Instrukcja obsługi

HP Sure Recover

Wydanie pierwsze: luty 2020

Numer katalogowy dokumentu: L93434-241

Objaśnienie składni poleceń wprowadzanych przez użytkownika

Tekst, który trzeba wprowadzić do interfejsu użytkownika, jest oznaczony `czcionką o stałej szerokości`.

Tabela -1 Objaśnienie składni poleceń wprowadzanych przez użytkownika

Element	Opis
`Tekst bez nawiasów`	Elementy, które trzeba wprowadzić dokładnie tak, jak są pokazane
`<Tekst wewnątrz nawiasów kątowych>`	Miejsce zarezerwowane na wartość do wprowadzenia; pomiń nawiasy
`[Tekst wewnątrz nawiasów kwadratowych]`	Elementy opcjonalne; pomiń nawiasy
`{Tekst wewnątrz nawiasów klamrowych}`	Zbiór elementów, z których trzeba wybrać tylko jeden; pomiń nawiasy
`|`	Separator elementów, z których trzeba wybrać tylko jeden; pomiń kreskę pionową
`...`	Elementy, które można lub trzeba powtórzyć; pomiń wielokropek

Spis treści

1 Rozpoczęcie pracy

Oprogramowanie HP Sure Recover pomaga bezpiecznie zainstalować system operacyjny z sieci przy minimalnym udziale użytkownika. Systemy z oprogramowaniem HP Sure Recover z funkcją Embedded Reimaging obsługują również instalację z lokalnego urządzenia pamięci masowej.

WAŻNE: Przed skorzystaniem z oprogramowania HP Sure Recover należy wykonać kopię zapasową danych. Proces przetwarzania obrazu sformatuje dysk, co spowoduje utratę danych.

Obrazy odzyskiwania dostarczane przez firmę HP zawierają podstawowy instalator systemu Windows 10®. Opcjonalnie oprogramowanie HP Sure Recover może zainstalować zoptymalizowane sterowniki do urządzeń HP. Obrazy odzyskiwania HP zawierają tylko agenty odzyskiwania danych dostarczane z systemem Windows 10, takie jak usługa OneDrive. Korporacje mogą tworzyć własne niestandardowe obrazy w celu dodania ustawień firmowych, aplikacji, sterowników i agentów odzyskiwania danych.

Agent odzyskiwania systemu operacyjnego wykonuje czynności niezbędne do zainstalowania obrazu odzyskiwania. Agent odzyskiwania dostarczony przez firmę HP wykonuje typowe czynności, takie jak partycjonowanie, formatowanie i wyodrębnianie obrazu odzyskiwania do urządzenia docelowego. Ze względu na to, że agent odzyskiwania HP jest dostępny w witrynie hp.com, potrzebny jest dostęp do Internetu, chyba że system jest wyposażony w wbudowaną funkcję tworzenia obrazów. Korporacje mogą również udostępniać agenta odzyskiwania HP wewnątrz zapory lub tworzyć niestandardowe agenty odzyskiwania w przypadku bardziej skomplikowanych środowisk odzyskiwania.

Oprogramowanie HP Sure Recover można uruchomić w przypadku braku systemu operacyjnego. Oprogramowanie HP Sure Recover można również uruchamiać zgodnie z harmonogramem, na przykład w celu upewnienia się, że złośliwe oprogramowanie zostało usunięte. Te ustawienia można konfigurować przy użyciu narzędzia HP Client Security Manager (CSM), zestawu Manageability Integration Kit (MIK) lub biblioteki HP Client Management Script Library.

Wykonywanie odzyskiwania sieciowego

UWAGA: W celu wykonania odzyskiwania sieciowego należy użyć połączenia przewodowego. Firma HP zaleca utworzenie kopii zapasowej ważnych plików, danych, zdjęć, filmów itd. przed skorzystaniem z oprogramowania HP Sure Recover, aby zapobiec utracie danych.

1. Komputer kliencki należy podłączyć do sieci, w której dostępny jest punkt dystrybucji HTTP lub FTP.
2. Uruchom ponownie komputer kliencki, a gdy zostanie wyświetlone logo HP, naciśnij klawisz f11.
3. Wybierz opcję **Restore from network** (Odzyskaj z sieci).

Wykonywanie odzyskiwania z dysku lokalnego

Jeśli komputer kliencki obsługuje wbudowane tworzenie obrazów, a w zastosowanych zasadach włączono opcję pobierania obrazu zgodnie z harmonogramem, obraz zostanie pobrany do komputera klienckiego o zaplanowanej godzinie. Po pobraniu obrazu do komputera klienckiego uruchom go ponownie, aby skopiować obraz do urządzenia pamięci masowej funkcji Embedded Reimaging.

Aby wykonać odzyskiwanie lokalne za pomocą obrazu na urządzeniu pamięci masowej funkcji Embedded Reimaging:

1. Uruchom ponownie komputer kliencki, a gdy zostanie wyświetlone logo HP, naciśnij klawisz f11.
2. Wybierz opcję **Restore from local drive** (Przywróć z dysku lokalnego).

Na komputerach z funkcją Embedded Reimaging należy skonfigurować harmonogram pobierania i użyć agenta pobierania w celu sprawdzania aktualizacji. Agent pobierania jest dostarczany z dodatkiem HP Sure Recover Plug-in do narzędzia HP Client Security Manager i można go również skonfigurować w zestawie MIK. Instrukcje dotyczące korzystania z zestawu MIK można znaleźć na stronie https://www.hp.com/go/clientmanagement.

Można również utworzyć zaplanowane zadanie, aby skopiować agenta do partycji SR_AED i obraz do partycji SR_IMAGE. Następnie przy użyciu biblioteki HP Client Management Script Library można wysłać zdarzenie usługi informujące system BIOS o konieczności weryfikacji zawartości i wykonania kopii na urządzeniu pamięci masowej funkcji Embedded Reimaging podczas kolejnego ponownego uruchomienia.

2 Tworzenie obrazu firmowego

Większość firm używa narzędzia Microsoft Deployment Tools , zestawu Windows 10 Assessment and Deployment lub obu tych rozwiązań w celu tworzenia plików zawierających obraz w formacie pliku archiwum Windows Imaging (WIM).

Wymagania

- Najnowsza wersja zestawu Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (lub inne rozwiązanie do tworzenia pary kluczy prywatnych/publicznych RSA)

  Służy do generowania pary kluczy RSA używanej do zabezpieczenia integralności tworzonego i udostępnianego obrazu firmowego.
- Serwerowe rozwiązanie hostingowe (takie jak Microsoft Internet Information Services [IIS])

Tworzenie obrazu

Przed rozpoczęciem procesu tworzenia obrazu skonfiguruj działający system lub zbuduj system z zainstalowanymi wymaganymi narzędziami do przetwarzania obrazu, zgodnie z poniższymi instrukcjami:

1. Jako Administrator otwórz wiersz polecenia środowiska `Deployment and Imaging Tools Environment` (zainstalowanego z narzędziami do wdrażania z zestawu ADK dla systemu Windows).
2. Utwórz obszar tymczasowy dla obrazu przy użyciu następującego polecenia:

   ```
   mkdir C:\staging
   ```
3. Utwórz obraz przy użyciu jednego z następujących przykładów:

   Przykład 1: Tworzenie obrazu w oparciu o obraz instalacyjny systemu Microsoft Windows na stronie 3

   Przykład 2: Tworzenie obrazu na podstawie systemu odniesienia na stronie 5

Przykład 1: Tworzenie obrazu w oparciu o obraz instalacyjny systemu Microsoft Windows

1. Zamontuj lub otwórz obraz instalacyjny systemu Microsoft Windows (z pliku ISO firmy Microsoft lub HP OSDVD).
2. Z zamontowanego obrazu instalacyjnego systemu Windows skopiuj plik install.wim do obszaru tymczasowego przy użyciu następującego polecenia:

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

   UWAGA: Litera `<M:>` oznacza zamontowany napęd. Zastąp ją prawidłową literą napędu.
3. Zmień nazwę pliku install.wim na nazwę pliku obrazu („my-image” w tym przykładzie) przy użyciu następującego polecenia:

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

(Opcjonalnie) Oprogramowanie HP Sure Recover obejmuje funkcję odzyskiwania określonej wersji z obrazu wieloindeksowego opartego na wersji systemu Windows, dla której pierwotnie uzyskano licencję dla systemu docelowego HP w fabryce. Ten mechanizm działa, jeśli indeksy są nazwane prawidłowo. Jeśli obraz instalacji systemu Windows pochodzi z obrazu HP OSDVD, prawdopodobnie masz obraz zawierający wiele wersji. Jeśli to zachowanie jest niepożądane i chcesz mieć pewność, że jedna konkretna wersja jest używana we wszystkich systemach docelowych, upewnij się, że obraz instalacyjny zawiera tylko jeden indeks.

4. Sprawdź zawartość obrazu instalacyjnego za pomocą następującego polecenia:

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

   Poniżej przedstawiono przykładowe dane wyjściowe z obrazu instalacyjnego obsługującego pięć wersji (do dopasowania na podstawie systemu BIOS poszczególnych systemów docelowych):

   Szczegóły obrazu: `my-image.wim`

   Indeks: `1`

   Nazwa: `CoreSingleLanguage`

   Opis: `Windows 10 May 2019 Update – Home Single Language Edition`

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

   Indeks: `2`

   Nazwa: `Core`

   Opis: `Windows 10 May 2019 Update – Home edition`

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

   Indeks: `3`

   Nazwa: `Professional`

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

   Rozmiar: `19.758,019,520 bytes`

   Indeks: `4`

   Nazwa: `ProfessionalEducation`

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

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

   Indeks: `5`

   Nazwa: `ProfessionalWorkstation`

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

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

UWAGA: Jeśli istnieje tylko jeden indeks, obraz jest używany do odzyskiwania niezależnie od jego nazwy. Rozmiar pliku obrazu może być większy niż przed usunięciem.

5. Jeśli zachowanie związane z dostępnością wielu wersji jest niepożądane, usuń poszczególne niepotrzebne indeksy.

   Jak pokazano na poniższym przykładzie, jeśli potrzebna jest tylko wersja Professional (przy założeniu posiadania licencji dla wszystkich systemów docelowych), usuń indeksy 5, 4, 2 i 1. Za każdym razem, gdy usuwany jest indeks, numery indeksu są ponownie przypisywane. Dlatego należy usuwać numery indeksu w kolejności od najwyższego do najniższego. Uruchom polecenie `Get-ImageInfo` po każdym usunięciu, aby wizualnie potwierdzić, który indeks ma zostać usunięty w następnej kolejności.

   ```
   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
   ```

   Wybierz tylko jeden indeks wersji (na przykład Professional). Jeśli istnieje tylko jeden indeks, obraz jest używany do odzyskiwania niezależnie od jego nazwy. Należy pamiętać, że rozmiar pliku obrazu może być większy niż przed usunięciem, ze względu na sposób modyfikacji metadanych WIM i normalizacji zawartości.

6. (Opcjonalnie) Aby dołączyć sterowniki do firmowego obrazu odzyskiwania, wykonaj następujące czynności:

   a. Zamontuj obraz w pustym folderze przy użyciu następujących poleceń:

   ```
   mkdir C:\staging\mount

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

   b. Zamontuj odpowiedni obraz HP Windows 10 Driver DVD (DRDVD) dla obsługiwanego systemu docelowego. Z zamontowanego nośnika ze sterownikami skopiuj podfoldery sterowników do obszaru tymczasowego za pomocą następującego polecenia:

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

   UWAGA: Litera `<M:>` oznacza zamontowany napęd. Zastąp ją prawidłową literą napędu.

   Możesz dołączyć dodatkowe sterowniki w plikach .inf, umieszczając je w folderze C:\staging\mount \SWSETUP\DRV. Aby dowiedzieć się, w jaki sposób ta zawartość jest przetwarzana przez oprogramowanie HP Sure Recover przy użyciu funkcji `dism /Add-Driver /Recurse`, zobacz punkt „Dodawanie sterowników do obrazu offline systemu Windows i usuwanie ich” w następującym temacie: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ta funkcja nie obsługuje sterowników w plikach .exe, które wymagają uruchomienia aplikacji.

   c. Zapisz zmiany i odmontuj obraz przy użyciu następującego polecenia:

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

   Wynikowy plik obrazu to: C:\staging\my-image.wim.

   d. Przejdź na stronę Dzielenie obrazu na stronie 6.

Przykład 2: Tworzenie obrazu na podstawie systemu odniesienia

1. Utwórz rozruchowy nośnik USB środowiska WinPE.

UWAGA: Informacje na temat dodatkowych sposobów przechwytywania obrazu zawiera dokumentacja zestawu ADK.

Upewnij się, że na urządzeniu USB jest wystarczająca ilość wolnego miejsca do zapisania przechwyconego obrazu systemu odniesienia.

2. Utwórz obraz w systemie odniesienia.
3. Przechwyć obraz, uruchamiając system odniesienia przy użyciu nośnika USB środowiska WinPE, a następnie użyj narzędzia DISM.

UWAGA: Litera `<U:>` oznacza napęd USB. Zastąp ją prawidłową literą napędu.

Edytuj część nazwy pliku „my-image” i opis `<my-image>` zależnie od potrzeb.

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

4. Skopiuj obraz z urządzenia USB do obszaru tymczasowego w systemie roboczym przy użyciu następującego polecenia:

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

Powinien istnieć następujący plik obrazu: C:\staging\my-image.wim.

5. Przejdź na stronę Dzielenie obrazu na stronie 6.

Dzielenie obrazu

Firma HP zaleca dzielenie obrazu na mniejsze pliki w celu zwiększenia niezawodności pobierania przez sieć przy użyciu następującego polecenia:

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

UWAGA: Wartość FileSize jest wyświetlana w megabajtach. Edytuj je w razie potrzeby.

UWAGA: Ze względu na sposób działania algorytmu dzielenia narzędzia DISM rozmiary wygenerowanych plików SWM mogą być mniejsze lub większe niż deklarowany rozmiar pliku.

Tworzenie manifestu

Pliki manifestu należy tworzyć w formacie UTF-8 bez BOM (Byte Order Mark).

Można zmienić nazwę pliku manifestu (custom.mft) użytą w poniższych procedurach, ale nie należy zmieniać rozszerzeń .mft i .sig, a nazwy plików manifestu i podpisu muszą być zgodne. Na przykład można zmienić parę (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

Właściwość `mft_version` służy do określania formatu pliku obrazu i obecnie musi mieć wartość 1.

Właściwość `image_version` jest używana w celu określenia, czy dostępna jest nowsza wersja obrazu, oraz w celu zapobiegnięcia instalacji starszych wersji.

Obie wartości muszą być 16-bitowymi liczbami całkowitymi bez podpisu, a separatorem wierszy w manifeście musi być „`\r\n`” `(CR + LF)`.

Generowanie manifestu

Podzielony obraz może obejmować kilka plików, dlatego należy wygenerować manifest za pomocą skryptu programu PowerShell.

Wszystkie pozostałe czynności należy wykonywać w folderze C:\staging.

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

1. Utwórz skrypt programu PowerShell za pomocą edytora, który może wygenerować plik tekstowy w formacie UTF-8 bez BOM, używając następującego polecenia: `notepad C:\staging\generate-manifest.ps1`

   Utwórz następujący skrypt:

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

   `$imageVersion = 1907` **(Uwaga: Może to być 16-bitowa liczba całkowita).**

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

}
```

UWAGA: Manifesty dla oprogramowania HP Sure Recover nie mogą zawierać BOM, dlatego poniższe polecenia zapisują ponownie plik w formacie UTF8 bez BOM.

```
$content = Get-Content $mftFilename

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

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

2. Zapisz skrypt.
3. Uruchom skrypt.

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

Generowanie podpisu manifestu

Oprogramowanie Sure Recover weryfikuje agenta i obraz przy użyciu podpisów kryptograficznych. W poniższych przykładach użyto pary kluczy prywatnego/publicznego w formacie PEM X.509 (rozszerzenie .PEM). Dostosuj odpowiednio polecenia, aby użyć plików binarnych certyfikatów DER (rozszerzenie .CER lub .CRT), certyfikatów PEM z szyfrowaniem BASE-64 (rozszerzenie .CER lub .CRT) lub plików PEM PKCS1 (rozszerzenie .PEM). W tym przykładzie używane jest również narzędzie OpenSSL, które generuje podpisy w formacie big-endian. Do podpisywania manifestów można użyć dowolnego narzędzia, ale niektóre wersje systemu BIOS obsługują tylko podpisy w formacie little-endian.

1. Wygeneruj 2048-bitowy klucz prywatny RSA przy użyciu następującego polecenia. Jeśli masz parę 2048-bitowych kluczy RSA prywatnych/publicznych w formacie pem, skopiuj je do folderu C:\staging, a następnie przejdź do kroku 3.

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

2. Wygeneruj klucz publiczny z klucza prywatnego (jeśli masz klucz publiczny odpowiadający Twojemu kluczowi prywatnemu w formacie PEM, skopiuj go do folderu C:\staging), używając następującego polecenia:

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

3. Utwórz plik podpisu (przy użyciu wartości skrótu sha256) w oparciu o 2048-bitowy klucz prywatny RSA z kroku 1 przy użyciu następującego polecenia:

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

4. Sprawdź plik podpisu, korzystając z klucza publicznego w poprzednim kroku, przy użyciu następującego polecenia:

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

UWAGA:

- Jeśli chcesz tylko utworzyć plik podpisu, wymagane są kroki 1 i 3.
- W przypadku oprogramowania HP Sure Recover minimalne wymagane kroki to 1, 2 i 3. Do zainicjowania systemu docelowego potrzebny jest klucz publiczny z kroku 2.
- Krok 4 jest opcjonalny, ale zaleca się, aby plik sygnatury i plik manifestu zostały prawidłowo zweryfikowane.

Hosting plików

Na serwerze należy udostępnić następujące pliki z folderu C:\staging:

- *.swm
- custom.mft (lub nazwa pliku wybrana dla pliku manifestu)
- custom.sig (lub zgodna nazwa pliku wybrana dla pliku podpisu)

UWAGA: Jeśli korzystasz z usług IIS jako rozwiązania hostingu, musisz skonfigurować wpisy MIME, aby zawierały następujące rozszerzenia, z których wszystkie muszą być skonfigurowane jako „application/octet-stream:”

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

Inicjowanie systemów docelowych

Systemy docelowe można zainicjować przy użyciu biblioteki HP Client Management Script Library, narzędzia HP Client Security Manager (CSM)/Sure Recover lub zestawu Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

W tym celu należy podać następujące informacje:

1. Adres URL pliku manifestu udostępnionego w poprzedniej sekcji (http://twoj_serwer.domena/sciezka/custom.mft)
2. Klucz publiczny służący do weryfikacji utworzonego wcześniej pliku podpisu (na przykład C:\staging \my-recovery-public.pem).

Rozwiązywanie problemów

Jeśli pojawi się komunikat dotyczący niepowodzenia weryfikacji zabezpieczeń niestandardowego procesu odzyskiwania, sprawdź następujące elementy:

1. Manifest musi być w formacie UTF-8 bez BOM.
2. Sprawdź skróty plików.
3. Upewnij się, że system został zainicjowany przy użyciu klucza publicznego odpowiadającego kluczowi prywatnemu użytemu do podpisania manifestu.

4. Wymagane typy mime serwera IIS to `application/octet-stream`.
5. Ścieżki plików w manifeście muszą zawierać pełną ścieżkę do katalogu najwyższego poziomu zawierającego obraz widziany z systemu klienckiego. Ta ścieżka nie jest pełną ścieżką, w której zapisane są pliki w punkcie dystrybucji.

3 Korzystanie z narzędzia HP Sure Recover Agent wewnątrz firmowej zapory sieciowej

Narzędzie HP Sure Recover Agent może być udostępniane w intranecie firmowym. Po zainstalowaniu pakietu HP Sure Recover SoftPaq skopiuj pliki agenta z katalogu agenta HP Sure Recover z lokalizacji instalacji do punktu dystrybucji HTTP lub FTP. Następnie zainicjuj system kliencki przy użyciu adresu URL punktu dystrybucji i klucza publicznego HP o nazwie `hpsr_agent_public_key.pem`, który jest dostarczany z pakietem SoftPaq agenta HP Sure Recover.

Instalowanie agenta HP Sure Recover

1. Pobierz agenta HP Sure Recover i wyodrębnij pliki do punktu dystrybucji HTTP lub FTP.
2. Ustaw odpowiednie uprawnienia do plików w punkcie dystrybucji.
3. W przypadku korzystania z usług IIS (Internet Information Services) utwórz typy MIME application/octet-stream dla następujących formatów plików:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

WAŻNE: Poniższe kroki opisują inicjowanie oprogramowania Sure Recover przy użyciu rozwiązania SCCM. Przykłady inicjowania oprogramowania Sure Recover przy użyciu biblioteki HP Client Management Script Library zawiera Praca z biblioteką HP Client Management Script Library (CMSL) na stronie 13.

4. Uruchom rozwiązanie SCCM, przejdź do obszaru **HP Client Security Suite**, a następnie wybierz stronę HP Sure Recover.

UWAGA: Adres URL punktu dystrybucji obejmuje protokół FTP lub HTTP jako protokół transmisji. Zawiera również pełną ścieżkę do katalogu najwyższego poziomu z manifestem agenta HP Sure Recover widzianym z systemu klienta. Ta ścieżka nie jest pełną ścieżką do miejsca zapisu plików w punkcie dystrybucji.

5. W sekcji **Platform Image** (Obraz platformy) wybierz opcję **Corporation** (Korporacja), aby odzyskać niestandardowy obraz systemu operacyjnego z firmowego punktu dystrybucji. Wprowadź adres URL podany przez administratora IT w polu wprowadzania **Image Location URL** (Adres URL lokalizacji obrazu). Wprowadź klucz publiczny `hpsr_agent_public_key.pem` w polu **Image Verification** (Weryfikacja obrazu).

UWAGA: Niestandardowy adres URL obrazu musi zawierać nazwę pliku manifestu obrazu.

6. W sekcji **Recovery Agent** (Agent odzyskiwania) wybierz opcję **Corporation** (Korporacja), aby użyć niestandardowego agenta odzyskiwania lub agenta odzyskiwania HP z firmowego punktu dystrybucji. Wprowadź adres URL podany przez administratora IT w polu wprowadzania **Agent Location URL** (Adres URL lokalizacji agenta). Wprowadź klucz publiczny `hpsr_agent_public_key.pem` w polu wprowadzania **Agent Verification Key** (Klucz weryfikacji agenta).

UWAGA: Nie dodawaj nazwy pliku manifestu agenta do adresu URL, ponieważ system BIOS wymaga, aby był nazwany recovery.mft.

7. Po zastosowaniu zasad do systemu klienckiego uruchom go ponownie.

8. Podczas wstępnego inicjowania wyświetlany jest monit o wprowadzenie 4-cyfrowego kodu zabezpieczającego w celu ukończenia aktywacji oprogramowania HP Sure Recover. Aby uzyskać więcej informacji przejdź do witryny hp.com i wyszukaj opracowanie techniczne dotyczące zestawu HP Manageability Integration Kit (MIK) dla rozwiązania Microsoft System Center Manager.

Po pomyślnym ukończeniu aktywacji oprogramowania HP Sure Recover niestandardowy adres URL zastosowany do zasad jest wyświetlany w menu ustawień oprogramowania HP Sure Recover w systemie BIOS.

Aby potwierdzić powodzenie aktywacji, uruchom ponownie komputer i po wyświetleniu logo HP naciśnij klawisz f10. Wybierz opcję **Advanced** (Zaawansowane), wybierz oprogramowanie **HP Sure Recover** i wybierz opcję **Recovery Agent** (Agent odzyskiwania), a następnie wybierz opcję **URL** (Adres URL).

4 Praca z biblioteką HP Client Management Script Library (CMSL)

Biblioteka HP Client Management Script Library umożliwia zarządzanie ustawieniami oprogramowania HP Sure Recover przy użyciu programu PowerShell. Poniższy przykładowy skrypt prezentuje sposób inicjowania oprogramowania HP Sure Recover, określania jego stanu, zmieniania jego konfiguracji i anulowania jego inicjowania.

UWAGA: Niektóre polecenia przekraczają długość wiersza tego podręcznika, ale muszą być wprowadzane w jednym wierszu.

```
$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
}
```

Przykład generowania kluczy przy użyciu narzędzia OpenSSL

Klucze prywatne należy przechowywać w bezpiecznym miejscu. Klucze publiczne będą używane do walidacji i muszą zostać podane podczas inicjowania. Te klucze muszą mieć długość 2048 bitów i używać wykładnika 0x10001. Zastąp temat w przykładach informacjami o swojej organizacji.

Ustaw następującą zmienną środowiskową przed kontynuowaniem:

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


# Tworzenie certyfikatu głównego CA z podpisem własnym na potrzeby
testowania
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"


# Tworzenie certyfikatu poręczenia klucza
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:


# Tworzenie klucza podpisywania poleceń

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:


# Tworzenie klucza podpisywania obrazu

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:
```

Za pomocą tego polecenia można zarejestrować manifest obrazu:

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


# Tworzenie klucza podpisywania agenta

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:
```

Za pomocą tego polecenia można zarejestrować manifest agenta:

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

Narzędzie OpenSSL generuje pliki podpisów w formacie big-endian, który nie jest obsługiwany przez niektóre wersje systemu BIOS, dlatego kolejność bajtów w pliku podpisu agenta może wymagać odwrócenia przed

wdrożeniem. Wersje systemu BIOS obsługujące kolejność bajtów big-endian obsługują również kolejność bajtów little-endian.

A Rozwiązywanie problemów

Niepowodzenie partycjonowania dysku

Niepowodzenie partycjonowania dysku może wystąpić, jeśli partycja SR_AED lub SR_IMAGE jest zaszyfrowana przy użyciu funkcji Bitlocker. Partycje te są zwykle tworzone z atrybutem gpt, który uniemożliwia ich szyfrowanie, ale jeśli użytkownik usunie i ponownie utworzy partycje lub utworzy je ręcznie na napędzie fizycznym, agent Sure Recover nie może ich usunąć, a jego działanie zostaje zakończone z powodu błędu podczas ponownego dzielenia dysku na partycje. Użytkownik musi je ręcznie usunąć, uruchamiając program DiskPart, wybierając wolumin i wydając zastępcze polecenie `del vol` lub podobne.

Dziennik audytu oprogramowania układowego

Informacje o zmiennych interfejsu EFI są następujące:

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

Interfejsy API istnieją w systemie Windows w celu odczytywania zmiennych interfejsu EFI lub umożliwiają zrzucanie zawartości zmiennej do pliku za pomocą narzędzia dmpstore środowiska UEFI Shell.

Dziennik audytu można zrzucić za pomocą polecenia `Get-HPFirmwareAuditLog` dostarczonego przez bibliotekę HP Client Management Script Library.

Dziennik zdarzeń systemu Windows

Zdarzenia uruchomienia i zatrzymania oprogramowania Sure Recover są wysyłane do dziennika audytu systemu BIOS, który można wyświetlić w narzędziu Podgląd zdarzeń systemu Windows w dzienniku Sure Start, jeśli zainstalowane jest oprogramowanie HP Notifications. Informacje o tych zdarzeniach zawierają datę i godzinę, identyfikator źródła, identyfikator zdarzenia oraz kod konkretnego zdarzenia. Na przykład wpis `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` oznacza niepowodzenie odzyskiwania z powodu braku możliwości uwierzytelnienia manifestu o kodzie c3f 23000, które zostało zarejestrowane o godzinie 2:26:40 w dniu 6/27/18.

UWAGA: Dzienniki te są zgodne z amerykańskim formatem daty miesiąc/dzień/rok.

HP Secure Platform Management (identyfikator źródła = 84h)

Tabela A-1 HP Secure Platform Management

Identyfikator zdarzenia:	Liczba urządzeń (wszystkie/ DaaS)	Liczba zdarzeń (wszystkie/ DaaS)	Opis	Uwagi
40	256/178	943/552	Proces odzyskiwania systemu operacyjnego platformy został uruchomiony przez oprogramowanie układowe.	Uruchomiono odzyskiwanie platformy.

Tabela A-1 HP Secure Platform Management (ciąg dalszy)

Identyfikator zdarzenia:	Liczba urządzeń (wszystkie/ DaaS)	Liczba zdarzeń (wszystkie/ DaaS)	Opis	Uwagi
41	221/147	588/332	Proces odzyskiwania systemu operacyjnego platformy został zakończony pomyślnie.	Ukończono odzyskiwanie platformy.
42	54/42	252/156	Proces odzyskiwania systemu operacyjnego platformy nie powiódł się.	Odzyskiwanie platformy nie powiodło się.

Dziennik audytu oprogramowania układowego można pobrać przy użyciu polecenia Get-HPFirmwareAuditLog w bibliotece HP Client Management Script Library dostępnej na stronie http://www.hp.com/go/clientmanagement. Zdarzenia HP Secure Platform Management o identyfikatorach 40, 41 i 42 zwracają w polu danych kody zdarzeń, które oznaczają wynik operacji oprogramowania Sure Recover. Na przykład następujący wpis w dzienniku oznacza, że pobieranie pliku manifestu lub podpisu przez oprogramowanie Sure Recover nie powiodło się z błędem o identyfikatorze błędu event_id 42 i danymi: 00:30:f1:c3, które należy interpretować jako wartość dword 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:30:f1:c3
```

Pomyślne odzyskiwanie jest wyświetlane jako identyfikator zdarzenia event_id = 41 i dane: 00:00:00:00, na przykład:

```
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
```

Oprogramowanie HP Sure Recover używa następujących kodów zdarzeń.

Tabela A-2 Kody zdarzeń

Opis zdarzenia	Kod zdarzenia
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

User Guide

AMD is a trademark of Advanced Micro Devices, Inc. Bluetooth is a trademark owned by its proprietor and used by HP Inc. under license. Intel, Celeron, Pentium, and Thunderbolt are trademarks of Intel Corporation in the U.S. and other countries. Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: February 2018

Document Part Number: L11998-001

Product notice

This user guide describes features that are common to most models. Some features may not be available on your computer.

Not all features are available in all editions or versions of Windows. Systems may require upgraded and/or separately purchased hardware, drivers, software or BIOS update to take full advantage of Windows functionality. Windows 10 is automatically updated, which is always enabled. ISP fees may apply and additional requirements may apply over time for updates. See http://www.microsoft.com.

To access the latest user guides, go to http://www.hp.com/support, and follow the instructions to find your product. Then select **User Guides**.

Software terms

By installing, copying, downloading, or otherwise using any software product preinstalled on this computer, you agree to be bound by the terms of the HP End User License Agreement (EULA). If you do not accept these license terms, your sole remedy is to return the entire unused product (hardware and software) within 14 days for a full refund subject to the refund policy of your seller.

For any further information or to request a full refund of the price of the computer, please contact your seller.

Safety warning notice

⚠ **WARNING!** To reduce the possibility of heat-related injuries or of overheating the computer, do not place the computer directly on your lap or obstruct the computer air vents. Use the computer only on a hard, flat surface. Do not allow another hard surface, such as an adjoining optional printer, or a soft surface, such as pillows or rugs or clothing, to block airflow. Also, do not allow the AC adapter to come into contact with the skin or a soft surface, such as pillows or rugs or clothing, during operation. The computer and the AC adapter comply with the user-accessible surface temperature limits defined by the International Standard for Safety of Information Technology Equipment (IEC 60950).

Processor configuration setting (select products only)

IMPORTANT: Select computer products are configured with an Intel® Pentium® N35xx/N37xx series or a Celeron® N28xx/N29xx/N30xx/N31xx series processor and a Windows® operating system. **If your computer is configured as described, do not change the processor configuration setting in msconfig.exe from 4 or 2 processors to 1 processor.** If you do so, your computer will not restart. You will have to perform a factory reset to restore the original settings.

Table of contents

1 Welcome

After you set up and register the computer, we recommend the following steps to get the most out of your smart investment:

- **TIP:** To quickly return to the computer Start screen from an open app or the Windows desktop, press the Windows key on your keyboard. Pressing the Windows key again will return you to the previous screen.

- **Connect to the Internet**—Set up your wired or wireless network so that you can connect to the Internet. For more information, see Network connections on page 25.
- **Update your antivirus software**—Protect your computer from damage caused by viruses. The software is preinstalled on the computer. For more information, see Using antivirus software on page 58.
- **Get to know your computer**—Learn about your computer features. See Components on page 4 and Navigating the screen on page 32 for additional information.
- **Find installed software**—Access a list of the software preinstalled on the computer:

  Select the **Start** button.

  – or –

  Right-click the **Start** button, and then select **Apps and Features**.
- Back up your hard drive by creating recovery discs or a recovery flash drive. See Backing up, restoring, and recovering on page 65.

Finding information

To locate resources that provide product details, how-to information, and more, use this table.

Resource	Contents
Setup Instructions	• Overview of computer setup and features
HP support For HP support, go to http://www.hp.com/support.	• Online chat with an HP technician • Support telephone numbers • Replacement parts videos (select products only) • Maintenance and service guides • HP service center locations
Safety & Comfort Guide To access this guide: ▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**. – or – ▲ Select the **Start** button, select **HP**, and then select **HP Documentation**. – or – ▲ Go to http://www.hp.com/ergo. **IMPORTANT:** You must be connected to the Internet to access the latest version of the user guide.	• Proper workstation setup • Guidelines for posture and work habits that increase your comfort and decrease your risk of injury • Electrical and mechanical safety information
Regulatory, Safety and Environmental Notices To access this document: ▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**. – or – ▲ Select the **Start** button, select **HP**, and then select **HP Documentation**.	• Important regulatory notices, including information about proper battery disposal, if needed.
*Limited Warranty** To access this document: ▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**. – or – ▲ Select the **Start** button, select **HP**, and then select **HP Documentation**. – or – ▲ Go to http://www.hp.com/go/orderdocuments. **IMPORTANT:** You must be connected to the Internet to access the latest version of the user guide.	• Specific warranty information about this computer

*You can find your HP Limited Warranty located with the user guides on your product and/or on the CD or DVD provided in the box. In some countries or regions, HP may provide a printed warranty in the box. For countries or regions where the warranty is not provided in printed format, you can request a copy from http://www.hp.com/go/orderdocuments. For products purchased in Asia Pacific, you

Resource	Contents
	can write to HP at POD, PO Box 161, Kitchener Road Post Office, Singapore 912006. Include your product name, and your name, phone number, and postal address.

2 Components

Your computer features top-rated components. This chapter provides details about your components, where they're located, and how they work.

Locating hardware

To find out what hardware is installed on your computer:

- Type `device manager` in the taskbar search box, and then select the **Device Manager** app.

  A list displays all the devices installed on your computer.

For information about system hardware components and the system BIOS version number, press fn+esc (select products only).

Locating software

To find out what software is installed on your computer:

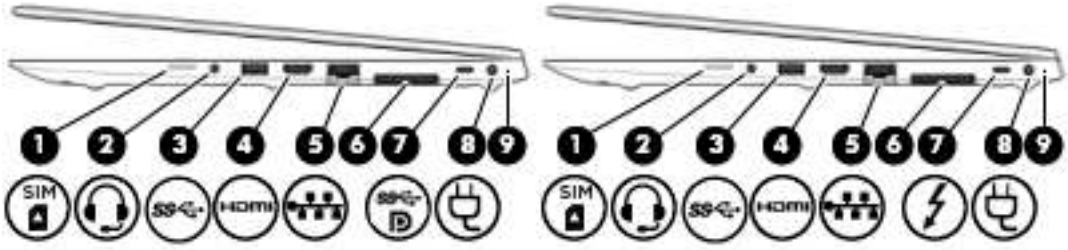
- Select the **Start** button.

  – or –

  Right-click the **Start** button, and then select **Apps and Features**.

Right

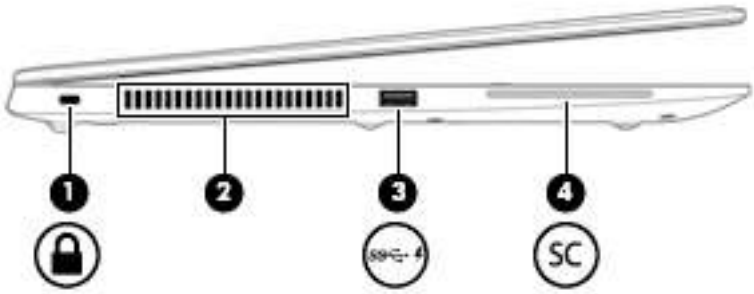
NOTE: Refer to the illustration that most closely matches your computer.



Component			Description
(1)	SIM	SIM card slot or plug	Supports a wireless subscriber identity module (SIM) card or plug. **NOTE:** All models have a SIM card slot and icon, but models that do not have the HP Mobile Broadband Module, a wireless wide area network (WWAN) device, installed at the factory are shipped with a non-removable plug inserted into the slot.
(2)		Audio-out (headphone)/Audio-in (microphone) combo jack	Connects optional powered stereo speakers, headphones, earbuds, a headset, or a television audio cable. Also connects an optional headset microphone. This jack does not support optional standalone microphones. **WARNING!** To reduce the risk of personal injury, adjust the volume before putting on headphones, earbuds, or a headset. For additional safety information, refer to the *Regulatory, Safety, and Environmental Notices*. To access this guide: ▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**. – or – ▲ Select the **Start** button, select **HP**, and then select **HP Documentation**. **NOTE:** When a device is connected to the jack, the computer speakers are disabled.
(3)	SS	USB 3.x SuperSpeed port	Connects a USB device, such as a cell phone, camera, activity tracker, or smartwatch, and provides high-speed data transfer.
(4)	HDMI	HDMI port	Connects an optional video or audio device, such as a high-definition television, any compatible digital or audio component, or a high-speed High Definition Multimedia Interface (HDMI) device.
(5)		RJ-45 (network) jack/status lights	Connects a network cable. • Green (left): The network is connected. • Amber (right): Activity is occurring on the network.
(6)		Docking connector	Connects an optional docking device.

Component		Description
(7)	USB Type-C SuperSpeed port and DisplayPort	When the computer is on, connects and charges most USB devices that have a Type-C connector, such as a cell phone, camera, activity tracker, or smartwatch, and provides high-speed data transfer. **NOTE:** Cables and/or adapters (purchased separately) may be required. – and – Connects a DisplayPort device that has a USB Type-C connector, providing display output.
(7)	USB Type-C power connector and Thunderbolt™ port with HP Sleep and Charge	Connects an AC adapter that has a USB Type-C connector, supplying power to the computer and, if needed, charging the computer battery. – and – Connects and charges most USB devices that have a Type-C connector, such as a cell phone, camera, activity tracker, or smartwatch, and provides high-speed data transfer. – and – Connects a display device that has a USB Type-C connector, providing DisplayPort output. **NOTE:** Your computer may also support a Thunderbolt docking station. **NOTE:** Cables and/or adapters (purchased separately) may be required.
(8)	Power connector	Connects an AC adapter.
(9)	Battery light	When AC power is connected: • White: The battery charge is greater than 90 percent. • Amber: The battery charge is from 0 to 90 percent. • Off: The battery is not charging. When AC power is disconnected (battery not charging): • Blinking amber: The battery has reached a low battery level. When the battery has reached a critical battery level, the battery light begins blinking rapidly. • Off: The battery is not charging.

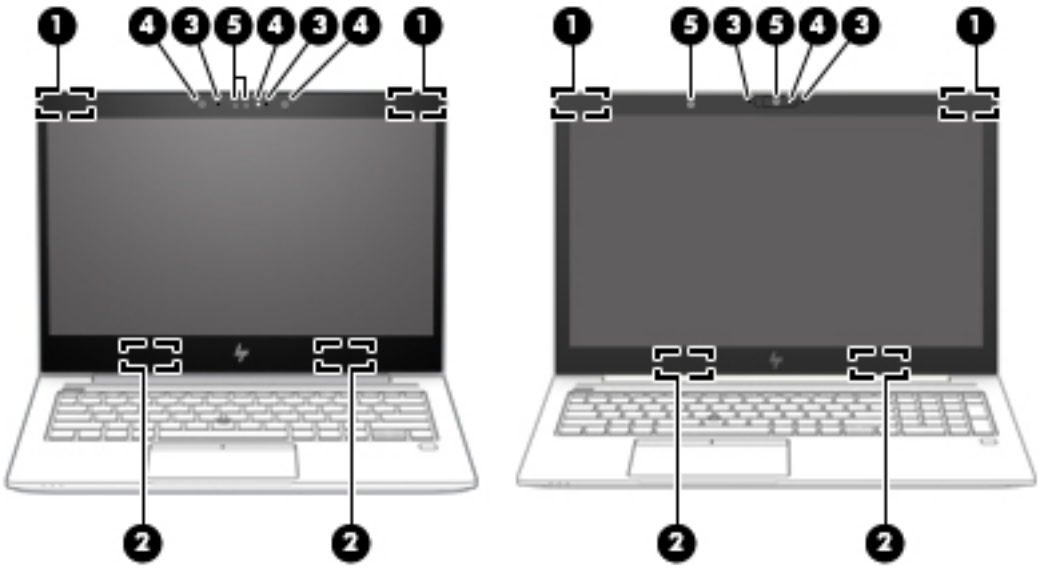
Left



Component			Description
(1)		Security cable slot	Attaches an optional security cable to the computer. **NOTE:** The security cable is designed to act as a deterrent, but it may not prevent the computer from being mishandled or stolen.
(2)		Vent	Enables airflow to cool internal components. **NOTE:** The computer fan starts up automatically to cool internal components and prevent overheating. It is normal for the internal fan to cycle on and off during routine operation.
(3)		USB 3.x SuperSpeed port with HP Sleep and Charge	Connects a USB device, provides high-speed data transfer, and even when the computer is off, charges most products such as a cell phone, camera, activity tracker, or smartwatch.
(4)	SC	Smart card reader	Supports optional smart cards.

Display

NOTE: Refer to the illustration that most closely matches your computer.



Component		Description
(1)	WWAN antennas* (select products only)	Send and receive wireless signals to communicate with wireless wide area networks (WWANs).
(2)	WLAN antennas* (select products only)	Send and receive wireless signals to communicate with wireless local area networks (WLANs).
(3)	Internal microphones	Record sound.
(4)	Camera light(s) (select products only)	On: One or more cameras are in use.
(5)	Camera(s) (select products only)	Allow(s) you to video chat, record video, and record still images. To use your camera, see Using a camera (select products only) on page 36. Some cameras also allow a facial recognition logon to Windows, instead of a password logon. For more information, see Using Windows Hello (select products only) on page 58. **NOTE:** Camera functions vary depending on the camera hardware and software installed on your product.

*The antennas are not visible from the outside of the computer. For optimal transmission, keep the areas immediately around the antennas free from obstructions.

For wireless regulatory notices, see the section of the *Regulatory, Safety, and Environmental Notices* that applies to your country or region.

To access this guide:

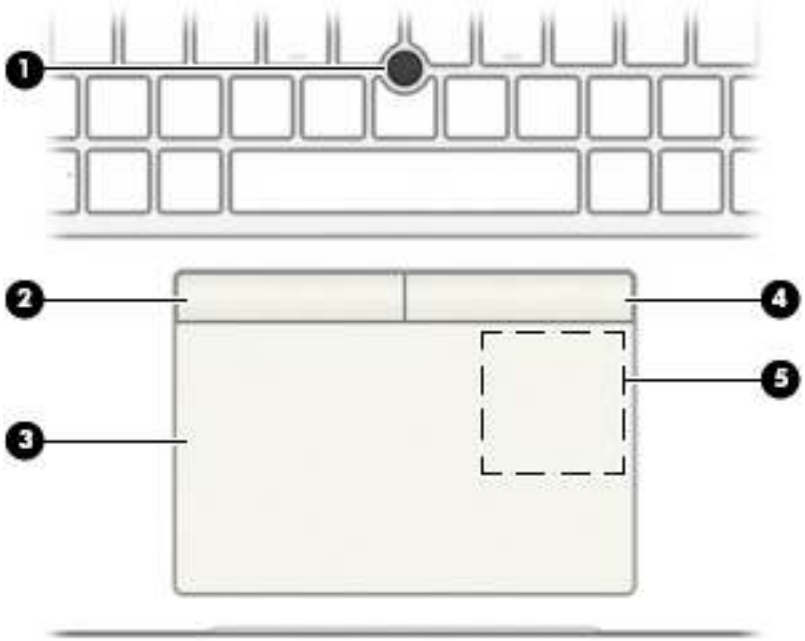
▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**.

– or –

▲ Select the **Start** button, select **HP**, and then select **HP Documentation**.

Keyboard area

TouchPad



Component		Description
(1)	Pointing stick	Moves the pointer on the screen.
(2)	Left pointing stick button	Functions like the left button on an external mouse.
(3)	TouchPad zone	Reads your finger gestures to move the pointer or activate items on the screen.
(4)	Right pointing stick button	Functions like the right button on an external mouse.
(5)	Near Field Communications (NFC) tapping area and antenna* (select products only)	Allows you to wirelessly share information when you tap it with an NFC-enabled device.

*The antenna is not visible from the outside of the computer. For optimal transmission, keep the area immediately around the antenna free from obstructions.

For wireless regulatory notices, see the section of the *Regulatory, Safety, and Environmental Notices* that applies to your country or region.

To access this guide:

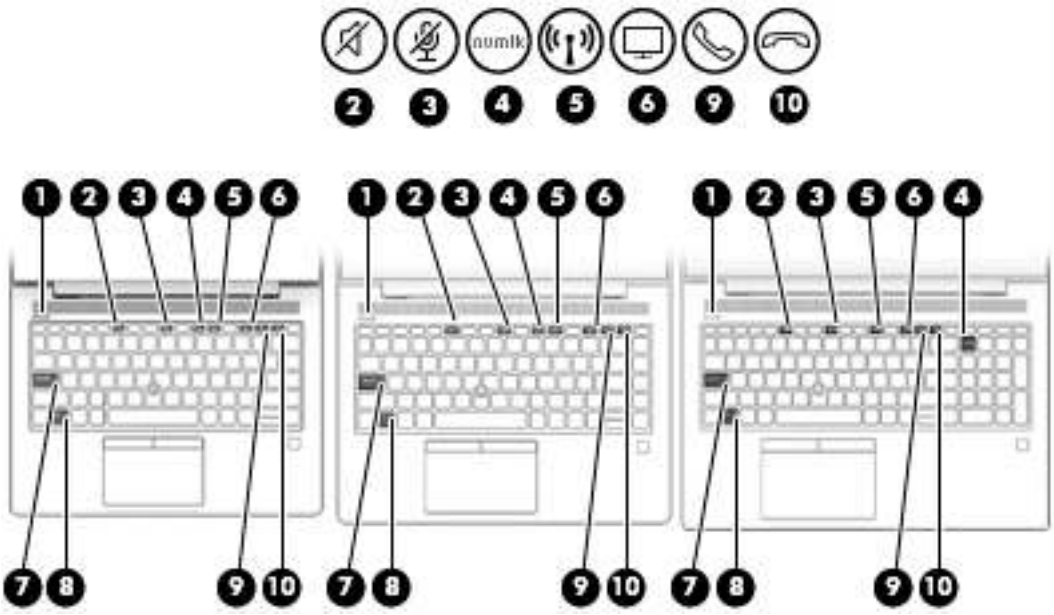
▲ Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**.

– or –

▲ Select the **Start** button, select **HP**, and then select **HP Documentation**.

Lights

NOTE: Refer to the illustration that most closely matches your computer.

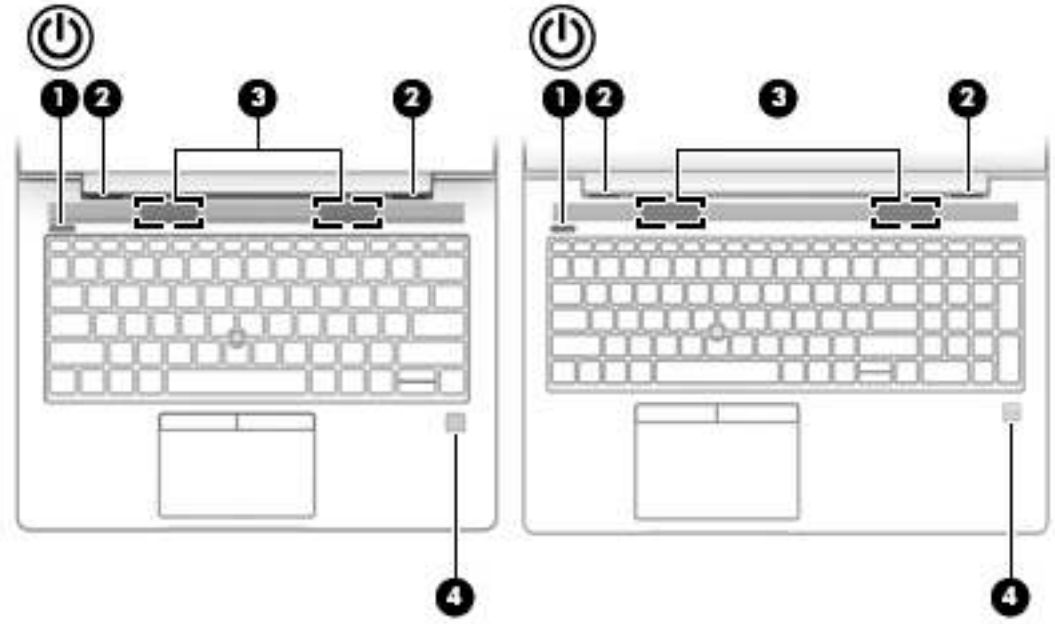


Component			Description
(1)		Power light	• On: The computer is on. • Blinking: The computer is in the Sleep state, a power-saving state. The computer shuts off power to the display and other unneeded components. • Off: The computer is off or in Hibernation. Hibernation is a power-saving state that uses the least amount of power.
(2)		Mute light	• On: Computer sound is off. • Off: Computer sound is on.
(3)		Microphone mute light	• On: Microphone is off. • Off: Microphone is on.
(4)	num lk	Num lk light	On: Num lock is on.
(5)		Wireless light	On: An integrated wireless device, such as a wireless local area network (WLAN) device and/or a Bluetooth® device, is on. **NOTE:** On some models, the wireless light is amber when all wireless devices are off.
(6)		Sharing or presenting light	On: Sharing is on.
(7)		Caps lock light	On: Caps lock is on, which switches the key input to all capital letters.
(8)		Fn lock light	On: The fn key is locked. For more information, see Hot keys (select products only) on page 18.

Component		Description
(9)	Call answer light	On: Call answer is on.
(10)	Call end light	On: Call end is on.

Buttons, speakers, and fingerprint reader

NOTE: Refer to the illustration that most closely matches your computer.

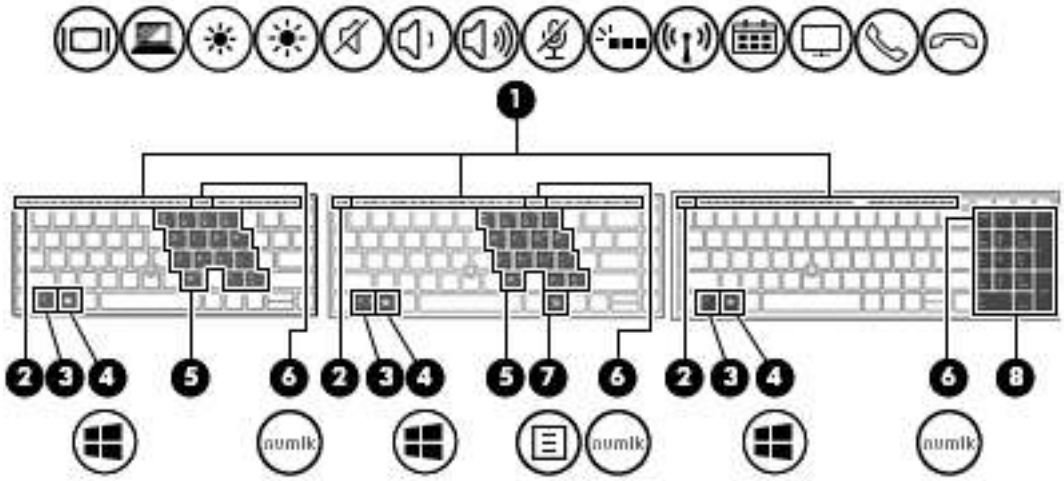


Component		Description
(1)	Power button	• When the computer is off, press the button to turn on the computer. • When the computer is on, press the button briefly to initiate Sleep. • When the computer is in the Sleep state, press the button briefly to exit Sleep. • When the computer is in Hibernation, press the button briefly to exit Hibernation. **CAUTION:** Pressing and holding down the power button results in the loss of unsaved information. If the computer has stopped responding and shutdown procedures are ineffective, press and hold the power button for at least 5 seconds to turn off the computer. To learn more about your power settings, see your power options. ▲ Right-click the **Power meter** icon and then select **Power Options**.
(2)	Vents (2)	Enable airflow to cool internal components. **NOTE:** The computer fan starts up automatically to cool internal components and prevent overheating. It is normal for the internal fan to cycle on and off during routine operation.

Component		Description
(3)	Speakers (2)	Produce sound.
(4)	Fingerprint reader or plug	Allows a fingerprint logon to Windows, instead of a password logon. **NOTE:** The fingerprint reader and plug look similar. To verify you have a fingerprint reader and not a plug, press the Windows key on your keyboard, select **Settings**, select **Accounts**, and then select **Sign-in options** and follow the on-screen instructions.

Special keys

NOTE: Refer to the illustration that most closely matches your computer.



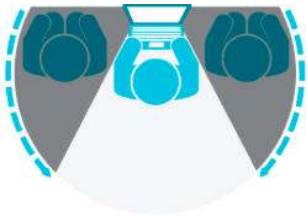
Component		Description
(1)	Action keys	Execute frequently used system functions. See Action keys on page 16.
(2)	esc key	Displays system information when pressed in combination with the fn key.
(3)	fn key	Executes frequently used system functions when pressed in combination with another key. Such key combinations are called *hot keys*. See Hot keys (select products only) on page 18.
(4)	Windows key	Opens the **Start** menu. **NOTE:** Pressing the Windows key again will close the **Start** menu.
(5)	Embedded numeric keypad	A numeric keypad superimposed over the keyboard alphabet keys. When fn+num lk is pressed, the keypad can be used like an external numeric keypad. Each key on the keypad performs the function indicated by the icon in the upper-right corner of the key. **NOTE:** If the keypad function is active when the computer is turned off, that function is reinstated when the computer is turned back on.
(6)	num lk key	Turns the embedded numeric keypad on and off. – or – Alternates between the navigational and numeric functions on the integrated numeric keypad.
(7)	Windows application key (select products only)	Displays options for a selected object.
(8)	Integrated numeric keypad	A separate keypad to the right of the alphabet keyboard. When num lk is pressed, the integrated keypad can be used like an external numeric keypad.

Component	Description
	NOTE: If the keypad function is active when the computer is turned off, that function is reinstated when the computer is turned back on.

Action keys

An action key performs the function indicated by the icon on the key. To determine which keys are on your product, see Special keys on page 14.

▲ To use an action key, press and hold the key.

Icon	Description
	Switches the screen image among display devices connected to the system. For example, if a monitor is connected to the computer, repeatedly pressing the key alternates the screen image from computer display to monitor display to simultaneous display on both the computer and monitor.
	Helps prevent side-angle viewing from onlookers. If needed, decrease or increase brightness for well-lit or darker environments. Press the key again to turn off the privacy screen. **NOTE:** To quickly turn on the highest privacy setting, press fn+p. 
	Decreases the screen brightness incrementally as long as you hold down the key.
	Increases the screen brightness incrementally as long as you hold down the key.
	Mutes or restores speaker sound.
	Decreases speaker volume incrementally while you hold down the key.
	Increases speaker volume incrementally while you hold down the key.
	Mutes the microphone.
	Turns the keyboard backlight off or on. **NOTE:** To conserve battery power, turn off this feature.
	Turns the wireless feature on or off. **NOTE:** A wireless network must be set up before a wireless connection is possible.
	Provides quick access to your Skype for Business calendar. **NOTE:** This feature requires Skype® for Business or Lync® 2013 running on Microsoft Exchange or Office 365® servers.
	Turns the screen sharing function on or off. **NOTE:** This feature requires Skype for Business or Lync 2013 running on Microsoft Exchange or Office 365 servers.

Icon	Description
	• Answers a call. • Starts a call during a 1-on-1 chat. • Places a call on hold. **NOTE:** This feature requires Skype for Business or Lync 2013 running on Microsoft Exchange or Office 365 servers.
	• Ends a call. • Declines incoming calls. • Ends screen sharing. **NOTE:** This feature requires Skype for Business or Lync 2013 running on Microsoft Exchange or Office 365 servers.

NOTE: The action key feature is enabled at the factory. You can disable this feature by pressing and holding the fn key and the left shift key. The fn lock light will turn on. After you have disabled the action key feature, you can still perform each function by pressing the fn key in combination with the appropriate action key.

Hot keys (select products only)

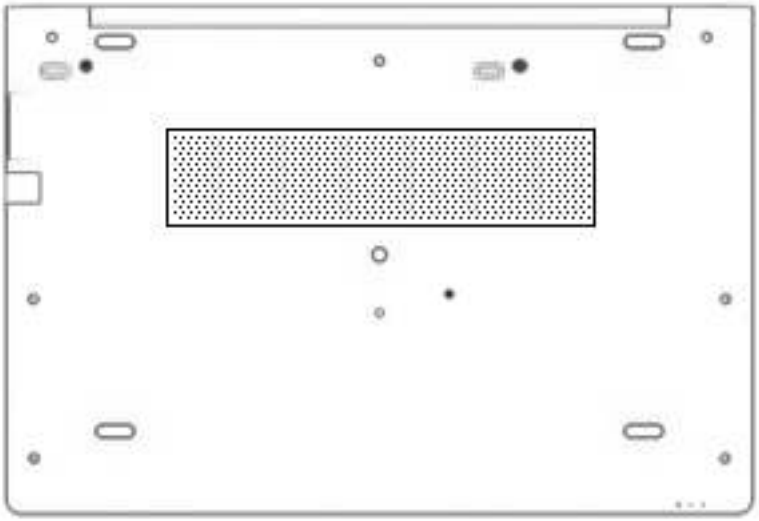
A hot key is the combination of the fn key and another key.

To use a hot key:

▲ Press the fn key, and then press one of the keys listed in the following table.

Key	Description
C	Turns on scroll lock.
R	Breaks the operation.
S	Sends a programing query.

Bottom



Component	Description
Vent	Enables airflow to cool internal components. **NOTE:** The computer fan starts up automatically to cool internal components and prevent overheating. It is normal for the internal fan to cycle on and off during routine operation.

Front

Component			Description
(1)		Power light	• On: The computer is on. • Blinking: The computer is in the Sleep state, a power-saving state. The computer shuts off power to the display and other unneeded components. • Off: The computer is off or in Hibernation. Hibernation is a power-saving state that uses the least amount of power.
(2)		Wireless light	On: An integrated wireless device, such as a wireless local area network (WLAN) device and/or a Bluetooth® device, is on. **NOTE:** On some models, the wireless light is amber when all wireless devices are off.
(3)		Drive light	• Blinking white: The hard drive is being accessed. • Amber: HP 3D DriveGuard has temporarily parked the hard drive. **NOTE:** For more information about HP 3D DriveGuard, see Using HP 3D DriveGuard (select products only) on page 61.

Cover

NOTE: Refer to the illustration that most closely matches your computer.

Component	Description
Internal microphone(s) (1 or 2 depending on model)	Record(s) sound.

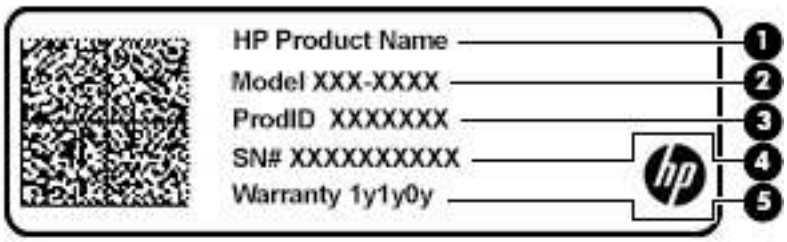
Labels

The labels affixed to the computer provide information you may need when you troubleshoot system problems or travel internationally with the computer. Labels may be in paper form or imprinted on the product.

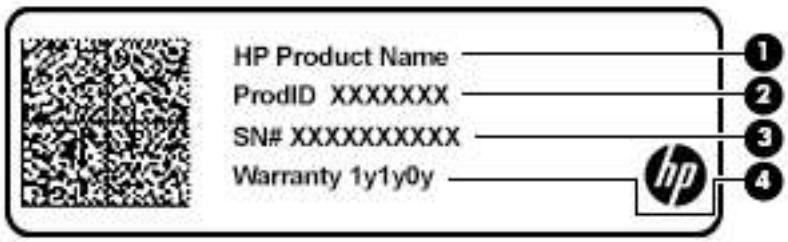
IMPORTANT: Check the following locations for the labels described in this section: the bottom of the computer, inside the battery bay, under the service door, on the back of the display, or on the bottom of a tablet kickstand.

- Service label—Provides important information to identify your computer. When contacting support, you may be asked for the serial number, the product number, or the model number. Locate this information before you contact support.

  Your service label will resemble one of the examples shown below. Refer to the illustration that most closely matches the service label on your computer.



Component	
(1)	HP product name (select products only)
(2)	Model number
(3)	Product ID
(4)	Serial number
(5)	Warranty period



Component	
(1)	HP product name (select products only)
(2)	Product ID

Component	
(3)	Serial number
(4)	Warranty period

- Regulatory label(s)—Provide(s) regulatory information about the computer.
- Wireless certification label(s)—Provide(s) information about optional wireless devices and the approval markings for the countries or regions in which the devices have been approved for use.

Inserting a SIM card (select products only)

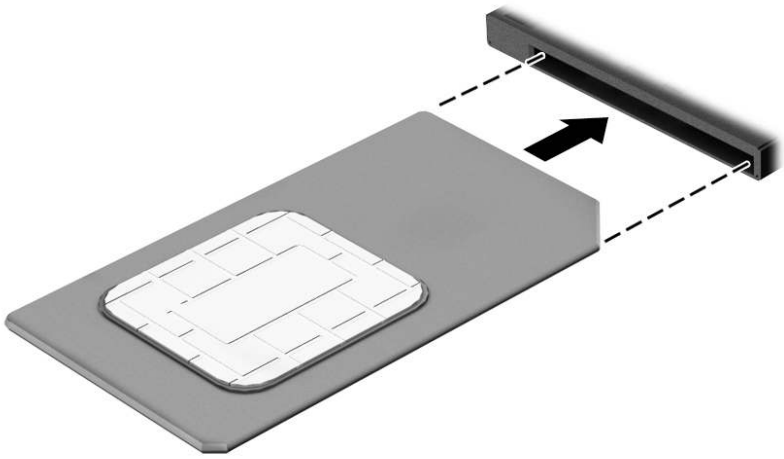
CAUTION: To prevent damage to the connectors, use minimal force when inserting a SIM card.

To insert a SIM card, follow these steps:

1. Turn off the computer by using the Shut down command.
2. Insert the SIM card into the SIM card slot, and then press in on the SIM card until it is firmly seated.

NOTE: The SIM card in your computer may look slightly different from the illustration in this section.

NOTE: See the image on the battery bay to determine which way the SIM card should be inserted into your computer.



To remove a SIM card, press in on the SIM card, and then remove it from the slot.

3 Network connections

Your computer can travel with you wherever you go. But even at home, you can explore the globe and access information from millions of websites using your computer and a wired or wireless network connection. This chapter will help you get connected to that world.

Connecting to a wireless network

Your computer may be equipped with one or more of the following wireless devices:

- WLAN device—Connects the computer to wireless local area networks (commonly referred to as Wi-Fi networks, wireless LANs, or WLANs) in corporate offices, your home, and public places such as airports, restaurants, coffee shops, hotels, and universities. In a WLAN, the mobile wireless device in your computer communicates with a wireless router or a wireless access point.
- HP Mobile Broadband Module (select products only)—A wireless wide area network (WWAN) device that gives you wireless connectivity over a much larger area. Mobile network operators install base stations (similar to cell phone towers) throughout large geographic areas, effectively providing coverage across entire states, regions, or even countries.
- Bluetooth® device—Creates a personal area network (PAN) to connect to other Bluetooth-enabled devices such as computers, phones, printers, headsets, speakers, and cameras. In a PAN, each device communicates directly with other devices, and devices must be relatively close together—typically within 10 meters (approximately 33 feet) of each other.

Using the wireless controls

You can control the wireless devices in your computer using one or more of these features:

- Wireless button (also called airplane mode key or wireless key) (referred to in this chapter as wireless button)
- Operating system controls

Wireless button

The computer may have a wireless button, one or more wireless devices, and one or two wireless lights. All the wireless devices on your computer are enabled at the factory.

The wireless light indicates the overall power state of your wireless devices, not the status of individual devices.

Operating system controls

The Network and Sharing Center allows you to set up a connection or network, connect to a network, and diagnose and repair network problems.

To use operating system controls:

1. Type `control panel` in the taskbar search box, and then select **Control Panel**.
2. Select **Network and Internet**, and then select **Network and Sharing Center**.

Connecting to a WLAN

NOTE: When you are setting up Internet access in your home, you must establish an account with an Internet service provider (ISP). To purchase Internet service and a modem, contact a local ISP. The ISP will help set up the modem, install a network cable to connect your wireless router to the modem, and test the Internet service.

To connect to a WLAN, follow these steps:

1. Be sure that the WLAN device is on.
2. Select the network status icon in the taskbar, and then connect to one of the available networks.

   If the WLAN is a security-enabled WLAN, you are prompted to enter a security code. Enter the code, and then select **Next** to complete the connection.

   NOTE: If no WLANs are listed, you may be out of range of a wireless router or access point.

   NOTE: If you do not see the WLAN you want to connect to, right-click the network status icon in the taskbar, and then select **Open Network and Sharing Center**. Select **Set up a new connection or network**. A list of options is displayed, allowing you to manually search for and connect to a network or to create a new network connection.
3. Follow the on-screen instructions to complete the connection.

After the connection is made, select the network status icon at the far right of the taskbar, to verify the name and status of the connection.

NOTE: The functional range (how far your wireless signals travel) depends on WLAN implementation, router manufacturer, and interference from other electronic devices or structural barriers such as walls and floors.

Using HP Mobile Broadband (select products only)

Your HP Mobile Broadband computer has built-in support for mobile broadband service. Your new computer, when used with a mobile operator's network, gives you the freedom to connect to the Internet, send e-mail, or connect to your corporate network without the need for Wi-Fi hotspots.

NOTE: If your computer includes HP Mobile Connect, the instructions in this section do not apply. See Using HP Mobile Connect Pro (select products only) on page 27.

You might need the HP Mobile Broadband Module IMEI and/or MEID number to activate mobile broadband service. The number may be printed on a label located on the bottom of your computer, inside the battery bay, under the service door, or on the back of the display.

– or –

You can find the number following these steps:

1. From the taskbar, select the network status icon.
2. Select **View Connection Settings**.
3. Under the **Mobile broadband** section, select the network status icon.

Some mobile network operators require the use of a SIM card. A SIM card contains basic information about you, such as a personal identification number (PIN), as well as network information. Some computers include a SIM card that is preinstalled. If the SIM card is not preinstalled, it may be provided in the HP Mobile Broadband information provided with your computer or the mobile network operator may provide it separately from the computer.

For information about HP Mobile Broadband and how to activate service with a preferred mobile network operator, see the HP Mobile Broadband information included with your computer.

Using HP Mobile Connect Pro (select products only)

HP Mobile Connect Pro is a prepaid, mobile broadband service that provides a cost-effective, secure, simple, and flexible mobile broadband connection for your computer. To use HP Mobile Connect Pro, your computer must have a SIM card and the HP Mobile Connect app. For more information about HP Mobile Connect Pro and where it is available, go to http://www.hp.com/go/mobileconnect.

Using GPS (select products only)

Your computer may be equipped with a Global Positioning System (GPS) device. GPS satellites deliver location, speed, and direction information to GPS-equipped systems.

To enable GPS, make sure location is enabled under the Windows privacy setting.

1. Type `location` in the taskbar search box, and then select **Location privacy settings**.
2. Follow the on-screen instructions for using location settings.

Using Bluetooth wireless devices (select products only)

A Bluetooth device provides short-range wireless communications that replace the physical cable connections that traditionally link electronic devices such as the following:

- Computers (desktop, notebook)
- Phones (cellular, cordless, smartphone)
- Imaging devices (printer, camera)
- Audio devices (headset, speakers)
- Mouse
- External keyboard

Connecting Bluetooth devices

Before you can use a Bluetooth device, you must establish a Bluetooth connection.

1. Type `bluetooth` in the taskbar search box, and then select **Bluetooth and other devices settings**.
2. Turn on Bluetooth, if it is not already turned on.
3. Select your device from the list, and then follow the on-screen instructions.

NOTE: If the device requires verification, a pairing code is displayed. On the device you are adding, follow the on-screen instructions to verify that the code on your device matches the pairing code. For more information, refer to the documentation provided with the device.

NOTE: If your device does not appear in the list, be sure that Bluetooth on that device is turned on. Some devices may have additional requirements; refer to the documentation provided with the device.

Using NFC to share information (select products only)

Your computer supports Near Field Communication (NFC), which allows you to wirelessly share information between two NFC-enabled devices. Information is transferred by tapping the tapping area (antenna) of the

computer with the antenna of your phone or other device. With NFC and supported apps, you can share websites, transfer contact information, transfer payments, and print on NFC-enabled printers.

NOTE: To locate the tapping area on your computer, see Components on page 4.

Sharing

1. Confirm that the NFC function is enabled.
   a. Type `wireless` in the taskbar search box, and then select **Turn wireless devices on or off**.
   b. Confirm that the selection for NFC is **On**.
2. Tap the NFC tapping area with an NFC-enabled device. You may hear a sound when the devices connect.

   NOTE: To find the location of the antenna on the other NFC device, refer to your device instructions.
3. Follow any on-screen instructions to continue.

Connecting to a wired network

Select products may allow wired connections: local area network (LAN) and modem connection. A LAN connection uses a network cable and is much faster than a modem, which uses a telephone cable. Both cables are sold separately.

⚠ **WARNING!** To reduce the risk of electric shock, fire, or damage to the equipment, do not plug a modem cable or telephone cable into an RJ-45 (network) jack.

Connecting to a local area network (LAN) (select products only)

Use a LAN connection if you want to connect the computer directly to a router in your home (instead of working wirelessly), or if you want to connect to an existing network at your office.

NOTE: A feature called HP LAN-WLAN Protection may be enabled on your computer. It closes your wireless (Wi-Fi) connection when you connect directly to a LAN. For more information about HP LAN-WLAN Protection, see Using HP LAN-WLAN Protection (select products only) on page 30.

If there is no RJ-45 port on the computer, connecting to a LAN requires an 8-pin, RJ-45 network cable or an optional docking device or expansion product.

To connect the network cable, follow these steps:

1. Plug the network cable into the network jack **(1)** on the computer or on an optional docking device or expansion product.
2. Plug the other end of the network cable into a network wall jack **(2)** or router.

NOTE: If the network cable contains noise suppression circuitry **(3)**, which prevents interference from TV and radio reception, orient the circuitry end of the cable toward the computer.

Using HP LAN-WLAN Protection (select products only)

In a LAN environment, you can set HP LAN-WLAN Protection to safeguard your LAN network from unauthorized wireless access. When HP LAN-WLAN Protection is enabled, the WLAN (Wi-Fi) connection is turned off when the computer is connected directly to a LAN.

Turning on and customizing HP LAN-WLAN Protection

1. Connect a network cable to the network jack on the computer, or on an optional docking device or expansion product.
2. Start Computer Setup (BIOS).
   - Computers or tablets with keyboards:
     - ▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     - ▲ Turn on or restart the tablet, and then quickly hold down the volume down button until the Startup menu is displayed. Tap **f10** to enter Computer Setup.
3. Select **Advanced**, and then select **Built-in Device Options**.
4. Select the check box for **LAN/WLAN Auto Switching** to turn off WLAN connections when connected to a LAN network.
5. To save your changes and exit Computer Setup, select the **Save** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Using HP MAC Address Manager to identify your computer on a network (select products only)

You can enable a system Media Access Control (MAC) address to provide a customizable way of identifying your computer and its communications on networks. This system MAC address provides unique identification even when your computer is connected through an external device, such as a docking station or external wireless adapter. This address is disabled by default.

Turning on and customizing the system MAC address

1. Connect a network cable to the network jack on the computer, or on an optional docking device or expansion product.
2. Start Computer Setup (BIOS).
   - Computers or tablets with keyboards:
     - ▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     - ▲ Turn on or restart the tablet, and then quickly hold down the volume down button until the Startup menu is displayed. Tap **f10** to enter Computer Setup.

3. Select **Advanced**, and then select **Host Based MAC Address**.
4. In the box to the right of **Host Based MAC Address**, select either **System** to enable the host-based MAC address or **Custom** to customize the address.
5. Make selections for boot order and devices supported.
6. If you selected Custom, select **MAC ADDRESS**, enter your customized system MAC address, and then press enter to save the address.
7. To save your changes and exit Computer Setup, select the **Save** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

For additional documentation about HP MAC Address Manager and using system MAC addresses, go to http://www.hp.com/support. Select **Find your product**, and then follow the on-screen instructions.

4 Navigating the screen

You can navigate the computer screen in one or more of the following ways:

- Use touch gestures directly on the computer screen
- Use touch gestures on the TouchPad
- Use an optional mouse or keyboard (purchased separately)
- Use an on-screen keyboard
- Use a pointing stick

Using TouchPad and touch screen gestures

The TouchPad helps you navigate the computer screen and control the pointer using simple touch gestures. You can also use the left and right TouchPad buttons as you would use the corresponding buttons on an external mouse. To navigate a touch screen (select products only), touch the screen directly using gestures described in this chapter.

You can also customize gestures and view demonstrations of how they work. Type `control panel` in the taskbar search box, select **Control Panel**, and then select **Hardware and Sound**. Under **Devices and Printers**, select **Mouse**.

NOTE: Unless noted, gestures can be used on the TouchPad or a touch screen (select products only).

Tap

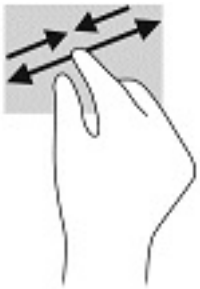
Use the tap/double-tap gesture to select or open an item on the screen.

- Point to an item on the screen, and then tap one finger on the TouchPad zone or touch screen to select the item. Double-tap an item to open it.

Two-finger pinch zoom

Use the two-finger pinch zoom to zoom out or in on images or text.

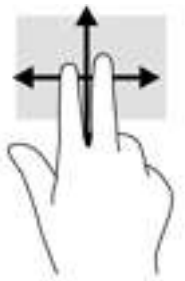
- Zoom out by placing two fingers apart on the TouchPad zone or touch screen and then moving your fingers together.
- Zoom in by placing two fingers together on the TouchPad zone or touch screen and then moving your fingers apart.



Two-finger slide (TouchPad only)

Use the two-finger slide to move up, down, or sideways on a page or image.

- Place two fingers slightly apart on the TouchPad zone and then drag them up, down, left, or right.



Two-finger tap (TouchPad only)

Use the two-finger tap to open the menu for an object on the screen.

NOTE: The two-finger tap performs the same function as right-clicking with the mouse.

- Tap two fingers on the TouchPad zone to open the options menu for the selected object.

Four-finger tap (TouchPad only)

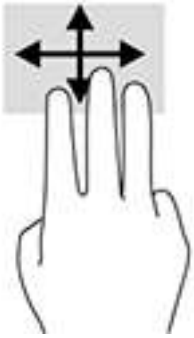
Use the four-finger tap to open the action center.

- Tap four fingers on the Touchpad to open the action center and view current settings and notifications.

Three-finger swipe (TouchPad only)

Use the three-finger swipe to view open windows and to switch between open windows and the desktop.

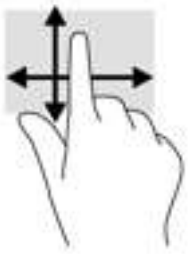
- Swipe 3 fingers away from you to see all open windows.
- Swipe 3 fingers toward you to show the desktop.
- Swipe 3 fingers left or right to switch between open windows.



One-finger slide (touch screen only)

Use the one-finger slide to pan or scroll through lists and pages, or to move an object.

- To scroll across the screen, lightly slide one finger across the screen in the direction you want to move.
- To move an object, press and hold your finger on an object, and then drag your finger to move the object.



Using an optional keyboard or mouse

An optional keyboard or mouse allows you to type, select items, scroll, and perform the same functions as you do using touch gestures. The keyboard also allows you to use action keys and hot keys to perform specific functions.

Using an on-screen keyboard (select products only)

1. To display an on-screen keyboard, tap the keyboard icon in the notification area, at the far right of the taskbar.
2. Begin typing.

NOTE: Suggested words may be displayed above the on-screen keyboard. Tap a word to select it.

NOTE: Action keys and hot keys do not display or function on the on-screen keyboard.

5 Entertainment features

Use your HP computer for business or pleasure to meet with others via the camera, mix audio and video, or connect external devices like a projector, monitor, TV, or speakers. See Components on page 4 to locate the audio, video and camera features on your computer.

Using a camera (select products only)

Your computer has a camera (integrated camera) that records video and captures photographs. Some models allow you to video conference and chat online using streaming video.

- To access the camera, type `camera` in the taskbar search box, and then select **Camera** from the list of applications.

Using audio

You can download and listen to music, stream audio content (including radio) from the web, record audio, or mix audio and video to create multimedia. You can also play music CDs on the computer (on select models) or attach an external optical drive to play CDs. To enhance your listening enjoyment, attach headphones or speakers.

Connecting speakers

You can attach wired speakers to your computer by connecting them to a USB port or to the audio-out (headphone)/audio-in (microphone) combo jack on your computer or on a docking station.

To connect wireless speakers to your computer, follow the device manufacturer's instructions. To connect high-definition speakers to the computer, see Setting up HDMI audio on page 40. Before connecting speakers, lower the volume setting.

Connecting headphones

⚠ **WARNING!** To reduce the risk of personal injury, lower the volume setting before putting on headphones, earbuds, or a headset. For additional safety information, see the *Regulatory, Safety and Environmental Notices*.

To access this guide:

- Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**.

– or –

- Select the **Start** button, select **HP**, and then select **HP Documentation**.

You can connect wired headphones to the audio-out (headphone)/audio-in (microphone) combo jack on your computer.

To connect wireless headphones to your computer, follow the device manufacturer's instructions.

Connecting headsets

WARNING! To reduce the risk of personal injury, lower the volume setting before putting on headphones, earbuds, or a headset. For additional safety information, see the *Regulatory, Safety and Environmental Notices*.

To access this guide:

- Select the **Start** button, select **HP Help and Support**, and then select **HP Documentation**.

– or –

- Select the **Start** button, select **HP**, and then select **HP Documentation**.

Headphones combined with a microphone are called headsets. You can connect wired headsets to the audio-out (headphone)/audio-in (microphone) combo jack on your computer.

To connect wireless headsets to your computer, follow the device manufacturer's instructions.

Using sound settings

Use sound settings to adjust system volume, change system sounds, or manage audio devices.

To view or change sound settings:

- Type `control panel` in the taskbar search box, select **Control Panel**, select **Hardware and Sound**, and then select **Sound**.

Your computer may include an enhanced sound system by Bang & Olufsen, DTS, Beats audio, or another provider. As a result, your computer may include advanced audio features that can be controlled through an audio control panel specific to your audio system.

Use the audio control panel to view and control audio settings.

- Type `control panel` in the taskbar search box, select **Control Panel**, select **Hardware and Sound**, and then select the audio control panel specific to your system.

Using video

Your computer is a powerful video device that enables you to watch streaming video from your favorite websites and download video and movies to watch on your computer when you are not connected to a network.

To enhance your viewing enjoyment, use one of the video ports on the computer to connect an external monitor, projector, or TV.

IMPORTANT: Be sure that the external device is connected to the correct port on the computer, using the correct cable. Follow the device manufacturer's instructions.

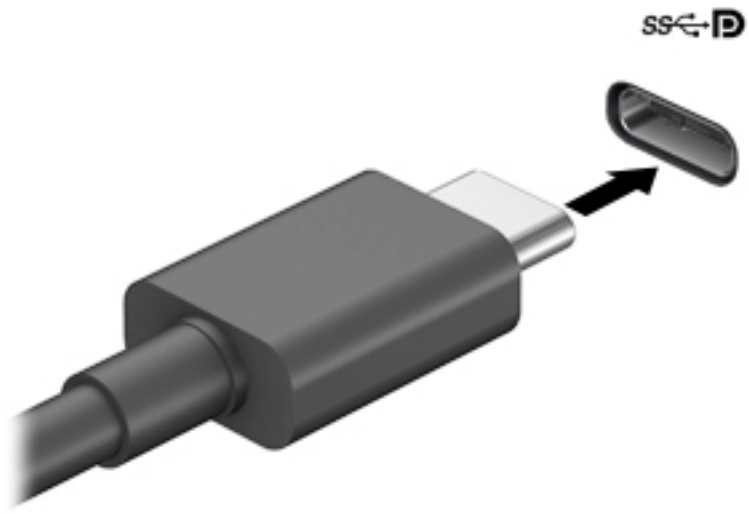
For information on using your video features, refer to HP Support Assistant.

Connecting a DisplayPort device using a USB Type-C cable (select products only)

NOTE: To connect a USB Type-C DisplayPort device to your computer, you need a USB Type-C cable, purchased separately.

To see video or high-resolution display output on an external DisplayPort device, connect the DisplayPort device according to the following instructions:

1. Connect one end of the USB Type-C cable to the USB SuperSpeed and DisplayPort port on the computer.



2. Connect the other end of the cable to the external DisplayPort device.
3. Press f1 to alternate the computer screen image between 4 display states.
   - **PC screen only:** View the screen image on the computer only.
   - **Duplicate:** View the screen image simultaneously on both the computer and external device.
   - **Extend:** View the screen image extended across both the computer and external device.
   - **Second screen only:** View the screen image on the external device only.

   Each time you press f1 the display state changes.

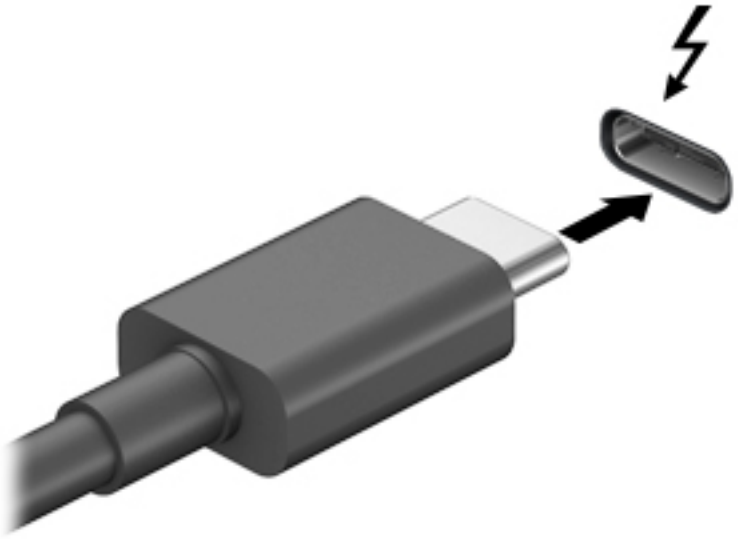
NOTE: For best results, especially if you choose the "Extend" option, increase the screen resolution of the external device, as follows. Select the **Start** button, select **Settings**, and then select **System**. Under **Display**, select the appropriate resolution, and then select **Keep changes**.

Connecting a Thunderbolt device using a USB Type-C cable (select products only)

NOTE: To connect a USB Type-C Thunderbolt device to your computer, you need a USB Type-C cable, purchased separately.

To see video or high-resolution display output on an external Thunderbolt device, connect the Thunderbolt device according to the following instructions:

1. Connect one end of the USB Type-C cable to the USB Type-C Thunderbolt port on the computer.



2. Connect the other end of the cable to the external Thunderbolt device.
3. Press fn+f1 to alternate the computer screen image between 4 display states.
   - **PC screen only:** View the screen image on the computer only.
   - **Duplicate:** View the screen image simultaneously on both the computer and external device.
   - **Extend:** View the screen image extended across both the computer and external device.
   - **Second screen only:** View the screen image on the external device only.

   Each time you press fn+f1 the display state changes.

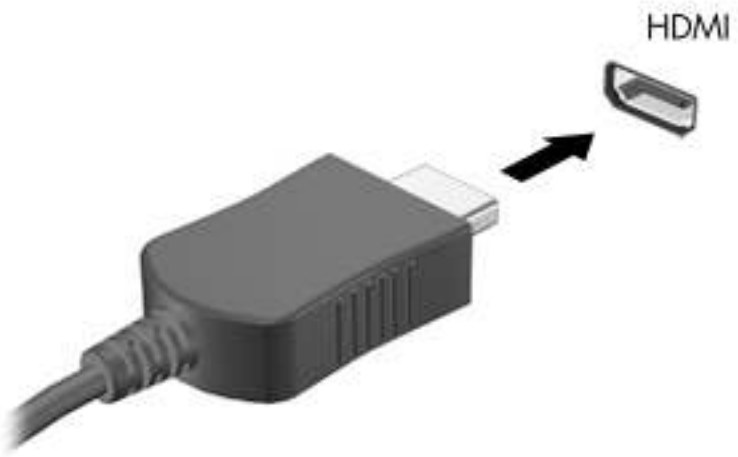
NOTE: For best results, especially if you choose the "Extend" option, increase the screen resolution of the external device, as follows. Type `control panel` in the taskbar search box, select **Control Panel**, select **Appearance and Personalization**. Under **Display**, select **Adjust resolution**.

Connecting video devices using an HDMI cable (select products only)

NOTE: To connect an HDMI device to your computer, you need an HDMI cable, purchased separately.

To see the computer screen image on a high-definition TV or monitor, connect the high-definition device according to the following instructions:

1. Connect one end of the HDMI cable to the HDMI port on the computer.



2. Connect the other end of the cable to the high-definition TV or monitor.
3. Press f1 to alternate the computer screen image between 4 display states:
   - **PC screen only:** View the screen image on the computer only.
   - **Duplicate:** View the screen image simultaneously on both the computer and the external device.
   - **Extend:** View the screen image extended across both the computer and the external device.
   - **Second screen only:** View the screen image on the external device only.

   Each time you press f1, the display state changes.

NOTE: For best results, especially if you choose the "Extend" option, increase the screen resolution of the external device, as follows. Select the **Start** button, select **Settings**, and then select **System**. Under **Display**, select the appropriate resolution, and then select **Keep changes**.

Setting up HDMI audio

HDMI is the only video interface that supports high-definition video and audio. After you connect an HDMI TV to the computer, you can then turn on HDMI audio by following these steps:

1. Right-click the **Speakers** icon in the notification area, at the far right of the taskbar, and then select **Playback devices**.
2. On the **Playback** tab, select the name of the digital output device.
3. Click **Set Default**, and then click **OK**.

To return the audio stream to the computer speakers:

1. Right-click the **Speakers** icon in the notification area, at the far right of the taskbar, and then click **Playback devices**.
2. On the Playback tab, click **Speakers**.
3. Click **Set Default**, and then click **OK**.

Discovering and connecting wired displays using MultiStream Transport

MultiStream Transport (MST) allows you to connect multiple wired display devices to your computer by connecting to the VGA or DisplayPorts on your computer and also to the VGA or DisplayPorts on a hub or an external docking station. You can connect in several ways, depending on the type of graphics controller installed on your computer and whether or not your computer includes a built-in hub. Go to Device Manager to find out what hardware is installed on your computer.

- ▲ Type `device manager` in the taskbar search box, and then select the **Device Manager** app. A list displays all the devices installed on your computer.

Connect displays to computers with AMD or Nvidia graphics (with an optional hub)

NOTE: With an AMD graphics controller and optional hub, you can connect up to 6 external display devices.

NOTE: With an Nvidia graphics controller and optional hub, you can connect up to 4 external display devices.

To set up multiple display devices, follow these steps:

1. Connect an external hub (purchased separately) to the DisplayPort on your computer, using a DP-to-DP cable (purchased separately). Be sure that the hub power adapter is connected to AC power.
2. Connect your external display devices to the VGA ports or DisplayPorts on the hub.
3. To see all of your connected display devices, type `device manager` in the taskbar search box, and then select the **Device Manager** app. If you don't see all of your connected displays, be sure that each is connected to the correct port on the hub.

NOTE: Multiple display choices include **Duplicate**, which mirrors your computer screen on all enabled display devices, or **Extend**, which spans your computer screen across all enabled display devices.

Connect displays to computers with Intel graphics (with an optional hub)

NOTE: With an Intel graphics controller and optional hub, you can connect up to 3 display devices.

To set up multiple display devices, follow these steps:

1. Connect an external hub (purchased separately) to the DisplayPort on your computer, using a DP-to-DP cable (purchased separately). Be sure that the hub power adapter is connected to AC power.
2. Connect your external display devices to the VGA ports or DisplayPorts on the hub.
3. When Windows detects a monitor connected to the DP hub, the **DisplayPort Topology Notification** dialog box is displayed. Click the appropriate options to configure your displays. Multiple display choices include **Duplicate**, which mirrors your computer screen on all enabled display devices, or **Extend**, which extends the screen image across all enabled display devices.

NOTE: If this dialog box does not appear, be sure that each external display device is connected to the correct port on the hub. Select the **Start** button, select **Settings**, and then select **System**. Under **Display**, select the appropriate resolution, and then select **Keep changes**.

Connect displays to computers with Intel graphics (with a built-in hub)

With your internal hub and Intel graphics controller, you can connect up to 3 display devices in the following configurations:

- Two 1920 x 1200 DP monitors connected to the computer + one 1920 x 1200 VGA monitor connected to an optional docking station
- One 2560 x 1600 DP monitor connected to the computer + one 1920 x 1200 VGA monitor connected to an optional docking station

To set up multiple display devices, follow these steps:

1. Connect your external display devices to the VGA ports or DisplayPorts (DP) on the computer base or the docking station.
2. When Windows detects a monitor connected to the DP hub, the **DisplayPort Topology Notification** dialog box is displayed. Click the appropriate options to configure your displays. Multiple display choices include **Duplicate**, which mirrors your computer screen on all enabled display devices, or **Extend**, which extends the screen image across all enabled display devices.

NOTE: If this dialog box does not appear, be sure that each external display device is connected to the correct port on the hub. Select the **Start** button, select **Settings**, and then select **System**. Under **Display**, select the appropriate resolution, and then select **Keep changes**.

Discovering and connecting to Miracast-compatible wireless displays (select products only)

NOTE: To learn what type of display you have (Miracast-compatible or Intel WiDi), refer to the documentation that came with your TV or secondary display.

To discover and connect to Miracast-compatible wireless displays without leaving your current apps, follow the steps below.

To open Miracast:

▲ Type `project` in the taskbar search box, and then click **Project to a second screen**. Click **Connect to a wireless display**, and then follow the on-screen instructions.

Using data transfer

Your computer is a powerful entertainment device that enables you to transfer photos, videos and movies from your USB devices to view on your computer.

To enhance your viewing enjoyment, use one of the USB Type-C ports on the computer to connect a USB device, such as a cell phone, camera, activity tracker, or smartwatch, and transfer the files to your computer.

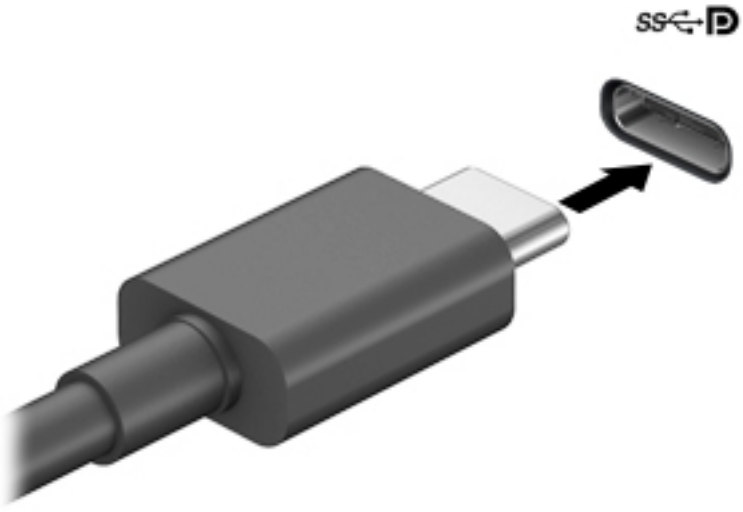
IMPORTANT: Be sure that the external device is connected to the correct port on the computer, using the correct cable. Follow the device manufacturer's instructions.

For information on using your USB Type-C features, refer to HP Support Assistant.

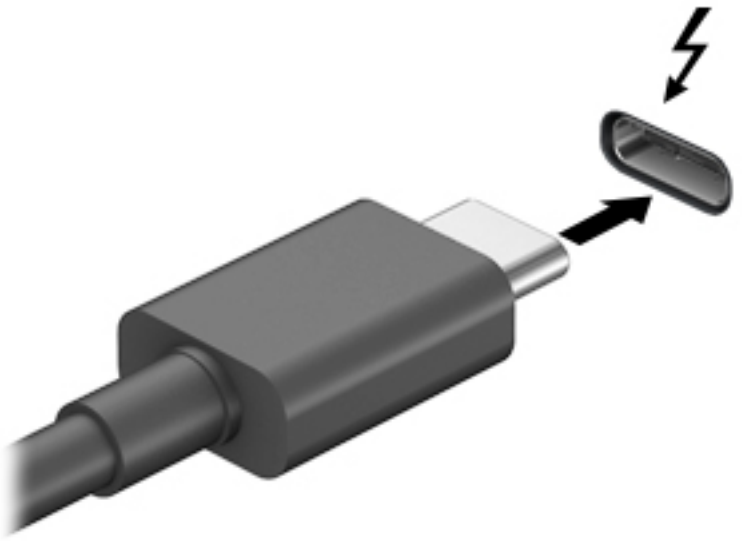
Connecting devices to a USB Type-C port (select products only)

NOTE: To connect a USB Type-C device to your computer, you need a USB Type-C cable, purchased separately.

1. Connect one end of the USB Type-C cable to the USB Type-C port on the computer.



– or –



2. Connect the other end of the cable to the external device.

6 Managing power

Your computer can operate on either battery power or external power. When the computer is running on battery power and an external power source is not available to charge the battery, it is important to monitor and conserve the battery charge.

Some power management features described in this chapter may not be available on your computer.

Using Sleep and Hibernation

⚠ **CAUTION:** Several well-known vulnerabilities exist when a computer is in the Sleep state. To prevent an unauthorized user from accessing data on your computer, even encrypted data, HP recommends that you always initiate Hibernation instead of Sleep anytime the computer will be out of your physical possession. This practice is particularly important when you travel with your computer.

CAUTION: To reduce the risk of possible audio and video degradation, loss of audio or video playback functionality, or loss of information, do not initiate Sleep while reading from or writing to a disc or an external media card.

Windows has two power-saving states, Sleep and Hibernation.

- Sleep—The Sleep state is automatically initiated after a period of inactivity. Your work is saved to memory, allowing you to resume your work very quickly. You can also initiate Sleep manually. For more information, see Initiating and exiting Sleep on page 44.
- Hibernation—The Hibernation state is automatically initiated if the battery reaches a critical level. In the Hibernation state, your work is saved to a hibernation file and the computer powers down. You can also initiate Hibernation manually. For more information, see Initiating and exiting Hibernation (select products only) on page 45.

Initiating and exiting Sleep

You can initiate Sleep in any of the following ways:

- Close the display (select products only).
- Select the **Start** button, select the **Power** icon, and then select **Sleep**.
- Press the Sleep hot key; for example, fn+f3 (select products only).

You can exit Sleep in any of the following ways:

- Briefly press the power button.
- If the computer is closed, raise the display (select products only).
- Press a key on the keyboard (select products only).
- Tap the TouchPad (select products only).

When the computer exits Sleep, your work returns to the screen.

NOTE: If you have set a password to be required on exiting Sleep, you must enter your Windows password before your work returns to the screen.

Initiating and exiting Hibernation (select products only)

You can enable user-initiated Hibernation and change other power settings and timeouts using Power Options.

1. Right-click the **Power** icon  , and then select **Power Options**.
2. In the left pane, select **Choose what the power buttons do** (wording may vary by product).
3. Depending on your product, you can enable Hibernation for battery power or external power in any of the following ways:
   - **Power button**—Under **Power and sleep buttons and lid settings** (wording may vary by product), select **When I press the power button**, and then select **Hibernate**.
   - **Sleep button** (select products only)—Under **Power and sleep buttons and lid settings** (wording may vary by product), select **When I press the sleep button**, and then select **Hibernate**.
   - **Lid** (select products only)—Under **Power and sleep buttons and lid settings** (wording may vary by product), select **When I close the lid**, and then select **Hibernate**.
   - **Power menu**—Select **Change Settings that are currently unavailable**, and then, under **Shutdown settings**, select the **Hibernate** check box.

     The Power menu can be accessed by selecting the **Start** button.
4. Select **Save changes**.

▲ To initiate Hibernation, use the method that you enabled in step 3.

▲ To exit Hibernation, briefly press the power button.

NOTE: If you have set a password to be required on exiting Hibernation, you must enter your Windows password before your work returns to the screen.

Shutting down (turning off) the computer

CAUTION: Unsaved information is lost when the computer shuts down. Be sure to save your work before shutting down the computer.

The Shut down command closes all open programs, including the operating system, and then turns off the display and the computer.

Shut down the computer when it will be unused and disconnected from external power for an extended period.

The recommended procedure is to use the Windows Shut down command.

NOTE: If the computer is in the Sleep state or in Hibernation, first exit Sleep or Hibernation by briefly pressing the power button.

1. Save your work and close all open programs.
2. Select the **Start** button, select the **Power** icon, and then select **Shut down**.

If the computer is unresponsive and you are unable to use the preceding shutdown procedures, try the following emergency procedures in the sequence provided:

- Press ctrl+alt+delete, select the **Power** icon, and then select **Shut down**.
- Press and hold the power button for at least 10 seconds.
- If your computer has a user-replaceable battery (select products only), disconnect the computer from external power, and then remove the battery.

Using the Power icon and Power Options

The Power icon  is located on the Windows taskbar. The Power icon allows you to quickly access power settings and view the remaining battery charge.

- To view the percentage of remaining battery charge and the current power plan, place the mouse pointer over the **Power** icon  .
- To use Power Options, right–click the **Power** icon  , and then select **Power Options**.

Different Power icons indicate whether the computer is running on battery or external power. Placing the mouse pointer over the icon reveals a message if the battery has reached a low or critical battery level.

Running on battery power

WARNING! To reduce potential safety issues, use only the battery provided with the computer, a replacement battery provided by HP, or a compatible battery purchased from HP.

When a charged battery is in the computer and the computer is not plugged into external power, the computer runs on battery power. When the computer is off and unplugged from external power, the battery in the computer slowly discharges. The computer displays a message when the battery reaches a low or critical battery level.

Computer battery life varies, depending on power management settings, programs running on the computer, screen brightness, external devices connected to the computer, and other factors.

NOTE: When you disconnect external power, the display brightness is automatically decreased to conserve battery charge. Select computer products can switch between graphic modes to conserve battery charge.

Using HP Fast Charge (select products only)

The HP Fast Charge feature allows you to quickly charge your computer battery. Charging time may vary by +/- 10%. Depending on your computer model and the HP AC adapter provided with your computer, HP Fast Charge operates in one of the following ways:

- When the remaining battery charge is between zero and 50%, the battery will charge to 50% of full capacity in no more than 30 minutes.
- When the remaining battery charge is between zero and 90%, the battery will charge to 90% of full capacity in no more than 90 minutes.

To use HP Fast Charge, shut down your computer, and then connect the AC adapter to your computer and to external power.

Displaying battery charge

To view the percentage of remaining battery charge and the current power plan, place the mouse pointer over the **Power** icon  .

Finding battery information in HP Support Assistant (select products only)

To access battery information:

1. Type `support` in the taskbar search box, and then select the **HP Support Assistant** app.

   – or –

   Select the question mark icon in the taskbar.

2. Select **My PC**, select the **Diagnostics and tools** tab, and then select **HP Battery Check**. If HP Battery Check indicates that your battery should be replaced, contact support.

HP Support Assistant provides the following tools and information about the battery:

- HP Battery Check
- Information about battery types, specifications, life cycles, and capacity

Conserving battery power

To conserve battery power and maximize battery life:

- Lower the brightness of the display.
- Select the **Power saver** setting in Power Options.
- Turn off wireless devices when you are not using them.
- Disconnect unused external devices that are not plugged into an external power source, such as an external hard drive connected to a USB port.
- Stop, disable, or remove any external media cards that you are not using.
- Before you leave your work, initiate Sleep or shut down the computer.

Identifying low battery levels

When a battery that is the sole power source for the computer reaches a low or critical battery level, the following behavior occurs:

- The battery light (select products only) indicates a low or critical battery level.

– or –

- The Power icon  shows a low or critical battery notification.

NOTE: For additional information about the Power icon, see Using the Power icon and Power Options on page 46.

The computer takes the following actions for a critical battery level:

- If Hibernation is disabled and the computer is on or in the Sleep state, the computer remains briefly in the Sleep state and then shuts down and loses any unsaved information.
- If Hibernation is enabled and the computer is on or in the Sleep state, the computer initiates Hibernation.

Resolving a low battery level

Resolving a low battery level when external power is available

Connect one of the following to the computer and to external power:

- AC adapter
- Optional docking device or expansion product
- Optional power adapter purchased as an accessory from HP

Resolving a low battery level when no power source is available

Save your work and shut down the computer.

Resolving a low battery level when the computer cannot exit Hibernation

1. Connect the AC adapter to the computer and to external power.
2. Exit Hibernation by pressing the power button.

Factory-sealed battery

To monitor the status of the battery, or if the battery is no longer holding a charge, run HP Battery Check in the HP Support Assistant app (select products only).

1. Type `support` in the taskbar search box, and then select the **HP Support Assistant** app.

   – or –

   Select the question mark icon in the taskbar.

2. Select **My PC**, select the **Diagnostics and tools** tab, and then select **HP Battery Check**. If HP Battery Check indicates that your battery should be replaced, contact support.

The battery[ies] in this product cannot be easily replaced by users themselves. Removing or replacing the battery could affect your warranty coverage. If a battery is no longer holding a charge, contact support.

When a battery has reached the end of its useful life, do not dispose of the battery in general household waste. Follow the local laws and regulations in your area for battery disposal.

Running on external power

For information about connecting to external power, refer to the *Setup Instructions* poster provided in the computer box.

The computer does not use battery power when the computer is connected to external power with an approved AC adapter or an optional docking device or expansion product.

⚠ **WARNING!** To reduce potential safety issues, use only the AC adapter provided with the computer, a replacement AC adapter provided by HP, or a compatible AC adapter purchased from HP.

⚠ **WARNING!** Do not charge the computer battery while you are aboard aircraft.

Connect the computer to external power under any of the following conditions:

- When charging or calibrating a battery
- When installing or updating system software
- When updating the system BIOS
- When writing information to a disc (select products only)
- When running Disk Defragmenter on computers with internal hard drives
- When performing a backup or recovery

When you connect the computer to external power:

- The battery begins to charge.
- The screen brightness increases.
- The Power icon  changes appearance.

When you disconnect external power:

- The computer switches to battery power.
- The screen brightness automatically decreases to conserve battery charge.
- The Power icon  changes appearance.

7 Security

Protecting the computer

Standard security features provided by the Windows operating system and the Windows Computer Setup utility (BIOS, which runs under any operating system) can protect your personal settings and data from a variety of risks.

NOTE: Security solutions are designed to act as deterrents. These deterrents may not prevent a product from being mishandled or stolen.

NOTE: Before you send your computer for service, back up and delete confidential files, and remove all password settings.

NOTE: Some features listed in this chapter may not be available on your computer.

NOTE: Your computer supports Computrace, which is an online security-based tracking and recovery service available in select regions. If the computer is stolen, Computrace can track the computer if the unauthorized user accesses the Internet. You must purchase the software and subscribe to the service in order to use Computrace. For information about ordering the Computrace software, go to http://www.hp.com.

Computer risk	Security feature
Unauthorized use of the computer	• HP Client Security software, in combination with a password, smart card, contactless card, registered fingerprints, or other authentication credential • BIOS power-on password
Unauthorized access to Computer Setup (BIOS)	BIOS administrator password in Computer Setup*
Unauthorized access to the contents of a hard drive	DriveLock password (select products only) in Computer Setup*
Unauthorized startup from an optional external optical drive (select products only), optional external hard drive (select products only), or internal network adapter	Boot options feature in Computer Setup*
Unauthorized access to a Windows user account	Windows user password
Unauthorized access to data	Windows BitLocker
Unauthorized removal of the computer	Security cable slot (used with an optional security cable on select products only)

*Computer Setup is an embedded, ROM-based utility that can be used even when the operating system is not working or will not load. You can use a pointing device (TouchPad, pointing stick, or USB mouse) or the keyboard to navigate and make selections in Computer Setup.

NOTE: On tablets without keyboards, you can use the touch screen.

Using passwords

A password is a group of characters that you choose to secure your computer information. Several types of passwords can be set, depending on how you want to control access to your information. Passwords can be set in Windows or in Computer Setup, which is preinstalled on the computer.

- BIOS administrator, power-on, and DriveLock passwords are set in Computer Setup and are managed by the system BIOS.
- Windows passwords are set only in the Windows operating system.
- If you forget both the DriveLock user password and the DriveLock master password set in Computer Setup, the hard drive that is protected by the passwords is permanently locked and can no longer be used.

You can use the same password for a Computer Setup feature and for a Windows security feature.

Use the following tips for creating and saving passwords:

- When creating passwords, follow requirements set by the program.
- Do not use the same password for multiple applications or websites, and do not reuse your Windows password for any other application or website.
- Use the Password Manager feature of HP Client Security to store your user names and passwords for your websites and applications. You can securely read them in the future if they cannot be remembered.
- Do not store passwords in a file on the computer.

The following tables list commonly used Windows and BIOS administrator passwords and describe their functions.

Setting passwords in Windows

Password	Function
Administrator password*	Protects access to a Windows administrator-level account. **NOTE:** Setting the Windows administrator password does not set the BIOS administrator password.
User password*	Protects access to a Windows user account.
*For information about setting a Windows administrator password or a Windows user password, type `support` in the taskbar search box, and then select the **HP Support Assistant** app.	

Setting passwords in Computer Setup

Password	Function
BIOS administrator password*	Protects access to Computer Setup. **NOTE:** If features have been enabled to prevent removing the BIOS administrator password, you may not be able to remove it until those features have been disabled.
Power-on password	• Must be entered each time you turn on or restart the computer. • If you forget your power-on password, you cannot turn on or restart the computer.
DriveLock master password*	Protects access to the internal hard drive that is protected by DriveLock, and is set under DriveLock Passwords during the enable process. This password is also used to remove DriveLock protection.
DriveLock user password*	Protects access to the internal hard drive that is protected by DriveLock, and is set under DriveLock Passwords during the enable process.
*For details about each of these passwords, see the following topics.	

Managing a BIOS administrator password

To set, change, or delete this password, follow these steps:

Setting a new BIOS administrator password

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     - ▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     - ▲ Turn off the tablet. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. Select **Security**, select **Create BIOS administrator password** or **Set Up BIOS administrator Password** (select products only), and then press enter.
3. When prompted, type a password.
4. When prompted, type the new password again to confirm.
5. To save your changes and exit Computer Setup, select the **Save** icon and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Changing a BIOS administrator password

1. Start Computer Setup.

- Computers or tablets with keyboards:
  - ▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
- Tablets without keyboards:
  - ▲ Turn off the tablet. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.

2. Enter your current BIOS administrator password.
3. Select **Security**, select **Change BIOS administrator Password** or **Change Password** (select products only), and then press enter.
4. When prompted, type your current password.
5. When prompted, type your new password.
6. When prompted, type your new password again to confirm.
7. To save your changes and exit Computer Setup, select the **Save** icon, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Deleting a BIOS administrator password

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     - ▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     - ▲ Turn off the tablet. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. Enter your current BIOS administrator password.
3. Select **Security**, select **Change BIOS administrator Password** or **Change Password** (select products only), and then press enter.
4. When prompted, type your current password.
5. When prompted for the new password, leave the field empty, and then press enter.
6. When prompted to type your new password again, leave the field empty, and then press enter.
7. To save your changes and exit Computer Setup, select the **Save** icon, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Entering a BIOS administrator password

At the **BIOS administrator password** prompt, type your password (using the same kind of keys you used to set the password), and then press enter. After two unsuccessful attempts to enter the BIOS administrator password, you must restart the computer and try again.

Using DriveLock Security Options

DriveLock protection prevents unauthorized access to the contents of a hard drive. DriveLock can be applied only to the internal hard drive(s) of the computer. After DriveLock protection is applied to a drive, the appropriate password must be entered to access the drive. The drive must be inserted into the computer or an advanced port replicator in order for it to be unlocked.

DriveLock Security Options offers the following features:

- **Automatic DriveLock**—See Selecting Automatic DriveLock (select products only) on page 54.
- **Set DriveLock Master Password**—See Selecting manual DriveLock on page 55.
- **Enable DriveLock**—See Enabling DriveLock and setting a DriveLock user password on page 56.

Selecting Automatic DriveLock (select products only)

A BIOS administrator password must be set before you can enable Automatic DriveLock. When Automatic DriveLock is enabled, a random DriveLock user password and a DriveLock master password derived from the BIOS administrator password are created. When the computer is turned on, the random user password automatically unlocks the drive. If the drive is moved to another computer, you must enter the BIOS administrator password for the original computer at the DriveLock password prompt to unlock the drive.

Enabling Automatic DriveLock

To enable Automatic DriveLock, follow these steps:

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     1. Turn off the computer.
     2. Press the power button, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     1. Turn off the tablet.
     2. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. At the BIOS administrator password prompt, enter the BIOS administrator password, and then press enter.
3. Select **Security**, select **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
4. Use the enter key, left mouse click, or touch screen to select the **Automatic DriveLock** check box.
5. To save your changes and exit Computer Setup, select the **Save** icon and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Disabling Automatic DriveLock

To disable Automatic DriveLock, follow these steps:

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     1. Turn off the computer.
     2. Press the power button, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     1. Turn off the tablet.
     2. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. At the BIOS administrator password prompt, enter the BIOS administrator password, and then press enter.
3. Select **Security**, select **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
4. Select an internal hard drive, and then press enter.
5. Use the enter key, left mouse click, or touch screen to clear the **Automatic DriveLock** check box.
6. To save your changes and exit Computer Setup, select the **Save** icon, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Entering an Automatic DriveLock password

While Automatic DriveLock is enabled and the drive remains attached to the original computer, you will not be prompted to enter a DriveLock password to unlock the drive. However, if the drive is moved to another computer, or the system board is replaced on the original computer, you will be prompted to provide the DriveLock password.

If this happens, at the **DriveLock Password** prompt, type the BIOS administrator password for the original computer (using the same kind of keys you used to set the password), and then press enter to unlock the drive.

After three incorrect attempts to enter the password, you must shut down the computer and try again.

Selecting manual DriveLock

⚠ **CAUTION:** To prevent a DriveLock-protected hard drive from becoming permanently unusable, record the DriveLock user password and the DriveLock master password in a safe place away from your computer. If you forget both DriveLock passwords, the hard drive will be permanently locked and can no longer be used.

To manually apply DriveLock protection to an internal hard drive, a master password must be set, and DriveLock must be enabled in Computer Setup. Note the following considerations about using DriveLock protection:

- After DriveLock protection is applied to a hard drive, the hard drive can be accessed only by entering either the DriveLock user password or the master password.
- The owner of the DriveLock user password should be the day-to-day user of the protected hard drive. The owner of the DriveLock master password may be either a system administrator or the day-to-day user.
- The DriveLock user password and the DriveLock master password can be identical.

Setting a DriveLock master password

To set a DriveLock master password, follow these steps:

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     1. Turn off the computer.
     2. Press the power button, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     1. Turn off the tablet.
     2. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. Select **Security**, make the selection for **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
3. Select the hard drive you want to protect, and then press enter.
4. Select **Set DriveLock Master Password**, and then press enter.
5. Carefully read the warning.
6. Follow the on-screen instructions to set a DriveLock master password.

NOTE: You can enable DriveLock and set a DriveLock user password before exiting from Computer Setup. For more information, see Enabling DriveLock and setting a DriveLock user password on page 56.

7. To exit Computer Setup, select **Main**, select **Save Changes and Exit**, and then select **Yes**.

Enabling DriveLock and setting a DriveLock user password

To enable DriveLock, and set a DriveLock user password, follow these steps:

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     1. Turn off the computer.
     2. Press the power button, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:

1. Turn off the tablet.
2. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.

2. Select **Security**, select **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
3. Select the hard drive you want to protect, and then press enter.
4. Select **Enable DriveLock** and then press enter.
5. Carefully read the warning.
6. Follow the on-screen instructions to set a DriveLock user password and enable DriveLock.
7. To exit Computer Setup, select **Main**, select **Save Changes and Exit**, and then select **Yes**.

Disabling DriveLock

1. Start Computer Setup.
   - Computers or tablets with keyboards:
     1. Turn off the computer.
     2. Press the power button, and when the HP logo appears, press f10 to enter Computer Setup.
   - Tablets without keyboards:
     1. Turn off the tablet.
     2. Press the power button in combination with the volume down button until the Startup menu is displayed, and then tap **f10** to enter Computer Setup.
2. Select **Security**, select **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
3. Select the hard drive you want to manage, and then press enter.
4. Select **Disable DriveLock**, and then press enter.
5. Follow the on-screen instructions to disable DriveLock.
6. To exit Computer Setup, select **Main**, select **Save Changes and Exit**, and then select **Yes**.

Entering a DriveLock password

Be sure that the hard drive is inserted into the computer (not into an optional docking device or external MultiBay).

At the **DriveLock Password** prompt, type your DriveLock user or master password (using the same kind of keys you used to set the password), and then press enter.

After three incorrect attempts to enter the password, you must shut down the computer and try again.

Changing a DriveLock password

To change a DriveLock password in Computer Setup, follow these steps:

1. Turn off the computer.
2. Press the power button.

3. At the **DriveLock Password** prompt, type the current DriveLock user password or master password that you are changing, press enter, and then press or tap f10 to enter Computer Setup.
4. Select **Security**, select **Hard Drive Utilities**, select **DriveLock/Automatic DriveLock**, and then press enter.
5. Select the hard drive you want to manage, and then press enter.
6. Make the selection for the DriveLock password that you want to change, and then follow the on-screen instructions to enter passwords.

> **NOTE:** The **Change DriveLock Master Password** option is visible only if the DriveLock master password was provided at the DriveLock Password prompt in step 3.

7. To exit Computer Setup, select **Main**, select **Save Changes and Exit**, and then follow the on-screen instructions.

Using Windows Hello (select products only)

On products equipped with a fingerprint reader or an infrared camera, you can use Windows Hello to sign in by swiping your finger or looking at the camera.

To set up Windows Hello, follow these steps:

1. Select the **Start** button, select **Settings**, select **Accounts**, and then select **Sign-in options**.
2. Under **Windows Hello**, follow the on-screen instructions to add both a password and a numeric PIN, and then enroll your fingerprint or facial ID.

> **NOTE:** The PIN is not limited in length, but it must consist of numbers only. No alphabetic or special characters are allowed.

Using antivirus software

When you use the computer to access e-mail, a network, or the Internet, you potentially expose it to computer viruses. Computer viruses can disable the operating system, programs, or utilities, or cause them to function abnormally.

Antivirus software can detect most viruses, destroy them, and, in most cases, repair any damage they have caused. To provide ongoing protection against newly discovered viruses, antivirus software must be kept up to date.

Windows Defender is preinstalled on your computer. It is strongly recommended that you continue to use an antivirus program in order to fully protect your computer.

For more information about computer viruses, access the HP Support Assistant.

Using firewall software

Firewalls are designed to prevent unauthorized access to a system or network. A firewall can be a software program you install on your computer and/or network, or it can be a solution made up of both hardware and software.

There are two types of firewalls to consider:

- Host-based firewalls—Software that protects only the computer it is installed on.
- Network-based firewalls—Installed between your DSL or cable modem and your home network to protect all the computers on the network.

When a firewall is installed on a system, all data sent to and from the system is monitored and compared with a set of user-defined security criteria. Any data that does not meet those criteria is blocked.

Your computer or networking equipment may already have a firewall installed. If not, firewall software solutions are available.

NOTE: Under some circumstances a firewall can block access to Internet games, interfere with printer or file sharing on a network, or block authorized e-mail attachments. To temporarily resolve the problem, disable the firewall, perform the task that you want to perform, and then reenable the firewall. To permanently resolve the problem, reconfigure the firewall.

Installing software updates

HP, Windows, and third-party software installed on your computer should be regularly updated to correct security problems and improve software performance.

IMPORTANT: Microsoft sends out alerts regarding Windows updates, which may include security updates. To protect the computer from security breaches and computer viruses, install all updates from Microsoft as soon as you receive an alert.

You can install these updates automatically.

To view or change the settings:

1. Select the **Start** button, select **Settings**, and then select **Update & Security**.
2. Select **Windows Update**, and then follow the on-screen instructions.
3. To schedule a time for installing updates, select **Advanced Options**, and then follow the on-screen instructions.

Using HP Client Security (select products only)

HP Client Security software is preinstalled on your computer. This software can be accessed through the HP Client Security icon at the far right of the taskbar or Windows Control Panel. It provides security features that help protect against unauthorized access to the computer, networks, and critical data. For more information, see the HP Client Security software Help.

Using HP Managed Services (select products only)

HP Managed Services is a cloud-based IT solution that enables businesses to effectively manage and secure their company assets. HP Managed Services helps protect devices against malware and other attacks, monitors device health, and helps reduce time spent solving device and security issues. You can quickly download and install the software, which is highly cost effective relative to traditional in-house solutions. For more information, go to https://www.hptouchpointmanager.com/.

Using an optional security cable (select products only)

A security cable (purchased separately) is designed to act as a deterrent, but it may not prevent the computer from being mishandled or stolen. To connect a security cable to your computer, follow the device manufacturer's instructions.

Using a fingerprint reader (select products only)

Integrated fingerprint readers are available on select products. In order to use the fingerprint reader, you must enroll your fingerprints in HP Client Security's Credential Manager. Refer to the HP Client Security software Help.

After you enroll your fingerprints in Credential Manager, you can use HP Client Security's Password Manager to store and fill in your user names and passwords in supported websites and applications.

Locating the fingerprint reader

The fingerprint reader is a small metallic sensor that is located in one of the following areas of your computer:

- Near the bottom of the TouchPad
- On the right side of the keyboard
- On the upper-right side of the display
- On the left side of the display
- On the back of the display

Depending on your product, the reader may be oriented horizontally or vertically.

8 Maintenance

It is important to perform regular maintenance to keep your computer in optimal condition. This chapter explains how to use tools like Disk Defragmenter and Disk Cleanup. It also provides instructions for updating programs and drivers, steps to clean the computer, and tips for traveling with (or shipping) the computer.

Improving performance

You can improve the performance of your computer by performing regular maintenance tasks with tools such as Disk Defragmenter and Disk Cleanup.

Using Disk Defragmenter

HP recommends using Disk Defragmenter to defragment your hard drive at least once a month.

NOTE: It is not necessary to run Disk Defragmenter on solid-state drives.

To run Disk Defragmenter:

1. Connect the computer to AC power.
2. Type `defragment` in the taskbar search box, and then select **Defragment and optimize your drives**.
3. Follow the on-screen instructions.

For additional information, access the Disk Defragmenter software Help.

Using Disk Cleanup

Use Disk Cleanup to search the hard drive for unnecessary files that you can safely delete to free up disk space and help the computer run more efficiently.

To run Disk Cleanup:

1. Type `disk` in the taskbar search box, and then select **Disk Cleanup**.
2. Follow the on-screen instructions.

Using HP 3D DriveGuard (select products only)

HP 3D DriveGuard protects a hard drive by parking the drive and halting data requests under either of the following conditions:

- You drop the computer.
- You move the computer with the display closed while the computer is running on battery power.

A short time after the end of one of these events, HP 3D DriveGuard returns the hard drive to normal operation.

NOTE: Only internal hard drives are protected by HP 3D DriveGuard. A hard drive installed in an optional docking device or connected to a USB port is not protected by HP 3D DriveGuard.

NOTE: Because solid-state drives (SSDs) lack moving parts, HP 3D DriveGuard is unnecessary for these drives.

For more information, see the HP 3D DriveGuard software Help.

Identifying HP 3D DriveGuard status

The hard drive light on the computer changes color to show that the drive in a primary hard drive bay and/or the drive in a secondary hard drive bay (select products only) is parked. To determine whether a drive is currently protected or whether it is parked, view the icon on the Windows desktop in the notification area, at the far right of the taskbar.

Updating programs and drivers

HP recommends that you update your programs and drivers on a regular basis. Updates can resolve issues and bring new features and options to your computer. For example, older graphics components might not work well with the most recent gaming software. Without the latest driver, you would not be getting the most out of your equipment.

Go to http://www.hp.com/support to download the latest versions of HP programs and drivers. In addition, register to receive automatic notifications when updates become available.

If you would like to update your programs and drivers, follow these instructions:

1. Type `support` in the taskbar search box, and then select the **HP Support Assistant** app.

   – or –

   Click the question mark icon in the taskbar.
2. Select **My PC**, select the **Updates** tab, and then select **Check for updates and messages**.
3. Follow the on-screen instructions.

Cleaning your computer

Use the following products to safely clean your computer:

- Dimethyl benzyl ammonium chloride 0.3 percent maximum concentration (for example, disposable wipes, which come in a variety of brands)
- Alcohol-free glass-cleaning fluid
- Solution of water and mild soap
- Dry microfiber cleaning cloth or a chamois (static-free cloth without oil)
- Static-free cloth wipes

⚠ **CAUTION:** Avoid strong cleaning solvents that can permanently damage your computer. If you are not sure that a cleaning product is safe for your computer, check the product contents to make sure that ingredients such as alcohol, acetone, ammonium chloride, methylene chloride, and hydrocarbons are not included in the product.

Fibrous materials, such as paper towels, can scratch the computer. Over time, dirt particles and cleaning agents can get trapped in the scratches.

Cleaning procedures

Follow the procedures in this section to safely clean your computer.

WARNING! To prevent electric shock or damage to components, do not attempt to clean your computer while it is on.

1. Turn off the computer.
2. Disconnect AC power.
3. Disconnect all powered external devices.

CAUTION: To prevent damage to internal components, do not spray cleaning agents or liquids directly on any computer surface. Liquids dripped on the surface can permanently damage internal components.

Cleaning the display

Gently wipe the display using a soft, lint-free cloth moistened with an alcohol-free glass cleaner. Be sure that a display is dry before you close the computer.

Cleaning the sides or cover

To clean the sides or cover, use a soft microfiber cloth or chamois moistened with one of the cleaning solutions listed previously, or use an acceptable disposable wipe.

NOTE: When cleaning the cover of the computer, use a circular motion to aid in removing dirt and debris.

Cleaning the TouchPad, keyboard, or mouse (select products only)

WARNING! To reduce the risk of electric shock or damage to internal components, do not use a vacuum cleaner attachment to clean the keyboard. A vacuum cleaner can deposit household debris on the keyboard surface.

CAUTION: To prevent damage to internal components, do not allow liquids to drip between the keys.

- To clean the TouchPad, keyboard, or mouse, use a soft microfiber cloth or a chamois moistened with one of the cleaning solutions listed previously or use an acceptable disposable wipe.
- To prevent keys from sticking and to remove dust, lint, and particles from the keyboard, use a can of compressed air with a straw extension.

Traveling with or shipping your computer

If you have to travel with or ship your computer, follow these tips to keep your equipment safe.

- Prepare the computer for traveling or shipping:
  - Back up your information to an external drive.
  - Remove all discs and all external media cards, such as memory cards.
  - Turn off and then disconnect all external devices.
  - Shut down the computer.
- Take along a backup of your information. Keep the backup separate from the computer.
- When traveling by air, carry the computer as hand luggage; do not check it in with the rest of your luggage.

CAUTION: Avoid exposing a drive to magnetic fields. Security devices with magnetic fields include airport walk-through devices and security wands. Airport conveyer belts and similar security devices that check carry-on baggage use X-rays instead of magnetism and do not damage drives.

- If you plan to use the computer during a flight, listen for the in-flight announcement that tells you when you are allowed to use your computer. In-flight computer use is at the discretion of the airline.
- If you are shipping the computer or a drive, use suitable protective packaging and label the package “FRAGILE.”
- The use of wireless devices may be restricted in some environments. Such restrictions may apply aboard aircraft, in hospitals, near explosives, and in hazardous locations. If you are uncertain of the policy that applies to the use of a wireless device in your computer, ask for authorization to use your computer before you turn it on.
- If you are traveling internationally, follow these suggestions:
  - Check the computer-related customs regulations for each country or region on your itinerary.
  - Check the power cord and adapter requirements for each location in which you plan to use the computer. Voltage, frequency, and plug configurations vary.

    ⚠ **WARNING!** To reduce the risk of electric shock, fire, or damage to the equipment, do not attempt to power the computer with a voltage converter kit sold for appliances.

9 Backing up, restoring, and recovering

This chapter provides information about the following processes. The information in the chapter is standard procedure for most products.

- Creating recovery media and backups
- Restoring and recovering your system

For additional information, refer to the HP Support Assistant app.

▲ Type `support` in the taskbar search box, and then select the **HP Support Assistant** app.

– or –

Select the question mark icon in the taskbar.

IMPORTANT: If you will be performing recovery procedures on a tablet, the tablet battery must be at least 70% charged before you start the recovery process.

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning any recovery process.

Creating recovery media and backups

The following methods of creating recovery media and backups are available on select products only. Choose the available method according to your computer model.

- Use HP Recovery Manager to create HP Recovery media after you successfully set up the computer. This step creates a backup of the HP Recovery partition on the computer. The backup can be used to reinstall the original operating system in cases where the hard drive is corrupted or has been replaced. For information on creating recovery media, see Using HP Recovery media (select products only) on page 65. For information on the recovery options that are available using the recovery media, see Using Windows tools on page 66.
- Use Windows tools to create system restore points and create backups of personal information. See Using Windows tools on page 66.

NOTE: If storage is 32 GB or less, Microsoft System Restore is disabled by default.

- On select products, use the HP Cloud Recovery Download Tool to create a bootable USB flash drive for your HP recovery media. For more information, see Using the HP Cloud Recovery Download Tool (select products only) on page 67.

Using HP Recovery media (select products only)

If possible, check for the presence of the Recovery partition and the Windows partition. Right-click the **Start** button, select **File Explorer**, and then select **This PC**.

- If your computer does not list the Windows partition and the Recovery partition, you can obtain recovery media for your system from support. You can find contact information on the HP website. Go to http://www.hp.com/support, select your country or region, and follow the on-screen instructions.
- If your computer does list the Recovery partition and the Windows partition, you can use HP Recovery Manager to create recovery media after you successfully set up the computer. HP Recovery media can be

used to perform system recovery if the hard drive becomes corrupted. System recovery reinstalls the original operating system and software programs that were installed at the factory and then configures the settings for the programs. HP Recovery media can also be used to customize the system or restore the factory image if you replace the hard drive.

- Only one set of recovery media can be created. Handle these recovery tools carefully, and keep them in a safe place.
- HP Recovery Manager examines the computer and determines the required storage capacity for the media that will be required.
- To create recovery discs, your computer must have an optical drive with DVD writer capability, and you must use only high-quality blank DVD-R, DVD+R, DVD-R DL, or DVD+R DL discs. Do not use rewritable discs such as CD±RW, DVD±RW, double-layer DVD±RW, or BD-RE (rewritable Blu-ray) discs; they are not compatible with HP Recovery Manager software. Or, instead, you can use a high-quality blank USB flash drive.
- If your computer does not include an integrated optical drive with DVD writer capability, but you would like to create DVD recovery media, you can use an external optical drive (purchased separately) to create recovery discs. If you use an external optical drive, it must be connected directly to a USB port on the computer; the drive cannot be connected to a USB port on an external device, such as a USB hub. If you cannot create DVD media yourself, you can obtain recovery discs for your computer from HP. You can find contact information on the HP website. Go to http://www.hp.com/support, select your country or region, and follow the on-screen instructions.
- Be sure that the computer is connected to AC power before you begin creating the recovery media.
- The creation process can take an hour or more. Do not interrupt the creation process.
- If necessary, you can exit the program before you have finished creating all of the recovery DVDs. HP Recovery Manager will finish burning the current DVD. The next time you start HP Recovery Manager, you will be prompted to continue.

To create HP Recovery media using HP recovery manager:

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning these steps.

1. Type `recovery` in the taskbar search box, and then select **HP Recovery Manager**.
2. Select **Create recovery media**, and then follow the on-screen instructions.

If you ever need to recover the system, see Recovering using HP Recovery Manager on page 67.

Using Windows tools

You can create recovery media, system restore points, and backups of personal information using Windows tools.

NOTE: If storage is 32 GB or less, Microsoft System Restore is disabled by default.

For more information and steps, see the Get Help app.

▲ Select the **Start** button, and then select the **Get Help** app.

NOTE: You must be connected to the Internet to access the Get Help app.

Using the HP Cloud Recovery Download Tool (select products only)

To create HP Recovery media using the HP Cloud Recovery Download Tool:

1. Go to http://www.hp.com/support.
2. Select **Software and Drivers**, and then follow the on-screen instructions.

Restore and recovery

There are several options for recovering your system. Choose the method that best matches your situation and level of expertise:

IMPORTANT: Not all methods are available on all products.

- Windows offers several options for restoring from backup, refreshing the computer, and resetting the computer to its original state. For more information see the Get Help app.

  ▲ Select the **Start** button, and then select the **Get Help** app.

  NOTE: You must be connected to the Internet to access the Get Help app.

- If you need to correct a problem with a preinstalled application or driver, use the Reinstall drivers and/or applications option (select products only) of HP Recovery Manager to reinstall the individual application or driver.

  ▲ Type `recovery` in the taskbar search box, select **HP Recovery Manager**, select **Reinstall drivers and/or applications**, and then follow the on-screen instructions.

- If you want to recover the Windows partition to original factory content, you can choose the System Recovery option from the HP Recovery partition (select products only) or use the HP Recovery media. For more information, see Recovering using HP Recovery Manager on page 67. If you have not already created recovery media, see Using HP Recovery media (select products only) on page 65.
- On select products, if you want to recover the computer's original factory partition and content, or if you have replaced the hard drive, you can use the Factory Reset option of HP Recovery media. For more information, see Recovering using HP Recovery Manager on page 67.
- On select products, if you want to remove the Recovery partition to reclaim hard drive space, HP Recovery Manager offers the Remove Recovery Partition option.

  For more information, see Removing the HP Recovery partition (select products only) on page 69.

Recovering using HP Recovery Manager

HP Recovery Manager software allows you to recover the computer to its original factory state by using the HP Recovery media that you either created or that you obtained from HP, or by using the HP Recovery partition (select products only). If you have not already created recovery media, see Using HP Recovery media (select products only) on page 65.

What you need to know before you get started

- HP Recovery Manager recovers only software that was installed at the factory. For software not provided with this computer, you must either download the software from the manufacturer's website or reinstall the software from the media provided by the manufacturer.

IMPORTANT: Recovery through HP Recovery Manager should be used as a final attempt to correct computer issues.

- HP Recovery media must be used if the computer hard drive fails. If you have not already created recovery media, see Using HP Recovery media (select products only) on page 65.
- To use the Factory Reset option (select products only), you must use HP Recovery media. If you have not already created recovery media, see Using HP Recovery media (select products only) on page 65.
- If your computer does not allow the creation of HP Recovery media or if the HP Recovery media does not work, you can obtain recovery media for your system from support. You can find contact information from the HP website. Go to http://www.hp.com/support, select your country or region, and follow the on-screen instructions.

IMPORTANT: HP Recovery Manager does not automatically provide backups of your personal data. Before beginning recovery, back up any personal data you want to retain.

Using HP Recovery media, you can choose from one of the following recovery options:

NOTE: Only the options available for your computer display when you start the recovery process.

- System Recovery—Reinstalls the original operating system, and then configures the settings for the programs that were installed at the factory.
- Factory Reset—Restores the computer to its original factory state by deleting all information from the hard drive and re-creating the partitions. Then it reinstalls the operating system and the software that was installed at the factory.

The HP Recovery partition (select products only) allows System Recovery only.

Using the HP Recovery partition (select products only)

The HP Recovery partition allows you to perform a system recovery without the need for recovery discs or a recovery USB flash drive. This type of recovery can be used only if the hard drive is still working.

To start HP Recovery Manager from the HP Recovery partition:

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning these steps (select products only).

1. Type `recovery` in the taskbar search box, select **HP Recovery Manager**, and then select **Windows Recovery Environment**.

   – or –

   For computers or tablets with keyboards attached, press f11 while the computer boots, or press and hold f11 as you press the power button.

   For tablets without keyboards:

   - Turn on or restart the tablet, and then quickly hold down the volume up button; then select **f11**.

   – or –

   - Turn on or restart the tablet, and then quickly hold down the volume down button; then select **f11**.
2. Select **Troubleshoot** from the boot options menu.
3. Select **Recovery Manager**, and then follow the on-screen instructions.

Using HP Recovery media to recover

You can use HP Recovery media to recover the original system. This method can be used if your system does not have an HP Recovery partition or if the hard drive is not working properly.

1. If possible, back up all personal files.
2. Insert the HP Recovery media, and then restart the computer.

   NOTE: If the computer does not automatically restart in HP Recovery Manager, change the computer boot order. See Changing the computer boot order on page 69.

3. Follow the on-screen instructions.

Changing the computer boot order

If your computer does not restart in HP Recovery Manager, you can change the computer boot order, which is the order of devices listed in BIOS where the computer looks for startup information. You can change the selection to an optical drive or a USB flash drive.

To change the boot order:

IMPORTANT: For a tablet with a detachable keyboard, connect the tablet to the keyboard base before beginning these steps.

1. Insert the HP Recovery media.
2. Access the system **Startup** menu.

   For computers or tablets with keyboards attached:

   ▲ Turn on or restart the computer or tablet, quickly press esc, and then press f9 for boot options.

   For tablets without keyboards:

   ▲ Turn on or restart the tablet, and then quickly hold down the volume up button; then select **f9**.

   – or –

   Turn on or restart the tablet, and then quickly hold down the volume down button; then select **f9**.
3. Select the optical drive or USB flash drive from which you want to boot.
4. Follow the on-screen instructions.

Removing the HP Recovery partition (select products only)

HP Recovery Manager software allows you to remove the HP Recovery partition to free up hard drive space.

IMPORTANT: After you remove the HP Recovery partition, you will not be able to perform System Recovery or create HP Recovery media from the HP Recovery partition. So before you remove the Recovery partition, create HP Recovery media; see Using HP Recovery media (select products only) on page 65.

NOTE: The Remove Recovery Partition option is only available on products that support this function.

Follow these steps to remove the HP Recovery partition:

1. Type `recovery` in the taskbar search box, and then select **HP Recovery Manager**.
2. Select **Remove Recovery Partition**, and then follow the on-screen instructions.

10 Computer Setup (BIOS), TPM, and HP Sure Start

Using Computer Setup

Computer Setup, or Basic Input/Output System (BIOS), controls communication between all the input and output devices on the system (such as disk drives, display, keyboard, mouse, and printer). Computer Setup includes settings for the types of devices installed, the startup sequence of the computer, and the amount of system and extended memory.

NOTE: Use extreme care when making changes in Computer Setup. Errors can prevent the computer from operating properly.

Starting Computer Setup

▲ Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.

Using a USB keyboard or USB mouse to start Computer Setup (BIOS)

You can start Computer Setup by using a keyboard or mouse connected to a USB port, but you must first disable FastBoot.

1. Turn on or restart the computer, and when the HP logo appears, press f9 to enter the Boot Device Options menu.
2. Clear the check box for **Fast Boot**.
3. To save your changes and exit, select the **Save** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

– or –

Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Navigating and selecting in Computer Setup

- To select a menu or a menu item, use the tab key and the keyboard arrow keys and then press enter, or use a pointing device to select the item.
- To scroll up and down, select the up arrow or the down arrow in the upper-right corner of the screen, or use the up arrow key or the down arrow key on the keyboard.
- To close open dialog boxes and return to the main Computer Setup screen, press esc, and then follow the on-screen instructions.

To exit Computer Setup menus, choose one of the following methods:

- To exit Computer Setup menus without saving your changes:

  Select the **Exit** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

  – or –

  Select **Main**, select **Ignore Changes and Exit**, and then press enter.

- To save your changes and exit Computer Setup menus:

  Select the **Save** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

  – or –

  Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

Restoring factory settings in Computer Setup

NOTE: Restoring defaults will not change the hard drive mode.

To return all settings in Computer Setup to the values that were set at the factory, follow these steps:

1. Start Computer Setup. See Starting Computer Setup on page 70.
2. Select **Main**, and then select **Apply Factory Defaults and Exit**.

   NOTE: On select products, the selections may display **Restore Defaults** instead of **Apply Factory Defaults and Exit**.

3. Follow the on-screen instructions.
4. To save your changes and exit, select the **Save** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Save Changes and Exit**, and then press enter.

Your changes go into effect when the computer restarts.

NOTE: Your password settings and security settings are not changed when you restore the factory settings.

Updating the BIOS

Updated versions of the BIOS may be available on the HP website.

Most BIOS updates on the HP website are packaged in compressed files called *SoftPaqs*.

Some download packages contain a file named Readme.txt, which contains information regarding installing and troubleshooting the file.

Determining the BIOS version

To decide whether you need to update Computer Setup (BIOS), first determine the BIOS version on your computer.

BIOS version information (also known as *ROM date* and *System BIOS*) can be accessed by pressing fn+esc (if you are already in Windows) or by using Computer Setup.

1. Start Computer Setup. See Starting Computer Setup on page 70.
2. Select **Main**, and then select **System Information**.
3. To exit Computer Setup without saving your changes, select the **Exit** icon in the lower-right corner of the screen, and then follow the on-screen instructions.

   – or –

   Select **Main**, select **Ignore Changes and Exit**, and then press enter.

To check for later BIOS versions, see Downloading a BIOS update on page 72.

Downloading a BIOS update

CAUTION: To reduce the risk of damage to the computer or an unsuccessful installation, download and install a BIOS update only when the computer is connected to reliable external power using the AC adapter. Do not download or install a BIOS update while the computer is running on battery power, docked in an optional docking device, or connected to an optional power source. During the download and installation, follow these instructions:

Do not disconnect power on the computer by unplugging the power cord from the AC outlet.

Do not shut down the computer or initiate Sleep.

Do not insert, remove, connect, or disconnect any device, cable, or cord.

1. Type `support` in the taskbar search box, and then select the HP Support Assistant app.

   – or –

   Select the question mark icon in the taskbar.
2. Select **Updates**, and then select **Check for updates and messages**.
3. Follow the on-screen instructions.
4. At the download area, follow these steps:
   a. Identify the most recent BIOS update and compare it to the BIOS version currently installed on your computer. Make a note of the date, name, or other identifier. You may need this information to locate the update later, after it has been downloaded to your hard drive.
   b. Follow the on-screen instructions to download your selection to the hard drive.

      Make a note of the path to the location on your hard drive where the BIOS update is downloaded. You will need to access this path when you are ready to install the update.

NOTE: If you connect your computer to a network, consult the network administrator before installing any software updates, especially system BIOS updates.

BIOS installation procedures vary. Follow any instructions that are displayed on the screen after the download is complete. If no instructions are displayed, follow these steps:

1. Type `file` in the taskbar search box, and then select **File Explorer**.
2. Select your hard drive designation. The hard drive designation is typically Local Disk (C:).
3. Using the hard drive path you recorded earlier, open the folder that contains the update.
4. Double-click the file that has an .exe extension (for example, *filename*.exe).

   The BIOS installation begins.
5. Complete the installation by following the on-screen instructions.

NOTE: After a message on the screen reports a successful installation, you can delete the downloaded file from your hard drive.

Changing the boot order using the f9 prompt

To dynamically choose a boot device for the current startup sequence, follow these steps:

1. Access the Boot Device Options menu:
   - Turn on or restart the computer, and when the HP logo appears, press f9 to enter the Boot Device Options menu.
2. Select a boot device, press enter, and then follow the on-screen instructions.

TPM BIOS settings (select products only)

IMPORTANT: Before enabling Trusted Platform Module (TPM) functionality on this system, you must ensure that your intended use of TPM complies with relevant local laws, regulations and policies, and approvals or licenses must be obtained if applicable. For any compliance issues arising from your operation/usage of TPM which violates the above mentioned requirement, you shall bear all the liabilities wholly and solely. HP will not be responsible for any related liabilities.

TPM provides additional security for your computer. You can modify the TPM settings in Computer Setup (BIOS).

NOTE: If you change the TPM setting to Hidden, TPM is not visible in the operating system.

To access TPM settings in Computer Setup:

1. Start Computer Setup. See Starting Computer Setup on page 70.
2. Select **Security**, select **TPM Embedded Security**, and then follow the on-screen instructions.

Using HP Sure Start (select products only)

Select computer models are configured with HP Sure Start, a technology that monitors the computer's BIOS for attacks or corruption. If the BIOS becomes corrupted or is attacked, HP Sure Start automatically restores the BIOS to its previously safe state, without user intervention.

HP Sure Start is configured and already enabled so that most users can use the HP Sure Start default configuration. The default configuration can be customized by advanced users.

To access the latest documentation on HP Sure Start, go to http://www.hp.com/support. Select **Find your product**, and then follow the on-screen instructions.

11 Using HP PC Hardware Diagnostics (UEFI)

HP PC Hardware Diagnostics is a Unified Extensible Firmware Interface (UEFI) that allows you to run diagnostic tests to determine whether the computer hardware is functioning properly. The tool runs outside the operating system so that it can isolate hardware failures from issues that are caused by the operating system or other software components.

When HP PC Hardware Diagnostics (UEFI) detects a failure that requires hardware replacement, a 24-digit Failure ID code is generated. This ID code can then be provided to support to help determine how to correct the problem.

NOTE: To start diagnostics on a convertible computer, your computer must be in notebook mode and you must use the keyboard attached.

To start HP PC Hardware Diagnostics (UEFI), follow these steps:

1. Turn on or restart the computer, and quickly press esc.
2. Press f2.

   The BIOS searches three places for the diagnostic tools, in the following order:

   a. Connected USB drive

      NOTE: To download the HP PC Hardware Diagnostics (UEFI) tool to a USB drive, see Downloading HP PC Hardware Diagnostics (UEFI) to a USB device on page 75.

   b. Hard drive

   c. BIOS
3. When the diagnostic tool opens, select the type of diagnostic test you want to run, and then follow the on-screen instructions.

NOTE: If you need to stop a diagnostic test, press esc.

Downloading HP PC Hardware Diagnostics (UEFI) to a USB device

NOTE: The HP PC Hardware Diagnostics (UEFI) download instructions are provided in English only, and you must use a Windows computer to download and create the HP UEFI support environment because only .exe files are offered.

There are two options to download HP PC Hardware Diagnostics to a USB device.

Download the latest UEFI version

1. Go to http://www.hp.com/go/techcenter/pcdiags. The HP PC Diagnostics home page is displayed.
2. In the HP PC Hardware Diagnostics section, select the **Download** link, and then select **Run**.

Download any version of UEFI for a specific product

1. Go to http://www.hp.com/support.
2. Select **Get software and drivers**.
3. Enter the product name or number.
4. Select your computer, and then select your operating system.
5. In the **Diagnostic** section, follow the on-screen instructions to select and download the UEFI version you want.

Using Remote HP PC Hardware Diagnostics (UEFI) settings (select products only)

Your computer supports Remote HP PC Hardware Diagnostics (UEFI). This is a firmware (BIOS) feature that downloads HP PC Hardware Diagnostics UEFI to your computer.

It executes the diagnostics on your computer, and then may upload results to a preconfigured server.

Using the Remote HP PC Hardware Diagnostics setting in Computer Setup (BIOS), you can perform the following customizations:

- Set a schedule for running diagnostics unattended. You can also start diagnostics immediately in interactive mode by selecting **Execute Remote HP PC Hardware Diagnostics**.
- Set the location for downloading the diagnostic tools. This feature provides access to the tools from the HP website or from a server that has been preconfigured for use. Your computer does not require the traditional local storage (such as a disk drive or USB flash drive) to run remote diagnostics.
- Set a location for storing the test results. You can also set the user name and password settings used for uploads.
- Display status information about the diagnostics run previously.

Customizing Remote HP PC Hardware Diagnostics (UEFI) settings

1. Turn on or restart the computer, and when the HP logo appears, press f10 to enter Computer Setup.
2. Select **Advanced**, and then select **Settings**.
3. Make your customization selections.
4. Select **Main**, and then **Save Changes and Exit** to save your settings.

Your changes take effect when the computer restarts.

To access documentation on using Remote HP PC Hardware Diagnostics (UEFI) to configure a server for remote diagnostics or to customize which diagnostic tests are run, go to http://www.hp.com/support. Select **Find your product**, and then follow the on-screen instructions.

12 Specifications

Input power

The power information in this section may be helpful if you plan to travel internationally with the computer.

The computer operates on DC power, which can be supplied by an AC or a DC power source. The AC power source must be rated at 100–240 V, 50–60 Hz. Although the computer can be powered from a standalone DC power source, it should be powered only with an AC adapter or a DC power source supplied and approved by HP for use with this computer.

The computer can operate on DC power within the following specifications. The voltage and current for your computer is located on the regulatory label.

Input Power	Rating
Operating voltage and current	19.5 V dc @ 2.31 A – 45 W
	19.5 V dc @ 3.33 A – 65 W

NOTE: This product is designed for IT power systems in Norway with phase-to-phase voltage not exceeding 240 V rms.

Operating environment

Factor	Metric	U.S.
Temperature		
Operating (writing to optical disc)	**5°C to 35°C**	41°F to 95°F
Nonoperating	**-20°C to 60°C**	-4°F to 140°F
Relative humidity (noncondensing)		
Operating	**10% to 90%**	10% to 90%
Nonoperating	**5% to 95%**	5% to 95%
Maximum altitude (unpressurized)		
Operating	**-15 m to 3,048 m**	-50 ft to 10,000 ft
Nonoperating	**-15 m to 12,192 m**	-50 ft to 40,000 ft

13 Electrostatic Discharge

Electrostatic discharge is the release of static electricity when two objects come into contact—for example, the shock you receive when you walk across the carpet and touch a metal door knob.

A discharge of static electricity from fingers or other electrostatic conductors may damage electronic components.

To prevent damage to the computer, damage to a drive, or loss of information, observe these precautions:

- If removal or installation instructions direct you to unplug the computer, first be sure that it is properly grounded.
- Keep components in their electrostatic-safe containers until you are ready to install them.
- Avoid touching pins, leads, and circuitry. Handle electronic components as little as possible.
- Use nonmagnetic tools.
- Before handling components, discharge static electricity by touching an unpainted metal surface.
- If you remove a component, place it in an electrostatic-safe container.

14 Accessibility

HP designs, produces, and markets products and services that can be used by everyone, including people with disabilities, either on a stand-alone basis or with appropriate assistive devices. To access the latest information on HP accessibility, go to http://www.hp.com/accessibility.

Supported assistive technologies

HP products support a wide variety of operating system assistive technologies and can be configured to work with additional assistive technologies. Use the Search feature on your device to locate more information about assistive features.

NOTE: For additional information about a particular assistive technology product, contact customer support for that product.

Contacting support

We are constantly refining the accessibility of our products and services and welcome feedback from users. If you have an issue with a product or would like to tell us about accessibility features that have helped you, please contact us at +1 (888) 259-5707, Monday through Friday, 6 a.m. to 9 p.m. North American Mountain Time. If you are deaf or hard-of-hearing and use TRS/VRS/WebCapTel, contact us if you require technical support or have accessibility questions by calling +1 (877) 656-7058, Monday through Friday, 6 a.m. to 9 p.m. North American Mountain Time.

NOTE: Support is in English only.

Index

Benutzerhandbuch

HP Sure Recover

Erste Ausgabe: Februar 2020

Dokumentennummer: 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

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 Imageerstellungsarchiv 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 Dateinamensteil 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/clientmanagementabrufen. 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.

Tabelle 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

Felhasználói útmutató

HP Sure Recover

Első kiadás: 2020. február

A dokumentum cikkszáma: L93434-211

Magyarázat a felhasználó által beírandó szintaxishoz

A felhasználói felületen a felhasználó által beírandó szöveg `rögzített szélességű betűkészlettel` van jelölve.

-1. táblázat: Magyarázat a felhasználó által beírandó szintaxishoz

Elem	Leírás
`Szöveg zárójel vagy kapcsos zárójel nélkül`	Pontosan a megadott módon beírandó elemek
`<Csúcsos zárójelbe tett szöveg>`	A felhasználó által megadandó érték helyőrzője; hagyja el a zárójelet
`[Szögletes zárójelbe tett szöveg]`	Nem kötelező elemek; hagyja el a zárójelet
`{Kapcsos zárójelbe tett szöveg}`	Olyan választható elemek, amelyek közül csak egyet választhat; hagyja el a zárójelet
`|`	Elválasztó olyan elemek között, amelyek közül csak egyet választhat; hagyja el a függőleges vonalat
`. . .`	Elemek, amelyeket lehetséges vagy kötelező ismételni; hagyja el a három pontot

Tartalomjegyzék

1 Első lépések

A HP Sure Recover segítségével biztonságosan, minimális felhasználói beavatkozással telepítheti az operációs rendszert a hálózatról. A HP Sure Recover with Embedded Reimaging megoldással rendelkező rendszerek helyi tárolóeszközről is támogatják a telepítést.

FONTOS: A HP Sure Recover használata előtt készítsen biztonsági másolatot az adatokról. Mivel a lemezkép-telepítési folyamat újraformázza a meghajtót, adatvesztés fog bekövetkezni.

A HP által biztosított helyreállítási lemezképek az alapszintű Windows 10®-telepítőprogramot tartalmazzák. A HP Sure Recoverrel azt is megteheti, hogy HP-eszközökhöz optimalizált illesztőprogramokat telepít. A HP helyreállítási lemezképek csak a Windows 10 részét képező adat-helyreállítási ügynököket tartalmazzák, például a OneDrive-ot. A vállalatok létrehozhatják saját egyéni lemezképeiket a vállalati beállítások, alkalmazások, illesztőprogramok és adat-helyreállítási ügynökök hozzáadásához.

A helyreállítási lemezkép telepítéséhez szükséges lépéseket egy operációsrendszer-helyreállítási ügynök hajtja végre. Ez a HP által biztosított ügynök általános lépéseket hajt végre: particionál, formáz, és kicsomagolja a helyreállítási lemezképet a céleszközre. Mivel a HP helyreállítási ügynöke a hp.com webhelyen található, internet-hozzáférésre is szüksége lesz, ha a rendszer nem tartalmaz beágyazott lemezkép-helyreállítást. A vállalatok a saját tűzfalukon belül is üzemeltethetik a HP helyreállítási ügynökét, de egyéni helyreállítási ügynököket is létrehozhatnak a bonyolultabb helyreállítási környezetekhez.

A HP Sure Recover akkor indítható el, ha nem található operációs rendszer. A HP Sure Recover ütemezés szerint is futtatható, például a kártevők eltávolítása érdekében. A kapcsolódó beállításokat a HP Client Security Manager (CSM), a Manageability Integration Kit (MIK) vagy a HP Client Management Script Library segítségével konfigurálhatja.

Hálózati helyreállítás végrehajtása

MEGJEGYZÉS: A hálózati helyreállítást csak vezetékes kapcsolaton lehet végrehajtani. A HP azt javasolja, hogy a HP Sure Recover használata előtt készítsen biztonsági másolatot a fontos fájlokról, adatokról, fényképekről, videókról stb., hogy elkerülje az adatvesztést.

1. Csatlakoztassa az ügyfélrendszert ahhoz a hálózathoz, amelyen a HTTP- vagy FTP-terjesztési pont elérhető.
2. Indítsa újra az ügyfélrendszert, és amikor megjelenik a HP embléma, nyomja le az F11 billentyűt.
3. Válassza a **Restore from network** (Visszaállítás hálózatról) lehetőséget.

Helyreállítás helyi meghajtóról

Ha az ügyfélrendszer támogatja a beágyazott lemezkép-helyreállítást, és az ütemezett lemezképletöltés engedélyezve lett a vonatkozó szabályzatban, akkor az ügyfélrendszer letölti a lemezképet az ütemezett időpontban. Miután a lemezkép letöltődött az ügyfélrendszerre, indítsa újra a rendszert, hogy átmásolja a lemezképet a beágyazott lemezkép-helyreállítási tárolóeszközre.

Helyi helyreállítás a beágyazott lemezkép-helyreállítási tárolóeszközön található lemezképpel:

1. Indítsa újra az ügyfélrendszert, és amikor megjelenik a HP embléma, nyomja le az F11 billentyűt.
2. Válassza a **Restore from local drive** (Visszaállítás helyi meghajtóról) lehetőséget.

A beágyazott lemezkép-helyreállítással rendelkező rendszereken konfigurálni kell egy letöltési ütemezést, és a letöltési ügynökkel ellenőriztetni kell, hogy vannak-e elérhető frissítések. A letöltési ügynököt a HP Client Security Manager HP Sure Recover beépülő modulja tartalmazza, és az MIK készletben is konfigurálható. Az MIK használatával kapcsolatban itt talál útmutatást: https://www.hp.com/go/clientmanagement.

Ütemezett feladatot is létrehozhat, amellyel az SR_AED partícióra másolhatja az ügynököt, az SR_IMAGE partícióra pedig a lemezképet. Ezután a HP Client Management Script Library használatával elküldhet egy szolgáltatási eseményt, amely felszólítja a BIOS-t, hogy érvényesítse a tartalmakat, és másolja őket a beágyazott lemezkép-helyreállítási tárolóeszközre a következő újraindításkor.

2 Vállalati lemezkép létrehozása

A vállalatok többsége a Microsoft Deployment Toolst, a Windows 10 Assessment and Deployment Kitet vagy mindkettőt használja lemezképet tartalmazó, a Windows Imaging (WIM) fájlformátumú archívumban megtalálható fájlok létrehozásához.

Előfeltételek

- A Windows 10 Assessment and Deployment Kit (Windows ADK) legújabb verziója
- PowerShell
- OpenSSL (vagy valamilyen más megoldás a személyes/nyilvános RSA-kulcspár létrehozásához)

  RSA-kulcspár létrehozására szolgál, amellyel a létrehozott és tárolt vállalati lemezkép védelméről lehet gondoskodni.
- Egy kiszolgálóüzemeltetési megoldás (például a Microsoft Internet Information Services, IIS)

A lemezkép létrehozása

A lemezkép-létrehozási folyamat megkezdése előtt az alábbi lépéseket követve állítsa be azt a munkavégzési vagy összeállítási rendszert, amelyen a lemezkép feldolgozásához szükséges eszközöket telepítette:

1. Nyissa meg rendszergazdaként a `Deployment and Imaging Tools Environment` parancssorát (a környezet a Windows ADK üzembehelyezési eszközeivel települ).
2. Hozzon létre egy átmeneti területet a lemezkép számára az alábbi paranccsal:

   ```
   mkdir C:\staging
   ```
3. Hozza létre a lemezképet az alábbi példák valamelyike alapján:

   1. példa: Lemezkép létrehozása a Microsoft Windows telepítési lemezképe alapján 3. oldal

   2. példa: Lemezkép létrehozása referencia-rendszer alapján 5. oldal

1. példa: Lemezkép létrehozása a Microsoft Windows telepítési lemezképe alapján

1. Csatlakoztassa vagy nyissa meg a Microsoft Windows telepítési lemezképét (Microsoft ISO-fájlból vagy HP OSDVD-ről).
2. A csatlakoztatott Windows telepítési lemezképből másolja az install.wim fájlt az átmeneti területre az alábbi paranccsal:

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

   MEGJEGYZÉS: Az `<M:>` a csatlakoztatott meghajtó. Cserélje le a megfelelő meghajtó betűjelére.
3. Nevezze át az install.wim fájlt arra a névre, amelynek a lemezképet hívni szeretné (ebben a példában „my-image”) az alábbi paranccsal:

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

(Választható) A HP Sure Recover tartalmaz egy olyan funkciót, amellyel helyre lehet állítani egy adott kiadást egy többindexes lemezképből a Windows azon kiadása alapján, amely eredetileg licencelve lett a HP-célrendszer számára a gyárban. Ez a mechanizmus csak akkor működik, ha az indexek megfelelően lettek elnevezve. Ha a Windows telepítési lemezkép HP OSDVD-lemezképből származik, akkor nagy a valószínűsége, hogy egy többkiadásos lemezképről van szó. Ha nem kívánja használni ezt a funkciót, és gondoskodni szeretne róla, hogy minden célrendszeren egy adott kiadás legyen használatban, meg kell arról győződnie, hogy csak egyetlen index van a telepítési lemezképben.

4. Ellenőrizze a telepítési lemezkép tartalmát az alábbi paranccsal:

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

Az alábbiakban egy olyan telepítési lemezkép példakimenete látható, amely öt kiadást támogat (amelyeket az egyes célrendszerek BIOS-a alapján kell egyeztetni):

Lemezkép részletei: `my-image.wim`

Index: `1`

Név: `CoreSingleLanguage`

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

Méret: `19,512,500,682 bytes`

Index: `2`

Név: `Core`

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

Méret: `19,512,500,682 bytes`

Index: `3`

Név: `Professional`

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

Méret: `19.758,019,520 bytes`

Index: `4`

Név: `ProfessionalEducation`

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

Méret: `19,758,019,480 bytes`

Index: `5`

Név: `ProfessionalWorkstation`

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

Méret: `19,758,023,576 bytes`

MEGJEGYZÉS: Ha csak egy index van, a rendszer azt a lemezképet használja a helyreállításhoz a névre való tekintet nélkül. Előfordulhat, hogy a lemezképfájl mérete nagyobb lesz, mint a törlések előtt volt.

5. Ha nem szeretné használni a többkiadásos viselkedést, törölje a nem kívánt indexeket.

   Ha csak a Professional kiadást szeretné használni (feltételezve, hogy a célrendszerek mindegyike rendelkezik licenccel), törölje az 5., 4., 2. és 1. indexet, ahogy az alábbi példában is látható. Minden egyes indextörléskor a rendszer ismételten kiosztja az indexszámokat. Ezért a törlést a legmagasabbtól a legalacsonyabb indexszám felé haladva hajtsa végre. Minden törlés után futtassa a `Get-ImageInfo` parancsot, és vizuálisan ellenőrizze, hogy melyik indexet fogja következőként törölni.

   ```
   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
   ```

   Csak a kívánt kiadás indexét válassza ki (ebben a példában ez a Professional). Ha csak egy index van, a rendszer azt a lemezképet használja a helyreállításhoz a névre való tekintet nélkül. Vegye figyelembe, hogy a lemezképfájl mérete esetenként nagyobb lehet, mint a törlések előtt volt, a WIM metaadat-módosításainak és tartalomnormalizálásának a működési módja miatt.

6. (Választható) Ha illesztőprogramokat is hozzá szeretne adni a vállalati helyreállítási lemezképhez, kövesse az alábbi lépéseket:

   a. Csatlakoztassa a lemezképet egy üres mappához az alábbi parancsokkal:

   ```
   mkdir C:\staging\mount

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

   b. Csatlakoztassa a támogatott célrendszer illesztőprogramokat tartalmazó, megfelelő HP Windows 10 Driver DVD-jét (DRDVD). Az illesztőprogramok csatlakoztatott adathordozójáról másolja az illesztőprogramokat tartalmazó almappákat az átmeneti területre az alábbi paranccsal:

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

   MEGJEGYZÉS: Az `<M:>` a csatlakoztatott meghajtó. Cserélje le a megfelelő meghajtó betűjelére.

   Ha további .inf típusú illesztőprogramokat is hozzá szeretne adni a lemezképhez, helyezze azokat a C:\staging\mount\SWSETUP\DRV mappába. Annak ismertetését, hogy a HP Sure Recover hogyan dolgozza fel ezeket a tartalmakat a `dism /Add-Driver /Recurse` paranccsal, a következő cikkben tekintheti át, amely többek között az illesztőprogramok offline Windows-lemezképhez történő hozzáadásával és onnan való eltávolításával foglalkozik: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ez a funkció nem támogatja az alkalmazások futtatásához szükséges .exe típusú illesztőprogramokat.

   c. Mentse a módosításokat, és válassza le a lemezképet az alábbi paranccsal:

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

   Az eredményül kapott lemezképfájl: C:\staging\my-image.wim.

   d. Lépjen a következő lépésre: A lemezkép felosztása 6. oldal.

2. példa: Lemezkép létrehozása referencia-rendszer alapján

1. Hozzon létre egy rendszerindításra alkalmas, a WinPE-t tartalmazó USB-adathordozót.

MEGJEGYZÉS: A lemezkép rögzítésének további módszerei az ADK dokumentációjában találhatók.

Győződjön meg róla, hogy az USB-meghajtó elegendő szabad területtel rendelkezik a referencia-rendszeren rögzített lemezkép tárolásához.

2. Hozzon létre egy lemezképet egy referencia-rendszeren.
3. Rögzítse a lemezképet úgy, hogy a referencia-rendszert a WinPE-t tartalmazó USB-adathordozóval indítja el, majd használja az alábbi DISM-parancsot.

MEGJEGYZÉS: Az `<U:>` az USB-meghajtóra vonatkozik. Cserélje le a megfelelő meghajtó betűjelére.

Módosítsa a fájlnév „my-image” részét, valamint a `<my-image>` leírást igény szerint.

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

4. Másolja a lemezképet az USB-meghajtóról a munkavégzési rendszer átmeneti területére az alábbi paranccsal:

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

A következő lemezképfájlt kell kapnia: C:\staging\my-image.wim.

5. Lépjen a következő lépésre: A lemezkép felosztása 6. oldal.

A lemezkép felosztása

A HP azt javasolja, hogy a hálózati letöltések megbízhatóságának javítása érdekében ossza fel a lemezképet kisebb fájlokra az alábbi paranccsal:

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

MEGJEGYZÉS: A FileSize megabájtban megadott méretet jelöl. Módosítsa az értékét igény szerint.

MEGJEGYZÉS: A DISM felosztási algoritmusának jellege miatt előfordulhat, hogy a létrehozott SWM-fájlok mérete kisebb vagy nagyobb lesz a megadott fájlméretnél.

Jegyzékfájl létrehozása

A jegyzékfájlokat UTF-8 formátumban formázza, bájtsorrendjelző (Byte Order Mark, BOM) nélkül.

A következő eljárásokban használt jegyzékfájl neve (custom.mft) módosítható, de nem módosíthatja az .mft és az .sig kiterjesztést, a jegyzékfájl és az aláírásfájlok fájlnévrészének pedig meg ugyanannak kell lennie. A custom.mft, custom.sig párt például a myimage.mft, myimage.sig párra módosíthatja.

Az `mft_version` a lemezképfájl formátumának a meghatározására szolgál, és jelenleg 1 értékűre kell beállítani.

Az `image_version` annak megállapítására szolgál, hogy elérhető-e a lemezkép újabb verziója, valamint megakadályozza a régebbi verziók telepítését.

Mindkét értéknek előjel nélküli 16 bites egész számnak kell lennie, a jegyzékfájlban pedig az `'\r\n' (CR + LF)` karakterláncot kell sorelválasztóként használni.

Jegyzékfájl létrehozása

Mivel a felosztott lemezkép több fájlt is tartalmazhat, hozzon létre egy jegyzékfájlt egy PowerShell-szkripttel.

A hátralévő lépéseket a C:\staging mappában kell végrehajtani.

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

1. Hozzon létre egy PowerShell-szkriptet az alábbi paranccsal és egy olyan szerkesztővel, amely képes UTF-8 formátumú, bájtsorrendjelző nélküli szövegfájl létrehozására: `notepad C:\staging \generate-manifest.ps1`

   Hozza létre az alábbi szkriptet:

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

   ```
   $imageVersion = 1907
   ```
   (Megjegyzés: A szám bármilyen 16 bites egész szám lehet.)

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

}
```

MEGJEGYZÉS: A HP Sure Recover jegyzékfájlja nem tartalmazhat bájtsorrendjelzőt, így az alábbi parancsok bájtsorrendjelző nélküli UTF-8 formátumú fájllá írják át a fájlt.

```
$content = Get-Content $mftFilename

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

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

2. Mentse a szkriptet.
3. Hajtsa végre a szkriptet.

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

Jegyzékfájl-aláírás létrehozása

A Sure Recover titkosított aláírással ellenőrzi az ügynököt és a lemezképet. Az alábbi példák egy X.509 PEM formátumú (.PEM kiterjesztésű) személyes/nyilvános kulcspárt használnak. Módosítsa a parancsokat igény szerint, hogy DER bináris tanúsítványokat (.CER vagy .CRT kiterjesztés), BASE-64 kódolású PEM-tanúsítványokat (.CER vagy .CRT kiterjesztés) vagy PKCS1 PEM-fájlokat (.PEM kiterjesztés) használjanak. A példa OpenSSL-t is használ, amely csökkenő bájtsorrendű formátumban hozza létre az aláírásokat. Bármilyen segédprogrammal aláírhatja a jegyzékfájlokat, de vegye figyelembe, hogy néhány BIOS-verzió csak a növekvő bájtsorrendű aláírásokat támogatja.

1. Hozzon létre egy 2048 bites személyes RSA-kulcsot az alábbi paranccsal. Ha rendelkezik PEM formátumú, 2048 bites személyes/nyilvános RSA-kulcspárral, másolja a C:\staging mappába, majd ugorjon a 3. lépésre.

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

2. Hozza létre a nyilvános kulcsot a személyes kulcsból az alábbi paranccsal (ha rendelkezik PEM formátumú, a személyes kulcsnak megfelelő nyilvános kulccsal, akkor másolja a C:\staging mappába):

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

3. Hozzon létre egy aláírásfájlt (SHA-256-alapú kivonattal) az 1. lépésben létrehozott 2048 bites személyes RSA-kulcs alapján az alábbi paranccsal:

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

4. Ellenőrizze az aláírásfájlt az előző lépésben létrehozott nyilvános kulcsot használva az alábbi paranccsal:

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

MEGJEGYZÉS:

- Ha csak aláírásfájlt kell létrehoznia, csak az 1. és a 3. lépést kell végrehajtani.
- A HP Sure Recover esetén legalább az 1., 2. és 3. lépést végre kell hajtani. A 2. lépésben létrehozott nyilvános kulcs a célrendszer üzembe helyezéséhez szükséges.
- A 4. lépés nem kötelező, de ajánlott, hogy az aláírásfájl és a jegyzékfájl ellenőrzése se maradjon el.

A fájlok tárolása

Az alábbi fájlokat a kiszolgáló C:\staging mappájában tárolja:

- *.swm
- custom.mft (vagy a jegyzékfájlnak adott fájlnév)
- custom.sig (vagy az aláírásfájlnak adott, a jegyzékfájllal egyező fájlnév)

MEGJEGYZÉS: Ha tárolási megoldásként az IIS-t használja, a MIME-bejegyzéseket úgy kell konfigurálni, hogy magukban foglalják az alábbi kiterjesztéseket, mindegyiket „application/octet-stream” típusúként konfigurálva:

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

A célrendszerek üzembe helyezése

A célrendszerek a HP Client Management Script Library, a HP Client Security Manager (CSM)/Sure Recover vagy a Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement) használatával helyezhetők üzembe.

Adja meg az alábbi információkat az üzembe helyezéshez:

1. Az előző szakaszban található jegyzékfájl URL-címe (http://saját_kiszolgáló.tartomány/útvonal/custom.mft)
2. A korábban létrehozott aláírásfájl ellenőrzésére használt nyilvános kulcs (például: C:\staging\my-recovery-public.pem).

Hibaelhárítás

Ha olyan üzenetet kap, amely szerint az egyéni helyreállítási folyamat biztonsági ellenőrzése sikertelen volt, ellenőrizze az alábbiakat:

1. A jegyzékfájlnak BOM nélküli UTF-8 formátumú fájlnak kell lennie.
2. Ellenőrizze a fájlkivonatokat.
3. Ellenőrizze, hogy a rendszer üzembe helyezése a jegyzékfájl aláírásához használt személyes kulcsnak megfelelő nyilvános kulccsal történt-e.

4. AZ IIS-kiszolgáló MIME-inek `application/octet-stream` típusúnak kell lenniük.
5. A jegyzékfájlon belüli fájlútvonalaknak a lemezképet tartalmazó legfelső szintű könyvtár teljes elérési útját tartalmazniuk kell, az ügyfélrendszerről nézve. Ez az elérési út nem annak a helynek a teljes elérési útja, ahol a fájlok mentve lettek a terjesztési ponton.

3 A HP Sure Recover-ügynök használata vállalati tűzfalon belül

A HP Sure Recover-ügynök vállalati tűzfalon belül is üzemeltethető. Miután telepítette a HP Sure Recover SoftPaq csomagot, másolja az ügynök fájljait a HP Sure Recover-ügynöknek a telepítési helyen található könyvtárából egy HTTP- vagy FTP-terjesztési pontra. Ezután helyezze üzembe az ügyfélrendszert a terjesztési pont URL-címével és a `hpsr_agent_public_key.pem` nevű nyilvános HP-kulccsal, amelynek a terjesztése a HP Sure Recover-ügynök SoftPaq csomagjával történik.

A HP Sure Recover-ügynök telepítése

1. Töltse le a HP Sure Recover-ügynököt, és bontsa ki a fájlokat a HTTP- vagy FTP-terjesztési pontra.
2. Állítsa be a megfelelő fájlengedélyeket a terjesztési ponton.
3. Ha az Internet Information Services (IIS) megoldást használja, hozzon létre application/octet-stream MIME-típusokat az alábbi fájlformátumokhoz:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

FONTOS: Az alábbi lépések a Sure Recover SCCM használatával történő üzembe helyezését ismertetik. A Sure Recover HP Client Management Script Library használatával történő üzembe helyezésével kapcsolatban lásd: A HP Client Management Script Library (CMSL) használata, 13. oldal.

4. Indítsa el az SCCM-et, lépjen a **HP Client Security Suite** (HP Client Security szoftvercsomag) részre, majd válassza a HP Sure Recover oldalt.

MEGJEGYZÉS: A terjesztési pont URL-címe tartalmazza vagy az FTP-t vagy a HTTP-t mint átviteli protokollt. Annak a legfelső szintű könyvtárnak az ügyfélrendszerről látható teljes elérési útvonalát is tartalmazza, amelyen HP Sure Recover-ügynök jegyzékfájlja megtalálható. Ez az elérési út nem annak a helynek a teljes elérési útja, ahol a fájlok mentve lettek a terjesztési ponton.

5. A **Platform Image** (Platform lemezképe) szakaszban válassza a **Corporation** (Vállalat) lehetőséget az operációs rendszer egyéni lemezképének egy vállalati terjesztési pontról való visszaállításához. Adja meg az informatikai rendszergazdától kapott URL-címet az **Image Location URL** (A lemezkép helyének URL-címe) beviteli mezőben. Adja meg a `hpsr_agent_public_key.pem` nyilvános kulcsot az **Image Verification** (Lemezkép ellenőrzése) mezőben.

MEGJEGYZÉS: Az egyéni lemezkép URL-címének tartalmaznia kell a lemezkép jegyzékfájljának a nevét.

6. A **Recovery Agent** (Helyreállítási ügynök) szakaszban válassza a **Corporation** (Vállalat) lehetőséget az egyéni helyreállítási ügynöknek vagy a HP helyreállítási ügynökének egy vállalati terjesztési pontról való használatához. Adja meg az informatikai rendszergazdától kapott URL-címet az **Agent Location URL** (Ügynök helyének URL-címe) mezőben. Adja meg a `hpsr_agent_public_key.pem` nyilvános kulcsot az **Agent Verification Key** (Ügynök ellenőrzési kulcsa) mezőben.

MEGJEGYZÉS: Az URL-címben ne szerepeljen az ügynök jegyzékfájljának a neve, mert a BIOS megköveteli, hogy a név recovery.mft legyen.

7. Miután alkalmazta a szabályzatot az ügyfélrendszerre, indítsa újra a rendszert.

8. A kezdeti üzembe helyezés során megjelenik egy, a HP Sure Recover aktiválásához szükséges négyjegyű biztonsági kód megadására felszólító üzenet. További részletekért keresse fel a hp.com webhelyet, és keressen rá a HP Manageability Integration Kit (MIK) for Microsoft System Center Manager megoldással foglalkozó dokumentációra.

A HP Sure Recover sikeres aktiválása után a szabályzat által alkalmazott egyéni URL-cím megjelenik a HP Sure Recover BIOS-beállításainak menüjében.

Ha meg szeretné erősíteni, hogy az aktiválás sikerrel járt, indítsa újra a számítógépet, és amikor megjelenik a HP embléma, nyomja le az F10 billentyűt. Válassza az **Advanced** (Speciális), a **HP Sure Recover**, a **Recovery Agent** (Helyreállítási ügynök), végül pedig az **URL** lehetőséget.

4 A HP Client Management Script Library (CMSL) használata

A HP Client Management Script Library lehetővé teszi a HP Sure Recover beállításainak PowerShell-lel való kezelését. Az alábbi példaszkript bemutatja, hogyan lehet a HP Sure Recovert üzembe helyezni, az állapotát meghatározni, a konfigurációját módosítani, valamint kivonni a használatból.

MEGJEGYZÉS: Több parancs is hosszabb annál, hogy ebben az útmutatóban egyetlen sorban kiférjen, de ettől függetlenül egyetlen sorba kell írni őket.

```
$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
}
```

Példakulcs létrehozása az OpenSSL-lel

A személyes kulcsokat tárolja biztonságos helyen. A nyilvános kulcsokat az érvényesítéshez kell használni, és az üzembe helyezés során meg kell adni őket. Ezeknek a kulcsoknak 2048 bit hosszúságúnak kell lenniük, és 0x10001 kitevőt kell használniuk. A példákban szereplő megfelelő adatokat helyettesítse be cégének vagy szervezetének az adataival.

Állítsa be következő környezeti változót, mielőtt folytatná:

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

# Create a self-signed root CA certificate for testing
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

# Create a key endorsement certificate
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

```
openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:


# Create a command signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:


# Create an image signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

A lemezkép jegyzékfájlját a következő paranccsal írhatja alá:

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


# Create an agent signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Az ügynök jegyzékfájlját a következő paranccsal írhatja alá:

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

Az OpenSSL az aláírásfájlokat csökkenő bájtsorrendű formátumban hozza létre, amely néhány BIOS-verzióval nem kompatibilis, ezért előfordulhat, hogy az ügynök aláírásfájljának bájtsorrendjét meg kell fordítani az üzembe helyezés előtt. Azok a BIOS-verziók, amelyek támogatják a csökkenő bájtsorrendet, a növekvőt is támogatják.

A Hibaelhárítás

A meghajtó particionálása nem sikerült

A meghajtó particionálása akkor bizonyulhat sikertelennek, ha az SR_AED vagy SR_IMAGE partíció BitLockerrel van titkosítva. Ezeket a partíciókat általában egy GPT attribútummal hozzák létre, amely megakadályozza, hogy a BitLocker titkosítsa őket, de ha egy felhasználó törli és újra létrehozza a partíciókat, vagy manuálisan hozza létre őket egy operációs rendszer nélküli meghajtón, akkor a Sure Recover ügynök nem tudja törölni őket, és hibajelzéssel kilép, amikor megpróbálja újraparticionálni a meghajtót. A felhasználónak manuálisan kell törölnie a partíciókat a DiskPart futtatásával. Ki kell választania a kötetet, és végre kell hajtania a `del vol` felülírási parancsot vagy valamilyen hasonló műveletet.

Firmware-naplófájl

Az EFI-változó adatai a következők:

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

Az EFI-változókat API-kkal lehet olvasni a Windowsban, de egy fájlba is kiírhatja a tartalmukat az UEFI Shell dmpstore segédprogrammal.

A naplófájlt a HP Client Management Script Library által biztosított `Get-HPFirmwareAuditLog` paranccsal írhatja ki.

Windows Eseménynapló

A Sure Recover indítási és leállítási eseményeit a rendszer a BIOS naplófájljába küldi, amelyet a Windows Eseménynaplóban tekinthet meg a Sure Start naplófájljában, amennyiben a HP Notifications telepítve van. A rögzített események tartalmazzák a dátumot és az időpontot, a forrásazonosítót, az eseményazonosítót és egy eseményspecifikus kódot. Az `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` például azt jelzi, hogy a helyreállítás nem sikerült, mert a jegyzékfájlt nem lehetett hitelesíteni a c3f 23000 eseményspecifikus kóddal, amely a következő napon és időpontban rögzült a naplóban: 6/27/18, 2:26:40.

MEGJEGYZÉS: Ezek a naplók az Amerikai Egyesült Államokban használt hónap/nap/év formátumot követik.

HP Secure Platform Management (forrásazonosító = 84h)

A-1. táblázat: HP Secure Platform Management

Eseményazonosító	Eszközök száma (összes/DaaS)	Események száma (összes/DaaS)	Leírás	Megjegyzések
40	256/178	943/552	A platform operációs rendszerének helyreállítási folyamatát a firmware megkezdte.	A platform helyreállítása elindult

A-1. táblázat: HP Secure Platform Management (folytatás)

Eseményazonosító	Eszközök száma (összes/DaaS)	Események száma (összes/DaaS)	Leírás	Megjegyzések
41	221/147	588/332	A platform operációs rendszerének helyreállítási folyamata sikeresen befejeződött.	A platform helyreállítása befejeződött
42	54/42	252/156	A platform operációs rendszerének helyreállítási folyamata sikertelen.	A platform helyreállítása sikertelen

A firmware-naplófájlt a Get-HPFirmwareAuditLog paranccsal kérheti le a HP Client Management Script Libraryben, amely itt érhető el: http://www.hp.com/go/clientmanagement. A HP Secure Platform Management 40-es, 41-es és 42-es eseményazonosítói visszaküldik az eseményspecifikus kódokat az adatmezőbe, amely megjeleníti a Sure Recover-műveletek eredményét. Az alábbi naplóbejegyzés például a következőkkel jelzi, hogy a Sure Recovernek nem sikerült letöltenie a jegyzékfájlt vagy az aláírásfájlt: event_id 42 és 00:30:f1:c3, amelyet 0xC3F13000 = MftOrSigDownloadFailed DWORD értékként kell értelmezni.

```
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
```

A sikeres helyreállítást a következők jelzik: event_id = 41 és 00:00:00:00, például:

```
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

A HP Sure Recover az alábbi eseményspecifikus kódokat használja.

A-2. táblázat: Eseményspecifikus kódok

Esemény leírása	Eseménykód
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

Používateľská príručka

HP Sure Recover

Prvé vydanie: február 2020

Katalógové číslo dokumentu: L93434-231

Štýl syntaxe zadávanej používateľom

Text, ktorý musíte zadať v používateľskom rozhraní, je označený `neproporcionálnym písmom`.

Tabuľka -1 Štýl syntaxe zadávanej používateľom

Položka	Popis
`Text bez lomených, hranatých alebo zložených zátvoriek`	Položky, ktoré musíte zadať presne tak, ako sú zobrazené.
`<Text v lomených zátvorkách>`	Zástupný symbol hodnoty, ktorú musíte zadať. Zátvorky vynechajte.
`[Text v hranatých zátvorkách]`	Voliteľné položky. Zátvorky vynechajte.
`{Text v zložených zátvorkách}`	Skupina položiek, z ktorých musíte vybrať len jednu. Zložené zátvorky vynechajte.
`|`	Oddeľovač položiek, z ktorých musíte vybrať len jednu. Zvislú čiaru vynechajte.
`...`	Položky, ktoré sa môžu alebo musia opakovať. Tri bodky vynechajte.

Obsah

1 Úvodné informácie

Program HP Sure Recover vám pomôže bezpečne nainštalovať operačný systém zo siete s minimálnou interakciou používateľa. Systémy s konfiguráciou HP Sure Recover with Embedded Reimaging podporujú aj inštaláciu z lokálneho ukladacieho zariadenia.

DÔLEŽITÉ: Pred použitím programu HP Sure Recover zálohujte údaje. Keďže sa pri vytváraní obrazu preformátuje jednotka, dôjde k strate údajov.

Obnovovacie obrazy, ktoré poskytuje spoločnosť HP, zahŕňajú základný inštalátor systému Windows 10®. Voliteľne môže program HP Sure Recover nainštalovať optimalizované ovládače pre zariadenia HP. Obnovovacie obrazy od spoločnosti HP obsahujú len agentov na obnovenie údajov, ktorí sú súčasťou systému Windows 10, napríklad OneDrive. Firmy môžu vytvárať vlastné obrazy na pridanie firemných nastavení, aplikácií, ovládačov a agentov na obnovu údajov.

Agent na obnovu operačného systému (OS) vykonáva kroky potrebné na inštaláciu obrazu na obnovenie. Agent na obnovu poskytovaný spoločnosťou HP vykonáva bežné kroky, ako je delenie, formátovanie a extrakcia obrazu na obnovenie do cieľového zariadenia. Keďže sa agent na obnovu od spoločnosti HP nachádza na lokalite hp.com, na jeho načítanie budete potrebovať prístup na internet (ak systém neobsahuje integrovanú tvorbu obrazov). Firmy tiež môžu hostiť agenta na obnovu od spoločnosti HP za bránou firewall alebo vytvoriť vlastných agentov na obnovu pre zložitejšie obnovovacie prostredia.

Ak sa nenájde žiadny operačný systém, môžete iniciovať program HP Sure Recover. Program HP Sure Recover môžete spustiť aj plánovane, napríklad na zabezpečenie odstránenia malvéru. Konfiguráciu týchto nastavení vykonajte prostredníctvom aplikácie HP Client Security Manager (CSM), Manageability Integration Kit (MIK) alebo HP Client Management Script Library.

Vykonanie sieťovej obnovy

POZNÁMKA: Ak chcete vykonať sieťovú obnovu, musíte použiť káblové pripojenie. Spoločnosť HP odporúča pred použitím programu HP Sure Recover zálohovať dôležité súbory, údaje, fotografie, videá a ďalší obsah, aby nedošlo k strate údajov.

1. Zapojte klientsky systém do siete, v ktorej možno získať prístup k distribučnému bodu HTTP alebo FTP.
2. Reštartujte klientsky systém a po zobrazení loga spoločnosti HP stlačte kláves f11.
3. Vyberte položku **Restore from network** (Obnoviť zo siete).

Vykonanie obnovy lokálnej jednotky

Ak klientsky systém podporuje integrovanú tvorbu obrazov a v použitej politike je povolená možnosť prevzatia obrazu, v plánovanom čase sa obraz prevezme do klientskeho systému. Po prevzatí obrazu do klientskeho systému ho reštartujte, aby sa obraz skopíroval do ukladacieho zariadenia na integrovanú tvorbu obrazov.

Ak chcete vykonať lokálnu obnovu pomocou obrazu na ukladacom zariadení na integrovanú tvorbu obrazov:

1. Reštartujte klientsky systém a po zobrazení loga spoločnosti HP stlačte kláves f11.
2. Vyberte položku **Restore from local drive** (Obnoviť z lokálnej jednotky).

Systémy s integrovanou tvorbou obrazov musia nakonfigurovať plán preberania a pomocou agenta preberania vyhľadať aktualizácie. Agent preberania je súčasťou doplnku HP Sure Recover Plug-in pre aplikáciu HP Client Security Manager a možno ho tiež nakonfigurovať v aplikácii MIK. Pokyny na používanie aplikácie MIK nájdete na lokalite https://www.hp.com/go/clientmanagement.

Môžete tiež vytvoriť plánovanú úlohu na skopírovanie agenta do oblasti SR_AED a obrazu do oblasti SR_IMAGE. Potom môžete použiť knižnicu HP Client Management Script Library na odoslanie servisnej udalosti, ktorá informuje systém BIOS, že pri nasledujúcom reštartovaní treba overiť obsah a vykonať kopírovanie do ukladacieho zariadenia na integrovanú tvorbu obrazov.

2 Vytvorenie firemného obrazu

Väčšina spoločností používa aplikáciu Microsoft Deployment Tools, súpravu Windows 10 Assessment and Deployment Kit alebo oboje na vytvorenie súborov obsahujúcich obraz v archíve s formátom súboru Windows Imaging (WIM).

Požiadavky

- Najnovšia verzia súpravy Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (alebo iné riešenie na generovanie dvojice súkromného/verejného kľúča RSA)

  Použite na generovanie dvojice kľúčov RSA, ktorá sa používa na zabezpečenie integrity vytváraného a hosteného firemného obrazu.
- Riešenie na hosťovanie servera (napríklad Microsoft Internet Information Services [IIS])

Vytvorenie obrazu

Pred spustením procesu tvorby obrazu nastavte pracovný systém alebo systém zostavy, v ktorom ste nainštalovali potrebné nástroje na prípravu na spracovanie obrazu, ako je uvedené v nasledujúcich krokoch:

1. Ako správca otvorte príkazový riadok `Deployment and Imaging Tools Environment` (nainštalovaný s nástrojmi nasadenia súpravy Windows ADK).
2. Vytvorte pracovnú oblasť pre obraz pomocou nasledujúceho príkazu:

   ```
   mkdir C:\staging
   ```
3. Vytvorte obraz pomocou jedného z nasledujúcich príkladov:

   Príklad 1: Vytvorenie obrazu na základe inštalačného obrazu systému Microsoft Windows na strane 3

   Príklad 2: Vytvorenie obrazu na základe referenčného systému na strane 5

Príklad 1: Vytvorenie obrazu na základe inštalačného obrazu systému Microsoft Windows

1. Pripojte alebo otvorte inštalačný obraz systému Microsoft Windows (zo súboru ISO od spoločnosti Microsoft alebo z disku HP OSDVD).
2. Z pripojeného inštalačného obrazu systému Windows skopírujte súbor install.wim do pracovnej oblasti pomocou nasledujúceho príkazu:

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

   POZNÁMKA: Písmeno `<M:>` označuje pripojenú jednotku. Nahraďte ho správnym písmenom jednotky.
3. Premenujte súbor install.wim na názov súboru obrazu (v tomto príklade „my-image“) pomocou nasledujúceho príkazu:

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

(Voliteľné) Program HP Sure Recover obsahuje funkciu na obnovu konkrétneho vydania z obrazu s viacerými indexmi, a to na základe vydania systému Windows pôvodne licencovaného pre cieľový systém HP od výrobcu. Tento mechanizmus funguje, ak sú indexy pomenované správne. Ak inštalačný obraz systému Windows pochádza z obrazu HP OSDVD, pravdepodobne máte obraz s viacerými vydaniami. Ak si neželáte toto správanie a chcete zabezpečiť používanie jedného konkrétneho vydania pre všetky cieľové systémy, musíte sa uistiť, že v inštalačnom obraze je len jeden index.

4. Skontrolujte obsah inštalačného obrazu pomocou nasledujúceho príkazu:

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

   Nasleduje vzorový výstup z inštalačného obrazu, ktorý podporuje päť vydaní (na porovnanie podľa systému BIOS jednotlivých cieľových systémov):

   Podrobné informácie o obraze: `my-image.wim`

   Index: `1`

   Názov: `CoreSingleLanguage`

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

   Veľkosť: `19,512,500,682 bytes`

   Index: `2`

   Názov: `Core`

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

   Veľkosť: `19,512,500,682 bytes`

   Index: `3`

   Názov: `Professional`

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

   Veľkosť: `19.758,019,520 bytes`

   Index: `4`

   Názov: `ProfessionalEducation`

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

   Veľkosť: `19,758,019,480 bytes`

   Index: `5`

   Názov: `ProfessionalWorkstation`

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

   Veľkosť: `19,758,023,576 bytes`

POZNÁMKA: Ak je k dispozícii len jeden index, obraz sa použije na obnovu bez ohľadu na názov. Veľkosť súboru obrazu môže byť väčšia ako pred odstráneniami.

5. Ak nechcete správanie s viacerými vydaniami, odstráňte všetky neželané indexy.

   Ako je uvedené v nasledujúcom príklade, ak chcete len vydanie Professional (za predpokladu, že všetky cieľové systémy majú licenciu), odstráňte indexy 5, 4, 2 a 1. Pri každom odstránení indexu sa čísla indexov priradia znova. Preto by ste mali odstraňovať od najväčšieho po najmenšie číslo indexu. Po každom odstránení spustite príkaz `Get-ImageInfo` na vizuálne potvrdenie indexu, ktorý budete odstraňovať ako ďalší.

   ```
   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
   ```

   Vyberte len jeden index vydania (v tomto príklade Professional). Ak je k dispozícii len jeden index, obraz sa použije na obnovu bez ohľadu na názov. Veľkosť súboru obrazu môže byť väčšia ako pred odstráneniami v dôsledku spôsobu fungovania úprav metadát a štandardizácie obsahu WIM.

6. (Voliteľné) Ak chcete do firemného obnovovacieho obrazu zahrnúť ovládače, postupujte podľa týchto krokov:

   a. Obraz pripojte k prázdnemu priečinku pomocou nasledujúcich príkazov:

   ```
   mkdir C:\staging\mount

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

   b. Pripojte príslušný disk HP Windows 10 Driver DVD (DRDVD) pre podporovaný cieľový systém. Z pripojeného média s ovládačmi skopírujte podpriečinky s ovládačmi do pracovnej oblasti pomocou nasledujúceho príkazu:

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

   POZNÁMKA: Písmeno `<M:>` označuje pripojenú jednotku. Nahraďte ho správnym písmenom jednotky.

   Ďalšie ovládače vo formáte .inf môžete zahrnúť ich umiestnením do priečinka C:\staging\mount \SWSETUP\DRV. Vysvetlenie spôsobu spracovania tohto obsahu programom HP Sure Recover pomocou funkcie `dism /Add-Driver /Recurse` nájdete v časti „Pridanie a odstránenie ovládačov z obrazu systému Windows v režime offline“ v nasledujúcej téme: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Táto funkcia nepodporuje ovládače vo formáte .exe, ktoré vyžadujú spustenie aplikácie.

   c. Uložte zmeny a odpojte obraz pomocou nasledujúceho príkazu:

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

   Výsledný súbor obrazu je: C:\staging\my-image.wim.

   d. Prejdite na lokalitu Rozdelenie obrazu na strane 6.

Príklad 2: Vytvorenie obrazu na základe referenčného systému

1. Vytvorte spustiteľné médium USB WinPE.

POZNÁMKA: Ďalšie spôsoby zachytenia obrazu možno nájsť v dokumentácii súpravy ADK.

Uistite sa, že jednotka USB má dostatok voľného miesta na uloženie zachyteného obrazu z referenčného systému.

2. Vytvorte obraz v referenčnom systéme.
3. Zachyťte obraz spustením referenčného systému pomocou média USB WinPE a potom použite príkaz DISM.

POZNÁMKA: Písmeno `<U:>` označuje jednotku USB. Nahraďte ho správnym písmenom jednotky.

V prípade potreby upravte časť názvu súboru „my-image“ a popis `<my-image>`.

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

4. Skopírujte obraz z jednotky USB do pracovnej oblasti v pracovnom systéme pomocou nasledujúceho príkazu:

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

Mali by ste mať nasledujúci súbor s obrazom: C:\staging\my-image.wim.

5. Prejdite na lokalitu Rozdelenie obrazu na strane 6.

Rozdelenie obrazu

Spoločnosť HP odporúča rozdeliť obraz na menšie súbory, aby sa zlepšila spoľahlivosť preberania v sieti. Použite nasledujúci príkaz:

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

POZNÁMKA: Parameter FileSize sa zobrazuje v megabajtoch. Upravte ho podľa potreby.

POZNÁMKA: Vzhľadom na povahu algoritmu rozdelenia DISM je možné, že veľkosti generovaných súborov SWM budú menšie alebo väčšie ako uvedená veľkosť súboru.

Vytvorenie manifestu

Formátujte súbory manifestu vo formáte UTF-8 bez značky poradia bajtov (BOM).

Môžete zmeniť názov súboru manifestu (custom.mft), ktorý sa používa v nasledujúcich postupoch. Nesmiete však zmeniť prípony .mft a .sig a časť názvu súboru manifestu sa musí zhodovať so súbormi podpisu. Môžete napríklad zmeniť dvojicu (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

`mft_version` sa používa na určenie formátu súboru obrazu a aktuálne musí byť nastavený na 1.

`image_version` sa používa na určenie, či je k dispozícii novšia verzia obrazu, a na zabránenie v inštalácii starších verzií.

Obe hodnoty musia byť nepodpísané 16-bitové celé čísla a ako oddeľovač riadkov sa musí v manifeste používať `\r\n (CR + LF)`.

Generovanie manifestu

Rozdelený obraz sa môže týkať niekoľkých súborov, a preto pomocou skriptu PowerShell vygenerujte manifest.

Vo všetkých zostávajúcich krokoch musíte byť v priečinku C:\staging.

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

1. Vytvorte skript PowerShell pomocou editora, ktorý dokáže vytvoriť textový súbor vo formáte UTF-8 bez značky BOM. Použite nasledujúci príkaz: `notepad C:\staging\generate-manifest.ps1`

   Vytvorte nasledujúci skript:

```
$mftFilename = "custom.mft"

$imageVersion = 1907
```

(Poznámka: Môže ísť o ľubovoľné 16-bitové celé číslo.)

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

}
```

POZNÁMKA: Manifesty pre program HP Sure Recover nemôžu obsahovať značku BOM, takže nasledujúce príkazy prepíšu súbor na formát UTF8 bez značky BOM.

```
$content = Get-Content $mftFilename

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

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

2. Uložte skript.
3. Spustite skript.

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

Vytvorenie podpisu manifestu

Program Sure Recover overuje agenta a obraz pomocou kryptografických podpisov. Nasledujúce príklady používajú dvojicu súkromného/verejného kľúča vo formáte X.509 PEM (prípona .PEM). Podľa potreby upravte príkazy, aby sa mohli používať binárne certifikáty DER (prípona .CER alebo .CRT), certifikáty PEM s kódovaním BASE-64 (prípona .CER alebo .CRT) alebo súbory PKCS1 PEM (prípona .PEM). Príklad používa aj riešenie OpenSSL, ktoré generuje podpisy vo formáte Big Endian. Manifesty môžete podpísať pomocou ľubovoľného nástroja, ale niektoré verzie systému BIOS podporujú len podpisy vo formáte Little Endian.

1. Vygenerujte 2048-bitový súkromný kľúč RSA pomocou nasledujúceho príkazu. Ak máte 2048-bitovú dvojicu súkromného/verejného kľúča RSA vo formáte PEM, skopírujte kľúče do priečinka C:\staging a prejdite na krok 3.

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

2. Vygenerujte verejný kľúč zo súkromného kľúča (ak máte verejný kľúč zodpovedajúci súkromnému kľúču vo formáte PEM, skopírujte ho do priečinka C:\staging) pomocou nasledujúceho príkazu:

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

3. Vytvorte súbor podpisu (pomocou hodnoty hash SHA256) na základe 2048-bitového súkromného kľúča RSA z kroku 1 pomocou nasledujúceho príkazu:

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

4. Overte súbor podpisu pomocou verejného kľúča z predchádzajúceho kroku pomocou nasledujúceho príkazu:

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

POZNÁMKA:

- Ak potrebujete vytvoriť len súbor podpisu, požadujú sa kroky 1 a 3.
- V prípade programu HP Sure Recover sa požadujú minimálne kroky 1, 2 a 3. Na poskytnutie cieľového systému potrebujete verejný kľúč z kroku 2.
- Krok 4 je voliteľný, ale odporúča sa, aby sa súbor podpisu a súbor manifestu správne overili.

Hostenie súborov

Na serveri hostite nasledujúce súbory z priečinka C:\staging:

- *.swm
- custom.mft (alebo názov súboru, ktorý ste vybrali pre súbor manifestu)
- custom.sig (alebo zodpovedajúci názov súboru, ktorý ste vybrali pre súbor podpisu)

POZNÁMKA: Ak ako riešenie na hosťovanie používate server IIS, musíte nakonfigurovať položky MIME tak, aby zahŕňali nasledujúce prípony, ktoré sú všetky nakonfigurované ako „application/octet-stream:“

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

Poskytovanie cieľových systémov

Cieľové systémy môžete poskytovať pomocou knižnice HP Client Management Script Library, programu HP Client Security Manager (CSM)/Sure Recover alebo súpravy Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Pre toto poskytovanie poskytnite nasledujúce informácie:

1. Adresa URL súboru manifestu hosťovaného v predchádzajúcej časti (http://váš_server.doména/cesta/custom.mft)
2. Verejný kľúč používaný na overenie súboru podpisu, ktorý bol vytvorený predtým (napríklad C:\staging\my-recovery-public.pem).

Riešenie problémov

Ak sa zobrazí hlásenie, že zlyhalo overenie zabezpečenia procesu vlastnej obnovy, skontrolujte nasledujúce:

1. Manifest musí byť vo formáte UTF-8 bez BOM.
2. Skontrolujte hodnoty hash súborov.
3. Skontrolujte, či bol systém poskytnutý pomocou verejného kľúča, ktorý zodpovedá súkromnému kľúču použitému na podpis manifestu.
4. Typy MIME servera IIS musia byť `application/octet-stream`.
5. Cesty k súborom v rámci manifestu musia obsahovať úplnú cestu k hlavnému adresáru obsahujúcemu obraz, ako sa zobrazuje z klientskeho systému. Táto cesta nie je úplná cesta k miestu uloženia súborov v distribučnom bode.

3 Používanie agenta programu HP Sure Recover za firemnou bránou firewall

Agenta programu HP Sure Recover možno hosťovať na firemnom intranete. Po nainštalovaní balíka HP Sure Recover SoftPaq skopírujte súbory agenta z adresára agenta programu HP Sure Recover v mieste inštalácie do distribučného bodu HTTP alebo FTP. Potom poskytnite klientsky systém pomocou adresy URL distribučného bodu a verejného kľúča spoločnosti HP s názvom `hpsr_agent_public_key.pem`, ktorý sa distribuuje s balíkom SoftPaq agenta programu HP Sure Recover.

Inštalácia agenta programu HP Sure Recover

1. Prevezmite agenta programu HP Sure Recover a extrahujte súbory do distribučného bodu HTTP alebo FTP.
2. Nastavte príslušné povolenia súborov v distribučnom bode.
3. Ak používate server Internet Information Services (IIS), vytvorte typy MIME application/octet-stream pre nasledujúce formáty súborov:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

DÔLEŽITÉ: Nasledujúci postup opisuje poskytovanie programu Sure Recover pomocou aplikácie SCCM. Príklady, ako poskytnúť program Sure Recover pomocou knižnice HP Client Management Script Library, nájdete v časti Práca s knižnicou HP Client Management Script Library (CMSL) na strane 12.

4. Spustite aplikáciu SCCM, prejdite na položku **HP Client Security Suite** a vyberte stránku HP Sure Recover.

POZNÁMKA: Adresa URL distribučného bodu zahŕňa prenosový protokol ftp alebo http. Zahŕňa aj úplnú cestu k hlavnému adresáru obsahujúcemu manifest pre agenta programu HP Sure Recover, ako sa zobrazuje z klientskeho systému. Táto cesta nie je úplná cesta k miestu uloženia súborov v distribučnom bode.

5. V časti **Platform Image** (Obraz platformy) vyberte možnosť **Corporation** (Firma) na obnovenie prispôsobeného obrazu operačného systému z firemného distribučného bodu. Do vstupného poľa **Image Location URL** (Adresa URL umiestnenia obrazu) zadajte adresu URL, ktorú poskytol správca IT. Do poľa **Image Verification** (Overenie obrazu) zadajte verejný kľúč `hpsr_agent_public_key.pem`.

POZNÁMKA: Adresa URL vlastného obrazu musí obsahovať názov súboru manifestu obrazu.

6. V časti **Recovery Agent** (Agent na obnovu) vyberte možnosť **Corporation** (Firma) na použitie vlastného agenta na obnovu alebo agenta na obnovu od spoločnosti HP z firemného distribučného bodu. Do vstupného poľa **Agent Location URL** (Adresa URL umiestnenia agenta) zadajte adresu URL, ktorú poskytol správca IT. Do vstupného poľa **Agent Verification Key** (Kľúč overenia agenta) zadajte verejný kľúč `hpsr_agent_public_key.pem`.

POZNÁMKA: Adresa URL nesmie obsahovať názov súboru pre manifest agenta, pretože systém BIOS vyžaduje názov recovery.mft.

7. Po použití politiky na klientsky systém ho reštartujte.

8. Počas úvodného poskytovania sa zobrazí výzva na zadanie 4-ciferného kódu zabezpečenia na dokončenie aktivácie programu HP Sure Recover. Ak chcete získať ďalšie informácie, prejdite na lokalitu hp.com a vyhľadajte technickú dokumentáciu k súprave HP Manageability Integration Kit (MIK) pre Microsoft System Center Manager.

Po úspešnom aktivovaní programu HP Sure Recover sa vlastná adresa URL použitá politikou bude zobrazovať v ponuke nastavení HP Sure Recover systému BIOS.

Ak chcete skontrolovať úspešnú aktiváciu, reštartujte počítač a po zobrazení loga spoločnosti HP stlačte kláves f10. Postupne vyberte položky **Advanced** (Rozšírené), **HP Sure Recover**, **Recovery Agent** (Agent na obnovu) a **URL**.

4 Práca s knižnicou HP Client Management Script Library (CMSL)

Knižnica HP Client Management Script Library umožňuje spravovať nastavenia programu HP Sure Recover v prostredí PowerShell. Nasledujúci vzorový skript ukazuje, ako poskytnúť, určiť stav, zmeniť konfiguráciu a zrušiť poskytnutie programu HP Sure Recover.

POZNÁMKA: Niektoré príkazy prekračujú dĺžku riadka v tejto príručke, ale musia sa zadávať ako jeden riadok.

```
$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
}
```

Generovanie vzorového kľúča pomocou riešenia OpenSSL

Súkromné kľúče ukladajte na bezpečnom mieste. Verejné kľúče sa použijú na overenie a musia sa poskytnúť počas poskytovania. Tieto kľúče musia mať dĺžku 2048 bitov a používať exponent 0x10001. Predmet v príkladoch nahraďte informáciami o svojej organizácii.

Pred pokračovaním nastavte nasledujúcu premennú prostredia:

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

# Create a self-signed root CA certificate for testing
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

# Create a key endorsement certificate
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"
```

```
openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:


# Create a command signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:


# Create an image signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Manifest obrazu môžete podpísať pomocou tohto príkazu:

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


# Create an agent signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Manifest agenta môžete podpísať pomocou tohto príkazu:

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

OpenSSL generuje súbory podpisu vo formáte Big Endian, ktorý je nekompatibilný s niektorými verziami systému BIOS, takže pred nasadením sa môže požadovať obrátenie poradia bajtov súboru podpisu agenta. Verzie systému BIOS, ktoré podporujú poradie bajtov Big Endian, podporujú aj poradie bajtov Little Endian.

A Riešenie problémov

Nepodarilo sa vytvoriť oddiely na jednotke

Ak je oblasť SR_AED alebo SR_IMAGE zašifrovaná pomocou funkcie BitLocker, vytvorenie oddielov môže zlyhať. Tieto oddiely sa zvyčajne vytvárajú pomocou atribútu GPT, ktorý zabraňuje ich šifrovaniu pomocou nástroja BitLocker. Ak však používateľ odstráni a vytvorí oddiely znova alebo ich vytvorí manuálne na jednotke nevyžadujúcej operačný systém, agent programu Sure Recover ich nedokáže odstrániť a pri zmene oddielov jednotky skončí s chybou. Používateľ ich musí odstrániť manuálne spustením aplikácie diskpart, výberom zväzku a spustením príkazu prepísania `del vol` alebo podobného príkazu.

Denník auditu firmvéru

Informácie o premennej EFI sú nasledujúce:

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

V systéme Windows existujú rozhrania API na čítanie premenných EFI alebo môžete vytvoriť výpis obsahu premenných do súboru pomocou nástroja UEFI Shell dmpstore.

Z denníka auditu môžete vytvoriť výpis pomocou príkazu `Get-HPFirmwareAuditLog`, ktorý je súčasťou knižnice HP Client Management Script Library.

Denník udalostí systému Windows

Udalosti spustenia a zastavenia programu Sure Recover sa odosielajú do denníka auditu systému BIOS, ktorý môžete zobraziť v Zobrazovači udalostí systému Windows v denníku Sure Start, ak je nainštalovaný program HP Notifications. Súčasťou týchto udalostí je dátum a čas, identifikátor zdroja, identifikátor udalosti a špecifický kód udalosti. Kód `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` napríklad označuje, že obnovenie zlyhalo, pretože manifest nebolo možné overiť pomocou špecifického kódu udalosti c3f 23000, ktorý bol prihlásený 27.6.2018 o 2:26:40.

POZNÁMKA: Tieto denníky používajú americký formát mesiac/dátum/rok.

HP Secure Platform Management (identifikátor zdroja = 84h)

Tabuľka A-1 HP Secure Platform Management

Identifikátor udalosti	Počet zariadení (všetky/DaaS)	Počet udalostí (všetky/DaaS)	Popis	Poznámky
40	256/178	943/552	Proces obnovy platformy operačného systému bol spustený firmvérom.	Obnova platformy sa spustila

Tabuľka A-1 HP Secure Platform Management (pokračovanie)

Identifikátor udalosti	Počet zariadení (všetky/DaaS)	Počet udalostí (všetky/DaaS)	Popis	Poznámky
41	221/147	588/332	Proces obnovy platformy operačného systému sa úspešne dokončil.	Obnova platformy sa dokončila
42	54/42	252/156	Proces obnovy platformy operačného systému sa nepodarilo úspešne dokončiť.	Obnova platformy zlyhala

Denník auditu firmvéru môžete načítať pomocou príkazu Get-HPFirmwareAuditLog v knižnici HP Client Management Script Library, ktorá je k dispozícii na lokalite http://www.hp.com/go/clientmanagement. Identifikátory udalostí 40, 41 a 42 v aplikácii HP Secure Platform Management vrátia špecifické kódy udalostí v údajovom poli, ktoré označujú výsledok operácií programu Sure Recover. Napríklad nasledujúca položka denníka označuje, že programu Sure Recover sa nepodarilo prevziať súbor manifestu alebo podpisu s chybou event_id 42 a údajmi: 00:30:f1:c3, ktoré by sa mali interpretovať ako hodnota DWORD 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:30:f1:c3
```

Úspešné obnovenie sa zobrazuje ako event_id = 41 a data: 00:00:00:00, napríklad:

```
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
```

Program HP Sure Recover používa nasledujúce špecifické kódy udalostí.

Tabuľka A-2 Špecifické kódy udalostí

Popis udalosti	Kód udalosti
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

Uživatelská příručka

HP Sure Recover

První vydání: únor 2020

Číslo dokumentu: L93434-221

Formátování uživatelských vstupů

Text, který musíte zadat do uživatelského rozhraní, je označen `neproporcionálním písmem`.

Tabulka -1 Formátování uživatelských vstupů

Položka	Popis
`Text bez závorek`	Položky musíte zadávat tak, jak jsou zobrazeny
`<Text uvnitř ostrých závorek>`	Zástupný objekt pro hodnotu, kterou musíte zadat; vynechte závorky
`[Text uvnitř hranatých závorek]`	Volitelné položky; vynechte závorky
`{Text uvnitř složených závorek}`	Sada položek, ze které si musíte vybrat jen jednu; vynechte závorky
`|`	Oddělovač položek, ze kterých si musíte vybrat jen jednu; vynechte svislou čáru
`...`	Položky, které se mohou nebo musí opakovat; vynechte výpustku

Obsah

1 Začínáme

Software HP Sure Recover vám pomůže bezpečně nainstalovat operační systém ze sítě s minimálním zásahem uživatele. Systémy s technologií HP Sure Recover s technologií Embedded Reimaging také podporují instalaci z místního paměťového zařízení.

DŮLEŽITÉ: Než použijete nástroj HP Sure Recover, zálohujte data. Vzhledem k tomu, že proces obnovení z bitové kopie disku přeformátuje jednotku, dojde ke ztrátě dat.

Bitové kopie pro obnovení, které společnost HP poskytuje, obsahují základní instalační soubor systému Windows 10®. V případě potřeby může nástroj HP Sure Recover nainstalovat optimalizované ovladače pro zařízení HP. Bitové kopie nástroje HP Recovery obsahují pouze agenty obnovování dat, které jsou součástí systému Windows 10, jako je OneDrive. Korporace mohou vytvářet své vlastní bitové kopie, které slouží k přidání korporátních nastavení, aplikací, ovladačů a agentů obnovování dat.

Agent obnovování operačního systému (OS) provádí kroky nezbytné k instalaci bitové kopie pro zotavení. Agent obnovování poskytovaný společností HP provádí běžné kroky, jako je vytváření oddílů, formátování a extrahování bitové kopie pro zotavení na cílové zařízení. Vzhledem k tomu, že agent obnovování HP je umístěn na webové stránce hp.com, budete k jeho získání potřebovat přístup k internetu, pokud systém nezahrnuje technologii Embedded Reimaging. Společnosti mohou také hostovat agenta obnovování HP v rámci jejich brány firewall nebo vytvořit vlastní agenty obnovování pro složitější prostředí obnovení.

Pokud není nalezen žádný operační systém, můžete aktivovat nástroj HP Sure Recover. Můžete také spustit nástroj HP Sure Recover podle plánu, např. abyste se ujistili, že došlo k odstranění malwaru. Proveďte konfiguraci těchto nastavení prostřednictvím nástroje HP Client Security Manager (CSM), Management Integration Kit (MIK) nebo knihovny HP Client Management Script Library.

Obnovení ze sítě

POZNÁMKA: Chcete-li provést obnovení ze sítě, musíte použít kabelové připojení. Společnost HP doporučuje před použitím nástroje HP Sure Recover zálohovat důležité soubory, data, fotografie, videa a tak dále, aby nedošlo ke ztrátě dat.

1. Připojte klientský systém k síti, ve které je přístup k distribučnímu bodu HTTP nebo FTP.
2. Restartujte systém klienta a jakmile se zobrazí logo HP, stiskněte klávesu f11.
3. Vyberte položku **Obnovení ze sítě**.

Obnovení z místní jednotky

Pokud systém klienta podporuje funkci Embedded Reimaging a naplánovaná bitová kopie je povolena v použitých zásadách, pak se bitová kopie stáhne do klientského systému v naplánovaném čase. Po stažení bitové kopie do klientského systému jej restartujte, aby se obraz zkopíroval do paměťového zařízení s funkcí Embedded Reimaging.

Chcete-li provést místní obnovení pomocí bitové kopie na paměťovém zařízení s funkcí Embedded Reimaging, postupujte takto:

1. Restartujte systém klienta a jakmile se zobrazí logo HP, stiskněte klávesu f11.
2. Vyberte položku **Obnovení z místní jednotky**.

Systémy s funkcí Embedded Reimaging musí konfigurovat plán stahování a používat agenta stahování ke kontrole aktualizací. Agent stahování je obsažen v doplňku HP Sure Recover pro nástroj HP Client Security Manager a může být také konfigurován v MIK. Pokyny k použití MIK naleznete v části https://www.hp.com/go/clientmanagement.

Můžete také vytvořit naplánovanou úlohu, která bude kopírovat agenta do oddílu SR_AED a bitové kopie do oddílu SR_IMAGE. Poté můžete použít nástroj HP Client Management Library a odeslat servisní událost informující systém BIOS, že by měl ověřit obsah a zkopírovat jej na paměťové zařízení s technologií Embedded Reimaging při příštím restartu.

2 Vytvoření korporátní bitové kopie

Většina společností používá nástroje Microsoft Deployment, Windows 10 Assessment and Deployment Kit nebo obojí k výrobě souborů obsahujících bitovou kopii v archivu formátu souborů WIM (Windows Imaging).

Požadavky

- Nejnovější verze Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (nebo jiné řešení pro generování páru soukromého/veřejného klíče RSA)

  Slouží ke generování páru klíčů RSA, který se používá k zajištění integrity korporátní bitové kopie, kterou vytváříte a hostujete.
- Server hostující řešení (například Microsoft Internet Information Services [IIS])

Vytvoření bitové kopie

Před zahájením procesu vytváření bitové kopie nastavte pracovní systém nebo systém sestavení, kde jste nainstalovali požadované nástroje, abyste se připravili na zpracování bitové kopie, jak je znázorněno v následujících krocích:

1. Jako správce otevřete příkazový řádek nástroje `Deployment and Imaging` (nainstalován s nástroji pro nasazení systému Windows ADK).
2. Vytvořte pracovní oblast pro bitovou kopii pomocí následujícího příkazu:

   ```
   mkdir C:\staging
   ```
3. Vytvořte bitovou kopii pomocí jednoho z následujících příkladů:

   Příklad 1: Vytvoření bitové kopie založené na bitové kopii instalace systému Microsoft Windows na stránce 3

   Příklad 2: Vytvoření bitové kopie založené na referenčním systému na stránce 5

Příklad 1: Vytvoření bitové kopie založené na bitové kopii instalace systému Microsoft Windows

1. Vložte nebo otevřete bitovou kopii instalace systému Microsoft Windows (z aplikace Microsoft ISO nebo z aplikace HP OSDVD).
2. Z vložené bitové kopie instalace systému Windows zkopírujte soubor install.wim do pracovní oblasti pomocí následujícího příkazu:

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

   POZNÁMKA: `< M: >` odkazuje na vloženou jednotku. Nahraďte správným písmenem jednotky.
3. Přejmenujte soubor install. wim na název souboru bitové kopie („My-Image“ pro tento příklad) pomocí následujícího příkazu:

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

(Volitelné) Software HP Sure Recover obsahuje funkci pro obnovení konkrétní edice z bitové kopie s více indexy, která je založena na edici Windows původně licencované pro cílový systém HP u výrobce. Tento mechanismus funguje, pokud jsou indexy správně pojmenovány. Pokud vaše bitová kopie instalace systému Windows pochází z bitové kopie HP OSDVD, budete pravděpodobně mít bitovou kopii s více edicemi. Pokud si to nepřejete a chcete zajistit, aby byla jedna konkrétní edice použita pro všechny cílové systémy, musíte mít jistotu, že bitová kopie instalace bude mít pouze jeden index.

4. Zkontrolujte obsah bitové kopie instalace pomocí následujícího příkazu:

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

   Následující příklad zobrazuje ukázkový výstup z bitové kopie instalace, která podporuje pět edic (bude odpovídat podle systému BIOS každého cílového systému):

   Podrobnosti o bitové kopii: `my-image.wim`

   Index: `1`

   Název: `CoreSingleLanguage`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Home Single Language`

   Velikost: `19 512 500 682 bajtů`

   Index: `2`

   Název: `Core`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Home`

   Velikost: `19 512 500 682 bajtů`

   Index: `3`

   Název: `Professional`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional`

   Velikost: `19 758 019 520 bajtů`

   Index: `4`

   Název: `ProfessionalEducation`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional Education`

   Velikost: `19 758 019 480 bajtů`

   Index: `5`

   Název: `ProfessionalWorkstation`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional Workstation`

   Velikost: `19 758 023 576 bajtů`

POZNÁMKA: Je-li k dispozici pouze jeden index, bitová kopie bude použita pro obnovení bez ohledu na název. Velikost souboru bitové kopie může být větší než před odstraněním.

5. Pokud nechcete více edic, odstraňte každý index, který nechcete.

   Jak je znázorněno v následujícím příkladu, pokud chcete pouze edici Professional (za předpokladu, že jsou všechny cílové systémy licencovány), odstraňte index 5, 4, 2 a 1. Pokaždé, když odstraníte index, budou čísla indexu znovu přiřazena. Proto byste měli odstraňovat indexy od nejvyššího po nejnižší číslo. Po každém odstranění spusťte příkaz `Get-ImageInfo`, abyste vizuálně potvrdili, který index budete dále odstraňovat.

   ```
   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
   ```

   Zvolte pouze jeden index edice (například Professional). Je-li k dispozici pouze jeden index, bitová kopie bude použita pro obnovení bez ohledu na název. Uvědomte si, že velikost souboru bitové kopie může být větší než před odstraněním kvůli způsobu, jakým se provádějí změny metadat WIM a normalizace obsahu.

6. (Volitelné) Chcete-li zahrnout ovladače do korporátní bitové kopie pro obnovení, postupujte následovně:

   a. Bitovou kopii vložte do prázdné složky pomocí následujících příkazů:

   ```
   mkdir C:\staging\mount

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

   b. Vložte příslušný disk DVD s ovladači HP Windows 10 (DRDVD) pro podporovaný cílový systém. Z vložených médií ovladače zkopírujte podsložky ovladače do své pracovní oblasti pomocí následujícího příkazu:

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

   POZNÁMKA: `< M: >` odkazuje na vloženou jednotku. Nahraďte správným písmenem jednotky.

   Do složky C:\staging\mount\SWSETUP\DRV můžete umístit další ovladače typu .inf. Chcete-li získat vysvětlení o tom, jak je tento obsah zpracován nástrojem HP Sure Recover pomocí funkce `dism /Add-Driver /Recurse`, přečtěte si část „Přidání a odebrání ovladačů do offline bitové kopie systému Windows" v následujícím tématu: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Tato funkce nepodporuje ovladače typu .exe, které vyžadují spuštění aplikace.

   c. Uložte změny a odpojte bitovou kopii pomocí následujícího příkazu:

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

   Výsledný soubor bitové kopie je: C:\staging\my-image.wim.

   d. Přejděte na Rozdělení bitové kopie na stránce 6.

Příklad 2: Vytvoření bitové kopie založené na referenčním systému

1. Vytvořte spustitelné médium USB WinPE.

POZNÁMKA: Další metody snímání bitové kopie naleznete v dokumentaci ADK.

Ujistěte se, zda je na jednotce USB dostatek volného místa pro uložení vytvořené bitové kopie z referenčního systému.

2. Vytvoření bitové kopie z referenčního systému
3. Bitovou kopii vytvořte spuštěním referenčního systému s médiem USB WinPE a poté použijte nástroj DISM.

POZNÁMKA: `< U: >` odkazuje na jednotku USB. Nahraďte správným písmenem jednotky.

Podle potřeby upravte část názvu souboru „my-image" a popis `<my-image>`.

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

4. Zkopírujte bitovou kopii z paměťového zařízení USB do pracovní oblasti vašeho pracovního systému pomocí následujícího příkazu:

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

   Měli byste mít následující soubor bitové kopie: C:\staging\my-image.wim.

5. Přejděte na Rozdělení bitové kopie na stránce 6.

Rozdělení bitové kopie

Společnost HP doporučuje, abyste pomocí následujícího příkazu rozdělili bitovou kopii na menší soubory a zlepšili tak spolehlivost stahování ze sítě:

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

POZNÁMKA: Velikost souboru je uvedena v megabajtech. Podle potřeby upravte.

POZNÁMKA: Vzhledem k povaze algoritmu rozdělování DISM může být velikost generovaných souborů SWM menší nebo větší než uvedená velikost souboru.

Vytvoření manifestu

Zformátujte soubory manifestu jako UTF-8 bez značky pořadí bajtů (BOM).

Můžete změnit název souboru manifestu (custom.mft), který se používá v následujících postupech, ale nesmíte měnit přípony .mft a .sig a název souboru části manifestu a podpisu se musí shodovat. Můžete například změnit pár (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

`mft_version` se používá k určení formátu souboru bitové kopie a musí být aktuálně nastaven na hodnotu 1.

`image_version` se používá k určení, zda je k dispozici novější verze bitové kopie a k zabránění instalace starších verzí.

Obě hodnoty musí být 16bitová celá čísla bez znaménka a oddělovač řádků v manifestu musí být `'\r\n'` `(CR + LF)`.

Generování manifestu

Vzhledem k tomu, že součástí rozdělené bitové kopie může být několik souborů, vygenerujte manifest pomocí skriptu PowerShell.

U všech zbývajících kroků musíte být ve složce C:\staging.

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

1. Vytvořte skript PowerShell pomocí editoru, který může vytvořit textový soubor ve formátu UTF-8 bez BOM, a to pomocí následujícího příkazu: `notepad C:\staging\generate-manifest.ps1`

   Vytvořte následující skript:

```
$mftFilename = "custom.mft"
$imageVersion = 1907 (Poznámka: Může to být libovolné 16bitové celé číslo)


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

POZNÁMKA: Manifesty pro nástroj HP Sure Recover nemohou obsahovat BOM, takže následující příkazy přepisují soubor jako UTF8 bez BOM.

```
$content = Get-Content $mftFilename

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

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

2. Uložte skript.
3. Spusťte skript.

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

Generování podpisu manifestu

Nástroj Sure Recovery ověřuje agenta a bitovou kopii pomocí kryptografických podpisů. Následující příklady používají pár soukromých/veřejných klíčů ve formátu X.509 PEM (přípona.PEM). Podle potřeby upravte příkazy pro použití binárních certifikátů DER (přípony .CER nebo.CRT), kódovaných certifikátů BASE-64 PEM (přípony .CER nebo. CRT), nebo souborů PKCS1 PEM (přípona. PEM). Příklad také používá OpenSSL, který generuje podpisy ve formátu big-endian. K podepisování manifestů můžete použít libovolný nástroj, ale některé verze systému BIOS podporují pouze podpisy ve formátu little endian.

1. Pomocí následujícího příkazu vygenerujte soukromý klíč RSA 2048 bajtů. Máte-li ve formátu .pem pár soukromých/veřejných klíčů 2048 bajtů RSA, zkopírujte jej do C:\staging a poté přejděte ke kroku 3.

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

2. Vygenerujte veřejný klíč z vašeho soukromého klíče (pokud máte veřejný klíč odpovídající vašemu soukromému klíči ve formátu PEM, zkopírujte jej do C:\staging) pomocí následujícího příkazu:

   ```
   OpenSSL RSA-in my-Recovery-Private. pem-pubout-out my-Recovery-Public.
   pem
   ```

3. Vytvořte soubor s podpisem (pomocí hash algoritmu SHA256) na základě soukromého klíče RSA 2048 bajtů z kroku 1 pomocí následujícího příkazu:

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

4. Ověřte soubor s podpisem pomocí veřejného klíče z předchozího kroku pomocí následujícího příkazu:

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

POZNÁMKA:

- Pokud potřebujete vytvořit pouze soubor s podpisem, jsou požadované kroky 1 a 3.
- Pro nástroj HP Sure Recover jsou minimální požadované kroky 1, 2 a 3. Pro zajištění cílového systému budete potřebovat veřejný klíč z kroku 2.
- Krok 4 je volitelný, ale doporučuje se, aby soubor s podpisem a soubor manifestu správně ověřovaly.

Hostování souborů

Na serveru hostujte následující soubory ze složky C:\staging:

- *.swm
- custom.mft (nebo název souboru, který jste zvolili pro soubor manifestu)
- custom.sig (nebo odpovídající název souboru, který jste zvolili pro soubor signatury)

POZNÁMKA: Pokud používáte službu IIS jako své hostitelské řešení, musíte nakonfigurovat položky MIME tak, aby obsahovaly následující přípony, které jsou všechny konfigurovány jako „aplikace/octet-stream:“

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

Zřízení cílových systémů

Své cílové systémy můžete zřídit pomocí nástrojů HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover nebo Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Pro toto zřízení uveďte následující informace:

1. Adresa URL souboru manifestu hostovaného v předchozí části (http://your_server.domain/path/custom.mft)
2. Veřejný klíč použitý k ověření dříve vytvořeného souboru s podpisem (například C:\staging\my-recovery-public.pem).

Odstraňování potíží

Pokud se zobrazí zpráva o procesu vlastního obnovení, který selhal při ověřování zabezpečení, zkontrolujte následující:

1. Manifest musí být UTF-8 bez BOM.
2. Zkontrolujte hash soubory.
3. Zkontrolujte, zda byl systém zřízen s veřejným klíčem odpovídajícím soukromému klíči používanému k podepsání manifestu.
4. Typy MIME serveru služby IIS musí být `application/octet-stream`.
5. Cesty k souborům v rámci manifestu musí obsahovat úplnou cestu k vrchnímu adresáři s bitovou kopií, jak je vidět ze systému klienta. Tato cesta nepředstavuje úplnou cestu, kde se soubory ukládají v distribučním bodě.

3 Použití nástroje HP Sure Recover Agent v rámci korporátního firewallu

Nástroj HP Sure Recover Agent může být hostován v korporátní síti intranet. Po instalaci HP Sure Recover SoftPaq zkopírujte soubory agenta z adresáře HP Sure Recover Agent z umístění instalace do distribučního bodu HTTP nebo FTP. Poté zřiďte systém klienta s adresou URL distribučního bodu a veřejným klíčem HP nazvaným `hpsr_agent_public_key. pem`, který je distribuován s agentem HP Sure Recover SoftPaq.

Instalace agenta HP Sure Recover

1. Stáhněte si agenta HP Sure Recover a rozbalte soubory do distribučního bodu HTTP nebo FTP.
2. Nastavte odpovídající oprávnění pro soubory na distribučním bodu.
3. Pokud používáte internetovou informační službu (IIS), vytvořte typy application/octet-stream pro následující formáty souborů:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   DŮLEŽITÉ: Následující kroky popisují zajištění nástroje Sure Recover pomocí SCCM. Příklady zajištění nástroje Sure Recover pomocí nástroje HP Client Management Script Library naleznete v části Práce s nástrojem HP Client Management Script Library (CMSL) na stránce 12.
4. Spusťte nástroj SCCM, přejděte na položku **HP Client Security Suite** a poté vyberte stránku HP Sure Recover.

   POZNÁMKA: Adresa URL distribučního bodu obsahuje jako protokol přenosu buď ftp nebo http. Obsahuje také úplnou cestu k vrchnímu adresáři, který obsahuje manifest pro agenta HP Sure Recover, jak je vidět z klientského systému. Tato cesta nepředstavuje úplnou cestu k umístění souborů v distribučním bodu.
5. V části **Platform Image** (Platforma bitové kopie) vyberte možnost **Corporate** (Korporátní), která obnoví bitovou kopii operačního systému z korporátního distribučního bodu. Zadejte adresu URL poskytnutou správcem IT do pole **Image Location URL** (Adresa URL umístění bitové kopie). Do pole **Image Verification** (Ověření bitové kopie) zadejte veřejný klíč `hpsr_agent_public_key. pem`.

   POZNÁMKA: Adresa URL vlastní bitové kopie musí obsahovat název souboru manifestu bitové kopie.
6. V části **Recovery Agent** (Agent obnovování) vyberte možnost **Corporation** (Korporátní), abyste mohli používali vlastního agenta obnovení nebo agenta obnovení HP z podnikového distribučního bodu. Zadejte adresu URL poskytnutou správcem IT do pole **Agent Location URL** (URL adresa umístění

agenta). Zadejte veřejný klíč `hpsr_agent_public_key.pem` do pole **Agent Verification Key** (Klíč k ověření agenta).

POZNÁMKA: Nezahrnujte název souboru manifestu agenta do adresy URL, protože systém BIOS vyžaduje, aby byl pojmenován recovery.mft.

7. Po použití zásady na systém klienta proveďte jeho restart.
8. Během úvodního zajišťování se zobrazí výzva k zadání bezpečnostního kódu se čtyřmi číslicemi, aby bylo možno dokončit aktivaci nástroje HP Sure Recover. Chcete-li získat další informace, přejděte na web hp.com a vyhledejte dokument HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

Po úspěšném dokončení aktivace nástroje HP Sure Recover se v nabídce nastavení nástroje HP Sure Recover BIOS zobrazí vlastní adresa URL aplikovaná zásadami.

Chcete-li potvrdit úspěšnost aktivace, restartujte počítač a jakmile se zobrazí logo HP, stiskněte klávesu f10. Vyberte položku **Advanced** (Pokročilé), vyberte položku **HP Sure Recover**, vyberte položku **Recovery Agent** (Agent obnovení) a poté vyberte položku **URL**.

4 Práce s nástrojem HP Client Management Script Library (CMSL)

Nástroj HP Client Management Script Library umožňuje spravovat nastavení nástroje HP Sure Recover pomocí skriptu PowerShell. Následující příklad skriptu ukazuje, jak zřizovat, určovat stav, měnit konfiguraci a rušit zajištění nástroje HP Sure Recover.

POZNÁMKA: Několik příkazů překračuje délku řádku této příručky, ale musí být zadáno jako jeden řádek.

```
$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
}
```

Generování ukázkových klíčů pomocí OpenSSL

Soukromé klíče uložte na bezpečném místě. Veřejné klíče budou použity k ověření a musí být poskytnuty během zajišťování. Tyto klíče musí být dlouhé 2048 bajtů a musí používat exponent 0x10001. Nahraďte předmět v příkladech informacemi o vaší organizaci.

Než budete pokračovat, nastavte následující proměnnou prostředí:

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

# Vytvoření certifikátu kořenové certifikační autority podepsaného svým držitelem pro testování
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"

# Vytvoření klíče certifikátu potvrzení
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:


# Vytvoření podpisového klíče příkazu

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:


# Vytvoření podpisového klíče bitové kopie

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:
```

Manifest bitové kopie můžete podepsat pomocí tohoto příkazu:

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


# Vytvoření podpisového klíče agenta

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:
```

Manifest agenta můžete podepsat pomocí tohoto příkazu:

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

OpenSSL vytváří soubory podpisů ve formátu big-endian, který není kompatibilní s některými verzemi systému BIOS, takže pořadí bajtů souborů podpisů agenta může být nutné před nasazením stornovat. Verze systému BIOS, které podporují pořadí bytů big-endian, také podporují pořadí bytů little-endian.

A Odstraňování potíží

Rozdělování jednotky se nezdařilo

K selhání rozdělování jednotky může dojít v případě, že je oddíl SR_AED nebo SR_IMAGE zašifrován pomocí nástroje BitLocker. Tyto oddíly jsou obvykle vytvářeny s atributem gpt, který zamezuje nástroji BitLocker jejich šifrování, ale v případě, že uživatel odstraní a znovu vytvoří oddíly nebo je vytvoří ručně na holém kovovém disku, agent Sure Recovery při opětovném rozdělování disku nedokáže odstranit a skočí s chybou. Uživatel je musí ručně odstranit spuštěním nástroje diskpart, výběrem svazku a vykonáním příkazu `del vol` nebo podobného.

Protokol auditu firmwaru

Informace o proměnné EFI jsou následující:

- GUID: `{0xec8feb88, 0xb1d1, 0x4f0f, {0xAB, 0x9F, 0x86, 0xCD, 0xB5, 0x3e, 0xa4, 0x45}}`
- Název: `OsRecoveryInfoLog`

Rozhraní API existují v systému Windows pro čtení proměnných EFI, nebo můžete vypsat proměnný obsah do souboru pomocí nástroje UEFI Shell dmpstore.

Protokol auditu můžete vypsat pomocí příkazu `Get-HPFirmwareAuditLog`, který je součástí knihovny skriptů HP Client Management.

Protokolu událostí systému Windows

Události obnovení spuštění a zastavení nástroje Sure Recover jsou odesílány do protokolu auditu systému BIOS, který lze zobrazit v nástroji Prohlížeč událostí systému Windows v protokolu Sure Start, je-li nainstalována aplikace HP Notifications. Mezi tyto události patří datum a čas, ID zdroje, ID události a specifický kód události. Například `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 F2 C3]` označuje, že obnovení se nezdařilo, protože manifest nelze ověřit pomocí specifického kódu c3f 23000, který byl zaznamenán v 2:26:40 dne 6/27/18.

POZNÁMKA: Tyto protokoly se řídí AMERICKÝM formátem data měsíc/den/rok.

HP Secure Platform Management (zdroj ID = 84h)

Tabulka A-1 HP Secure Platform Management

ID události	Počet zařízení (Vše/DaaS)	Počet událostí (Vše/DaaS)	Popis	Poznámky
40	256/178	943/552	Proces obnovení platformy OS byl spuštěn firmwarem.	Spuštění obnovení platformy

Tabulka A-1 HP Secure Platform Management (pokračování)

ID události	Počet zařízení (Vše/DaaS)	Počet událostí (Vše/DaaS)	Popis	Poznámky
41	221/147	588/332	Proces obnovení platformy OS byl úspěšně dokončen.	Obnovení platformy dokončeno
42	54/42	252/156	Proces obnovení operačního systému platformy se nepodařilo úspěšně dokončit.	Obnovení platformy se nezdařilo

Protokol auditu firmwaru můžete načíst pomocí funkce Get-HPFirmwareAuditLog v nástroji HP Client Management Script Library, který je k dispozici na adrese http://www.hp.com/go/clientmanagement. ID události nástroje HP Secure Platform Management 40, 41 a 42 vrací specifické kódy událostí v datovém poli, které označují výsledek operací nástroje Sure Recover. Například následující položka protokolu indikuje, zda nástroj Sure Recover selhal při stažení souboru manifestu nebo podpisu s chybou event_id 42 a daty: 00:30:f1:c3, což by mělo být interpretováno jako hodnota dword 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

závažnost: Informace

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

časové razítko: 5/27/2019 2:44:18 PM

popis: Proces obnovení operačního systému platformy se nepodařilo úspěšně
dokončit.

data: 00:30:f1:c3
```

Úspěšné obnovení je zobrazeno jako event_id = 41 a daty: 00:00:00:00, například:

```
Specifické kódy událostí

Úspěch = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

závažnost: Informace

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

časové razítko: 5/27/2019 2:55:41 PM

popis: Proces obnovení operačního systému platformy se nepodařilo úspěšně
dokončit.

data: 00:00:00:00
```

Nástroj HP Sure Recover používá následující specifické kódy událostí.

Tabulka A-2 Specifické kódy událostí

Popis události	Kód události
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