# Guida per l'utente

## HP Sure Recover

Prima edizione: febbraio 2020

Numero di parte del documento: L93434-061

## Chiave di sintassi di input dell'utente

Il testo da immettere in un'interfaccia utente è indicato da un `carattere a spaziatura fissa`.

**Tabella -1 Chiave di sintassi di input dell'utente**

| Elemento | Descrizione |
|---|---|
| `Testo senza parentesi quadre o graffe` | Digitare gli elementi esattamente come indicato |
| `<Testo all'interno di parentesi acute>` | Un segnaposto per un valore da immettere; omettere le parentesi |
| `[Testo all'interno di parentesi quadre]` | Elementi opzionali; omettere le parentesi |
| `{Testo all'interno di parentesi graffe}` | Un insieme di elementi tra cui è necessario sceglierne solo uno; omettere le parentesi graffe |
| `\|` | Un separatore per gli elementi tra cui è necessario sceglierne solo uno; omettere la barra verticale |
| `...` | Elementi che possono o devono essere ripetuti; omettere i puntini di sospensione |

# Sommario

# 1 Guida introduttiva

HP Sure Recover consente di installare in modo sicuro il sistema operativo dalla rete con una minima interazione dell'utente. I sistemi con HP Sure Recover with Embedded Reimaging supportano inoltre l'installazione da un dispositivo di archiviazione locale.

**IMPORTANTE:** Effettuare il backup dei dati prima di utilizzare HP Sure Recover. Poiché il processo di imaging riformatta l'unità, i dati andranno persi.

Le immagini di ripristino fornite da HP includono il programma di installazione di base di Windows 10®. In alternativa, HP Sure Recover può installare driver ottimizzati per i dispositivi HP. Le immagini di ripristino HP includono solo agenti di recupero dati inclusi in Windows 10, come OneDrive. Le aziende possono creare immagini personalizzate per aggiungere impostazioni, applicazioni, driver e agenti di recupero dati.

Un agente di recupero del sistema operativo (OS) esegue i passaggi necessari per installare l'immagine di ripristino. L'agente di recupero fornito da HP esegue passaggi comuni come partizionamento, formattazione ed estrazione dell'immagine di ripristino al dispositivo di destinazione. Poiché l'agente di recupero HP si trova su hp.com, è necessario l'accesso a Internet per recuperarlo, a meno che il sistema non includa una funzione di Embedded Reimaging. Le aziende possono inoltre ospitare l'agente di recupero HP all'interno del firewall o creare agenti di recupero personalizzati per ambienti di ripristino più complessi.

È possibile avviare HP Sure Recover quando non viene trovato nessun sistema operativo. È inoltre possibile eseguire HP Sure Recover in base a una pianificazione, per esempio per assicurarsi che i malware vengano rimossi. Eseguire la configurazione di tali impostazioni tramite HP Client Security Manager (CSM), Manageability Integration Kit (MIK) o HP Client Management Script Library.

## Esecuzione di un ripristino di rete

**NOTA:** Per eseguire un ripristino di rete, è necessario utilizzare una connessione cablata. HP consiglia di eseguire il backup di file, dati, foto, video e altri contenuti importanti prima di utilizzare HP Sure Recover per evitare la perdita di dati.

1. Connettere il sistema client alla rete in cui è possibile accedere al punto di distribuzione HTTP o FTP.
2. Riavviare il sistema client e, quando viene visualizzato il logo HP, premere f11.
3. Selezionare **Restore from network** (Ripristino da rete).

## Esecuzione di un ripristino dell'unità locale

Se il sistema client supporta l'Embedded Reimaging e l'opzione di download programmato dell'immagine è abilitata nel criterio applicato, l'immagine viene scaricata nel sistema client all'ora pianificata. Dopo aver scaricato l'immagine nel sistema client, riavviarla per copiare l'immagine nel dispositivo di archiviazione Embedded Reimaging.

Per eseguire il ripristino locale utilizzando l'immagine sul dispositivo di archiviazione Embedded Reimaging:

1. Riavviare il sistema client e, quando viene visualizzato il logo HP, premere f11.
2. Selezionare **Ripristina dal disco locale**.

I sistemi con Embedded Reimaging devono configurare una pianificazione di download e utilizzare l'agente di download per controllare la disponibilità di aggiornamenti. L'agente di download è incluso nel plug-in HP Sure

Recover per HP Client Security Manager e può anche essere configurato in MIK. Vedere https://www.hp.com/go/clientmanagement per le istruzioni su come usare MIK.

È inoltre possibile creare un'attività pianificata per copiare l'agente nella partizione SR_AED e l'immagine nella partizione SR_IMAGE. È quindi possibile utilizzare HP Client Management Script Library per inviare un evento di servizio che informa il BIOS che deve convalidare il contenuto e copiarlo sul dispositivo di archiviazione Embedded Reimaging al successivo riavvio.

# 2 Creazione di un'immagine aziendale

La maggior parte delle aziende utilizza gli strumenti di distribuzione Microsoft, Windows 10 Assessment and Deployment Kit o entrambi per produrre file contenenti un'immagine all'interno di un archivio di file in formato Windows Imaging (WIM).

## Requisiti

- La versione più recente di Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (o altra soluzione per generare una coppia di chiavi pubbliche/private RSA)

  Da utilizzare per generare la coppia di chiavi RSA usata per proteggere l'integrità dell'immagine aziendale creata e ospitata.
- Una soluzione di server hosting (come Microsoft Internet Information Services [IIS])

## Creazione dell'immagine

Prima di avviare il processo di creazione dell'immagine, impostare il sistema operativo o il sistema di generazione in cui sono stati installati gli strumenti necessari per preparare l'elaborazione dell'immagine, come illustrato nei passaggi riportati di seguito:

1. Come amministratore, aprire il prompt dei comandi per la `Ambiente degli strumenti di distribuzione e creazione immagini` (installato con gli strumenti di distribuzione di Windows ADK).
2. Creare un'area di staging per l'immagine, utilizzando il comando seguente:

   ```
   mkdir C:\staging
   ```
3. Creare l'immagine utilizzando uno dei seguenti esempi:

   Esempio 1: Creazione di un'immagine basata sull'immagine di installazione di Microsoft Windows a pagina 3

   Esempio 2: Creazione di un'immagine basata su un sistema di riferimento a pagina 6

### Esempio 1: Creazione di un'immagine basata sull'immagine di installazione di Microsoft Windows

1. Montare o aprire l'immagine di installazione di Microsoft Windows (da un'immagine ISO Microsoft o da un'immagine OSDVD HP).
2. Dall'immagine di installazione di Windows montata, copiare il file install.wim nell'area di staging, utilizzando il comando riportato di seguito:

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

**NOTA:** `<M:>` indica l'unità montata. Sostituire con la lettera corretta dell'unità.

3. Rinominare install.wim con il nome di un file di immagine ("my-image" per questo esempio), utilizzando il comando riportato di seguito:

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

   Facoltativo - HP Sure Recover include una funzione per ripristinare un'edizione specifica da un'immagine multi-index basata sull'edizione di Windows originariamente concessa in licenza per il sistema target HP in fabbrica. Questo meccanismo funziona se gli indici sono denominati correttamente. Se l'immagine di installazione di Windows proviene da un'immagine OSDVD HP, è probabile che si disponga di un'immagine multiedition. Se non si desidera questo comportamento, ma si desidera garantire che una specifica edizione venga usata per tutti i sistemi target, occorre assicurarsi che l'unico indice sia nell'immagine di installazione.

4. Controllare il contenuto dell'immagine di installazione tramite il comando seguente:

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

   Di seguito è mostrato l'output di esempio di un'immagine di installazione che supporta cinque edizioni (da abbinare in base al BIOS di ciascun sistema target):

   Dettagli dell'immagine: `my-image.wim`

   Indice: `1`

   Nome: `CoreSingleLanguage`

   Descrizione: `Windows 10 May 2019 Update - Home Single Language Edition`

   Dimensioni: `19,512,500,682 bytes`

   Indice: `2`

   Nome: `Core`

   Descrizione: `Windows 10 May 2019 Update - Home edition`

   Dimensioni: `19,512,500,682 bytes`

   Indice: `3`

   Nome: `Professional`

   Descrizione: `Windows 10 May 2019 Update- Professional Update`

   Dimensioni: `19.758,019,520 bytes`

   Indice: `4`

   Nome: `ProfessionalEducation`

   Descrizione: `Windows 10 May 2019 Update - Professional Education edition`

   Dimensioni: `19,758,019,480 bytes`

   Indice: `5`

   Nome: `ProfessionalWorkstation`

   Descrizione: `Windows 10 May 2019 Update - Professional Workstation edition`

   Dimensioni: `19,758,023,576 bytes`

**NOTA:** Se è presente un solo indice, l'immagine viene utilizzata per il ripristino, indipendentemente dal nome. Le dimensioni del file di immagine potrebbero essere superiori a quelle precedenti alle eliminazioni.

5. Se non si desidera il comportamento multiedition, eliminare ogni indice non richiesto.

   Come illustrato nell'esempio riportato di seguito, se si desidera utilizzare solo l'edizione Professional (supponendo che tutti i sistemi target siano provvisti di licenza), eliminare gli indici 5, 4, 2 e 1. Ogni volta che si elimina un indice, i numeri di indice vengono riassegnati. Pertanto, è necessario eliminare i numeri degli indici dal più alto al più basso. Eseguire `Get-ImageInfo` dopo ciascuna eliminazione per confermare visivamente l'indice che si eliminerà dopo.

   ```
   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
   ```

   Selezionare un solo indice dell'edizione (per questo esempio, Professional). Se è presente un solo indice, l'immagine viene utilizzata per il ripristino, indipendentemente dal nome. Tenere presente che le dimensioni del file di immagine potrebbero essere superiori a quelle precedenti alle eliminazioni, a causa del modo in cui funzionano la normalizzazione dei contenuti e le modifiche ai metadati WIM.

6. Facoltativo - Se si desidera includere i driver nell'immagine di ripristino aziendale, attenersi alle istruzioni riportate di seguito:

   **a.** Montare l'immagine in una cartella vuota, utilizzando i seguenti comandi:

   ```
   mkdir C:\staging\mount

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

   **b.** Montare il DVD del driver HP Windows 10 (DRDVD) appropriato per il sistema target supportato. Dal supporto dei driver montato, copiare le sottocartelle dei driver nell'area di staging, utilizzando il comando riportato di seguito:

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

   **NOTA:** `<M:>` indica l'unità montata. Sostituire con la lettera corretta dell'unità.

   È possibile includere driver aggiuntivi in stile .inf posizionandoli nella cartella C:\staging\mount \SWSETUP\DRV. Per ulteriori informazioni sul modo in cui questo contenuto viene elaborato da HP Sure Recover tramite la funzione `dism /Add-Driver /Recurse`, vedere "Add and Remove Drivers to an Offline Windows image" (Aggiunta e rimozione di driver in un'immagine Windows offline) nell'argomento seguente: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Questa funzione non supporta i driver in stile .exe che richiedono l'esecuzione di un'applicazione.

   **c.** Salvare le modifiche e smontare l'immagine, utilizzando il comando seguente:

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

   Il file di immagine risultante è: C:\staging\my-image.wim.

   **d.** Fare riferimento a Suddivisione dell'immagine a pagina 6.

### Esempio 2: Creazione di un'immagine basata su un sistema di riferimento

1. Creare supporti di avvio WinPE USB.

   **NOTA:** Ulteriori metodi per acquisire l'immagine sono reperibili nella documentazione di ADK.

   Accertarsi che l'unità USB disponga di spazio libero sufficiente per memorizzare l'immagine acquisita dal sistema di riferimento.

2. Creare un'immagine su un sistema di riferimento.
3. Acquisire l'immagine avviando il sistema di riferimento con il supporto WinPE USB, quindi utilizzare DISM.

   **NOTA:** `<U:>` indica l'unità USB. Sostituire con la lettera corretta dell'unità.

   Modificare la parte "my-image" del nome file e la descrizione `<my-image>`, se necessario.

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

4. Copiare l'immagine dall'USB nell'area di staging sul sistema funzionante con il seguente comando:

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

   Si dovrebbe disporre del seguente file di immagine: C:\staging\my-image.wim.

5. Fare riferimento a Suddivisione dell'immagine a pagina 6.

## Suddivisione dell'immagine

HP consiglia di suddividere l'immagine in file di dimensioni inferiori per migliorare l'affidabilità dei download di rete, tramite il comando seguente:

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

**NOTA:** Le dimensioni del file sono indicate in megabyte. Modificare secondo necessità.

**NOTA:** A causa della natura dell'algoritmo di suddivisione di DISM, le dimensioni dei file SWM generati potrebbero essere inferiori o superiori rispetto alle dimensioni indicate.

## Creazione di un manifesto

Formattare i file manifesto come UTF-8 senza Byte Order Mark (BOM).

È possibile modificare il nome del file manifesto (custom.mft) utilizzato nelle procedure seguenti, ma non si devono modificare le estensioni .mft e .sig; la parte del nome file dei file di manifesto e firma deve corrispondere. Per esempio è possibile modificare la coppia (custom.mft, custom.sig) in (myimage.mft, myimage.sig).

`mft_version` viene utilizzato per determinare il formato del file di immagine e deve essere impostato su 1.

`image_version` viene utilizzato per determinare se è disponibile una versione più recente dell'immagine e per impedire l'installazione di versioni precedenti.

Entrambi i valori devono essere interi senza segno a 16 bit e il separatore di riga nel manifesto deve essere `'\r\n' (CR + LF)`.

## Generazione di un manifesto

Poiché diversi file potrebbero essere coinvolti con l'immagine suddivisa, utilizzare uno script PowerShell per generare un manifesto.

In tutti i passaggi restanti, è necessario essere nella cartella C:\staging.

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

1. Creare uno script PowerShell utilizzando un editor in grado di produrre un file di testo in formato UTF-8 senza BOM, utilizzando il comando riportato di seguito: `notepad C:\staging\generate-manifest.ps1`

   Creare lo script seguente:

```
$mftFilename = "custom.mft"

$imageVersion = 1907
```

(Nota: può essere qualsiasi intero a 16 bit)

```
$header = "mft_version=1, image_version=$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:** I manifesti per HP Sure Recover non possono includere un BOM, pertanto i seguenti comandi riscrivono il file come UTF8 senza BOM.

```
$content = Get-Content $mftFilename

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

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

2. Salvare lo script.
3. Eseguire lo script.

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

## Generazione della firma del manifesto

Sure Recover convalida l'agente e l'immagine utilizzando firme crittografiche. Negli esempi seguenti viene utilizzata una coppia di chiavi private/pubbliche nel formato X.509 PEM (estensione .PEM). Definire i comandi come appropriato per l'uso dei certificati binari DER (estensione .CER o .CRT), dei certificati PEM codificati BASE-64 (estensione .CER o .CRT) o dei file PEM PKCS1 (estensione .PEM). L'esempio utilizza anche OpenSSL, che genera firme nel formato big-endian. È possibile utilizzare qualsiasi utilità per firmare i manifesti, ma alcune versioni del BIOS supportano solo le firme in formato little-endian.

1. Generare una chiave privata RSA a 2048 bit tramite il comando seguente. Se si dispone di una coppia di chiavi pubbliche/private RSA a 2048 bit in formato PEM, copiarle su C:\staging, quindi andare al passaggio 3.

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

2. Generare la chiave pubblica dalla chiave privata (se si dispone di una chiave pubblica che corrisponde alla chiave privata in formato PEM, copiarla su C:\staging), utilizzando il comando seguente:

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

3. Creare un file di firma (utilizzando l'hash basato su sha256) in base alla chiave privata RSA a 2048 bit dal passaggio 1, utilizzando il comando riportato di seguito:

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

4. Verificare il file di firma, utilizzando la chiave pubblica dal passaggio precedente, utilizzando il comando seguente:

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

**NOTA:**

- Per creare solo un file di firma, i passaggi necessari sono 1 e 3.
- Per HP Sure Recover, i passaggi minimi necessari sono 1, 2 e 3. È necessario utilizzare la chiave pubblica dal passaggio 2 per eseguire il provisioning del sistema target.
- Il passaggio 4 è facoltativo ma consigliato per convalidare correttamente il file di firma e il file manifesto.

# Hosting dei file

Ospitare i seguenti file sul server dalla cartella C:\staging:

- *.swm
- custom.mft (o il nome file scelto per il file manifesto)
- custom.sig (o il nome file scelto per il file di firma)

**NOTA:** Se si utilizza IIS come soluzione di hosting, è necessario configurare le voci MIME in modo da includere le seguenti estensioni, tutte configurate come "application/octet-stream:"

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

# Provisioning dei sistemi target

È possibile eseguire il provisioning dei sistemi target mediante HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover o Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Per questo provisioning, fornire le seguenti informazioni:

1. L'indirizzo URL del file manifesto ospitato nella sezione precedente (http://your_server.domain/path/custom.mft)
2. La chiave pubblica utilizzata per verificare il file di firma creato in precedenza (per esempio, C:\staging\my-recovery-public.pem).

# Risoluzione dei problemi

Se viene visualizzato un messaggio relativo al processo di ripristino personalizzato a indicare che la convalida di sicurezza non è andata a buon fine, controllare quanto segue:

1. Il manifesto deve essere UTF-8 senza BOM.
2. Controllare gli hash di file.
3. Verificare che il provisioning del sistema sia stato eseguito con la chiave pubblica corrispondente alla chiave privata utilizzata per firmare il manifesto.

4. I tipi MIME di server IIS devono essere `application/octet-stream`.
5. I percorsi dei file all'interno del manifesto devono comprendere il percorso completo della directory in cui si trova l'immagine come visibile da un sistema client. Questo percorso non è il percorso completo in cui i file vengono salvati nel punto di distribuzione.

# 3 Utilizzo dell'agente HP Sure Recover all'interno di un firewall aziendale

L'agente HP Sure Recover può essere ospitato su una intranet aziendale. Dopo aver installato il SoftPaq di HP Sure Recover, copiare i file dell'agente dalla directory dell'agente HP Sure Recover dal percorso di installazione a un punto di distribuzione HTTP o FTP. Quindi eseguire il provisioning del sistema client con l'URL del punto di distribuzione e la chiave pubblica HP denominata `hpsr_agent_public_key.pem`, distribuita con il SoftPaq dell'agente HP Sure Recover.

## Installazione dell'agente HP Sure Recover

1. Scaricare l'agente HP Sure Recover ed estrarre i file nel punto di distribuzione HTTP o FTP.
2. Impostare le autorizzazioni file appropriate sul punto di distribuzione.
3. Se si utilizza Internet Information Services (IIS), creare tipi MIME application/octet-stream per i formati file seguenti:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

**IMPORTANTE:** I passaggi riportati di seguito descrivono il provisioning di Sure Recover with SCCM. Per esempi di come eseguire il provisioning di Sure Recover con HP Client Management Script Library, vedere Utilizzo di HP Client Management Script Library (CMSL) a pagina 13.

4. Avviare SCCM, accedere a **HP Client Security Suite**, quindi selezionare la pagina HP Sure Recover.

**NOTA:** L'URL del punto di distribuzione include FTP o HTTP come protocollo di trasporto. Include inoltre il percorso completo della directory in cui si trova il manifesto dell'agente HP Sure Recover come visibile da un sistema client. Questo percorso non è il percorso completo in cui i file vengono salvati nel punto di distribuzione.

5. Nella sezione **Image Platform** (Piattaforma immagine), selezionare l'opzione **Corporation** (Aziendale) per ripristinare un'immagine del sistema operativo personalizzata da un punto di distribuzione aziendale. Immettere l'URL fornito dall'amministratore IT nella casella **Image Location URL** (URL posizione immagine). Immettere la chiave pubblica `hpsr_agent_public_key.pem` nel campo **Image Verification** (Verifica immagine).

**NOTA:** L'URL dell'immagine personalizzata deve includere il nome del file manifesto dell'immagine.

6. Nella sezione **Recovery Agent** (Agente recupero), selezionare l'opzione **Corporation** (Aziendale) per usare un agente di recupero personalizzato o l'agente di recupero HP da un punto di distribuzione

aziendale. Immettere l'URL fornito dall'amministratore IT nella casella **Agent Location URL** (URL posizione agente). Immettere la chiave pubblica `hpsr_agent_public_key.pem` nel campo **Agente Verification Key** (Chiave verifica agente).

**NOTA:** Non includere il nome del file per il manifesto dell'agente nell'URL, in quanto il BIOS richiede che sia denominato recovery.mft.

7. Dopo aver applicato il criterio al sistema client, riavviarlo.
8. Durante il provisioning iniziale, viene visualizzato un prompt che richiede di immettere un codice di sicurezza a 4 cifre per completare l'attivazione di HP Sure Recover. Per ulteriori informazioni, visitare la pagina hp.com e cercare il whitepaper "HP Manageability Integration Kit (MIK) for Microsoft System Center Manager".

Dopo aver completato l'attivazione di HP Sure Recover, l'URL personalizzato applicato dal criterio viene visualizzato nel menu delle impostazioni del BIOS per HP Sure Recover.

Per confermare l'attivazione, riavviare il computer e, quando viene visualizzato il logo HP, premere f10. Selezionare **Advanced** (Avanzate), **HP Sure Recover**, **Recovery Agent** (Agente di recupero) e infine **URL**.

# 4 Utilizzo di HP Client Management Script Library (CMSL)

HP Client Management Script Library consente di gestire le impostazioni di HP Sure Recover con PowerShell. Lo script riportato di seguito mostra come eseguire il provisioning, determinare lo stato, modificare la configurazione ed eseguire il deprovisioning di HP Sure Recover.

**NOTA:** Diversi comandi superano la lunghezza della riga di questa guida ma devono essere immessi come una riga singola.

```
$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
}
```

# Esempio di generazione di chiavi con OpenSSL

Memorizzare le chiavi private in un luogo sicuro. Le chiavi pubbliche verranno utilizzate per la convalida e dovranno essere fornite durante il provisioning. Queste chiavi devono avere una lunghezza di 2048 bit e utilizzare un esponente di 0x10001. Sostituire il soggetto negli esempi con le informazioni sull'organizzazione.

Impostare la seguente variabile di ambiente prima di procedere:

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


# Creare un certificato CA radice autofirmato per il test
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"


# Creare un certificato di verifica autenticità della chiave
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:


# Creare una chiave di firma 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:


# Creare una chiave di firma immagine

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:
```

È possibile firmare il manifesto dell'immagine con questo comando:

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


# Creare una chiave di firma 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:
```

È possibile firmare il manifesto dell'agente mediante questo comando:

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

OpenSSL genera file di firma in formato big-endian, che non è compatibile con alcune versioni del BIOS, pertanto potrebbe essere necessario invertire l'ordine dei byte dei file di firma agente prima di distribuirli. Le versioni del BIOS che supportano l'ordine di byte big-endian supportano anche l'ordine di byte little-endian.

# A Risoluzione dei problemi

## Partizione dell'unità non riuscita

Se la partizione SR_AED o SR_IMAGE è crittografata con BitLocker, è possibile che si verifichi un errore nel partizionamento dell'unità. Tali partizioni vengono in genere create con un attributo gpt che impedisce a BitLocker di eseguirne la crittografia, ma se un utente elimina e ricrea le partizioni o le crea manualmente su un'unità bare metal, l'agente Sure Recover non è in grado di eliminarle e si chiude con un errore durante il ripartizionamento dell'unità. L'utente deve eliminarle manualmente eseguendo DiskPart, selezionando il volume ed eseguendo il comando di override `del vol` o simili.

## Registro di controllo del firmware

Le informazioni sulle variabili EFI sono le seguenti:

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

Le API esistono in Windows per la lettura di variabili EFI, oppure è possibile eseguire il dump del contenuto delle variabili in un file utilizzando l'utilità dmpstore della Shell UEFI.

È possibile eseguire il dump del registro di controllo mediante il comando `Get-HPFirmwareAuditLog` fornito da HP Client Management Script Library.

## Registro eventi di Windows

Gli eventi di avvio e interruzione di Sure Recover vengono inviati al registro di controllo del BIOS, visibile nel Visualizzatore eventi di Windows nel registro di Sure Start se HP Notifications è installato. Questi eventi comprendono data e ora, ID origine, ID evento e un codice specifico dell'evento. Per esempio, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indica che il ripristino non è riuscito perché il manifesto non può essere autenticato con il codice c3f 23000 registrato alle ore 2:26:40 del giorno 06/27/18.

**NOTA:** Il formato della data utilizzato in questi registri è mese/data/anno.

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

**Tabella A-1 HP Secure Platform Management**

| ID evento | Conteggio dispositivi (All/DaaS) | Conteggio eventi (All/DaaS) | Descrizione | Note |
|---|---|---|---|---|
| 40 | 256/178 | 943/552 | Il processo di ripristino del sistema operativo è stato avviato dal firmware. | Ripristino piattaforma avviato |

**Tabella A-1 HP Secure Platform Management (continuazione)**

| ID evento | Conteggio dispositivi (All/DaaS) | Conteggio eventi (All/DaaS) | Descrizione | Note |
|---|---|---|---|---|
| 41 | 221/147 | 588/332 | Il processo di ripristino del sistema operativo è stato completato correttamente. | Ripristino piattaforma completato |
| 42 | 54/42 | 252/156 | Il processo di ripristino del sistema operativo non è stato completato correttamente. | Ripristino piattaforma non riuscito |

È possibile recuperare il registro di controllo del firmware utilizzando Get-HPFirmwareAuditLog in HP Client Management Script Library, disponibile all'indirizzo http://www.hp.com/go/clientmanagement. Gli ID evento 40, 41 e 42 di HP Secure Platform Management restituiscono codici specifici dell'evento nel campo dati, a indicare il risultato delle operazioni di Sure Recover. Per esempio, la seguente voce di registro indica che Sure Recover non è riuscito a scaricare il file manifesto o il file di firma con l'errore event_id 42 e i dati: 00:30:f1:c3, che devono essere interpretati come il valore 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
```

Un ripristino riuscito viene visualizzato come event_id = 41 e dati: 00:00:00:00; per esempio:

```
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 utilizza i seguenti codici specifici dell'evento.

**Tabella A-2 Codici specifici dell'evento**

| Descrizione dell'evento | Codice 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 |