



사용 설명서

HP Sure Recover

© Copyright 2020 HP Development Company, L.P.

Microsoft 및 Windows는 미국 및 기타 국가에서 Microsoft Corporation의 등록 상표 또는 상표입니다.

기밀 컴퓨터 소프트웨어. 소유, 사용 또는 복사에 필요한 유효한 라이선스를 HP로부터 취득했습니다. FAR 12.211 및 12.212에 의거하여, 상용 컴퓨터 소프트웨어, 컴퓨터 소프트웨어 설명서 및 상용 품목의 기술 데이터는 공급업체의 표준 상용 라이선스에 따라 미국 정부에 사용이 허가되었습니다.

본 설명서의 내용은 사전 통지 없이 변경될 수 있습니다. HP 제품 및 서비스에 대한 유일한 보증은 제품 및 서비스와 함께 동봉된 보증서에 명시되어 있습니다. 본 설명서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. HP는 본 설명서의 기술상 또는 편집상 오류나 누락에 대해 책임지지 않습니다.

초판: 2020년 2월

문서 일련 번호: L93434-AD1

사용자 입력 구문 키

사용자 인터페이스에 입력해야 하는 텍스트는 고정 폭 글꼴로 표시되어 있습니다.

표 -1 사용자 입력 구문 키


항목	설명
괄호 또는 중괄호 없는 텍스트	표시된 대로 정확히 입력해야 하는 항목
<꺾쇠 괄호 안의 텍스트>	제공해야 하는 값에 대한 자리 표시자입니다. 괄호 생략
[대괄호 안의 텍스트]	선택적 항목; 괄호 생략
{중괄호 안의 텍스트}	하나만 선택해야 하는 항목 집합입니다. 중괄호 생략
	하나만 선택해야 하는 항목에 대한 구분 기호입니다. 세로 막대 생략
...	반복할 수 있거나 반복해야 하는 항목; 생략 부호 생략

목차

1 시작하기	1
네트워크 복구 수행	1
로컬 드라이브 복구 수행	1
2 회사 이미지 만들기	3
요구 사항	3
이미지 만들기	3
예 1: Microsoft Windows 설치 이미지를 기반으로 하는 이미지 만들기	3
예 2: 참조 시스템을 기반으로 이미지 만들기	5
이미지 분할	6
매니페스트 만들기	6
매니페스트 생성	6
매니페스트 서명 생성	8
파일 호스팅	8
대상 시스템 프로비저닝	9
문제 해결	9
3 회사 방화벽 내에서 HP Sure Recover 에이전트 사용	10
HP Sure Recover 에이전트 설치	10
4 HP Client Management Script Library(CMSL)를 사용하여 작업	12
OpenSSL을 사용하여 샘플 키 생성	14
부록 A 문제 해결	17
드라이브 분할에 실패함	17
펌웨어 감사 로그	17
Windows 이벤트 로그	17
HP Secure Platform Management(소스 ID = 84h)	17

1 시작하기

HP Sure Recover를 사용하면 최소한의 사용자 상호 작용으로 네트워크에서 운영 체제를 안전하게 설치할 수 있습니다. Embedded Reimaging 기능이 포함된 HP Sure Recover를 사용하는 시스템은 로컬 저장 장치에서의 설치도 지원합니다.


 **중요:** HP Sure Recover를 사용하기 전에 데이터를 백업하십시오. 이미징 프로세스는 드라이브를 다시 포맷하므로 데이터 손실이 발생합니다.

HP에서 제공하는 복구 이미지는 기본 Windows 10® 설치 프로그램이 포함됩니다. 필요에 따라 HP Sure Recover는 HP 장치용으로 최적화된 드라이버를 설치할 수 있습니다. HP 복구 이미지는 OneDrive 같은 Windows 10에 포함된 데이터 복구 에이전트만 포함됩니다. 기업은 자체 사용자 지정 이미지를 만들어 회사 설정, 응용 프로그램, 드라이버 및 데이터 복구 에이전트를 추가할 수 있습니다.

OS(운영 체제) 복구 에이전트는 복구 이미지를 설치하는 데 필요한 단계를 수행합니다. HP에서 제공하는 복구 에이전트는 복구 이미지를 파티션, 서식 지정 및 대상 장치로 추출하는 것과 같은 일반적인 단계를 수행합니다. HP 복구 에이전트는 hp.com에 있기 때문에 시스템에 내장된 이미지 재작성 기능이 포함되어 있지 않은 한 인터넷 액세스를 검색해야 합니다. 또한 회사는 방화벽 내에서 HP 복구 에이전트를 호스팅하고 더 복잡한 복구 환경에 대해 사용자 지정 복구 에이전트를 만들 수 있습니다.

운영 체제가 발견되지 않는 경우 HP Sure Recover를 시작할 수 있습니다. 또한 맬웨어가 제거되도록 스케줄에 따라 HP Sure Recover를 실행할 수 있습니다. HP Client Security Manager(CSM), 관리 효율성 통합 키트(MIK) 또는 HP Client Management Script Library를 통해 해당 설정의 구성을 수행합니다.

네트워크 복구 수행

 **참고:** 네트워크 복구를 수행하려면 유선 연결을 사용해야 합니다. HP는 데이터 손실을 방지하기 위해 HP Sure Recover를 사용하기 전에 중요한 파일, 데이터, 사진, 비디오 등을 백업할 것을 권장합니다.

1. HTTP 또는 FTP 배포 지점에 액세스할 수 있는 네트워크에 클라이언트 시스템을 연결합니다.
2. 클라이언트 시스템을 다시 시작하고 HP 로고가 나타나면 **f11** 키를 누릅니다.
3. **네트워크에서 복원**을 선택합니다.

로컬 드라이브 복구 수행

클라이언트 시스템에서 내포된 이미지 재작성을 지원하고 적용된 정책에서 예약된 이미지 다운로드 옵션이 활성화된 경우 예약된 시간에 이미지를 클라이언트 시스템에 다운로드합니다. 이미지를 클라이언트 시스템에 다운로드한 후 다시 시작하여 이미지를 내장된 이미지 재작성 저장 장치에 복사합니다.

내장된 이미징 재작성 저장 장치에서 이미지를 사용하여 로컬 복구를 수행하려면 다음 단계를 따르십시오.

1. 클라이언트 시스템을 다시 시작하고 HP 로고가 나타나면 **f11** 키를 누릅니다.
2. **로컬 드라이브에서 복구**를 선택합니다.

Embedded Reimaging 기능을 사용하는 시스템은 다운로드 일정을 구성하고 다운로드 에이전트를 사용하여 업데이트를 확인해야 합니다. 다운로드 에이전트는 HP Client Security Manager용 HP Sure Recover 플러그인에 포함되어 있으며, MIK에서 구성할 수도 있습니다. MIK 사용 지침은 <https://www.hp.com/go/clientmanagement>를 참조하십시오.

예약된 작업을 만들어 에이전트를 SR_AED 파티션에 복사하고, 이미지를 SR_IMAGE 파티션에 복사할 수도 있습니다. 그러면 HP Client Management Script Library를 사용하여 다음 재부팅 시 내용의 유효성을 검사하고 내장된 이미지 재작성 저장 장치에 복사해야 한다는 것을 BIOS에 알리는 서비스 이벤트를 전송할 수 있습니다.

2 회사 이미지 만들기

대부분의 회사는 Microsoft 배포 도구, Windows 10 평가 및 배포 키트를 사용하거나 둘 모두를 사용하여 WIM(Windows Imaging) 파일 형식 아카이브 안에 이미지가 담긴 파일을 생성합니다.

요구 사항

- Windows 10 평가 및 배포 키트(Windows ADK)의 최신 버전
- PowerShell
- OpenSSL(또는 RSA 개인/공개 키 쌍을 생성하기 위한 기타 솔루션)
생성하고 호스팅하는 회사 이미지의 무결성을 보호하는 데 사용되는 RSA 키 쌍을 생성하는 데 사용됩니다.
- Microsoft IIS(인터넷 정보 서비스)와 같은 서버 호스팅 솔루션

이미지 만들기

이미지 생성 프로세스를 시작하기 전에 다음 단계에 표시된 대로 필요한 도구를 설치한 작업 시스템 또는 빌드 시스템을 설정하여 이미지 처리를 준비하십시오.

1. 관리자는 배포 및 이미징 도구 환경 명령 프롬프트(Windows ADK의 배포 도구를 사용하여 설치됨)를 엽니다.
2. 다음 명령을 사용하여 이미지에 대한 준비 영역을 만듭니다.

```
mkdir C:\staging
```

3. 다음 예제 중 하나를 사용하여 이미지를 만듭니다.


[3페이지의 예 1: Microsoft Windows 설치 이미지를 기반으로 하는 이미지 만들기](#)

[5페이지의 예 2: 참조 시스템을 기반으로 이미지 만들기](#)

예 1: Microsoft Windows 설치 이미지를 기반으로 하는 이미지 만들기

1. Microsoft Windows 설치 이미지(Microsoft ISO 또는 HP OSDVD에서)를 탑재하거나 엽니다.
2. 탑재된 Windows 설치 이미지에서 다음 명령을 사용하여 install.wim 파일을 준비 영역에 복사합니다.

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

 **참고:** <M:>은 탑재된 드라이브를 의미합니다. 올바른 드라이브 문자로 대체합니다.

3. 다음 명령을 사용하여 install.wim을 이미지 파일 이름(이 예제의 경우 "my-image")으로 바꿉니다.

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

(옵션) HP Sure Recover에는 기본적으로 출하 시 HP 대상 시스템에 대해 라이선스를 받은 Windows 버전 기반으로 다중 색인 이미지에서 특정 버전을 복구하는 기능이 포함되어 있습니다. 색인의 이름이 적절하게 지정된 경우에는 이 메커니즘이 작동합니다. Windows 설치 이미지를 HP OSDVD 이미지에서 제공하는 경우 다중 버전 이미지가 있을 가능성이 높습니다. 이 동작을 원하지 않고 하나의 특정 버전이 모든 대상 시스템에 사용되도록 하려는 경우에는 하나의 색인만 설치 이미지에 있는지 확인해야 합니다.

4. 다음 명령을 사용하여 설치 이미지의 내용을 확인합니다.

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

다음은 5개의 버전(각 대상 시스템의 BIOS를 기반으로 일치하도록)을 지원하는 설치 이미지의 샘플 출력을 보여줍니다.

이미지에 대한 세부 정보:my-image.wim

색인: 1

이름:CoreSingleLanguage

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

크기:19,512,500,682 bytes

색인: 2

이름:Core

설명:Windows 10 May 2019 Update - Home edition

크기:19,512,500,682 bytes

색인: 3

이름:Professional

설명:Windows 10 May 2019 Update- Professional Update

크기:19.758,019,520 bytes

색인: 4

이름:ProfessionalEducation

설명:Windows 10 May 2019 Update - Professional Education edition


크기:19,758,019,480 bytes

색인: 5

이름:Profesalalworkstation

설명:Windows 10 May 2019 Update - Professional Workstation edition

크기:19,758,023,576 bytes

 **참고:** 인덱스가 한 개만 있는 경우 이름에 관계없이 이미지를 복구하는 데 사용됩니다. 이미지 파일의 크기는 삭제하기 전보다 더 클 수 있습니다.

5. 다중 버전 동작을 원하지 않을 경우 원하지 않는 각 색인을 삭제합니다.

다음 예에서 볼 수 있듯이 Professional Edition(모든 대상 시스템의 사용이 허가되었다고 가정할 경우)만 필요한 경우 색인 5, 4, 2 및 1을 삭제합니다. 색인을 삭제할 때마다 색인 번호가 다시 할당됩니다. 따라서 가장 높은 색인 번호에서 가장 낮은 색인 번호순으로 삭제해야 합니다. 다음에 삭제할 색인을 시각적으로 확인하기 위해 각각의 삭제 후 Get-ImageInfo를 실행합니다.

```
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
```

버전에서 한 개의 색인(이 예제에서는 Professional)만 선택합니다. 인덱스가 한 개만 있는 경우 이름에 관계없이 이미지를 복구하는 데 사용됩니다. 이미지 파일의 크기는 WIM 메타데이터 수정 및 콘텐츠 표준화가 작동하는 방식으로 인해 삭제하기 전보다 더 커질 수 있습니다.

6. (옵션) 회사 복구 이미지에 드라이버를 포함하려면 다음 단계를 따르십시오.

- a. 다음 명령을 사용하여 이미지를 빈 폴더에 탑재합니다.

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

- b. 지원되는 대상 시스템에 적합한 HP Windows 10 드라이버 DVD(DRDVD)를 탑재합니다. 탑재된 드라이버 미디어에서 다음 명령을 사용하여 드라이버 하위 폴더를 준비 영역에 복사합니다.

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

 **참고:** <M:>은 탑재된 드라이브를 의미합니다. 올바른 드라이브 문자로 대체합니다.

추가 .inf-style 드라이버를 C:\staging\mount\SWSETUP\DRV 폴더에 배치하여 포함시킬 수 있습니다. `dism /Add-Driver /Recurse` 기능을 사용하여 HP Sure Recover에서 이 콘텐츠를 처리하는 방법에 대한 설명은 다음 항목의 "오프라인 Windows 이미지에 드라이버 추가 및 제거"를 참조하십시오. <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

이 기능은 응용 프로그램을 실행해야 하는 .exe-style 드라이버를 지원하지 않습니다.

- c. 다음 명령을 사용하여 변경 사항을 저장하고 이미지를 탑재 해제합니다.


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

결과 이미지 파일은 다음과 같습니다. C:\staging\my-image.wim.

- d. [6페이지의 이미지 분할](#)로 이동합니다.

예 2: 참조 시스템을 기반으로 이미지 만들기

- 1. 부팅 가능한 USB WinPE 미디어를 만듭니다.

 **참고:** ADK 설명서에서 이미지를 캡처하는 추가 방법을 찾아볼 수 있습니다.

USB 드라이브에 참조 시스템에서 캡처된 이미지를 보관할 수 있는 충분한 여유 공간이 있는지 확인합니다.

- 2. 참조 시스템에 이미지를 만듭니다.

- 3. USB WinPE 미디어로 참조 시스템을 부팅하여 이미지를 캡처한 다음 DISM을 사용합니다.

 **참고:** <U:>는 USB 드라이브를 의미합니다. 올바른 드라이브 문자로 대체합니다.

파일 이름의 "my-image" 부분을 편집하고 필요에 따라 <my-image> 설명을 편집합니다.

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

4. 다음 명령을 사용하여 USB에서 작동 중인 시스템의 스테이징 영역으로 이미지를 복사합니다.

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


다음과 같은 이미지 파일이 있어야 합니다. C:\staging\my-image.wim.


5. [6페이지의 이미지 분할](#)로 이동합니다.

이미지 분할

다음 명령을 사용하여 이미지를 더 작은 파일로 분할하여 네트워크 다운로드의 안정성을 향상하는 것이 좋습니다.

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

 **참고:** FileSize(파일 크기)는 메가바이트 단위로 표시되어 있습니다. 필요한 경우 편집합니다.

 **참고:** DISM의 분할 알고리즘의 특성상 생성된 SWM 파일의 크기는 명시된 파일 크기보다 작거나 클 수 있습니다.

매니페스트 만들기

매니페스트 파일을 BOM(바이트 순서 표시) 없이 UTF-8로 형식을 지정합니다.

다음 절차에서 사용되는 매니페스트 파일 이름(custom.mft)을 변경할 수 있지만 확장명 .mft 및 .sig를 변경하고 매니페스트 및 시그니처 파일의 파일 이름 부분이 일치해야 합니다. 예를 들어 쌍 (custom.mft, custom.sig)를 (myimage.mft, myimage.sig)로 변경할 수 있습니다.

mft_version은 이미지 파일의 형식을 결정하는 데 사용되며 현재는 1로 설정되어 있어야 합니다.

image_version은 최신 버전의 이미지를 사용할 수 있는지 확인하고 이전 버전이 설치되는 것을 방지하는 데 사용됩니다.

두 값 모두 부호가 없는 16비트 정수이어야 하고 매니페스트의 줄 구분 기호는 '\r\n' (CR + LF) 이어야 합니다.

매니페스트 생성

분할 이미지에는 여러 개의 파일이 포함되어 있을 수 있으므로 powershell 스크립트를 사용하여 매니페스트를 생성합니다.

나머지 모든 단계에서는 C:\staging 폴더에 있어야 합니다.

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

1. 다음 명령을 사용하여 BOM 없이 텍스트 파일을 UTF-8 형식으로 생성할 수 있는 편집기를 사용하여 powershell 스크립트를 만듭니다. notepad C:\staging\generate-manifest.ps1

다음과 같은 스크립트를 만듭니다.

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

```
$imageVersion = 1907(참고: 이는 16비트 정수일 수 있습니다.)
```

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

```
Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header
```

```

$swmFiles = Get-ChildItem "." -Filter "*" .swm"

$ToNatural = { [regex]::Replace($_, '\d*\....$',
{ $args[0].Value.PadLeft(50) }) }

$spathToManifest = (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 = $hashObject.Path.Replace($spathToManifest + '\', '')
    $fileSize = (Get-Item $_.FullName).length
    $manifestContent = "$fileHash $filePath $fileSize"

    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
    $manifestContent -Append

    $current = $current + 1
}

```

 **참고:** HP Sure Recover의 매니페스트에는 BOM을 포함할 수 없기 때문에 다음 명령을 수행하면 BOM 없이 파일을 UTF8로 다시 쓸 수 있습니다.

```

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

```

2. 스크립트를 저장합니다.

3. 스크립트를 실행합니다.

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

매니페스트 서명 생성

Sure Recover는 암호화 서명을 사용하여 에이전트 및 이미지의 유효성을 검사합니다. 다음 예에서는 X.509 PEM 형식(.PEM 확장명)으로 개인/공개 키 쌍을 사용합니다. DER 바이너리 인증서(.CER 또는 .CRT 확장명), BASE-64 인코딩된 PEM 인증서(.CER 또는 .CRT 확장명) 또는 PKCS1 PEM 파일(.PEM 확장명)을 사용하도록 적절하게 명령을 조정합니다. 또한 이 예제에서는 big-endian 형식으로 서명을 생성하는 OpenSSL을 사용합니다. 모든 유틸리티를 사용하여 매니페스트에 서명할 수 있지만 일부 BIOS 버전은 little-endian 형식의 서명만 지원합니다.

1. 다음 명령을 사용하여 2048비트 RSA 개인 키를 생성합니다. 2048비트 RSA 개인/공개 키 쌍을 pem 형식으로 갖고 있는 경우 C:\staging에 복사한 다음 3 단계로 건너뛸니다.

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

2. 다음 명령을 사용하여 개인 키에서 공개 키를 생성합니다(PEM 형식의 개인 키에 해당하는 공개 키가 있는 경우 C:\staging에 복사).

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

3. 다음 명령을 사용하여 1단계에서 2048비트 RSA 개인 키를 기반으로 하는 서명 파일(sha256 기반 해시 사용)을 만듭니다.

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

4. 다음 명령을 사용하여 이전 단계에서 공개 키를 사용해 서명 파일을 확인합니다.

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


참고:

- 서명 파일만 생성해야 하는 경우 필요한 단계는 1과 3입니다.
- HP Sure Recover의 최소 필수 단계는 1, 2, 3입니다. 2단계에서는 공개 키가 있어야 대상 시스템을 프로비저닝할 수 있습니다.
- 4단계는 옵션이지만 서명 파일 및 매니페스트 파일이 올바르게 검증되도록 하는 것이 좋습니다.

파일 호스팅

C:\staging 폴더에서 서버에 다음 파일을 호스팅합니다.

- *.swm
- cutom.mft(또는 매니페스트 파일에 대해 선택한 파일 이름)
- custom.sig(또는 서명 파일에 대해 선택한 일치하는 파일 이름)

 **참고:** 호스팅 솔루션으로 IIS를 사용하는 경우 MIME 항목을 구성하여 모두 "application/octet-stream"으로 구성된 다음 확장명을 포함해야 합니다.

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

대상 시스템 프로비저닝

HP Client Management Script Library, HP Client Security Manager(CSM)/Sure Recover 또는 MIK(관리 효율성 통합 키트) (<https://www.hp.com/go/clientmanagement>)를 사용하여 대상 시스템을 프로비저닝할 수 있습니다.

이 프로비저닝에 대한 다음 정보를 제공합니다.

1. 이전 섹션에서 호스팅되는 매니페스트 파일의 URL 주소(http://your_server.domain/path/custom.mft)
2. 이전에 생성한 서명 파일을 확인하는 데 사용되는 공개 키(예: C:\staging\my-recovery-public.pem).

문제 해결

보안 유효성 검사에 실패하는 사용자 지정 복구 프로세스에 대한 메시지가 표시되면 다음을 확인하십시오.


1. 매니페스트는 BOM이 없는 UTF-8이어야 합니다.
2. 파일 해시를 검사합니다.
3. 매니페스트에 서명하는 데 사용되는 개인 키에 해당하는 공개 키를 사용하여 시스템을 프로비저닝한 상태인지 확인합니다.
4. IIS 서버 mime 유형은 `application/octet-stream`이어야 합니다.
5. 매니페스트 내의 파일 경로에는 이미지를 포함하는 최상위 디렉터리의 전체 경로가 클라이언트 시스템에서 표시되는 대로 포함되어야 합니다. 이 경로는 배포 지점에서 파일을 저장하는 전체 경로가 아닙니다.

3 회사 방화벽 내에서 HP Sure Recover 에이전트 사용


HP Sure Recover 에이전트는 회사 인트라넷에서 호스팅할 수 있습니다. HP Sure Recover SoftPaq를 설치한 후에는 설치 위치에서 HTTP 또는 FTP 배포 지점으로 HP Sure Recover 에이전트 디렉터리의 에이전트 파일을 복사합니다. 그런 다음, 배포 지점 URL과 HP Sure Recover 에이전트 SoftPaq를 사용하여 배포되는 `hpsr_agent_public_key.pem`이라는 HP 공개 키를 사용하여 클라이언트 시스템을 구축합니다.

HP Sure Recover 에이전트 설치

1. HP Sure Recover 에이전트를 다운로드하여 HTTP 또는 FTP 배포 지점으로 파일의 압축을 풉니다.
2. 배포 지점에 대한 적절한 파일 사용 권한을 설정합니다.
3. IIS(인터넷 정보 서비스)를 사용하는 경우 다음 파일 형식에 대한 `application/octet-stream` MIME 형식을 만듭니다.
 - .
 - .wim
 - .swm
 - .mft
 - .sig
 - .efi
 - .sdi

 **중요:** 다음 단계에서는 SCCM을 사용하여 Sure Recover를 프로비저닝하는 방법을 설명합니다. HP Client Management Script Library로 Sure Recover를 프로비저닝하는 방법에 대한 예는 [12페이지의 HP Client Management Script Library\(CMSL\)를 사용하여 작업을 참조하십시오.](#)


4. SCCM을 시작하고 **HP Client Security Suite**로 이동한 다음 HP Sure Recover 페이지를 선택합니다.

 **참고:** 배포 지점 URL에는 전송 프로토콜로 `ftp` 또는 `http`가 포함되어 있습니다. 또한 클라이언트 시스템에서 볼 수 있는 HP Sure Recover 에이전트에 대한 매니페스트가 포함된 최상위 디렉터리의 전체 경로를 포함합니다. 이 경로는 배포 지점에서 파일을 저장하는 전체 경로가 아닙니다.

5. 플랫폼 이미지 섹션에서 **회사** 옵션을 선택하여 회사 배포 지점에서 사용자 지정된 OS 이미지를 복원합니다. **이미지 위치 URL** 항목 상자에 IT 관리자가 제공하는 URL을 입력합니다. **이미지 확인** 필드에 공개 키 `hpsr_agent_public_key.pem`을 입력합니다.

 **참고:** 사용자 지정 이미지 URL에는 이미지 매니페스트 파일 이름이 포함되어야 합니다.

6. 복구 에이전트 섹션에서 **회사** 옵션을 선택하여 회사 배포 지점에서 사용자 지정 복구 에이전트 또는 HP 복구 에이전트를 사용합니다. IT 관리자가 제공하는 URL을 **에이전트 위치 URL** 항목 상자에 입력합니다. **에이전트 확인 키** 입력 필드에 공개 키 `hpsr_agent_public_key.pem`을 입력합니다.

 **참고:** BIOS가 `recovery.mft`라고 명명되어 있어야 하기 때문에 URL에 에이전트 매니페스트에 대한 파일 이름을 포함하지 않습니다.

7. 클라이언트 시스템에 정책이 적용되면 다시 시작합니다.
8. 초기 프로비저닝을 수행하는 동안 4자리의 보안 코드를 입력하라는 메시지가 나타나 HP Sure Recover 활성화를 완료해야 합니다. 자세한 내용은 hp.com으로 이동하여 Microsoft System Center Manager 백서에 대한 HP 관리 효율성 통합 키트(MIK)를 검색하십시오.

HP Sure Recover 활성화가 성공적으로 완료되면 정책에 따라 적용되는 사용자 지정 URL이 HP Sure Recover BIOS 설정 메뉴에 표시됩니다.

활성화 성공 여부를 확인하려면 컴퓨터를 다시 시작하고 HP 로고가 나타나면 **f10** 키를 누릅니다. **고급, HP Sure Recover, 복구 에이전트**를 차례로 선택한 다음 **URL**을 선택합니다.

4 HP Client Management Script Library(CMSL)를 사용하여 작업

HP Client Management Script Library를 사용하면 PowerShell을 사용하여 HP Sure Recover 설정을 관리할 수 있습니다. 다음 예제 스크립트는 프로비저닝, 상태 확인, 구성 변경 및 HP Sure Recover 프로비전 해제 방법을 보여 줍니다.

 **참고:** 명령 중 몇 개는 이 설명서의 라인 길이를 초과하지만 한 라인으로 입력해야 합니다.

```
$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
}

```

OpenSSL을 사용하여 샘플 키 생성

개인 키를 안전한 장소에 보관합니다. 공개 키는 유효성 검사에 사용되며 프로비저닝하는 동안 제공되어야 합니다. 이러한 키는 2048비트 길이어야 하고 0x10001의 지수를 사용해야 합니다. 예제의 주체를 조직에 대한 정보로 바꿉니다.

계속하기 전에 다음 환경 변수를 설정합니다.

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

```
# 테스트용으로 자체 서명된 루트 CA 인증서 생성
```

```
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"
```

키 승인 인증서 생성

```
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:
```

명령 서명 키 생성

```
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:
```

이미지 서명 키 생성

```
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:
```

다음 명령을 사용하여 이미지 매니페스트에 서명할 수 있습니다.

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

에이전트 서명 키 생성

```
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:
```

다음 명령을 사용하여 에이전트 매니페스트에 서명할 수 있습니다.

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

OpenSSL은 일부 BIOS 버전과 호환되지 않는 big-endian 형식으로 서명 파일을 생성하므로 에이전트 서명 파일 바이트 순서를 배포하기 전에 되돌려야 할 수도 있습니다. big-endian 바이트 순서를 지원하는 BIOS 버전도 little-endian 바이트 순서를 지원합니다.

A 문제 해결

드라이브 분할에 실패함

SR_AED 또는 SR_IMAGE 파티션이 Bitlocker를 사용하여 암호화된 경우 드라이브 파티셔닝 실패가 발생할 수 있습니다. 이러한 파티션은 일반적으로 Bitlocker가 암호화되지 않도록 하는 gpt 속성을 사용하여 생성되지만 사용자가 파티션을 삭제하고 다시 생성하거나 베어 메탈 드라이브에 수동으로 생성하는 경우 Sure Recover 에이전트는 이를 삭제할 수 없으며 드라이브를 다시 파티셔닝할 때 오류가 발생한 채로 종료할 수 없습니다. 사용자는 diskpart를 실행하고 볼륨을 선택하고 del vol 덮어쓰기 명령을 실행하여 수동으로 삭제해야 합니다.

펌웨어 감사 로그

EFI 변수 정보는 다음과 같습니다.


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

EFI 변수를 읽을 수 있도록 API가 Windows에 존재하거나 UEFI Shell dmpstore 유틸리티를 사용하여 변수 콘텐츠를 파일로 덤프할 수 있습니다.

HP Client Management Script Library가 제공하는 Get-HPFirmwareAuditLog 명령을 사용하여 감사 로그를 덤프할 수 있습니다.

Windows 이벤트 로그

Sure Recover 시작 및 중지 이벤트가 BIOS 감사 로그로 전송되어 HP 알림이 설치된 경우 Windows 이벤트 뷰어에서 확인할 수 있습니다. 이러한 이벤트에는 날짜 및 시간, 소스 ID, 이벤트 ID 및 이벤트 특정 코드가 포함되어 있습니다. 예를 들어 [fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]은 6/27/18 2:26:40에 기록된 이벤트 특정 코드 c3f 23000을 사용하여 매니페스트가 인증되지 않았기 때문에 복구가 실패했음을 나타냅니다.

 **참고:** 이러한 로그는 달/날짜/연도의 미국 날짜 형식을 따릅니다.

HP Secure Platform Management(소스 ID = 84h)

표 A-1 HP Secure Platform Management

이벤트 ID	장치 수(All/DaaS)	이벤트 수(All/DaaS)	설명	참고
40	256/178	943/552	플랫폼 OS 복구 프로세스는 펌웨어에서 시작했습니다.	플랫폼 복구가 시작됨
41	221/147	588/332	플랫폼 OS 복구 프로세스가 성공적으로 완료되었습니다.	플랫폼 복구가 완료됨
42	54/42	252/156	플랫폼 OS 복구 프로세스를 완료하지 못했습니다.	플랫폼 복구 실패

<http://www.hp.com/go/clientmanagement>에서 사용할 수 있는 HP Client Management Script Library에서 Get-HPFirmwareAuditLog를 사용하여 펌웨어 감사 로그를 검색할 수 있습니다. HP Secure Platform Management 이벤트 ID의 40, 41 및 42는 데이터 필드의 이벤트 특정 코드를 반환하며 이는 Sure Recover 작업의 결과를 표시합니다. 예를 들어 다음 로그 항목은 오류 event_id 42 및 데이터를 사용하여 매니페스트 또는 서명 파일을 다운로드하지 못했음을 나타냅니다. dword 값 0xC3F13000 = MftOrSigDownloadFailed로 해석되어야 하는 00:30:f1:c3.

```
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
```

성공적인 복구가 event_id = 41 및 .00:00:00:00 형식의 데이터로 표시됩니다. 예를 들면 다음과 같습니다.

```
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 Recover는 다음과 같은 이벤트 특정 코드를 사용합니다.

표 A-2 이벤트 특정 코드

이벤트 설명	이벤트 코드
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000

표 A-2 이벤트 특정 코드 (계속)

이벤트 설명	이벤트 코드
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
PartitioningFailed	0xC3F57000
DiskLayoutCreationFailed	0xC3F58000
UnexpectedProblemWithConfigJson	0xC3FF1000
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000