



Benutzerhandbuch

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

Microsoft und Windows sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Vertrauliche Computersoftware. Für den Besitz, die Verwendung oder die Vervielfältigung dieser Software ist eine gültige Lizenz von HP erforderlich. In Übereinstimmung mit FAR 12.211 und 12.212 sind kommerziell genutzte Computersoftware, Computersoftware-Dokumentationen und technische Dokumentationen für kommerziell genutzte Geräte gemäß den HP Standardlizenzbedingungen für die kommerzielle Nutzung an die US-Regierung lizenziert.

HP haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer.

Die Herstellergarantie für HP Produkte wird ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

Erste Ausgabe: Februar 2020

Dokumentnummer: L93434-041

Syntaxschlüssel für Benutzereingaben

Text, den Sie in einer Benutzeroberfläche eingeben müssen, wird durch eine Schriftart mit fester Breite dargestellt.

Tabelle -1 Syntaxschlüssel für Benutzereingaben


| Funktion | Beschreibung |
|---------------------------------|--|
| Text ohne Klammern | Elemente, die Sie exakt wie gezeigt eingeben müssen |
| <Text in spitzen Klammern> | Ein Platzhalter für einen Wert, den Sie angeben müssen. Lassen Sie dabei die Klammern weg. |
| [Text in eckigen Klammern] | Optionale Elemente; Lassen Sie dabei die Klammern weg. |
| {Text in geschweiften Klammern} | Mehrere Elemente, aus denen Sie nur eines auswählen müssen. Lassen Sie dabei die Klammern weg. |
| | Ein Trennzeichen für Elemente, von denen Sie nur eines auswählen müssen. Lassen Sie dabei den Senkrechtstrich weg. |
| ... | Elemente, die Sie wiederholen können oder müssen. Lassen Sie dabei die Auslassungszeichen weg. |

Inhaltsverzeichnis

| | |
|---|-----------|
| 1 Erste Schritte | 1 |
| Durchführen einer Netzwerkwiederherstellung | 1 |
| Durchführen der Wiederherstellung eines lokalen Laufwerks | 1 |
| 2 Erstellen eines Unternehmensimages | 3 |
| Anforderungen | 3 |
| Erstellen des Images | 3 |
| Beispiel 1: Erstellen eines Images basierend auf dem Microsoft Windows Installationsimage | 3 |
| Beispiel 2: Erstellen eines Images basierend auf einem Referenzsystem | 6 |
| Aufteilen des Images | 6 |
| Erstellen eines Manifests | 6 |
| Generieren eines Manifests | 7 |
| Generieren der Manifestsignatur | 8 |
| Hosten der Dateien | 9 |
| Bereitstellen Ihrer Zielsysteme | 9 |
| Fehlerbeseitigung | 9 |
| 3 Verwenden des HP Sure Recover-Agents innerhalb einer Unternehmensfirewall | 11 |
| Installieren des HP Sure Recover-Agents | 11 |
| 4 Arbeiten mit der HP Client Management Script Library (CMSL) | 13 |
| Generieren von Beispielschlüsseln mithilfe von OpenSSL | 15 |
| Anhang A Fehlerbeseitigung | 17 |
| Laufwerkpartitionierung fehlgeschlagen | 17 |
| Firmware-Überwachungsprotokoll | 17 |
| Windows Ereignisprotokoll | 17 |
| HP Secure Platform Management (Quell-ID = 84h) | 17 |

1 Erste Schritte

HP Sure Recover hilft Ihnen dabei, das Betriebssystem mit minimaler Benutzerinteraktion sicher über das Netzwerk zu installieren. Systeme mit HP Sure Recover mit eingebetteter erneuter Imageerstellung unterstützen auch die Installation über ein lokales Speichergerät.


 **WICHTIG:** Sichern Sie Ihre Daten, bevor Sie HP Sure Recover verwenden. Da bei der Imageerstellung das Laufwerk neu formatiert wird, gehen Daten verloren.

Die von HP bereitgestellten Wiederherstellungs-Images enthalten das einfache Windows 10® Installationsprogramm. Optional kann HP Sure Recover optimierte Treiber für HP Geräte installieren. HP Wiederherstellungs-Images enthalten nur Datenwiederherstellungs-Agents, die in Windows 10 enthalten sind, z. B. OneDrive. Unternehmen können eigene benutzerdefinierte Images erstellen, um Unternehmenseinstellungen, Anwendungen, Treiber und Datenwiederherstellungs-Agents hinzuzufügen.

Ein Betriebssystem-Wiederherstellungs-Agent führt die erforderlichen Schritte aus, um das Wiederherstellungs-Image zu installieren. Der von HP bereitgestellte Wiederherstellungs-Agent führt allgemeine Schritte durch, z. B. Partitionieren, Formatieren und Extrahieren des Wiederherstellungs-Images auf dem Zielgerät. Da sich der HP Wiederherstellungs-Agent auf hp.com befindet, benötigen Sie Internetzugriff, um ihn abzurufen, sofern das System keine eingebettete erneute Imageerstellung umfasst. Unternehmen können den HP Wiederherstellungs-Agent auch innerhalb Ihrer Firewall hosten oder benutzerdefinierte Wiederherstellungs-Agents für komplexere Wiederherstellungsumgebungen erstellen.

Sie können HP Sure Recover starten, wenn kein Betriebssystem gefunden wird. Sie können HP Sure Recover auch nach einem Zeitplan ausführen, um sicherzustellen, dass Malware entfernt wird. Führen Sie die Konfiguration dieser Einstellungen über HP Client Security Manager (CSM), Manageability Integration Kit (MIK) oder die Client Management Script Library durch.

Durchführen einer Netzwerkwiederherstellung

 **HINWEIS:** Um eine Netzwerkwiederherstellung durchzuführen, müssen Sie eine kabelgebundene Verbindung verwenden. Um Datenverluste zu vermeiden, empfiehlt HP, wichtige Dateien, Daten, Fotos, Videos usw. zu sichern, bevor Sie HP Sure Recover verwenden.

1. Verbinden Sie das Clientsystem mit dem Netzwerk, in dem auf den HTTP- oder FTP-Verteilungspunkt zugegriffen werden kann.
2. Starten Sie das Clientsystem neu. Wenn das HP Logo angezeigt wird, drücken Sie **f11**.
3. Wählen Sie **Wiederherstellen über das Netzwerk** aus.

Durchführen der Wiederherstellung eines lokalen Laufwerks

Wenn ein Clientsystem die eingebettete erneute Imageerstellung unterstützt und die Option für den geplanten Image-Download in der angewendeten Richtlinie aktiviert ist, wird das Image zur geplanten Zeit auf das Clientsystem heruntergeladen. Nachdem das Image auf das Clientsystem heruntergeladen wurde, starten Sie es neu, um das Image auf das Speichergerät für die eingebettete erneute Imageerstellung zu kopieren.

So führen Sie eine lokale Wiederherstellung mithilfe des Images auf dem Speichergerät für die eingebettete erneute Imageerstellung durch:

1. Starten Sie das Clientsystem neu. Wenn das HP Logo angezeigt wird, drücken Sie **F11**.
2. Wählen Sie **Wiederherstellen vom lokalen Laufwerk aus** aus.

Systeme mit eingebetteter erneuter Imageerstellung müssen einen Downloadzeitplan konfigurieren und den Download-Agent für die Suche nach Updates verwenden. Der Download-Agent ist im HP Sure Recover-Plug-in für HP Client Security Manager enthalten und kann auch in MIK konfiguriert werden. Weitere Informationen zur MIK-Verwendung finden Sie unter <https://www.hp.com/go/clientmanagement>.

Sie können auch einen geplanten Task erstellen, um den Agent auf die Partition SR_AED und das Image auf die Partition SR_IMAGE zu kopieren. Sie können dann die HP Client Management Script Library verwenden, um ein Serviceereignis zu senden, das das BIOS darüber informiert, dass es den Inhalt validieren und beim nächsten Neustart auf das Speichergerät für die eingebettete erneute Imageerstellung kopieren soll.

2 Erstellen eines Unternehmensimages

Die meisten Unternehmen verwenden die Microsoft Deployment Tools, das Windows 10 Assessment and Deployment Kit oder beides, um Dateien, die ein Image enthalten, in einem Windows Imageerstellungsschritt im WIM-Dateiformat zu erstellen.

Anforderungen

- Die neueste Version von Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (oder eine andere Lösung für das Generieren von Paaren aus privaten/öffentlichen RSA-Schlüsseln)

Verwenden Sie sie, um das RSA-Schlüsselpaar zu generieren, das verwendet wird, um die Integrität des von Ihnen erstellten und gehosteten Unternehmensimages zu sichern.

- Eine Serverhostinglösung (z. B. Microsoft Internetinformationsdienste [IIS])

Erstellen des Images

Richten Sie vor dem Starten der Imageerstellung das Arbeits- oder Buildsystem ein, in dem Sie die erforderlichen Tools zur Vorbereitung auf die Verarbeitung des Images installiert haben, wie in den folgenden Schritten dargestellt:

1. Öffnen Sie als Administrator die Eingabeaufforderung `Umgebung für Bereitstellungs- und Imageerstellungstools` (die mit den Bereitstellungstools des Windows ADK installiert wurde).
2. Erstellen Sie mit dem folgenden Befehl einen Stagingbereich für Ihr Image:

```
mkdir C:\staging
```

3. Erstellen Sie das Image mithilfe eines der folgenden Beispiele:

[Beispiel 1: Erstellen eines Images basierend auf dem Microsoft Windows Installationsimage auf Seite 3](#)

[Beispiel 2: Erstellen eines Images basierend auf einem Referenzsystem auf Seite 6](#)

Beispiel 1: Erstellen eines Images basierend auf dem Microsoft Windows Installationsimage

1. Aktivieren oder öffnen Sie das Microsoft Windows Installationsimage (über eine Microsoft ISO oder HP OSDVD).
2. Kopieren Sie die Datei „install.wim“ mit dem folgenden Befehl aus dem bereitgestellten Windows Installationsimage in Ihren Stagingbereich:

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



HINWEIS: <M:> ist das bereitgestellte Laufwerk. Ersetzen Sie es durch den korrekten Laufwerksbuchstaben.

3. Benennen Sie mit dem folgenden Befehl „install.wim“ in einen Imagedateinamen um („my-image“ in diesem Beispiel):

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

(Optional) HP Sure Recover bietet eine Funktion zur Wiederherstellung einer bestimmten Edition über ein Multi-Index-Image basierend auf der Windows Version, die ursprünglich werkseitig für das HP Zielsystem lizenziert wurde. Dieser Mechanismus funktioniert, wenn die Indizes richtig benannt sind. Wenn Ihr Windows Installationsimage aus einem HP OSDVD-Image stammt, haben Sie wahrscheinlich ein Multi-Edition-Image. Wenn Sie dieses Verhalten nicht wünschen und sicherstellen möchten, dass eine bestimmte Edition für alle Zielsysteme verwendet wird, müssen Sie darauf achten, dass sich nur ein Index im Installationsimage befindet.

4. Überprüfen Sie mithilfe des folgenden Befehls den Inhalt des Installationsimages:

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

Die folgende Abbildung zeigt eine Beispielausgabe eines Installationsimages, das fünf Editionen unterstützt (basierend auf dem BIOS der Zielsysteme):

Details für das Image: my-image.wim

Index: 1

Name: CoreSingleLanguage

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

Größe: 19,512,500,682 bytes

Index: 2

Name: Core

Beschreibung: Windows 10 May 2019 Update - Home edition

Größe: 19,512,500,682 bytes

Index: 3

Name: Professional

Beschreibung: Windows 10 May 2019 Update- Professional Update

Größe: 19.758,019,520 bytes

Index: 4

Name: ProfessionalEducation

Beschreibung: Windows 10 May 2019 Update - Professional Education edition

Größe: 19,758,019,480 bytes

Index: 5

Name: ProfessionalWorkstation

Beschreibung: Windows 10 May 2019 Update - Professional Workstation edition

Größe: 19,758,023,576 bytes



HINWEIS: Wenn nur ein Index vorhanden ist, wird das Image unabhängig vom Namen für die Wiederherstellung verwendet. Möglicherweise ist die Imagedatei größer als vor den Löschvorgängen.

5. Wenn Sie das Multi-Edition-Verhalten nicht wünschen, löschen Sie alle nicht gewünschten Indizes.

Wenn Sie nur die Professional-Edition benötigen (sofern alle Zielsysteme lizenziert sind), löschen Sie den Index 5, 4, 2 und 1, wie im folgenden Beispiel dargestellt. Jedes Mal, wenn Sie einen Index löschen, werden die Indexnummern neu zugewiesen. Aus diesem Grund sollten Sie beginnend mit den höchsten bis zu den niedrigsten Indexzahlen löschen. Führen Sie `Get-ImageInfo` nach jedem Löschvorgang aus, um visuell zu prüfen, welcher Index als Nächstes gelöscht werden muss.

```
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
```

Wählen Sie nur einen Index der Edition aus (in diesem Beispiel „Professional“). Wenn nur ein Index vorhanden ist, wird das Image unabhängig vom Namen für die Wiederherstellung verwendet. Die Imagedatei ist möglicherweise größer als vor den Löschvorgängen. Dies liegt an der Funktionsweise der WIM-Metadatenänderungen und der Inhaltsnormalisierung.

6. (Optional) Führen Sie die folgenden Schritte aus, wenn Sie Treiber in Ihr Wiederherstellungsimage für das Unternehmen einbinden möchten:

- a. Verwenden Sie die folgenden Befehle, um Ihr Image in einem leeren Ordner bereitzustellen:

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

- b. Stellen Sie die entsprechende HP Windows 10 Treiber-DVD (DRDVD) für das unterstützte Zielsystem bereit. Kopieren Sie mit dem folgenden Befehl die Treiberunterordner von den bereitgestellten Treibermedien in Ihren Stagingbereich:

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



HINWEIS: <M:> ist das bereitgestellte Laufwerk. Ersetzen Sie es durch den korrekten Laufwerksbuchstaben.

Sie können zusätzliche INF-Treiber einbeziehen, indem Sie sie im Ordner „C:\staging\mount\SWSETUP\DRV“ platzieren. Eine Erläuterung dazu, wie diese Inhalte von HP Sure Recover mithilfe der Funktion `dism /Add-Driver /Recurse` verarbeitet werden, finden Sie unter „Hinzufügen und Entfernen von Treibern zu einem Windows-Offlineimage“ im folgenden Thema: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

Diese Funktion unterstützt keine EXE-Treiber, die eine Anwendung ausführen müssen.

- c. Speichern Sie die Änderungen und deaktivieren Sie das Image, indem Sie den folgenden Befehl verwenden:

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

Die resultierende Imagedatei ist: C:\staging\my-image.wim.

- d. Gehen Sie zu [Aufteilen des Images auf Seite 6](#).

Beispiel 2: Erstellen eines Images basierend auf einem Referenzsystem

1. Erstellen Sie bootfähige USB-WinPE-Medien.



HINWEIS: Weitere Methoden zum Erfassen des Images finden Sie in der ADK-Dokumentation.

Stellen Sie sicher, dass das USB-Laufwerk über genügend freien Speicherplatz für das erfasste Image vom Referenzsystem verfügt.

2. Erstellen Sie ein Image auf einem Referenzsystem.
3. Erfassen Sie das Image, indem Sie das Referenzsystem mit den USB-WinPE-Medien starten, und verwenden Sie dann DISM.



HINWEIS: <U:> ist das USB-Laufwerk. Ersetzen Sie es durch den korrekten Laufwerksbuchstaben.

Bearbeiten Sie nach Bedarf den my-image-Teil des Dateinamens und die Beschreibung <my-image>.

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

4. Kopieren Sie das Image mit dem folgenden Befehl vom USB-Laufwerk in den Stagingbereich auf Ihrem Arbeitssystem:

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

Sie sollten die folgende Imagedatei erhalten: C:\staging\my-image.wim.

5. Gehen Sie zu [Aufteilen des Images auf Seite 6](#).

Aufteilen des Images

HP empfiehlt, das Image mit dem folgenden Befehl in kleinere Dateien aufzuteilen, um die Zuverlässigkeit der Netzwerkdownloads zu verbessern:

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



HINWEIS: Die Dateigröße (FileSize) wird in Megabyte angezeigt. Nehmen Sie bei Bedarf Änderungen vor.



HINWEIS: Aufgrund der Art des Aufteilungsalgorithmus von DISM können die Größen der generierten SWM-Dateien kleiner oder größer als die angegebene Dateigröße sein.

Erstellen eines Manifests

Formatieren Sie Manifestdateien als UTF-8 ohne Bytereihenfolge-Marke (BOM).

Sie können den Namen der Manifestdatei (custom.mft) ändern, der in den folgenden Vorgehensweisen verwendet wird, aber Sie dürfen die Erweiterungen .mft und .sig nicht ändern und der Dateiname der Manifest- und Signaturdateien muss übereinstimmen. Sie können beispielsweise das Paar (custom.mft, custom.sig) in (myimage.mft, myimage.sig) ändern.

mft_version wird verwendet, um das Format der Imagedatei zu bestimmen und muss derzeit auf 1 festgelegt sein.

image_version wird verwendet, um festzustellen, ob eine neuere Version des Images verfügbar ist, und um zu verhindern, dass ältere Versionen installiert werden.

Beide Werte müssen 16-Bit-Ganzzahlen ohne Vorzeichen sein und das Zeilentrennzeichen im Manifest muss '\r\n' (CR + LF) sein.

Generieren eines Manifests

Da möglicherweise mehrere Dateien zum geteilten Image gehören, generieren Sie ein Manifest mithilfe eines PowerShell-Skripts.

In allen verbleibenden Schritten müssen Sie sich im Ordner „C:\staging“ befinden.

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

1. Erstellen Sie mit dem folgenden Befehl ein PowerShell-Skript mit einem Editor, der eine Textdatei im Format UTF-8 ohne BOM erzeugen kann: `notepad C:\staging\generate-manifest.ps1`

Erstellen Sie das folgende Skript:

```
$mftFilename = "custom.mft"

$imageVersion = 1907 (Hinweis: Dies kann eine beliebige 16-Bit-Ganzzahl sein.)

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



HINWEIS: Manifeste für HP Sure Recover dürfen keine BOM enthalten, daher wird die Datei mit den folgenden Befehlen als UTF8 ohne BOM neu geschrieben.

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

2. Speichern Sie das Skript.
3. Führen Sie das Skript aus.

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

Generieren der Manifestsignatur

Sure Recover validiert den Agent und das Image mithilfe von kryptografischen Signaturen. Die folgenden Beispiele verwenden ein Paar aus privaten/öffentlichen Schlüsseln im X.509-PEM-Format (.PEM-Erweiterung). Passen Sie die Befehle entsprechend an, um binäre DER-Zertifikate (.CER- oder .CRT-Erweiterung), BASE-64-codierte PEM-Zertifikate (.CER- oder .CRT-Erweiterung) oder PKCS1-PEM-Dateien (.PEM-Erweiterung) zu verwenden. Das Beispiel verwendet auch OpenSSL, mit dem Signaturen im Big-Endian-Format generiert werden. Sie können beliebige Dienstprogramme verwenden, um Manifeste zu signieren, aber einige BIOS-Versionen unterstützen nur Signaturen im Little-Endian-Format.

1. Generieren Sie mit dem folgenden Befehl einen privaten 2048-Bit-RSA-Schlüssel. Wenn Sie über ein Paar aus privaten/öffentlichen 2048-Bit-RSA-Schlüsseln im PEM-Format verfügen, kopieren Sie sie in „C:\staging“ und fahren Sie dann mit Schritt 3 fort.

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

2. Generieren Sie mit dem folgenden Befehl den öffentlichen Schlüssel aus Ihrem privaten Schlüssel (wenn Sie über einen öffentlichen Schlüssel verfügen, der Ihrem privaten Schlüssel im PEM-Format entspricht, kopieren Sie ihn in „C:\staging“):

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

3. Erstellen Sie mit dem folgenden Befehl eine Signaturdatei (mithilfe des sha256-basierten Hashs) auf der Grundlage Ihres privaten 2048-Bit-RSA-Schlüssels aus Schritt 1:

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

4. Überprüfen Sie mit dem folgenden Befehl die Signaturdatei mithilfe des öffentlichen Schlüssels aus dem vorherigen Schritt:

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



HINWEIS:

- Wenn Sie nur eine Signaturdatei erstellen müssen, sind die erforderlichen Schritte 1 und 3.
- Für HP Sure Recover sind zumindest die Schritte 1, 2 und 3 erforderlich. Sie benötigen den öffentlichen Schlüssel aus Schritt 2, um Ihr Zielsystem bereitzustellen.
- Schritt 4 ist optional, wird jedoch empfohlen, um die Signaturdatei und die Manifestdatei korrekt zu validieren.

Hosten der Dateien

Hosten Sie die folgenden Dateien auf Ihrem Server über den Ordner „C:\staging“:

- *.swm
- custom.mft (oder der Dateiname, den Sie für die Manifestdatei ausgewählt haben)
- custom.sig (oder der entsprechende Dateiname, den Sie für die Signaturdatei ausgewählt haben)



HINWEIS: Wenn Sie IIS als Hostinglösung verwenden, müssen Sie Ihre MIME-Einträge so konfigurieren, dass die folgenden Erweiterungen enthalten sind (alle konfiguriert als „application/octet-stream“).

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

Bereitstellen Ihrer Zielsysteme

Sie können Ihre Zielsysteme über die HP Client Management Script Library, HP Client Security Manager (CSM)/ Sure Recover oder das Manageability Integration Kit (MIK) bereitstellen (<https://www.hp.com/go/clientmanagement>).

Geben Sie die folgenden Informationen für diese Bereitstellung an:

1. Die URL-Adresse der Manifestdatei, die im vorherigen Abschnitt gehostet wird (`http://your_server.domain/path/custom.mft`)
2. Den öffentlichen Schlüssel, der verwendet wird, um die zuvor erstellte Signaturdatei zu überprüfen (z. B.: `C:\staging\my-recovery-public.pem`).

Fehlerbeseitigung

Wenn Sie eine Meldung erhalten, dass für den benutzerdefinierten Wiederherstellungsprozess keine Sicherheitsüberprüfung durchgeführt werden kann, überprüfen Sie Folgendes:

1. Das Manifest muss UTF-8 ohne BOM sein.
2. Überprüfen Sie die Dateihashes.
3. Stellen Sie sicher, dass das System mit dem öffentlichen Schlüssel bereitgestellt wurde, der dem privaten Schlüssel entspricht, der zum Signieren des Manifests verwendet wurde.

4. Die MIME-Typen des IIS-Servers müssen `application/octet-stream` sein.
5. Dateipfade innerhalb des Manifests müssen den vollständigen Pfad zum höchsten Verzeichnis enthalten, das das Image enthält (aus Sicht eines Clientsystems). Bei diesem Pfad handelt es sich nicht um den vollständigen Pfad, in dem die Dateien auf dem Verteilungspunkt gespeichert werden.


3 Verwenden des HP Sure Recover-Agents innerhalb einer Unternehmensfirewall

Der HP Sure Recover-Agent kann im Intranet eines Unternehmens gehostet werden. Nachdem Sie das HP Sure Recover-SoftPaq installiert haben, kopieren Sie die Agent-Dateien aus dem HP Sure Recover-Agent-Verzeichnis vom Installationsspeicherort auf einen HTTP- oder FTP-Verteilungspunkt. Stellen Sie dann das Clientsystem mit der URL des Verteilungspunkts und dem öffentlichen HP Schlüssel `hpsr_agent_public_key.pem` bereit, der mit dem HP Sure Recover-Agent-SoftPaq verteilt wird.


Installieren des HP Sure Recover-Agents

1. Laden Sie den HP Sure Recover-Agent herunter und extrahieren Sie die Dateien auf Ihrem HTTP- oder FTP-Verteilungspunkt.
2. Legen Sie die entsprechenden Dateiberechtigungen auf dem Verteilungspunkt fest.
3. Wenn Sie Internetinformationsdienste (IIS) verwenden, erstellen Sie den MIME-Typ „application/octet-stream“ für die folgenden Dateiformate:

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

 **WICHTIG:** In den folgenden Schritten wird die Bereitstellung von Sure Recover mit SCCM beschrieben. Beispiele für die Bereitstellung von Sure Recover mit der HP Client Management Script Library finden Sie unter „[Arbeiten mit der HP Client Management Script Library \(CMSL\)](#)“ auf Seite 13.

4. Starten Sie SCCM, navigieren Sie zu **HP Client Security Suite** und wählen Sie dann die HP Sure Recover-Seite aus.

 **HINWEIS:** Die Verteilungspunkt-URL enthält entweder FTP oder HTTP als Transportprotokoll. Sie enthält auch den vollständigen Pfad zum höchsten Verzeichnis, das das Manifest für den HP Sure Recover-Agent enthält (aus Sicht eines Clientsystems). Bei diesem Pfad handelt es sich nicht um den vollständigen Pfad zum Speicherort der Dateien auf dem Verteilungspunkt.

5. Wählen Sie im Abschnitt **Plattform-Image** die Option **Unternehmen** aus, um ein benutzerdefiniertes Betriebssystem-Image über einen Unternehmensverteilungspunkt wiederherzustellen. Geben Sie die vom IT-Administrator bereitgestellte URL in das Eingabefeld **URL des Image-Speicherorts** ein. Geben Sie den öffentlichen Schlüssel `hpsr_agent_public_key.pem` in das Feld **Image-Überprüfung** ein.

 **HINWEIS:** Die benutzerdefinierte Image-URL muss den Namen der Image-Manifestdatei enthalten.

6. Wählen Sie im Abschnitt **Wiederherstellungs-Agent** die Option **Unternehmen** aus, um einen benutzerdefinierten Wiederherstellungs-Agent oder den HP Wiederherstellungs-Agent über einen Unternehmensverteilungspunkt zu verwenden. Geben Sie die vom IT-Administrator bereitgestellte URL in das Eingabefeld **URL des Agent-Speicherorts** ein. Geben Sie den öffentlichen Schlüssel `hpsr_agent_public_key.pem` in das Eingabefeld **Schlüssel zur Agent-Überprüfung** ein.



HINWEIS: Schließen Sie den Dateinamen für das Agent-Manifest nicht in die URL ein, da der Name für das BIOS „recovery.mft“ lauten muss.

7. Nachdem die Richtlinie auf das Clientsystem angewendet wurde, starten Sie es neu.
8. Während der ersten Bereitstellung wird eine Eingabeaufforderung angezeigt, in der Sie einen 4-stelligen Sicherheitscode eingeben können, um die HP Sure Recover-Aktivierung abzuschließen. Weitere Informationen finden Sie auf hp.com. Suchen Sie nach dem Whitepaper zum HP Manageability Integration Kit (MIK) für Microsoft System Center Manager.

Nachdem die HP Sure Recover-Aktivierung erfolgreich abgeschlossen wurde, wird die von der Richtlinie angewendete benutzerdefinierte URL im HP Sure Recover-Menü mit BIOS-Einstellungen angezeigt.

Um den Aktivierungserfolg zu bestätigen, starten Sie den Computer neu und drücken Sie **f10**, wenn das HP Logo angezeigt wird. Wählen Sie nacheinander **Erweitert**, **HP Sure Recover**, **Wiederherstellungs-Agent** und dann **URL** aus.

4 Arbeiten mit der HP Client Management Script Library (CMSL)

Die HP Client Management Script Library ermöglicht es Ihnen, HP Sure Recover-Einstellungen mit PowerShell zu verwalten. Das folgende Beispielskript zeigt, wie Sie HP Sure Recover bereitstellen, den Status ermitteln, die Konfiguration ändern und die Bereitstellung von HP Sure Recover aufheben.

 **HINWEIS:** Einige Befehle überschreiten die Zeilenlänge dieses Handbuchs, sie müssen aber in einer einzelnen Zeile eingegeben werden.

```
$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
}

```

Generieren von Beispielschlüsseln mithilfe von OpenSSL

Speichern Sie die privaten Schlüssel an einem sicheren Ort. Die öffentlichen Schlüssel werden zur Validierung verwendet und müssen während der Bereitstellung zur Verfügung stehen. Diese Schlüssel müssen 2048 Bit lang sein und den Exponenten 0x10001 verwenden. Ersetzen Sie den Betreff in den Beispielen durch Informationen über Ihre Organisation.

Legen Sie die folgende Umgebungsvariable fest, bevor Sie fortfahren:

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

```
# Erstellen eines selbstsignierten CA-Stammzertifikats für Tests
```

```
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"
```

```
# Erstellen eines Schlüsselbestätigungszertifikats
```

```
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:
```

```
# Erstellen eines Befehlsignaturschlüssels
```

```
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:
```

```
# Erstellen eines Imagesignaturschlüssels
```

```
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:
```

Sie können das Image-Manifest mit diesem Befehl signieren:

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

```
# Erstellen eines Agent-Signaturschlüssels
```

```
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:
```

Sie können das Agent-Manifest mit diesem Befehl signieren:

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

OpenSSL generiert Signaturdateien im Big-Endian-Format, das mit einigen BIOS-Versionen nicht kompatibel ist. Daher muss die Bytereihenfolge der Agent-Signaturdatei vor der Bereitstellung möglicherweise umgekehrt werden. BIOS-Versionen, die die Big-Endian-Bytereihenfolge unterstützen, unterstützen auch die Little-Endian-Bytereihenfolge.

A Fehlerbeseitigung

Laufwerkpartitionierung fehlgeschlagen

Die Laufwerkpartitionierung kann fehlschlagen, wenn die Partition SR_AED oder SR_IMAGE mit BitLocker verschlüsselt ist. Diese Partitionen werden normalerweise mit einem GPT-Attribut erstellt, das verhindert, dass sie von BitLocker verschlüsselt werden. Wenn aber ein Benutzer die Partitionen löscht und neu erstellt oder sie manuell auf einem Bare-Metal-Laufwerk erstellt, kann der Sure Recover-Agent sie nicht löschen und wird mit einem Fehler bei der Neupartitionierung des Laufwerks beendet. Der Benutzer muss sie manuell löschen, indem er „diskpart“ ausführt, das Volume auswählt und einen Befehl wie `del vol` zum Überschreiben ausgibt.

Firmware-Überwachungsprotokoll

Informationen zur EFI-Variablen lauten wie folgt:

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

APIs sind unter Windows zum Lesen von EFI-Variablen vorhanden. Sie können aber auch Variableninhalt mithilfe des UEFI-Shell-Dienstprogramms „dmpstore“ in eine Datei ausgeben.

Sie können das Überwachungsprotokoll mithilfe des Befehls `Get-HPFirmwareAuditLog` aus der HP Client Management Script Library ausgeben.

Windows Ereignisprotokoll

Sure Recover-Start- und -Stoppereignisse werden an das BIOS-Überwachungsprotokoll gesendet, das Sie in der Windows Ereignisanzeige im Sure Start-Protokoll anzeigen können, wenn HP Notifications installiert ist. Zu diesen Ereignissen gehören Datum und Uhrzeit, Quell-ID, Ereignis-ID und ein ereignisspezifischer Code. Beispiel: `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` gibt an, dass die Wiederherstellung fehlgeschlagen ist, da das Manifest nicht mit dem ereignisspezifischen Code `c3f 23000` authentifiziert werden konnte, der um 2:26:40 am 6/27/18 protokolliert wurde.

 **HINWEIS:** Diese Protokolle folgen dem US-Datumsformat Monat/Tag/Jahr.

HP Secure Platform Management (Quell-ID = 84h)

Tabelle A-1 HP Secure Platform Management

| Ereignis-ID | Geräteanzahl (Alle/DaaS) | Ereignisanzahl (Alle/DaaS) | Beschreibung | Hinweise |
|-------------|--------------------------|----------------------------|--|---------------------------------------|
| 40 | 256/178 | 943/552 | Der Wiederherstellungsprozess für das Betriebssystem der Plattform wurde von der Firmware gestartet. | Plattform-Wiederherstellung gestartet |

Tabelle A-1 HP Secure Platform Management (Fortsetzung)

| Ereignis-ID | Geräteanzahl (Alle/DaaS) | Ereignisanzahl (Alle/DaaS) | Beschreibung | Hinweise |
|-------------|--------------------------|----------------------------|---|--|
| 41 | 221/147 | 588/332 | Der Wiederherstellungsprozess für das Betriebssystem der Plattform wurde erfolgreich abgeschlossen. | Plattform-Wiederherstellung abgeschlossen |
| 42 | 54/42 | 252/156 | Der Wiederherstellungsprozess für das Betriebssystem der Plattform konnte nicht erfolgreich abgeschlossen werden. | Plattform-Wiederherstellung fehlgeschlagen |

Sie können das Firmware-Überwachungsprotokoll mithilfe von Get-HPFirmwareAuditLog aus der HP Client Management Script Library unter <http://www.hp.com/go/clientmanagement> abrufen. Die HP Secure Platform Management-Ereignis-IDs 40, 41 und 42 geben ereignisspezifische Codes im Datenfeld zurück, die das Ergebnis von Sure Recover-Vorgängen angeben. Der folgende Protokolleintrag zeigt beispielsweise, dass Sure Recover die Manifest- oder Signaturdatei mit dem Fehler „event_id 42“ und den Daten 00:30:f1:c3 nicht herunterladen konnte. Dies sollte als DWORD-Wert 0xC3F13000 = MftOrSigDownloadFailed interpretiert werden.

```
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
beschreibung: Der Wiederherstellungsprozess für das Betriebssystem der
Plattform konnte nicht erfolgreich abgeschlossen werden.
data: 00:30:f1:c3
```

**Eine erfolgreiche Wiederherstellung wird als „event_id = 41“ und mit den Daten 00:00:00:00 angegeben.
Beispiel:**

```
Ereignisspezifische 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
```


beschreibung: Der Wiederherstellungsprozess für das Betriebssystem der Plattform konnte nicht erfolgreich abgeschlossen werden.

data: 00:00:00:00

HP Sure Recover verwendet die folgenden ereignisspezifischen Codes.

Table A-2 Ereignisspezifische Codes

| Ereignisbeschreibung | Ereigniscode |
|--|--------------|
| 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 |