用户指南

HP Sure Recover

第一版：2020 年 2 月

文档部件号：L93434-AA1

用户输入语法键

必须输入用户界面的文本以固定宽度字体表示。

表 -1 用户输入语法键

项目	说明
无括号或大括号的文本	您必须按照所示内容准确键入的项目
<尖括号内的文本>	您必须提供的值的占位符；忽略括号
[方括号内的文本]	可选项目；忽略括号
{大括号内的文本}	一组项目，您只能从中选择一个；忽略大括号
|	分隔符，用于分隔多个项目，而您只能从中选择一个项目；忽略竖线
. . .	可以或必须重复的项目；忽略省略号

目录

1 使用入门

HP Sure Recover 可帮助您通过网络安全地安装操作系统，最大程度地减少用户交互。具有 HP Sure Recover with Embedded Reimaging 的系统还支持从本地存储设备进行安装。

切记：在使用 HP Sure Recover 之前，请备份您的数据。因为映像进程会重新格式化驱动器，所以会发生数据丢失。

HP 提供的恢复映像包括基本的 Windows 10® 安装程序。HP Sure Recover 可选择性地为 HP 设备安装优化驱动程序。HP 恢复映像仅包含 Windows 10 附带的数据恢复代理（比如 OneDrive）。公司可以创建自己的自定义映像，以添加公司设置、应用程序、驱动程序和数据恢复代理。

操作系统 (OS) 恢复代理可执行安装恢复映像所必需的步骤。HP 提供的恢复代理可以执行常用步骤，比如分区、格式化以及将恢复映像提取至目标设备。由于 HP 恢复代理位于 hp.com，您需要具有 Internet 访问才能获取，除非系统包含嵌入式重新映像。公司还可在其防火墙内托管 HP 恢复代理，或针对更复杂的恢复环境创建自定义恢复代理。

如果找不到操作系统，您可以启动 HP Sure Recover。您也可以按计划运行 HP Sure Recover，例如为了确保系统已删除恶意软件。通过 HP Client Security Manager (CSM)、Manageability Integration Kit (MIK) 或 HP Client Management Script Library，对这些设置进行配置。

执行网络恢复

注：要执行网络恢复，您必须使用有线连接。HP 建议在使用 HP Sure Recover 之前，备份重要的文件、数据、照片、视频等，以免丢失数据。

1. 将客户端系统连接到可以访问 HTTP 或 FTP 分发点的网络。
2. 重新启动客户端系统，在 HP 徽标出现时按 f11。
3. 选择**从网络还原**。

执行本地驱动器恢复

如果客户端系统支持嵌入式重新映像，而且已在应用的策略中启用了计划映像下载选项，则映像将在计划时间下载到客户端系统。将映像下载到客户端系统后，重新启动该映像，以将其复制到 Embedded Reimaging 存储设备。

要使用 Embedded Reimaging 存储设备上的映像执行本地恢复，请执行以下操作：

1. 重新启动客户端系统，在 HP 徽标出现时按 f11。
2. 选择**从本地驱动器还原**。

具有 Embedded Reimaging 的系统必须配置下载计划，并使用下载代理检查更新。下载代理包含在适用于 HP Client Security Manager 的 HP Sure Recover 插件中，亦可在 MIK 中进行配置。有关 MIK 的使用说明，请参阅 https://www.hp.com/go/clientmanagement。

您还可以创建计划任务，将代理复制到 SR_AED 分区，将映像复制到 SR_IMAGE 分区。然后，您可以使用 HP Client Management Script Library 发送服务事件，告知 BIOS 应在下次重启时验证内容，并复制到嵌入式重新映像存储设备。

2 创建公司映像

大多数公司使用 Microsoft 部署工具、Windows 10 评估和部署工具包或者同时使用两者，在 Windows Imaging (WIM) 文件格式存档中生成包含映像的文件。

要求

- Windows 10 评估和部署工具包 (Windows ADK) 的最新版本
- PowerShell
- OpenSSL（或其他用于生成 RSA 私人密钥/公共密钥对的解决方案）

  用于生成 RSA 密钥对，以保护您创建和托管的公司映像的完整性。
- 服务器托管解决方案（例如 Microsoft Internet 信息服务[IIS]）

创建映像

在启动映像创建进程之前，请按照如下步骤所示，对工作系统进行设置，或构建已安装所需工具的系统，从而为处理映像做好准备：

1. 以管理员身份打开 `Deployment and Imaging Tools Environment` 命令提示符（与 Windows ADK 的部署工具一起安装）。
2. 使用以下命令，为您的映像创建临时区域：

   ```
   mkdir C:\staging
   ```
3. 使用以下示例之一创建映像：

   第 2 页的示例 1：基于 Microsoft Windows 安装映像创建映像

   第 4 页的示例 2：基于参考系统创建映像

示例 1：基于 Microsoft Windows 安装映像创建映像

1. 安装或打开 Microsoft Windows 安装映像（来自 Microsoft ISO 或 HP OSDVD）。
2. 使用以下命令，将 install.wim 文件从已安装的 Windows 安装映像复制到临时区域：

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

   注： `<M:>` 是指已安装的驱动器。替换为正确的驱动器号。
3. 使用以下命令，将 install.wim 重命名为映像文件名（本示例中为“my-image”）：

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

   （可选）HP Sure Recover 包含根据出厂时针对 HP 目标系统最初获得许可的 Windows 版本，从多索引映像恢复特定版本的功能。如果正确命名了索引，此机制即可发挥作用。如果您的 Windows 安装映像来自 HP OSDVD 映像，则您可能具有多版本映像。如果不需要此行为，并希望确保您的所有目标系统都使用某一特定版本，则您需要确保安装映像中仅有一个索引。

4. **使用以下命令，检查安装映像的内容：**

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

   下面显示了来自支持五个版本（要根据每个目标系统的 BIOS 进行匹配）的安装映像的示例输出：

   映像详细信息： my-image.wim

   索引： 1

   名称： CoreSingleLanguage

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

   大小： 19,512,500,682 bytes

   索引： 2

   名称： Core

   描述： Windows 10 May 2019 Update - Home edition

   大小： 19,512,500,682 bytes

   索引： 3

   名称： Professional

   描述： Windows 10 May 2019 Update- Professional Update

   大小： 19.758,019,520 bytes

   索引： 4

   名称： ProfessionalEducation

   描述： Windows 10 May 2019 Update - Professional Education edition

   大小： 19,758,019,480 bytes

   索引： 5

   名称： ProfessionalWorkstation

   描述： Windows 10 May 2019 Update - Professional Workstation edition

   大小： 19,758,023,576 bytes

   注：只有一个索引时，映像将用于恢复，无论其名称是什么。映像文件可能会比删除之前更大。

5. **如果不需要多版本行为，请删除您不需要的每个索引。**

   如下例所示，如果您只想要专业版（假设所有目标系统都已获得许可），请删除索引 5、4、2 和 1。每当您删除索引时，索引编号都会进行重新分配。因此，应该按照从最高到最低的编号顺序删除索引。每次删除后，运行 Get-ImageInfo **以目视确认接下来要删除哪个索引。**

   ```
   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
```

仅选择该版本的一个索引（此示例中为专业版）。只有一个索引时，映像将用于恢复，无论其名称是什么。请注意，由于 WIM 元数据修改和内容规范化工作的方式，映像文件可能会比删除之前更大。

6. （可选）如果要在公司恢复映像中包含驱动程序，请按照下述步骤操作：

   a. 使用以下命令，将映像安装到空文件夹中：

   ```
   mkdir C:\staging\mount

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

   b. 为支持的目标系统安装相应的 HP Windows 10 驱动程序 DVD (DRDVD)。使用以下命令，将驱动程序子文件夹从已安装的驱动程序介质复制到临时区域：

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

   注： `<M:>` 是指已安装的驱动器。替换为正确的驱动器号。

   将其他 .inf 样式的驱动程序放在 C:\staging\mount\SWSETUP\DRV 文件夹下，即可将其包含在内。有关 HP Sure Recover 如何使用 `dism /Add-Driver /Recurse` 函数处理此内容的说明，请参阅以下主题中的“将驱动程序添加到脱机 Windows 映像和删除脱机 Windows 映像中的驱动程序”：https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   此功能不支持需要运行应用程序的 .exe 样式驱动程序。

   c. 使用以下命令，保存更改并卸载映像：

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

   得到的镜像文件是：C:\staging\my-image.wim。

   d. 转至第 5 页的拆分映像。

示例 2：基于参考系统创建映像

1. 创建可启动的 USB WinPE 介质。

注： 捕获映像的其他方法可在 ADK 文档中找到。

确保 USB 驱动器有足够的可用空间来存放从参考系统捕获的映像。

2. 在参考系统上创建映像。
3. 通过使用 USB WinPE 介质启动参考系统捕获映像，然后使用 DISM。

注： `<U:>` 是指 USB 驱动器。替换为正确的驱动器号。

根据需要，编辑文件名的“my-image”部分以及 `<my-image>` 描述。

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

4. 使用以下命令，将映像从 USB 复制到工作系统的临时区域：

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

您应可获得以下映像文件：C:\staging\my-image.wim。

5. 转至第 5 页的拆分映像。

拆分映像

HP 建议您使用以下命令，将映像拆分成较小的文件，以提高网络下载的可靠性：

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

注： 所示的 FileSize 单位为兆字节。可在必要时进行编辑。

注： 由于 DISM 拆分算法的性质，生成的 SWM 文件可能小于或大于指定的文件大小。

创建清单

将清单文件的格式设置为不带字节顺序标记 (BOM) 的 UTF-8。

您可以更改在以下程序中使用的清单文件名 (custom.mft)，但不得更改扩展名 .mft 和 .sig，而且清单文件和签名文件的文件名部分必须匹配。例如，您可以将二者的配对 (custom.mft, custom.sig) 更改为 (myimage.mft, myimage.sig)。

`mft_version` 可用于确定映像文件的格式，当前必须设置为 1。

`image_version` 可用于确定是否存在更新的可用映像版本，并防止安装旧版本。

这两个值都必须是无符号 16 位整数，而清单中的行分隔符必须是 `'\r\n' (CR + LF)`。

生成清单

由于拆分映像可能涉及多个文件，因此使用 powershell 脚本生成清单。

其余所有步骤都必须在 C:\staging 文件夹中进行。

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

1. 使用以下命令，通过可生成文本文件（格式为不带 BOM 的 UTF-8）的编辑器，创建 powershell 脚本：`notepad C:\staging\generate-manifest.ps1`

   创建以下脚本：

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

   `$imageVersion = 1907`（注意：这可以是任意 16 位整数）

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

注： HP Sure Recover 的清单不能包含 BOM，因此以下命令可将文件改写为不带 BOM 的 UTF-8。

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. 保存脚本。
3. 执行脚本。

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

生成清单签名

Sure Recover 使用加密签名验证代理和映像。以下示例使用 X.509 PEM 格式的私人密钥/公共密钥对（.PEM 扩展名）。根据需要调整命令，以使用 DER 二进制证书（.CER 或 .CRT 扩展名）、BASE-64 编码 PEM 证书（.CER 或 .CRT 扩展名）或 PKCS1 PEM 文件（.PEM 扩展名）。该示例还使用 OpenSSL，它可以生成大端格式的签名。您可以使用任何实用程序对清单进行签名，但部分 BIOS 版本仅支持小端格式的签名。

1. 使用以下命令，生成一个 2048 位的 RSA 私人密钥。如果您具有 pem 格式的 2048 位 RSA 私人密钥/公共密钥对，请将其复制到 C:\staging，然后跳到步骤 3。

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

2. 使用以下命令，从私人密钥生成公共密钥（如果有对应于私人密钥的 PEM 格式公共密钥，请将其复制到 C:\staging）：

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

3. 使用以下命令，根据步骤 1 的 2048 位 RSA 私人密钥，创建一个签名文件（使用基于 sha256 的哈希）：

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

4. 使用以下命令，利用上一步骤中的公共密钥，验证签名文件：

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

注：

- 如果您只需创建一个签名文件，则必须执行步骤 1 和 3。
- 对于 HP Sure Recover，至少必须执行步骤 1、2 和 3。您需要步骤 2 中的公共密钥来配置目标系统。
- 步骤 4 为可选步骤，但建议您执行该步骤，以正确验证签名文件和清单文件。

托管文件

在您的服务器上，托管来自 C:\staging 文件夹的以下文件：

- *.swm
- custom.mft（或您为清单文件选择的文件名）
- custom.sig（或您为签名文件选择的匹配文件名）

注：如果您将 IIS 用作托管解决方案，则必须配置 MIME 条目以包含以下扩展名，全部配置为“application/octet-stream:”

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

配置目标系统

您可以使用 HP Client Management Script Library、HP Client Security Manager (CSM)/Sure Recover 或 Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement) 来配置目标系统。

提供此配置的以下信息：

1. 上一部分中托管的清单文件的 URL 地址 (http://your_server.domain/path/custom.mft)
2. 用于验证先前创建的签名文件的公共密钥（例如 C:\staging\my-recovery-public.pem）。

故障排除

如果收到有关自定义恢复进程安全验证失败的消息，请检查以下内容：

1. 清单必须是不带 BOM 的 UTF-8。
2. 检查文件哈希。
3. 确保系统已配置公共密钥，而且该公共密钥与用来对清单进行签名的私人密钥相对应。
4. IIS 服务器 mime 类型必须是 `application/octet-stream`。
5. 清单内的文件路径必须包括，从客户端系统的角度看包含映像的最上层目录的完整路径。该路径并非文件在分发点的完整保存路径。

3 在公司防火墙内使用 HP Sure Recover 代理

HP Sure Recover 代理可托管在企业 Intranet 中。安装 HP Sure Recover SoftPaq 之后，将 HP Sure Recover 代理目录中的代理文件，从安装位置复制到 HTTP 或 FTP 分发点。然后，使用分发点的 URL 和名为 `hpsr_agent_public_key.pem` 的 HP 公共密钥，对客户端系统进行配置，该公共密钥与 HP Sure Recover 代理 SoftPaq 一起分发。

安装 HP Sure Recover 代理

1. 下载 HP Sure Recover 代理，然后将文件提取到 HTTP 或 FTP 分发点。
2. 在分发点，设置适当的文件权限。
3. 如果您使用 Internet 信息服务 (IIS)，请针对以下文件格式，创建“application/octet-stream”的 MIME 类型：
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   切记：以下步骤描述了使用 SCCM 配置 Sure Recover 的方法。有关如何使用 HP Client Management Script Library 配置 Sure Recover 的示例，请参阅 第 11 页的使用 HP Client Management Script Library (CMSL)。
4. 启动 SCCM，导航到 **HP Client Security Suite**，然后选择“HP Sure Recover”页面。

   注：分发点 URL 包含 ftp 或 http 作为传输协议。它还包括，从客户端系统的角度看 HP Sure Recover 代理包含清单的最上层目录的完整路径。该路径并非文件在分发点的完整保存路径。
5. 在**平台映像**部分中，选择**公司**选项，从公司分发点恢复自定义的 OS 映像。将 IT 管理员提供的 URL 输入**映像位置 URL** 输入框。将公共密钥 `hpsr_agent_public_key.pem` 输入**映像验证**字段。

   注：自定义映像 URL 必须包含映像清单文件名。
6. 在**恢复代理**部分，选择**公司**选项，以使用自定义恢复代理或来自公司分发点的 HP 恢复代理。将 IT 管理员提供的 URL 输入**代理位置 URL** 输入框。将公共密钥 `hpsr_agent_public_key.pem` 输入**代理验证密钥**输入字段。

   注：请不要在 URL 中加入代理清单的文件名，因为 BIOS 要求将其命名为 recovery.mft。

7. 将策略应用到客户端系统后，重新启动该系统。
8. 初始配置期间，系统会提示您输入 4 位安全代码，以完成 HP Sure Recover 激活。有关更多详细信息，请访问 hp.com，并搜索 HP Manageability Integration Kit (MIK) for Microsoft System Center Manager 白皮书。

HP Sure Recover 激活成功完成后，该策略应用的自定义 URL 将显示在 HP Sure Recover BIOS 设置菜单中。

要确认激活成功，请重新启动计算机，并在 HP 徽标出现时按 f10。依次选择**高级**、**HP Sure Recover**、**恢复代理**以及 **URL**。

4 使用 HP Client Management Script Library (CMSL)

HP Client Management Script Library 允许您使用 PowerShell 管理 HP Sure Recover 设置。下面的示例脚本演示了如何配置、确定状态、更改配置和取消配置 HP Sure Recover。

注： 有几个命令超出了本指南的行长度，但必须以单行形式输入。

```
$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
}
```

使用 OpenSSL 生成示例密钥

将私人密钥存放在安全的位置。公共密钥将用于验证，而且必须在配置期间提供。这些密钥的长度必须为 2048 位，而且必须使用 0x10001 的指数。用贵组织的相关信息替换示例中的主题。

在继续操作之前，请先设置以下环境变量：

```
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:
```

您可以使用以下命令对映像清单进行签名：

```
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:
```

您可以使用以下命令对代理清单进行签名：

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

OpenSSL 可以生成大端格式的签名文件，这些文件与某些 BIOS 版本不兼容；因此，代理签名文件的字节顺序可能需要在部署之前进行反转。支持大端字节排序的 BIOS 版本也支持小端字节排序。

A 故障排除

驱动器分区失败

如果使用 Bitlocker 对 SR_AED 或 SR_IMAGE 分区进行加密，则可能发生驱动器分区失败的情况。这些分区通常使用 gpt 属性创建，该属性可以防止 Bitlocker 对分区进行加密，但如果用户在删除分区后重新创建分区，或者在裸机驱动器上手动创建分区，那么 Sure Recover 代理将无法删除这些分区，而且会在对驱动器重新分区时退出并显示出错。用户必须通过运行 diskpart、选择卷、然后发出 `del vol` 覆盖命令或类似命令，来手动删除这些分区。

固件审核日志

EFI 变量信息如下：

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

Windows 下存在用于读取 EFI 变量的 API，或者您可以使用 UEFI Shell dmpstore 实用程序将变量内容转储到文件中。

您可以使用 HP Client Management Script Library 提供的 `Get-HPFirmwareAuditLog` 命令转储审核日志。

Windows 事件日志

Sure Recover 的启动和停止事件会发送到 BIOS 审核日志中，如果安装了 HP Notifications，则您可以使用 Windows 事件查看器在 Sure Start 日志中查看这些事件。这些事件包括日期和时间、源 ID、事件 ID 和事件特定代码。例如，`[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` 表示恢复失败，因为无法使用在 2018 年 6 月 27 日 2:26:40 记录的事件特定代码 c3f 23000 对清单进行身份验证。

注： 这些日志遵循“月/日/年”的美国日期格式。

HP Secure Platform Management（源 ID = 84h）

表 A-1 HP Secure Platform Management

事件 ID	设备数（全部/DaaS）	事件数（全部/DaaS）	说明	注释
40	256/178	943/552	平台 OS 恢复进程由固件启动。	已启动平台恢复
41	221/147	588/332	平台 OS 恢复进程已成功完成。	平台恢复已完成
42	54/42	252/156	平台 OS 恢复进程未能成功完成。	平台恢复失败

您可以使用 HP Client Management Script Library（可在 http://www.hp.com/go/clientmanagement 找到）中的 Get-HPFirmwareAuditLog 检索固件审核日志。HP Secure Platform Management 的事件 ID 为 40、41

和 42，可在数据字段中返回事件特定代码，以指示 Sure Recover 操作的结果。例如，以下日志条目表示 Sure Recover 未能下载清单或签名文件，并显示错误 event_id 42 和数据：00:30:f1:c3，这应解释为 dword value 0xC3F13000 = MftOrSigDownloadFailed。

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:30:f1:c3
```

成功的恢复显示为 event_id = 41 和数据：00:00:00:00，例如：

```
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 使用以下事件特定代码。

表 A-2 事件特定代码

事件描述	事件代码
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000

表 A-2 事件特定代码（续）

事件描述	事件代码
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