



Guia do Usuário

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

Microsoft e Windows são marcas comerciais ou marcas comerciais registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Software de computador confidencial. Licença válida da HP necessária para posse, utilização ou cópia. Consistente com o FAR 12.211 e 12.212, o Software de Computador Comercial, a Documentação de Software de Computador e os Dados Técnicos para Itens Comerciais estão licenciados para o Governo dos EUA sob a licença comercial do vendedor.

As informações contidas neste documento estão sujeitas a alterações sem aviso. As únicas garantias para produtos e serviços da HP são as estabelecidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma informação contida neste documento deve ser interpretada como uma garantia adicional. A HP não será responsável por erros técnicos ou editoriais nem por omissões contidos neste documento.

Primeira edição: fevereiro de 2020

Número de peça: L93434-201

Código de sintaxe de entrada do usuário

O texto que você deve inserir em uma interface de usuário é indicado por uma `fonte de tamanho fixo`.

Tabela -1 Código de sintaxe de entrada do usuário


Item	Descrição
Texto sem parênteses ou chaves	Itens que você deve digitar exatamente como mostrados
<Texto entre sinais de menor e maior>	Uma marcação de posição para um valor que você precisa fornecer; omite os parênteses
[Texto dentro de colchetes]	Itens opcionais; omite os parênteses
{Texto dentro de chaves}	Um conjunto de itens dos quais você deve escolher somente um; omite as chaves
	Um separador para itens dos quais você deve escolher somente um; omite a barra vertical
...	Itens que podem ou devem se repetir; omite as reticências

Conteúdo

1	Passos iniciais	1
	Execução de uma recuperação a partir da rede	1
	Execução de uma recuperação a partir da unidade local	1
2	Criação de uma imagem corporativa	3
	Requisitos	3
	Criação da imagem	3
	Exemplo 1: Criação de uma imagem com base na imagem de instalação do Microsoft Windows	3
	Exemplo 2: Criação de uma imagem com base em um sistema de referência	5
	Divisão da imagem	6
	Criação de um inventário	6
	Geração de um inventário	7
	Geração de assinatura de inventário	8
	Hospedagem dos arquivos	9
	Provisionamento dos seus sistemas de destino	9
	Solução de problemas	9
3	Utilização do HP Sure Recover Agent dentro de um firewall corporativo	11
	Instalação do agente HP Sure Recover	11
4	Operação com a HP Client Management Script Library (CMSL)	13
	Geração de chave de amostra usando OpenSSL	15
	Apêndice A Solução de problemas	17
	Falha ao particionar unidade	17
	Registro de auditoria de firmware	17
	Registro de eventos do Windows	17
	HP Secure Platform Management (Source ID = 84h)	17

1 Passos iniciais

O HP Sure Recover ajuda você a instalar com segurança o sistema operacional a partir da rede com interação mínima do usuário. Os sistemas com HP Sure Recover with Embedded Reimaging também suportam a instalação de um dispositivo de armazenamento local.


 **IMPORTANTE:** Faça backup de seus dados antes de usar o HP Sure Recover. Como o processo de criação de imagens reformata a unidade, haverá perda de dados.

As imagens de recuperação fornecidas pela HP incluem o instalador básico do Windows 10®. Como opcional, o HP Sure Recover pode instalar drivers otimizados para dispositivos HP. As imagens de recuperação HP incluem apenas agentes de recuperação de dados incluídos no Windows 10, como o OneDrive. As empresas podem criar suas próprias imagens personalizadas para adicionar configurações corporativas, aplicativos, drivers e agentes de recuperação de dados.

Um agente de recuperação do sistema operacional (SO) executa as etapas necessárias para instalar a imagem de recuperação. O agente de recuperação fornecido pela HP executa etapas comuns, como particionamento, formatação e extração da imagem de recuperação no dispositivo de destino. Como o agente de recuperação HP está localizado em hp.com, você precisa de acesso à Internet para recuperá-lo, a menos que o sistema inclua recriação de imagens incorporadas. As empresas também podem hospedar o agente de recuperação HP em seu firewall ou criar agentes de recuperação personalizados para ambientes de recuperação mais complicados.

Você pode iniciar o HP Sure Recover quando nenhum sistema operacional for encontrado. Você também pode executar o HP Sure Recover em uma programação, para garantir a remoção de malware. Faça essas configurações através do HP Client Security Manager (CSM), Manageability Integration Kit (MIK) ou da HP Client Management Script Library.

Execução de uma recuperação a partir da rede

 **NOTA:** Para executar uma recuperação a partir da rede, você deve usar uma conexão com fio. A HP recomenda fazer backup de arquivos, dados, fotos, vídeos importantes e outros antes de usar o HP Sure Recover para evitar a perda de dados.

1. Conecte o sistema do cliente à rede na qual o ponto de distribuição HTTP ou FTP pode ser acessado.
2. Reinicie o sistema do cliente e, quando o logotipo da HP aparecer, pressione **F11**.
3. Selecione **Restaurar a partir da rede**.

Execução de uma recuperação a partir da unidade local

Se um sistema cliente suportar recriação de imagem integrada e a opção de download da imagem agendada estiver ativada na política aplicada, a imagem será baixada no sistema do cliente no horário agendado. Após o download da imagem no sistema do cliente, reinicie-a para copiar a imagem no dispositivo de armazenamento da Recriação de imagem integrada.

Para realizar a recuperação local usando a imagem no dispositivo de armazenamento da Recriação de imagem integrada:

1. Reinicie o sistema do cliente e, quando o logotipo da HP aparecer, pressione **F11**.
2. Selecione **Restaurar a partir da unidade local**.

Os sistemas com Recriação de imagem integrada devem configurar um agendamento de download e usar o agente de download para verificar se há atualizações. O agente de download está incluído no plug-in HP Sure Recover para HP Client Security Manager e também pode ser configurado no MIK. Consulte <https://www.hp.com/go/clientmanagement> para obter as instruções sobre usar o MIK.

Você também pode criar uma tarefa agendada para copiar o agente na partição SR_AED e a imagem na partição SR_IMAGE. Em seguida, você pode usar a HP Client Management Script Library para enviar um evento de serviço informando ao BIOS que ele deve validar o conteúdo e copiar para o dispositivo de armazenamento da Recriação de imagem integrada na próxima reinicialização.

2 Criação de uma imagem corporativa

A maioria das empresas usa Microsoft Deployment Tools, Windows 10 Assessment and Deployment kit ou ambos para produzir arquivos que contêm uma imagem em um formato de arquivo do Windows Imaging (WIM).

Requisitos

- A versão mais recente do Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (ou outra solução para gerar par de chaves pública/privada RSA)
Use para gerar o par de chaves RSA usado para proteger a integridade da imagem corporativa que você cria e hospeda.
- Uma solução de hospedagem de servidores (como Microsoft Internet Information Services [IIS])

Criação da imagem

Antes de iniciar o processo de criação da imagem, configure o sistema de trabalho ou construa o sistema em que você instalou as ferramentas necessárias para se preparar para o processamento da imagem, conforme mostrado nas seguintes etapas:

1. Como Administrador, abra o prompt de comando do `Deployment and Imaging Tools Environment` (instalado com Deployment Tools do Windows ADK).
2. Crie uma área de preparação para sua imagem, usando o seguinte comando:

```
mkdir C:\staging
```

3. Crie a imagem usando um dos seguintes exemplos:

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

[Exemplo 2: Criação de uma imagem com base em um sistema de referência na página 5](#)

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

1. Monte ou abra a imagem de instalação do Microsoft Windows (de um ISO da Microsoft ou de um OSDVD da HP).
2. Na imagem de instalação montada do Windows, copie o arquivo `install.wim` para sua área de preparação, usando o seguinte comando:

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



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

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

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

(Opcional) O HP Sure Recover inclui um recurso para recuperar uma edição específica de uma imagem com vários índices, com base na edição do Windows originalmente licenciada para o sistema de destino HP na fábrica. Esse mecanismo funciona se os índices forem nomeados corretamente. Se a imagem de instalação do Windows for proveniente de uma imagem de um OSDVD da HP, é provável que você tenha uma imagem de várias edições. Se você não deseja esse comportamento e deseja garantir que uma edição específica seja usada para todos os seus sistemas de destino, será necessário garantir que apenas um índice esteja na imagem de instalação.

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

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

A seguir, temos uma amostra de saída de uma imagem de instalação que suporta cinco edições (a serem correspondidas com o BIOS de cada sistema de destino):

Detalhes para a imagem: my-image.wim

Índice: 1

Nome: CoreSingleLanguage

Descrição: Windows 10 May 2019 Update - Home Single Language Edition

Tamanho: 19,512,500,682 bytes

Índice: 2

Nome: Core

Descrição: Windows 10 May 2019 Update - Home edition

Tamanho: 19,512,500,682 bytes

Índice: 3

Nome: Professional

Descrição: Windows 10 May 2019 Update- Professional Update

Tamanho: 19.758,019,520 bytes

Índice: 4

Nome: ProfessionalEducation

Descrição: Windows 10 May 2019 Update - Professional Education edition

Tamanho: 19,758,019,480 bytes

Índice: 5

Nome: ProfessionalWorkstation

Descrição: Windows 10 May 2019 Update - Professional Workstation edition

Tamanho: 19,758,023,576 bytes



NOTA: Quando há apenas um índice, a imagem é usada para recuperação, independentemente do nome. O tamanho do seu arquivo de imagem pode ser maior do que antes das exclusões.

5. Se você não deseja o comportamento de várias edições, exclua cada índice que você não deseja.

Conforme mostrado no exemplo a seguir, se você deseja apenas a edição Professional (supondo que todos os sistemas de destino estejam licenciados), exclua os índices 5, 4, 2 e 1. Cada vez que você excluir um índice, os números de índice serão reatribuídos. Portanto, você deve excluir começando pelos números de índice mais alto até os de índice mais baixo. Execute `Get-ImageInfo` após cada exclusão para confirmar visualmente qual índice você irá excluir em seguida.

```
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 (neste exemplo, Professional). Quando há apenas um índice, a imagem é usada para recuperação, independentemente do nome. Observe que o tamanho do seu arquivo de imagem pode ser maior do que antes das exclusões, devido à maneira como as modificações de metadados do WIM e a normalização de conteúdo funcionam.

6. (Opcional) Se você deseja incluir drivers na sua imagem de recuperação corporativa, siga estas etapas:

- a. Monte sua imagem em uma pasta vazia, usando 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 do driver HP Windows 10 apropriado (DRDVD) para o sistema de destino suportado. A partir da mídia do driver montado, copie as subpastas do driver para sua área de preparação, usando o seguinte comando:

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



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

Você pode incluir drivers .inf-style adicionais colocando-os na pasta `C:\staging\mount\SWSETUP\DRV`. Para obter uma explicação sobre como esse conteúdo é processado pelo HP Sure Recover usando a função `dism /Add-Driver /Recurse`, consulte “Adicionar e remover drivers em uma imagem offline do Windows” no seguinte tópico: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

Esse recurso não suporta drivers no estilo .exe que exigem a execução de um aplicativo.

- c. Salve as alterações e desmonte sua imagem, usando o seguinte comando:


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

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

- d. Vá para [Divisão da imagem na página 6](#).

Exemplo 2: Criação de uma imagem com base em um sistema de referência

1. Cria uma mídia inicializável USB WinPE.

 **NOTA:** Métodos adicionais para capturar a imagem podem ser encontrados na documentação do ADK.

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

2. Crie uma imagem em um sistema de referência.
3. Capture a imagem inicializando o sistema de referência com a mídia USB WinPE e use o DISM.

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

Edite a parte “my-image” do nome do arquivo e a descrição <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 preparação do seu sistema de trabalho, usando o seguinte comando:

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

Você deve ter o seguinte arquivo de imagem: C:\staging\my-image.wim.


5. Vá para [Divisão da imagem na página 6](#).

Divisão da imagem

A HP recomenda que você divida a imagem em arquivos menores para melhorar a confiabilidade dos downloads da rede, usando o seguinte comando:

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

 **NOTA:** FileSize é mostrado em megabytes. Edite conforme necessário.

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

Criação de um inventário

Formate arquivos de inventário como UTF-8 sem Byte Order Mark (BOM).

Você pode alterar o nome do arquivo de inventário (custom.mft) usado nos procedimentos a seguir, mas não deve alterar as extensões .mft e .sig, e a parte do nome dos arquivos de inventário e assinatura deve corresponder. Por exemplo, você pode alterar o par (custom.mft, custom.sig) para (myimage.mft, myimage.sig).

mft_version é usado para determinar o formato do arquivo de imagem que atualmente deve estar definido como 1.

image_version é usado para determinar se uma versão mais recente da imagem está disponível e para impedir a instalação de versões mais antigas.

Ambos os valores devem ser números inteiros de 16 bits sem sinal e o separador de linhas no inventário deve ser '\r\n' (CR + LF).

Geração de um inventário

Como vários arquivos podem estar envolvidos com sua imagem dividida, use um script do PowerShell para gerar um inventário.

Em todas as etapas restantes, você deve estar na pasta C:\staging.

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

1. Crie um script do powershell usando um editor que possa produzir um arquivo de texto no formato UTF-8 sem BOM, usando o seguinte comando: `notepad C:\staging\generate-manifest.ps1`

Crie o seguinte script:

```
$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) }) }

$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
    }

```

 **NOTA:** Inventários para o HP Sure Recover não podem incluir uma BOM, portanto os seguintes comandos regravam o arquivo como UTF8 sem BOM.

```

$content = Get-Content $mftFilename

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

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

```

2. Salve o script.
3. Execute o script.

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

Geração de assinatura de inventário

O Sure Recover valida o agente e a imagem usando assinaturas criptográficas. Os exemplos a seguir usam um par de chaves públicas/privadas no formato X.509 PEM (extensão .PEM). Ajuste os comandos conforme apropriado para usar certificados binários DER (extensão .CER ou .CRT), certificados PEM codificados em BASE-64 (extensão .CER ou .CRT) ou arquivos PKCS1 PEM (extensão .PEM). O exemplo também usa o OpenSSL, que gera assinaturas no formato big-endian. Você pode usar qualquer utilitário para assinar inventários, mas algumas versões do BIOS suportam apenas assinaturas no formato little-endian.

1. Gere uma chave privada RSA de 2.048 bits usando o seguinte comando. Se você tiver um par de chaves privada/pública RSA de 2.048 bits no formato pem, copie-os para C:\staging e vá para a etapa 3.

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

2. Gere a chave pública a partir da sua chave privada (se você tiver uma chave pública correspondente à sua chave privada no formato PEM, copie-a para C:\staging), usando o seguinte comando:

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

3. Crie um arquivo de assinatura (usando o hash baseado em sha256) com base na chave privada RSA de 2048 bits da etapa 1, usando o seguinte comando:

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

4. Verifique o arquivo de assinatura, usando sua chave pública da etapa anterior, usando o seguinte comando:

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

**NOTA:**

- Se você precisar criar apenas um arquivo de assinatura, as etapas necessárias serão 1 e 3.
- Para o HP Sure Recover, as etapas mínimas necessárias são 1, 2 e 3. Você precisa da chave pública da etapa 2 para provisionar o sistema de destino.
- A etapa 4 é opcional, mas recomendada, para que seu arquivo de assinatura e arquivo de inventário sejam validados corretamente.

Hospedagem dos arquivos

Hospede os seguintes arquivos no seu servidor da pasta C:\staging:

- *.swm
- custom.mft (ou o nome do arquivo que você escolheu para o arquivo de inventário)
- custom.sig (ou o nome do arquivo correspondente que você escolheu para o arquivo de assinatura)



NOTA: Se você usa o IIS como sua solução de hospedagem, é necessário configurar suas entradas MIME para incluir as seguintes extensões, todas configuradas como "application/octet-stream:"

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

Provisionamento dos seus sistemas de destino

É possível provisionar seus sistemas de destino usando HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover ou o Manageability Integration Kit (MIK) (<https://www.hp.com/go/clientmanagement>).

Forneça as seguintes informações para esse provisionamento:

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

Solução de problemas

Se você receber uma mensagem sobre o processo de recuperação personalizado com falha na validação de segurança, verifique o seguinte:

1. O inventário deve ser UTF-8 sem BOM.
2. Verifique as hashes do arquivo.
3. Verifique se o sistema foi fornecido com a chave pública correspondente à chave privada usada para assinar o inventário.

4. Os tipos de mime do servidor IIS devem ser `application/octet-stream`.
5. Os caminhos de arquivo no inventário devem incluir o caminho completo para o diretório superior que contém a imagem, conforme visto em um sistema cliente. Esse caminho não é o caminho completo em que os arquivos são salvos no ponto de distribuição.


3 Utilização do HP Sure Recover Agent dentro de um firewall corporativo

O agente HP Sure Recover pode ser hospedado em uma intranet corporativa. Depois de instalar o HP Sure Recover SoftPaq, copie os arquivos do agente do diretório do agente do HP Sure Recover do local da instalação para um ponto de distribuição HTTP ou FTP. Em seguida, forneça ao sistema do cliente a URL do ponto de distribuição e a chave pública da HP denominada `hpsr_agent_public_key.pem`, que é distribuído com o SoftPaq do agente HP Sure Recover.


Instalação do agente HP Sure Recover

1. Baixe o agente HP Sure Recover e extraia os arquivos para o ponto de distribuição HTTP ou FTP.
2. Defina as permissões de arquivo apropriadas no ponto de distribuição.
3. Se estiver usando Internet Information Services (IIS), crie tipos MIME `application/octet-stream` para os seguintes formatos de arquivo:

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

 **IMPORTANTE:** As etapas a seguir descrevem o provisionamento do Sure Recover com SCCM. Para obter exemplos de como provisionar o Sure Recover com a HP Client Management Script Library, consulte [Operação com a HP Client Management Script Library \(CMSL\) na página 13](#).

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

 **NOTA:** A URL do ponto de distribuição inclui `ftp` ou `http` como o protocolo de transporte. Também inclui o caminho completo para o diretório superior que contém o inventário do agente HP Sure Recover, conforme visto em um sistema cliente. Esse caminho não é o caminho completo em que os arquivos são salvos no ponto de distribuição.

5. Na seção **Imagem de plataforma**, selecione a opção **Corporação** para restaurar uma imagem do SO personalizada a partir de um ponto de distribuição corporativo. Digite a URL fornecida pelo administrador de TI na caixa **URL do local da imagem**. Digite a chave pública `hpsr_agent_public_key.pem` no campo **Verificação de imagem**.

 **NOTA:** A URL da imagem personalizada deve incluir o nome do arquivo de inventário da imagem.

6. Na seção **Agente de recuperação**, selecione a opção **Corporação** para usar um agente de recuperação personalizado ou o agente de recuperação HP a partir de um ponto de distribuição corporativo. Digite a

URL fornecida pelo administrador de TI na caixa **URL do local do agente**. Digite a chave pública `hpsr_agent_public_key.pem` no campo **Chave de verificação de agente**.



NOTA: Não inclua o nome do arquivo do inventário do agente na URL porque o BIOS exige que ele seja denominado `recovery.mft`.


7. Após a política ser aplicada ao sistema do cliente, reinicie-o.
8. Durante o provisionamento inicial, é exibido um prompt para você digitar um código de segurança de quatro dígitos para concluir a ativação do HP Sure Recover. Para obter mais detalhes, acesse hp.com e procure pelo documento técnico HP Manageability Integration Kit (MIK) para Microsoft System Center Manager.

Depois que a ativação do HP Sure Recover for concluída com êxito, a URL personalizada aplicada pela política é exibida no menu de configurações do BIOS do HP Sure Recover.

Para confirmar o sucesso da ativação, reinicie o computador e, quando o logotipo da HP for exibido, pressione **f10**. Selecione **Avançado**, selecione **HP Sure Recover**, selecione **Agente de recuperação** e, em seguida, selecione **URL**.

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

A HP Client Management Script Library permite gerenciar as configurações do HP Sure Recover com PowerShell. O script de exemplo a seguir demonstra como provisionar, determinar o status, alterar a configuração e desprovisionar o HP Sure Recover.

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

```
$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
}

```

Geração de chave de amostra usando OpenSSL

Guarde as chaves privadas em um local seguro. As chaves públicas serão usadas para validação e devem ser fornecidas durante o provisionamento. Essas chaves devem ter 2.048 bits de comprimento e usar um expoente de 0x10001. Substitua o assunto nos exemplos por informações sobre sua organização.

Defina a seguinte variável de ambiente antes de continuar:

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

```
# Crie um certificado CA raiz de assinatura própria para teste
```

```
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"
```

```
# Crie um certificado de endosso da chave
```

```
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:

# Crie uma chave de assinatura de comando

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:

# Crie uma chave de assinatura de imagem

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:

```

Você pode assinar o inventário da imagem com este comando:

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

Crie uma chave de assinatura do agente

```

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:

```

Você pode assinar o inventário do agente com este comando:

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

O OpenSSL gera arquivos de assinatura no formato big-endian, que é incompatível com algumas versões de BIOS, portanto, a ordem dos bytes dos arquivos de assinatura do agente pode precisar ser invertida antes de ser implementada. As versões do BIOS que suportam a ordenação de bytes big-endian também suportam a ordenação de bytes little-endian.

A Solução de problemas

Falha ao particionar unidade

A falha ao particionar unidade pode ocorrer se a partição SR_AED ou SR_IMAGE for criptografada com Bitlocker. Essas partições são normalmente criadas com um atributo gpt que impede o Bitlocker de criptografá-las, mas se um usuário excluir e recriar as partições ou criá-las manualmente em uma unidade bare metal, o agente Sure Recover não poderá excluí-las e sair com um erro ao reparticionar a unidade. O usuário deve excluí-las manualmente executando `diskpart`, selecionando o volume e emitindo o comando de ignorar `del vol` ou similar.

Registro de auditoria de firmware

As informações de variáveis EFI são as seguintes:

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

As APIs existem no Windows para ler variáveis EFI ou você pode descarregar o conteúdo da variável em um arquivo usando o utilitário `dmptstore` UEFI Shell.

Você pode descarregar o registro de auditoria usando o comando `Get-HPFirmwareAuditLog` fornecido pela HP Client Management Script Library.

Registro de eventos do Windows

Os eventos de início e parada do Sure Recover são enviados ao registro de auditoria do BIOS, que você pode ver no Windows Event Viewer no registro do Sure Start se o HP Notifications estiver instalado. Esses eventos incluem a data e a hora, ID da fonte, 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 inventário não pôde ser autenticado com o código específico do evento `c3f 23000` registrado em 2:26:40 em 6/27/18.



NOTA: Esses registros seguem o formato de data dos EUA de mês/dia/ano.

HP Secure Platform Management (Source ID = 84h)

Tabela A-1 HP Secure Platform Management

ID do evento	Número de dispositivos (todos/DaaS)	Número de eventos (todos/DaaS)	Descrição	Observações
40	256/178	943/552	O processo de recuperação do SO da plataforma foi iniciado pelo firmware.	Recuperação da plataforma iniciada

Tabela A-1 HP Secure Platform Management (continuação)

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

Você pode recuperar o Registro de auditoria do firmware usando Get-HPFirmwareAuditLog na HP Client Management Script Library, disponível em <http://www.hp.com/go/clientmanagement>. As IDs de evento do HP Secure Platform Management 40, 41 e 42 retornam Códigos específicos de evento no campo de dados, que indicam o resultado das operações do Sure Recover. Por exemplo, a seguinte entrada de registro indica que o Sure Recover falhou ao baixar o arquivo de inventário ou assinatura com o erro event_id 42 e 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
description: The platform OS recovery process failed to complete successfully.
data: 00:30:f1:c3
```

Uma recuperação bem sucedida é mostrada como event_id = 41 e data: 00:00:00:00, por exemplo:

```
Event Specific Codes
Success = 0x00000000
CatalogDownloadFailed = 0xC3F11000
message_number: 0
severity: Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 41
timestamp_is_exact: 1
timestamp: 5/27/2019 2:55:41 PM
description: The platform OS recovery process failed to complete successfully.
data: 00:00:00:00
```


HP Sure Recover 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
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