. Estes eventos incluem a data e a hora, a ID de origem, a ID do evento e um código específico do evento. Por exemplo, [fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3] indica que a recuperação falhou porque o manifesto não pôde ser autenticado com o código específico do evento c3f 23000 que foi registado às 2:26:40 no dia 6/27/18.

 **NOTA:** Estes registos seguem o formato de data mês/dia/ano dos EUA.

HP Secure Platform Management (ID de origem = 84h)

Tabela A-1 HP Secure Platform Management

ID do evento	Contagem de dispositivo (All/DaaS)	Contagem de eventos (All/DaaS)	Descrição	Notas
40	256/178	943/552	O processo de recuperação do SO foi iniciado pelo firmware.	Início da recuperação da plataforma

Tabela A-1 HP Secure Platform Management (continuação)

ID do evento	Contagem de dispositivo (All/DaaS)	Contagem de eventos (All/DaaS)	Descrição	Notas
41	221/147	588/332	O processo de recuperação do SO foi concluído com êxito.	Recuperação da plataforma concluída
42	54/42	252/156	O processo de recuperação do SO não foi concluído com êxito.	Falha na recuperação da plataforma

Pode recuperar o Registo de Auditoria do Firmware utilizando Get-HPFirmwareAuditLog na HP Client Management Script Library, disponível <http://www.hp.com/go/clientmanagement>. Os eventos do HP Secure Platform Management com as ID 40, 41 e 42 devolveram códigos específicos do evento no campo de dados, que indicam o resultado das operações do Sure Recover. Por exemplo, a entrada de registo a seguir indica que o Sure Recover não conseguiu transferir o ficheiro de manifesto ou de assinatura com erro no event_id 42 e os dados: 00:30:f1:c3, que deve ser interpretado como o valor 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

Descrição: O processo de recuperação do SO não foi concluído com êxito.

data: 00:30:f1:c3

Uma recuperação bem-sucedida é apresentada como event_id = 41 e os dados: 00:00:00:00, por exemplo:

Códigos Específicos de Evento

Success = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

timestamp: 5/27/2019 2:55:41 PM

Descrição: O processo de recuperação do SO não foi concluído com êxito.

data: 00:00:00:00

O HP Sure Recover usa os seguintes códigos específicos de evento.

Tabela A-2 Códigos específicos de evento

Descrição do evento	Código do evento
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000
AwsDownloadUnattendedFailed	0xC3F16000
UnableToConnectToNetwork	0xC3F17000
CatalogNotAuthenticated	0xC3F21000
FtpHttpDownloadHashFailed	0xC3F22000
ManifestDoesNotAuthenticate	0xC3F23000
CatalogVersionMismatch	0xC3F31000
CatalogLoadFailed	0xC3F32000
OsDvdDidNotResolvedToOneComponent	0xC3F33000
DriversDvdDidNotResolvedToOneComponent	0xC3F34000
ManifestFileEmptyOrInvalid	0xC3F41000
ListedFileInManifestNotFound	0xC3F42000
FailedToInstallcontroladores	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