دليل المستخدم

HP Sure Recover

الإصدار الأول: فبراير 2020

الرقم المرجعي للمستند: L93434-171

مفتاح بناء جملة إدخال المستخدم

يشار إلى النص الذي يتعين إدخاله في واجهه المستخدم بـ `خط ذي عرض ثابت`.

جدول ١-٠ مفتاح بناء جملة إدخال المستخدم

العنصر	الوصف
`نص بدون أقواس أو أقواس مجموعة`	العناصر التي يتعين عليك كتابتها تمامًا كما هو موضح
`<النص داخل أقواس معقوفة>`	عنصر نائب لقيمة يتعين توافرها؛ احذف الأقواس
`[نص داخل أقواس مربعة]`	العناصر الاختيارية؛ احذف الأقواس
`{نص داخل أقواس مجموعة}`	مجموعه من العناصر التي يتعين عليك اختيار واحده منها فقط؛ احذف أقواس المجموعة
`|`	فاصل للعناصر التي يتعين عليك اختيار واحده منها فقط؛ احذف الشريط العمودي
`...`	العناصر التي يمكن أو يتعين تكرارها؛ تجاهل علامات الحذف

جدول المحتويات

١ بدء الاستخدام

يساعدك HP Sure Recover في تثبيت نظام التشغيل بأمان من الشبكة بأقل تفاعل من المستخدم. فالأنظمة المزوّدة ببرنامج HP Sure Recover with Embedded Reimaging تدعم أيضًا التثبيت من جهاز تخزين محلي.

هام: أنشئ نسخة احتياطية من بياناتك قبل استخدام HP Sure Recover. لأن عملية نسخ الصورة تعيد تهيئة محرك الأقراص، وسيحدث فقدان للبيانات.

تتضمن صور الاسترداد التي توفرها HP مثبت Windows 10® الأساسي. ويمكن لبرنامج HP Sure Recover تثبيت برامج تشغيل محسنة لأجهزة HP بشكل اختياري. إذ لا تتضمن صور الاسترداد من HP إلا عوامل استعادة البيانات المضمنة في Windows 10 فقط، مثل OneDrive. ويمكن للشركات إنشاء الصور المخصصة الخاصة بها لإضافة إعدادات الشركة والتطبيقات وبرامج التشغيل وعوامل استرداد البيانات.

يقوم وكيل استرداد نظام التشغيل (OS) بتنفيذ الخطوات اللازمة لتثبيت صورة الاسترداد. ويقوم وكيل الاسترداد الذي توفره شركة HP بتنفيذ الخطوات الشائعة، مثل التقسيم والتهيئة واستخراج صورة الاسترداد إلى الجهاز المستهدف. ونظرًا لأن وكيل الاسترداد من HP موجود على hp.com، فإنك تحتاج إلى الوصول إلى الإنترنت لاستردادها، ما لم يتضمن النظام إعادة نسخ صورة مضمّنة. ويمكن أيضًا للشركات استضافة وكيل الاسترداد من HP داخل جدار الحماية الخاص بها أو إنشاء عوامل استرداد مخصصه للحصول علي بيئات استرداد أكثر تعقيدًا.

يمكنك بدء تشغيل HP Sure Recover في حالة عدم العثور على أي نظام تشغيل. يمكنك أيضا تشغيل HP Sure Recover وفقًا لجدول زمني، كما هو الحال في حالة التأكد من إزالة البرامج الضارة. قم بتكوين هذه الإعدادات من خلال HP Client Security Manager (CSM) أو HP Manageability Integration Kit (MIK) أو HP Client Management Script Library.

إجراء استرداد شبكة

ملاحظة: لإجراء استرداد شبكة، يتعين عليك استخدام اتصال سلكي. توصي HP بالنسخ الاحتياطي لملفاتك وبياناتك وصورك الفوتوغرافية ومقاطع الفيديو الهامة لديك وما إلى ذلك قبل استخدام HP Sure Recover لتجنب فقدان البيانات.

١. وصِّل النظام التابع جزئيًا بالشبكة، حيث يمكن الوصول إلى نقطة توزيع HTTP أو FTP.

٢. أعد تشغيل النظام التابع جزئيًا. وعندما يظهر شعار HP، اضغط على f11.

٣. حدد **Restore from network** (استعادة من الشبكة).

إجراء استرداد لمحرك أقراص محلي

إذا كان النظام التابع جزئيًا يدعم إعادة تثبيت صورة مضمّنة، وتم تمكين خيار تنزيل الصورة المجدولة في السياسة المطبقة، يتم تنزيل الصورة إلى النظام التابع جزئيًا في الوقت المجدول. بعد تنزيل الصورة إلى النظام التابع جزئيًا، قم باعادة تشغيلها لنسخ الصورة إلى جهاز تخزين "إعادة تثبيت الصورة المضمّنة".

لإجراء الاسترداد المحلي باستخدام الصورة الموجودة على جهاز تخزين "إعادة تثبيت الصورة المضمّنة":

١. أعد تشغيل النظام التابع جزئيًا. وعندما يظهر شعار HP، اضغط على f11.

٢. حدد **Restore from local drive** (استعادة من جهاز محلي).

يجب أن تقوم الأنظمة المزوّدة بـ "إعادة نسخ الصورة المضمّنة" بتكوين جدول تنزيل واستخدام وكيل تنزيل للتحقق من وجود تحديثات. يتم تضمين وكيل التنزيل في HP Sure Recover Plug-in for HP Client Security Manager، كما يمكن تكوينه في MIK. راجع https://www.hp.com/go/clientmanagement للحصول على إرشادات استخدام MIK.

يمكنك أيضًا إنشاء مهمة مجدولة لنسخ الوكيل إلى قسم SR_AED والصورة إلى قسم SR_IMAGE. وحينئذ، يمكنك استخدام HP Client Management Script Library لإرسال حدث خدمة لإعلام BIOS بأنه يجب التحقق من صحة المحتويات ونسخها إلى جهاز تخزين إعادة نسخ الصورة المضمّنة عند إعادة التشغيل في المرة القادمة.

٢ إنشاء صورة لشركة

تستخدم معظم الشركات Microsoft Deployment Tools أو Windows 10 Assessment and Deployment kit أو كليهما لإنشاء ملفات تحتوي على صورة ضمن أرشيف تنسيق ملف Windows Imaging (WIM).

المتطلبات

- أحدث إصدار من Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (أو حل آخر لإنشاء زوج مفاتيح خاص/عام لـ RSA)

استخدمه لإنشاء زوج مفاتيح RSA يُستخدم لتأمين سلامة صورة الشركة التي تقوم بإنشائها واستضافتها.

- حل استضافة خادم (مثل Microsoft Internet Information Services [IIS])

إنشاء الصورة

قبل البدء في عملية إنشاء الصورة، قم بإعداد نظام العمل أو نظام البناء الذي قمت بتثبيت الأدوات المطلوبة للتحضير لمعالجة الصورة، كما هو موضح في الخطوات التالية:

١. بصفتك مسؤولاً، افتح موجه أوامر `Deployment and Imaging Tools Environment` (المثبت مع Deployment Tools of Windows ADK).

٢. أنشئ منطقة تجهيز لصورتك، باستخدام الأمر التالي:

```
mkdir C:\staging
```

٣. أنشئ الصورة باستخدام أحد الأمثلة التالية:

المثال الأول: إنشاء صورة استنادًا إلى صورة تثبيت Microsoft Windows في صفحة ٣

المثال الثاني: إنشاء صورة تستند إلى نظام مرجعي في صفحة ٥

المثال الأول: إنشاء صورة استنادًا إلى صورة تثبيت Microsoft Windows

١. قم بتحميل صورة تثبيت Microsoft Windows أو تثبيتها (من Microsoft ISO أو من HP OSDVD).

٢. من صورة تثبيت Windows التي تم تحميلها، انسخ ملف install.wim إلى منطقة التجهيز الخاصة بك باستخدام الأمر التالي:

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

ملاحظة: `<M:>` يشير إلى محرك الأقراص المحمّل. استبدله بحرف محرك الأقراص الصحيح.

٣. إعادة تسمية install.wim إلى اسم ملف صورة (على سبيل المثال، "my-image")، باستخدام الأمر التالي:

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

(اختياري) يتضمن HP Sure Recover ميزة لاستعادة إصدار معين من صورة متعددة الفهارس استنادًا إلى إصدار Windows المرخص أصلاً لنظام HP المستهدف في المصنع. تعمل هذه الآلية إذا تمت تسمية الفهارس بشكل صحيح. إذا كانت صورة تثبيت Windows لديك من صورة HP OSDVD، فمن المحتمل أن يكون لديك صورة متعددة الإصدارات. إذا كنت لا تريد هذا السلوك وتريد التأكد من استخدام إصدار واحد محدد لجميع أنظمتك المستهدفة، فأنت بحاجة إلى التأكد من وجود فهرس واحد فقط في صورة التثبيت.

٤. افحص محتويات صورة التثبيت باستخدام الأمر التالي:

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

يوضح المثال التالي عينة مستخرجة من صورة تثبيت تدعم خمسة إصدارات (تتم مطابقتها استنادًا إلى نظام BIOS لكل نظام مستهدف):

تفاصيل الصورة: my-image.wim

الفهرس: 1

الاسم: CoreSingleLanguage

الوصف: Windows 10 May 2019 Update – Home Single Language Edition

الحجم: 19,512,500,682 bytes

الفهرس: 2

الاسم: Core

الوصف: Windows 10 May 2019 Update – Home edition

الحجم: 19,512,500,682 bytes

الفهرس: 3

الاسم: Professional

الوصف: Windows 10 May 2019 Update- Professional Update

الحجم: 19.758,019,520 bytes

الفهرس: 4

الاسم: ProfessionalEducation

الوصف: Windows 10 May 2019 Update - Professional Education edition

الحجم: 19,758,019,480 bytes

الفهرس: 5

الاسم: ProfessionalWorkstation

الوصف: Windows 10 May 2019 Update - Professional Workstation edition

الحجم: bytes 19,758,023,576

ملاحظة: عندما يكون هناك فهرس واحد فقط، يتم استخدام الصورة للاسترداد، بغض النظر عن الاسم. قد يكون حجم ملف الصورة لديك أكبر مما كان عليه قبل عمليات الحذف.

٥. إذا كنت لا ترغب في استخدام سلوك متعدد الأقسام، فاحذف جميع الفهارس التي لا تريدها.

كما هو موضح في المثال التالي، إذا كنت تريد إصدار Professional فقط (بافتراض أن جميع الأنظمة المستهدفة مرخصة)، فاحذف الفهرس 5 و 4 و 2 و 1. وفي كل مرة تقوم فيها بحذف فهرس، تتم إعادة تعيين أرقام الفهرس. لذا، يجب الحذف أرقام الفهارس من أعلى إلى أسفل. شغِّل Get-ImageInfo بعد كل عملية حذف لتأكيد الفهرس الذي ستحذفه بعد ذلك.

```
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
```

اختر فهرس إصدار واحد فقط (في هذا المثال، اختر Professional). عندما يكون هناك فهرس واحد فقط، يتم استخدام الصورة للاسترداد، بغض النظر عن الاسم. لاحظ أنه قد يكون حجم ملف الصورة لديك أكبر مما كان عليه قبل عمليات الحذف بسبب الطريقة التي تعمل بها تعديلات بيانات التعريف WIM وعمل تسوية المحتوى.

٦. (اختياري) إذا كنت تريد تضمين برامج التشغيل في صورة استرداد الشركة، فاتبع الخطوات التالية:

أ. حمِّل الصورة الخاصة بك في مجلد فارغ، باستخدام الأوامر التالية:

```
mkdir C:\staging\mount

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

ب. حمِّل HP Windows 10 Driver DVD (DRDVD) المناسب للنظام المستهدف المدعوم. من وسائط برنامج التشغيل المحمِّل، انسخ مجلدات برنامج التشغيل الفرعية إلى منطقة التجهيز لديك باستخدام الأمر التالي:

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

ملاحظة: <M:> يشير إلى محرك الأقراص المحمّل. استبدله بحرف محرك الأقراص الصحيح.

ويمكنك تضمين برامج تشغيل بنمط inf. عن طريق وضعها في المجلد C:\staging\mount\SWSETUP\DRV\. للحصول على شرح حول كيفية معالجة هذا المحتوى بواسطة HP Sure Recover باستخدام وظيفة dism /Add-Driver /Recurse، راجع "إضافة برامج التشغيل وإزالتها إلى صورة Windows بدون اتصال" في الموضوع التالي: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

لا تدعم هذه الميزة برامج التشغيل بنمط exe. التي تتطلب تشغيل أحد التطبيقات.

ج. احفظ التغييرات وقم بإلغاء تحميل الصورة الخاصة بك باستخدام الأمر التالي:

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

ملف الصورة الناتج هو: C:\staging\my-image.wim.

د. انتقل إلى تقسيم الصورة في صفحة ٦.

المثال الثاني: إنشاء صورة تستند إلى نظام مرجعي

١. إنشاء وسائط USB WinPE قابلة لتمهيد التشغيل.

ملاحظة: يمكن العثور على طرق إضافية لالتقاط الصورة في وثائق ADK.

تأكد من احتواء محرك أقراص USB على مساحة خالية كافية لاحتواء الصورة الملتقطة من النظام المرجعي.

٢. إنشاء صورة علي نظام مرجعي.

٣. التقط الصورة عن طريق تشغيل النظام المرجعي باستخدام وسائط USB WinPE، ثم استخدم DISM.

ملاحظة: <U:> يشير إلى محرك أقراص USB. استبدله بحرف محرك الأقراص الصحيح.

حرِّر الجزء "my-image" من اسم الملف، ثم الوصف <my-image> حسب الحاجة.

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

٤. انسخ الصورة من USB إلى منطقة التجهيز الموجودة على النظام الذي تستخدمه باستخدام الأمر التالي:

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

يجب أن يكون لديك ملف الصورة التالي: C:\staging\my-image.wim.

٥. انتقل إلى تقسيم الصورة في صفحة ٦.

تقسيم الصورة

توصي شركة HP بتقسيم الصورة إلى ملفات أصغر لتحسين موثوقية تنزيلات الشبكة باستخدام الأمر التالي:

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

ملاحظة: يتم عرض حجم الملف بالميجابايت. قم بتحريره حسب الضرورة.

ملاحظة: نظرًا لطبيعة خوارزمية DISM المنقسمة، فقد تكون أحجام ملفات SWM التي تم إنشاؤها أصغر من حجم الملف المذكور أو أكبر منه.

إنشاء بيان

قم بتهيئة ملفات البيانات بتنسيق UTF-8 بدون علامة ترتيب البايب (BOM).

يمكنك تغيير اسم ملف البيان (custom.mft) المستخدم في الإجراءات التالية، ولكن يجب عدم تغيير التنسيقين ".mft" و".sig"، كما يتعين تطابق جزء اسم الملف لملف البيان وملف التوقيع. على سبيل المثال، يمكنك تغيير التنسيقين (custom.mft و custom.sig) إلى (myimage.mft و myimage.sig).

يُستخدم `mft_version` لتحديد تنسيق ملف الصورة، كما يتعين تعيينه حاليًا إلى 1.

يتم استخدام `image_version` لتحديد ما إذا كان هناك إصدار أحدث من الصورة متوفرًا ومنع تثبيت الإصدارات القديمة.

يتعين أن تكون كلتا القيمتين عددين صحيحين 16 بت غير موقعين، كما يتعين أن يكون فاصل الخط في البيان هو `'\r\n' (CR + LF)`.

إنشاء بيان

نظرًا لأن العديد من الملفات قد تكون متضمنة في صورتك المقسمة، استخدم البرنامج النصي powerhell لإنشاء بيان.

في جميع الخطوات المتبقية ، يتعين أن تكون في المجلد C:\staging folder.

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

١. قم بإنشاء برنامج نصي powershell باستخدام محرر يمكنه إنشاء ملف نصي بتنسيق UTF-8 بدون علامة ترتيب البايت، باستخدام الأمر التالي: `notepad C:\staging\generate-manifest.ps1`

إنشاء البرنامج النصي التالي:

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

`imageVersion = 1907$` (ملاحظة: قد يكون هذا الرقم أي عدد صحيح 16 بت)

```
"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 = $current + 1$
{
```

ملاحظة: لا يمكن أن تشتمل قوائم بيانات HP Sure Recover على علامة ترتيب البايب، لذا فإن الأوامر التالية تعيد كتابة الملف بتنسيق UTF8 بدون علامة ترتيب البايب.

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

٢. احفظ البرنامج النصي.

٣. قم بتنفيذ البرنامج النصي.

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

إنشاء توقيع بيان

يتحقق Sure Recover من صحة الوكيل والصورة باستخدام توقيعات مشفرة. تستخدم الأمثلة التالية زوج مفاتيح خاص/عام بتنسيق X.509 PEM (امتداد PEM.). اضبط الأوامر حسب الاقتضاء لاستخدام شهادات DER الثنائية (امتداد

CER. أو CRT.) أو شهادات PEM المشفرة BASE-64 (امتداد CER. أو CRT.) أو ملفات PKCS1 PEM (امتداد PEM.). يستخدم المثال أيضًا OpenSSL، الذي يقوم بإنشاء التوقيعات بتنسيق big-endian. يمكنك استخدام أي أداة مساعدة لتسجيل البيانات، ولكن بعض إصدارات BIOS لا تدعم إلا التوقيعات بتنسيق little-endian.

١. قم بإنشاء مفتاح RSA خاص 2048 بت باستخدام الأمر التالي. إذا كان لديك زوج مفاتيح RSA خاص/عام 2048 بت بتنسيق pem ، فانسخهما إلى C:\staging ، ثم انتقل إلى الخطوة 3.

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

٢. أنشئ المفتاح العام من مفتاحك الخاص (إذا كان لديك مفتاح عام مطابق لمفتاحك الخاص بتنسيق PEM، فانسخه إلى C:\staging)، باستخدام الأمر التالي:

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

٣. أنشئ ملف توقيع (باستخدام التجزئة المستندة إلى sha256) استنادًا إلى المفتاح RSA الخاص 2048 بت عن طريق الخطوة 1، باستخدام الأمر التالي:

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

٤. تحقق من ملف التوقيع، باستخدام مفتاحك العام من الخطوة السابقة، باستخدام الأمر التالي:

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

ملاحظة:

- إذا كنت بحاجة إلى إنشاء ملف توقيع فقط، فاستخدم الخطوتين 1 و 3.
- بخصوص HP Sure Recover، فإن الحد الأدنى من الخطوات المطلوبة هو 1 و 2 و 3. وستكون بحاجة إلى المفتاح العام من الخطوة 2 لتوفير نظامك المستهدف.
- الخطوة 4 اختيارية ولكن يوصى بها كي يتم التحقق من ملف التوقيع وملف البيان بشكل صحيح.

استضافة الملفات

قم باستضافة الملفات التالية علي الخادم من المجلد C:\staging:

- *.swm
- custom.mft (أو اسم الملف الذي اخترته لملف البيان)
- custom.sig (أو اسم الملف المطابق الذي اخترته لملف التوقيع)

ملاحظة: إذا كنت تستخدم IIS كحل استضافة، يتعين عليك تكوين إدخالات MIME الخاصة بك لتضمين الامتدادات التالية التي تم تكوينها بالكامل على أنها "application/octet-stream":

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

توفير أنظمتك المستهدفة

يمكنك توفير أنظمتك المستهدفة باستخدام HP Client Management Script Library أو HP Client Security Manager (CSM)/Sure Recover أو Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

قدِّم المعلومات التالية لتحقيق هذا التوفير:

١. عنوان URL لملف البيان الذي تمت استضافته في القسم السابق (http://your_server.domain/path/custom.mft)

٢. المفتاح العام المستخدم للتحقق من ملف التوقيع الذي تم إنشاؤه سابقًا (على سبيل المثال، C:\staging\my-recovery-public.pem).

استكشاف المشاكلات وإصلاحها

إذا تلقيت رسالة حول فشل عملية الاسترداد المخصصة للتحقق من الصحة، فتحقق مما يلي:

١. يتعين أنيكون البيان بتنسيق UTF-8 بدون علامة ترتيب البايت.

٢. تحقق من تجزئات الملفات.

٣. تأكد من تزويد النظام بالمفتاح العام المطابق للمفتاح الخاص المستخدم لتوقيع البيان.

٤. يتعين أن تكون أنواع MIME لخادم IIS هي `application/octet-stream`.

٥. يتعين أن تتضمن مسارات الملفات داخل البيان المسار الكامل لأعلى دليل يحتوي على الصورة كما يظهر بنظام العميل. فهذا المسار ليس المسار الكامل الذي يتم فيه حفظ الملفات عند نقطة التوزيع.

٣ استخدام وكيل HP Sure Recover داخل جدار حماية الشركة

يمكن استضافة وكيل HP Sure Recover على إنترانت الشبكة. بعد تثبيت HP Sure Recover SoftPaq، انسخ ملفات وكيل من دليل وكيل HP Sure Recover من موقع التثبيت إلى نقطة توزيع HTTP أو FTP. ثم وفِّر النظام التابع جزئيًا باستخدام عنوان URL لنقطة التوزيع ومفتاح HP العام باسم `hpsr_agent_public_key.pem` الذي يتم توزيعه باستخدام وكيل HP Sure Recover SoftPaq.

تثبيت وكيل HP Sure Recover

١. قم بتنزيل وكيل HP Sure Recover واستخراج الملفات إلى نقطه التوزيع HTTP أو FTP الخاصة بك.

٢. عيِّن أذونات الملف المناسبة على نقطة التوزيع.

٣. إذا كنت تستخدم خدمات معلومات الإنترنت (IIS)، فأنشئ أنواع MIME للتطبيق/بتدفق ثماني بتات لتنسيقات الملفات التالية:

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

هام: توضح الخطوات التالية توفير Sure Recover مع SCCM. للاطلاع على أمثلة بشأن كيفية توفير Sure Recover مع HP Client Management Script Library، راجع استخدام HP Client Management Script Library (CMSL) في صفحة ١٢.

٤. ابدأ SCCM، وانتقل إلى **HP Client Security Suite**، ثم حدد صفحة HP Sure Recover.

ملاحظة: يتضمن عنوان URL لنقطة التوزيع بروتوكول ftp أو http كبروتوكول النقل. ويتضمن أيضًا المسار الكامل إلى الدليل الأعلى الذي يحتوي على بيان وكيل HP Sure Recover كما يظهر من نظام تابع جزئيًا. فهذا المسار ليس المسار الكامل الذي يتم فيه حفظ الملفات عند نقطة التوزيع.

٥. في قسم **صورة النظام الأساسي**، حدد الخيار **شركة** لاستعاده صورة نظام التشغيل المخصصة من نقطة التوزيع الخاصة بالشركة. أدخل عنوان URL الذي قدمه مسؤول تكنولوجيا المعلومات في مربع إدخال **عنوان URL لموقع الصورة**. وأدخل المفتاح العام `hpsr_agent_public_key.pem` في حقل **التحقق من الصورة**.

ملاحظة: يتعين أن يتضمن عنوان URL المخصص للصورة اسم ملف بيان الصورة.

٦. من قسم **وكيل الاسترداد**، حدد الخيار **شركة** لاستخدام وكيل استرداد مخصص أو وكيل استرداد HP من نقطة توزيع الشركة. أدخل عنوان URL الذي قدمه مسؤول تكنولوجيا المعلومات في مربع إدخال **عنوان URL لموقع الوكيل**. وأدخل المفتاح العام `hpsr_agent_public_key.pem` في حقل الإدخال **مفتاح التحقق من الوكيل**.

ملاحظة: لا تقم بتضمين اسم ملف بيان الوكيل في عنوان URL لأن BIOS يتطلب تسميته بـ recovery.mft.

٧. وبعد تطبيق السياسة على النظام التابع جزئيًا، أعد تشغيله.

٨. أثناء التوافر الأولي، تظهر لك مطالبة بإدخال رمز أمان مكوّن من 4 أرقام لإكمال تنشيط HP Sure Recover. لمزيد من التفاصيل، انتقل إلى hp.com وابحث عن المستند التقني HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

بعد اكتمال تنشيط HP Sure Recover بنجاح، يتم عرض عنوان URL المخصص المطبّق بواسطة السياسة في قائمة إعدادات HP Sure Recover BIOS.

لتأكيد نجاح التنشيط، أعد تشغيل الكمبيوتر. وعندما يظهر شعار HP، اضغط على f10. حدد **Advanced** (خيارات متقدمة)، ثم **HP Sure Recover**، ثم حدد **Recovery Agent** (وكيل الاسترداد)، ثم حدد **URL**.

٤ استخدام HP Client Management Script Library (CMSL)

تتيح لك HP Client Management Script Library إدارة إعدادات HP Sure Recover باستخدام PowerShell. يوضح مثال البرنامج النصي التالي كيفية التوافر وتحديد الحالة وتغيير التكوين وإلغاء توافر HP Sure Recover.

ملاحظة: تتجاوز العديد من الأوامر طول سطر هذا الدليل، ومع ذلك يتعين إدخالها كسطر واحد.

```
"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
                                                                    {
```

إنشاء مفتاح عينة باستخدام OpenSSL

خزِّن المفاتيح الخاصة في مكان آمن. وسيتم استخدام المفاتيح العامة للتحقق من الصحة، كما يتعين تقديمها أثناء التوافر. فهذه المفاتيح مطلوبة لتكون 2048 بت من حيث الطول وتستخدم أس 0x10001. استبدل الموضوع في الأمثلة بمعلومات عن شركتك.

وقم بتعيين متغير البيئة التالي قبل المتابعة:

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

# إنشاء شهادة CA للجذر موقعة ذاتيا للاختبار
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/"

# إنشاء شهادة مصادقة رئيسية
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
```

```
# إنشاء مفتاح توقيع للأوامر
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
```

```
# إنشاء مفتاح توقيع صورة
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
```

يمكنك توقيع بيان الصورة باستخدام الأمر التالي:

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

```
# إنشاء مفتاح توقيع وكيل
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
```

يمكنك توقيع بيان وكيل باستخدام الأمر التالي:

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

ينشئ OpenSSL ملفات توقيع بتنسيق big-endian غير المتوافق مع بعض إصدارات BIOS، لذا قد يلزم عكس ترتيب بايت ملف توقيع الوكيل قبل نشره. إذ أن إصدارات BIOS التي تدعم ترتيب البايتات big-endian تدعم أيضًا ترتيب البايتات little-endian.

أ استكشاف المشاكل وإصلاحها

فشل تقسيم محرك الأقراص

قد يحدث فشل في تقسيم محرك الأقراص إذا كان قسم SR_AED أو SR_IMAGE مشفرًا باستخدام Bitlocker. إذ يتم إنشاء هذه الأقسام عادةً بسمة gpt التي تمنع Bitlocker من تشفيرها. ولكن إذا حذف مستخدم الأقسام وأعاد إنشائها أو أنشأها يدويًا على محرك أقراص متعطل، فلن يتمكن وكيل Sure Recover من حذفها والخروج مع وجود خطأ عند إعادة تقسيم محرك الأقراص. وبالتالي، يتعين على المستخدم حذفها يدويًا عن طريق تشغيل diskpart وتحديد وحدة التخزين وإصدار أمر التجاوز `del vol` أو ما يشابهه.

سجل تدقيق البرنامج الثابت

فيما يلي معلومات متغير EFI:

- المعرِّف الفريد العمومي: `0xec8feb88, 0xb1d1, 0x4f0f, {0xab, 0x9f, 0x86, 0xcd, {{0xb5, 0x3e, 0xa4, 0x45`
- الاسم: `OsRecoveryInfoLog`

توجد واجهات برمجة التطبيقات تحت Windows لقراءة متغيرات EFI، أو يمكنك تفريغ محتوى متغير إلى ملف باستخدام الأداة المساعدة UEFI Shell dmpstore.

يمكنك تفريغ سجل التدقيق باستخدام الأمر `Get-HPFirmwareAuditLog` المقدّم بواسطة HP Client Management Script Library.

سجل أحداث Windows

يتم إرسال أحداث بدء Sure Recover وإيقافه إلى سجل تدقيق BIOS الذي يمكنك عرضه في عارض أحداث Windows في سجل Sure Start إذا تم تثبيت HP Notifications. إذ تتضمن هذه الأحداث التاريخ والوقت ومعرِّف المصدر ومعرِّف الحدث ورمز خاص بالحدث. على سبيل المثال، يشير `[ 02 2a 84 18 06 27 02 26 40 00 fe]` `[01 00 30 f2 c3]` إلى فشل الاسترداد نظرًا لتعذر مصادقة البيان برمز c3f 23000 الخاص بالحدث الذي تم تسجيله في 2:26:40 بتاريخ 2018-6-27.

ملاحظة: وتتبع هذه السجلات تنسيق التاريخ الأمريكي للشهر/التاريخ/السنة.

HP Secure Platform Management (معرِّف المصدر = 84h)

جدول أ-١ HP Secure Platform Management

معرِّف الحدث	عدد الأجهزة (الكل/DaaS)	عدد الأحداث (الكل/DaaS)	الوصف	ملاحظات
40	256/178	943/552	بدأ البرنامج الثابت عملية استرداد نظام تشغيل النظام الأساسي.	بدء استرداد النظام الأساسي
41	221/147	588/332	اكتملت عملية استرداد نظام تشغيل النظام الأساسي بنجاح.	اكتمل استرداد النظام الأساسي
42	54/42	252/156	فشل إكمال عملية استرداد نظام تشغيل النظام الأساسي بنجاح.	فشل استرداد النظام الأساسي

يمكنك استرداد "سجل تدقيق البرنامج الثابت" باستخدام Get-HPFirmwareAuditLog في HP Client Management Script Library، المتوفر على http://www.hp.com/go/clientmanagement. ترجع معرِّفات HP Secure Platform Management Eventبالأرقام 40 و 41 و 42 إلى "الرموز الخاصة بالأحداث" في حقل البيانات، مما يشير إلى نتيجة عمليات Sure Recover. على سبيل المثال، يشير إدخال السجل التالي إلى فشل Sure Recover في تنزيل ملف البيان أو التوقيع مع الخطأ event_id 42 والبيانات: 00:30:f1:c3 التي يجب أن تفسر على أنها قيمة dword بالرمز 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
```

تظهر عملية استرداد ناجحة بمعرِّف حدث = 41 والبيانات: 00:00:00:00، على سبيل المثال:

```
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
```

يستخدم HP Sure Recover الرموز الخاصة بالأحداث التالية.

جدول أ-٢ الرموز الخاصة بالأحداث

وصف الحدث	رمز الحدث
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000

جدول أ-٢ الرموز الخاصة بالأحداث (يُتبع)

وصف الحدث	رمز الحدث
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