



使用指南

HP Sure Recover

© Copyright 2020 HP Development
Company, L.P.

Microsoft 和 Windows 是 Microsoft
Corporation 在美國和/或其他國家/地區
的註冊商標或商標。

此為機密電腦軟體。持有、使用或複製
均需要 HP 的有效授權。在遵守 FAR
12.211 和 12.212 條款的情況下，「商
用電腦軟體」、「電腦軟體說明文件」
和「商用項目技術資料」係按照廠商的
標準商用授權條款授權給美國政府。

本文件包含的資訊可能有所變更，恕不
另行通知。HP 產品與服務的保固僅列
於產品及服務隨附的明確保固聲明中。
本文件的任何部份都不可構成任何額外
的保固。HP 不負責本文件在技術上或
編輯上的錯誤或疏失。

第一版：2020 年 2 月

文件編號：L93434-AB1

使用者輸入語法金鑰

您必須輸入到使用者介面中的文字由固定寬度字型指示。

表格 -1 使用者輸入語法金鑰


項目	說明
沒有中括號或大括號的文字	您必須依所示內容完全輸入的項目
<角括號內的文字>	您必須為值提供的預留位置；省略括號
[方括號內的文字]	可選項目；省略括號
{大括號內的文字}	您只能從中選擇一者的一組項目；省略大括號
	您只能從中選擇一者的項目的分隔符號；省略分隔號
...	可以或必須重複的項目；省略省略符號

目錄

1 快速入門	1
執行網路復原	1
執行本機磁碟機復原	1
2 建立公司映像	2
需求	2
建立映像	2
範例 1：根據 Microsoft Windows 安裝映像建立映像	2
範例 2：根據參考系統建立映像	4
分割映像	5
建立資訊清單	5
產生資訊清單	5
產生資訊清單簽名	6
代管檔案	7
佈建您的目標系統	7
疑難排解	8
3 在公司防火牆內使用 HP Sure Recover 代理程式	9
安裝 HP Sure Recover 代理程式	9
4 使用 HP Client Management Script Library (CMSL)	11
使用 OpenSSL 產生金鑰的範例	13
附錄 A 疑難排解	16
磁碟機分割失敗	16
韌體稽核記錄檔	16
Windows 事件記錄檔	16
HP Secure 平台管理 (來源 ID = 84h)	16

1 快速入門

HP Sure Recover 可協助您從網路安全安裝作業系統，且只需最少的使用者互動。採用具有內嵌重建映像功能的 HP Sure Recover 的系統也支援從本機儲存裝置進行安裝。


 **重要：**使用 HP Sure Recover 前，請備份您的資料。由於映像建立程序會重新格式化磁碟機，因此將會遺失資料。

HP 提供的復原映像包含基本 Windows 10® 安裝程式。或者，HP Sure Recover 也可以安裝適用於 HP 裝置的最佳化驅動程式。HP 復原映像只包含 Windows 10 隨附的資料復原代理程式，例如 OneDrive。公司可以建立自己的自訂映像，以新增公司設定、應用程式、磁碟機與資料復原代理程式。

作業系統 (OS) 復原代理程式可執行安裝復原映像所需的步驟。HP 提供的復原代理程式可執行一般步驟，例如磁碟分割、格式化，以及將復原映像解壓縮至目標裝置。由於 HP 復原代理程式位於 hp.com，除非系統包含內嵌重建映像，否則您需要能夠存取網際網路才能擷取該程式。公司也可以在其防火牆內代管 HP 復原代理程式，或為更多複雜的復原環境建立自訂復原代理程式。

您可以在找不到作業系統時起始 HP Sure Recover。您也可以按照排程執行 HP Sure Recover，例如確保惡意軟體已經移除。透過 HP Client Security Manager (CSM)、Manageability Integration Kit (MIK) 或 HP Client Management Script Library 執行這些設定。

執行網路復原

 **附註：**若要執行網路復原，您必須使用有線連線。HP 建議在使用 HP Sure Recover 之前備份重要的檔案、資料、相片、影片等，以防資料遺失。

1. 將用戶端系統連線至可以存取 HTTP 或 FTP 分派點的網路。
2. 重新啟動用戶端系統，當 HP 標誌顯示時，按下 **f11**。
3. 選取**從網路復原**。

執行本機磁碟機復原

如果用戶端系統支援內嵌重建映像，且已在套用的原則中啟用排定的映像下載選項，則映像會在排定時間下載至用戶端系統。當映像下載至用戶端系統之後，請重新啟動以將映像複製到內嵌重建映像儲存裝置。

若要使用內嵌重建映像儲存裝置上的映像執行本機復原：

1. 重新啟動用戶端系統，當 HP 標誌顯示時，按下 **f11**。
2. 選取**從本機磁碟復原**。

具有內嵌重建映像功能的系統必須設定下載排程並使用下載代理程式檢查更新。下載代理程式隨附在適用於 HP Client Security Manager 的 HP Sure Recover 外掛程式中，也可以在 MIK 中設定。如需使用 MIK 的指示，請參閱 <https://www.hp.com/go/clientmanagement>。

您也可以建立排定工作來將代理程式複製到 SR_AED 分割區，以及將映像複製到 SR_IMAGE 分割區。然後您可以使用 HP Client Management Script Library 傳送服務事件，通知 BIOS 其應驗證內容，並在下次重新啟動時將內容複製到內嵌重建映像儲存裝置。

2 建立公司映像

大部分公司都使用 Microsoft Deployment Tools、Windows 10 評估與部署套件，或使用這兩者來產生在 Windows Imaging (WIM) 檔案格式封存內包含映像的檔案。

需求

- 最新版本的 Windows 10 評估與部署套件 (Windows ADK)
- PowerShell
- OpenSSL (或產生 RSA 私人/公用金鑰對的其他解決方案)
用來產生 RSA 金鑰對來保護您建立及代管之公司映像的完整性。
- 伺服器代管解決方案 (例如 Microsoft Internet Information Services [IIS])

建立映像

開始映像建立程序之前，設定安裝所需工具的工作系統或建立相關系統，以準備好處理映像，如以下步驟所示：

1. 以管理員身分開啟部署與映像工具環境命令提示字元 (隨 Windows ADK 的部署工具安裝)。
2. 使用下列指令建立映像的暫存區：

```
mkdir C:\staging
```

3. 使用以下其中一個範例建立映像：

[位於第 2 頁的範例 1：根據 Microsoft Windows 安裝映像建立映像](#)

[位於第 4 頁的範例 2：根據參考系統建立映像](#)

範例 1：根據 Microsoft Windows 安裝映像建立映像

1. 掛接或開啟 Microsoft Windows 安裝映像 (從 Microsoft ISO，或從 HP OSDVD)。
2. 從掛接的 Windows 安裝映像，使用下列指令將 install.wim 檔案複製到您的暫存區：

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



附註： <M:> 是指掛接的磁碟機。將其取代為正確的磁碟機代號。

3. 使用下列指令，將 install.wim 重新命名為映像檔名稱 (就本例而言為「my-image」)：

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

(可選) HP Sure Recover 包含根據原本針對原廠 HP 目標系統授權的 Windows 版本，從多索引映像復原特定版本的功能。如果索引命名正確，則適用此機制。如果您的 Windows 安裝映像來自 HP OSDVD 映像，您可能會有多个版本的映像。如果您不想採用此方式，而是要確保針對所有目標系統使用一個特定版本，則需要確保安裝映像中只有一個索引。

4. 使用下列指令檢查安裝映像的內容：

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


以下顯示從支援五個版本的安裝映像輸出的範例 (根據每個目標系統的 BIOS 進行比對) :

映像的詳細資料 : my-image.wim

索引 : 1

名稱 : CoreSingleLanguage

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

大小 : 19,512,500,682 bytes

索引 : 2

名稱 : Core

說明 : Windows 10 May 2019 Update - Home edition

大小 : 19,512,500,682 bytes

索引 : 3

名稱 : Professional

說明 : Windows 10 May 2019 Update- Professional Update

大小 : 19,758,019,520 bytes

索引 : 4

名稱 : ProfessionalEducation

說明 : Windows 10 May 2019 Update - Professional Education edition


大小 : 19,758,019,480 bytes

索引 : 5

名稱 : ProfessionalWorkstation

說明 : Windows 10 May 2019 Update - Professional Workstation edition

大小 : 19,758,023,576 bytes

 **附註：**當只有一個索引時，無論名稱為何，映像均可用於復原。映像檔的大小可能大於刪除之前的大小。

5. 如果您不想要多版本的方式，請刪除您不想要的每個索引。

如以下範例所示，如果只需要專業版 (假設所有目標系統均已獲得授權)，請刪除索引 5、4、2 與 1。每次您刪除索引時，都會重新指派索引編號。因此，您應從最高到最低的索引編號來刪除。每次刪除後執行 `Get-ImageInfo` 來以視覺化的方式確認您接下來要刪除哪個索引。

```
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
```

請只選擇版本的一個索引 (例如, 專業版)。當只有一個索引時, 無論名稱為何, 映像均可用於復原。請注意, 由於 WIM 中繼資料修改與內容正規化工作的方式, 映像檔的大小可能大於刪除之前的大小。


6. (可選) 如果您要在公司復原映像中包含磁碟機, 請遵循以下步驟:

a. 使用以下指令, 將您的映像掛接到空白資料夾:

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

b. 針對支援的目標系統掛接適當的 HP Windows 10 驅動程式 DVD (DRDVD)。從掛接的磁碟機媒體, 使用下列指令將驅動程式子資料夾複製到您的暫存區:

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

 **附註:** <M:> 是指掛接的磁碟機。將其取代為正確的磁碟機代號。

您可以將其他 .inf 樣式的驅動程式放在 C:\staging\mount\SWSETUP\DRV 資料夾底下來包含這些驅動程式。如需有關 HP Sure Recover 如何使用 `dism /Add-Driver /Recurse` 功能處理此內容的說明, 請參閱以下主題中的「將驅動程式新增至離線 Windows 映像及從中移除驅動程式」: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>。

此功能不支援需要執行應用程式的 .exe 樣式驅動程式。

c. 使用以下指令, 儲存變更並取消掛接映像:


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

所得映像檔為: C:\staging\my-image.wim。

d. 前往[位於第 5 頁的分割映像](#)。

範例 2 : 根據參考系統建立映像


1. 建立可開機的 USB WinPE 媒體。

 **附註:** 擷取映像的其他方法可在 ADK 文件中找到。

確保 USB 磁碟機擁有足夠的可用空間, 可以存放從參考系統擷取的映像。

2. 根據參考系統建立映像。

3. 使用 USB WinPE 媒體啟動參考系統來擷取映像, 然後使用 DISM。

 **附註:** <U:> 是指 USB 磁碟機。將其取代為正確的磁碟機代號。

依照需求編輯檔案名稱中的「my-image」部分, 以及 <my-image> 說明。

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

4. 使用以下指令, 將映像從 USB 複製到工作系統中的暫存區:

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

您應有下列映像檔：C:\staging\my-image.wim。


5. 前往 [位於第 5 頁的分割映像](#)。

分割映像

HP 建議您使用以下指令，將映像分割為較小的檔案，以改善網路下載的可靠性：

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

 **附註：** FileSize 會以百萬位元組為單位顯示。視需要進行編輯。

 **附註：** 由於 DISM 分割演算法的特性，所產生 SWM 檔案的大小可能會小於，也可能會大於表示的檔案大小。

建立資訊清單

請將資訊清單檔案格式化為無位元組順序標記 (BOM) 的 UTF-8。

您可以變更在下列程序中使用的資訊清單檔案名稱 (custom.mft)，但不得變更副檔名 .mft 與 .sig，且資訊清單與簽名檔案的檔案名稱部分必須相符。例如，您可以將配對 (custom.mft、custom.sig) 變更為 (myimage.mft、myimage.sig)。

mft_version 用來確定映像檔的格式，且目前必須設定為 1。

image_version 用來確定是否有較新版本的映像，並防止安裝舊版。

這兩個值都必須是無正負符號的 16 位元整數，資訊清單中的行分隔符號必須是「\r\n」(CR + LF)。

產生資訊清單

由於可能有數個檔案涉及您的分割映像，因此請使用 powershell 指令碼來產生資訊清單。

在所有剩餘的步驟中，您都必須位於 C:\staging 資料夾中。

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

1. 透過下列指令，使用可在無 BOM 的情況下以 UTF-8 格式產生文字檔案的編輯器建立 powershell 指令碼：notepad C:\staging\generate-manifest.ps1

建立下列指令碼：

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

```
$imageVersion = 1907 (注意：這可以是任何 16 位元的整數)
```

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

```

 **附註：** HP Sure Recover 的資訊清單不可包含 BOM，因此以下指令會將檔案重寫為不含 BOM 的 UTF8。

```

$content = Get-Content $mftFilename

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

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

```

2. 儲存指令碼。
3. 執行指令碼。

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

產生資訊清單簽名

Sure Recover 會使用加密簽名驗證代理程式與映像。以下範例使用 X.509 PEM 格式 (.PEM 副檔名) 的私人/公用金鑰對。視情況調整指令以使用 DER 二位憑證 (.CER 或 .CRT 副檔名)、BASE-64 編碼的 PEM 憑證 (.CER 或 .CRT 副檔名) 或 PKCS1 PEM 檔案 (.PEM 副檔名)。範例也使用 OpenSSL，它會以大位元組順序格式

產生簽名。您可以使用任何公用程式來為資訊清單簽名，但某些 BIOS 版本只支援小位元組順序格式的簽名。

1. 使用以下指令產生 2048 位元 RSA 私人金鑰。如果您有 pem 格式的 2048 位元 RSA 私人/公用金鑰對，請將其複製到 C:\staging，然後跳到步驟 3。

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

2. 使用以下指令，從您的私人金鑰產生公用金鑰 (如果您的公用金鑰對應於您的 PEM 格式私人金鑰，請將其複製到 C:\staging)：

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

3. 使用以下指令，根據您在步驟 1 中的 2048 位元 RSA 私人金鑰建立簽名檔案 (使用 sha256 式雜湊)：

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

4. 使用以下指令，透過您在上一步中的公用金鑰確認簽名檔案：

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


 **附註：**

- 如果您只需要建立簽名檔案，所需步驟為 1 與 3。
 - 針對 HP Sure Recover，最少需要執行的步驟為 1、2 與 3。您需要步驟 2 中的公用金鑰來佈建您的目標系統。
 - 步驟 4 為可選，但建議執行，這樣就能正確驗證您的簽名檔案與資訊清單檔案。
-

代管檔案

從 C:\staging 資料夾代管您伺服器上的下列檔案：

- *.swm
- custom.mft (或您為資訊清單檔案選擇的檔案名稱)
- custom.sig (或您為簽名檔案選擇的相符檔案名稱)

 **附註：** 如果您使用 IIS 做為您的代管解決方案，必須設定您的 MIME 項目以包含下列副檔名，全都設定為「application/octet-stream:」

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

佈建您的目標系統

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>) 佈建您的目標系統。

為此佈建提供下列資訊：

1. 在上一節中代管之資訊清單檔案的 URL 位址 (http://your_server.domain/path/custom.mft)
2. 用來確認之前建立之簽名檔案的公用金鑰 (例如，C:\staging\my-recovery-public.pem)。

疑難排解

如果您收到有關自訂復原程序無法完成安全性驗證的訊息，請檢查以下項目：

1. 資訊清單必須是沒有 BOM 的 UTF-8。
2. 檢查檔案雜湊。
3. 確保佈建系統所使用的公用金鑰對應於用來為資訊清單簽名的私人金鑰。
4. IIS 伺服器 mime 類型必須是 `application/octet-stream`。
5. 資訊清單內的檔案路徑必須包含最上層目錄的完整路徑，其中包含從用戶端系統中看見的映像。此路徑不是檔案儲存在分派點之處的完整路徑。

3 在公司防火牆內使用 HP Sure Recover 代理程式


HP Sure Recover 代理程式可在公司內部網路上代管。當您安裝 HP Sure Recover SoftPaq 之後，將 HP Sure Recover 代理程式目錄中的代理程式檔案從安裝位置複製到 HTTP 或 FTP 分派點。然後使用分派點的 URL 與名為 `hpsr_agent_public_key.pem` 的 HP 公用金鑰 (其透過 HP Sure Recover 代理程式 SoftPaq 分派) 佈建用戶端系統。

安裝 HP Sure Recover 代理程式


1. 下載 HP Sure Recover 代理程式，並將檔案解壓縮至您的 HTTP 或 FTP 分派點。
2. 在分派點上設定適當的檔案權限。
3. 如果您正在使用 Internet Information Services (IIS)，請為下列檔案格式建立 application/octet-stream MIME 類型：
 - .
 - .wim
 - .swm
 - .mft
 - .sig
 - .efi
 - .sdi

 **重要：** 以下步驟說明如何使用 SCCM 佈建 Sure Recover。如需如何使用 HP Client Management Script Library 佈建 Sure Recover 的範例，請參閱[位於第 11 頁的使用 HP Client Management Script Library \(CMSL\)](#)。


4. 啟動 SCCM，前往 **HP Client Security Suite**，然後選取 HP Sure Recover 頁面。

 **附註：** 分派點 URL 包含 ftp 或 http 做為傳輸通訊協定。其中也包含最上層目錄的完整路徑，該目錄包含從用戶端系統中看見之 HP Sure Recover 代理程式的資訊清單。此路徑不是檔案儲存在分派點之處的完整路徑。

5. 在**平台映像**區段中，選取**公司**選項以從公司分派點復原自訂 OS 映像。將 IT 管理員提供的 URL 輸入到**映像位置 URL** 輸入方塊中。將公用金鑰 `hpsr_agent_public_key.pem` 輸入到**映像驗證**欄位中。

 **附註：** 自訂映像 URL 必須包含映像資訊清單檔案名稱。

6. 在**復原代理程式**區段中，選取**公司**選項以從公司分派點使用自訂復原代理程式或 HP 復原代理程式。將 IT 管理員提供的 URL 輸入到**代理程式位置 URL** 輸入方塊中。將公用金鑰 `hpsr_agent_public_key.pem` 輸入到**代理程式驗證金鑰**輸入欄位中。

 **附註：**請勿在 URL 中包含代理程式資訊清單的檔案名稱，因為 BIOS 需要將其命名為 recovery.mft。


7. 將原則套用至用戶端系統之後，請重新啟動。
8. 在初始佈建期間，會顯示提示請您輸入 4 位數的安全代碼以完成 HP Sure Recover 啟動。如需詳細資訊，請前往 hp.com 並搜尋適用於 Microsoft System Center Manager 白皮書的 HP Manageability Integration Kit (MIK)。

HP Sure Recover 啟動成功完成後，原則套用的自訂 URL 會顯示在 HP Sure Recover BIOS 設定功能表中。

若要確認啟動成功，請重新啟動電腦，並於顯示 HP 標誌時按下 **f10**。依次選取**進階**、**HP Sure Recover**、**復原代理程式**、**URL**。

4 使用 HP Client Management Script Library (CMSL)

HP Client Management Script Library 可以讓您透過 PowerShell 管理 HP Sure Recover 設定。以下範例指令碼展示如何佈建、確定狀態、變更設定及解除佈建 HP Sure Recover。

 **附註：**有一些指令超出了本指南的行長度，但必須輸入為一行。

```
$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 產生金鑰的範例

將私人金鑰儲存在安全的位置。公用金鑰將用於驗證，且必須在佈建期間提供。這些金鑰的長度需為 2048 位元，並且使用 0x10001 的指數。請用您組織的相關資訊取代範例中的對象。

請先設定下列環境變數然後再繼續：

```

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:

```

您可以使用以下指令為映像資訊清單簽名：

```
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:

```

您可以使用以下指令為代理程式資訊清單簽名：

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

OpenSSL 會以大位元組順序格式產生簽名檔案，而此格式與某些 BIOS 版本不相容，因此可能需要先反轉代理程式簽名檔案位元組順序才能部署。支援大位元組順序的 BIOS 版本也支援小位元組順序。

A 疑難排解

磁碟機分割失敗

如果使用 Bitlocker 加密 SR_AED 或 SR_IMAGE 分割區，便可能發生磁碟機分割失敗的情形。這些分割區通常使用 gpt 屬性建立，此屬性會防止 Bitlocker 為其加密，但如果使用者刪除並重建分割區，或在裸機磁碟機上手動建立分割區，Sure Recover 代理程式就無法刪除分割區，並於分割磁碟機時因發生錯誤而退出。使用者必須執行 diskpart、選取磁碟區，然後發出 del vol 覆寫指令或類似指令來手動刪除分割區。

韌體稽核記錄檔

EFI 變數資訊如下：

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

API 存在於 Windows 之下，可用於讀取 EFI 變數，或者您可以使用 UEFI Shell dmpstore 公用程式將變數內容傾印至檔案。

您可以使用 HP Client Management Script Library 提供的 Get-HPFirmwareAuditLog 指令來傾印稽核記錄檔。

Windows 事件記錄檔

Sure Recover 啟動與停止事件會傳送至 BIOS 稽核記錄檔，如果安裝了 HP Notifications，便可使用 Windows 事件檢視器在 Sure Start 記錄檔中檢視。這些事件包含日期與時間、來源 ID、事件 ID 以及事件特定代碼。例如，[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3] 指示由於資訊清單無法使用記錄於 6/27/18 2:26:40 的事件特定代碼 c3f 23000 驗證，因此復原失敗。

 **附註：** 這些記錄檔遵循美國日期格式月/日/年。

HP Secure 平台管理 (來源 ID = 84h)

表格 A-1 HP Secure 平台管理

事件 ID	裝置計數 (All/DaaS)	事件計數 (All/DaaS)	說明	註
40	256/178	943/552	平台 OS 復原程序由韌體啟動。	平台復原開始
41	221/147	588/332	平台 OS 復原程序已成功完成。	平台復原完成
42	54/42	252/156	平台 OS 復原程序無法成功完成。	平台復原失敗

您可以使用 HP Client Management Script Library 中的 Get-HPFirmwareAuditLog 擷取韌體稽核記錄檔，其位於 <http://www.hp.com/go/clientmanagement>。HP Secure 平台管理事件 ID 40、41 與 42 會在資料欄位

中傳回事件特定代碼，指示 Sure Recover 作業的結果。例如，以下記錄檔項目指示 Sure Recover 無法下載資訊清單或簽名檔案，錯誤為 event_id 42，資料：00:30:f1:c3，其應解讀為 dword 值 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
```

成功復原會顯示為 event_id = 41，資料：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 使用下列事件特定代碼。

表格 A-2 事件特定代碼

事件說明	事件代碼
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000

表格 A-2 事件特定代碼 (續)

事件說明	事件代碼
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