

מדריך למשתמש



HP Sure Recover

© Copyright 2020 HP Development Company,
L.P.

Microsoft ו-Windows הם סימנים מסחריים או
סימנים מסחריים רשומים של Microsoft
Corporation בארצות הברית ו/או במדינות אחרות.

תוכנת מחשב חסויה. נדרש רישיון חוקי מחברת HP
לצורך החזקה, שימוש או העתקה. בהתאם לתקנות
FAR 12.211 ו-FAR 12.212, הרישיונות לתוכנות
מחשב מסחריות, לתיעוד לתוכנות מחשב ולנתונים
טכניים של פריטים מסחריים מוענקים לממשלת
ארה"ב במסגרת הרישיון המסחרי הסטנדרטי של
הספק.

המידע הנכלל במסמך זה נתון לשינויים ללא הודעה
מוקדמת. האחריות הבלעדית למוצרים ולשירותים של
HP מפורטת במפורש בכתב האחריות הנלווה למוצרים
ולשירותים אלו. אין להבין מתוך הכתוב לעיל כי תחול
על המוצר אחריות נוספת כלשהי. חברת HP לא תישא
באחריות לשגיאות טכניות או לשגיאות עריכה או
להשמטות הכלולות במסמך זה.

מהדורה ראשונה: פברואר 2020

מק"ט מסמך: L93434-BB1

מקש תחביר של קלט משתמש

טקסט שעליך להזין בממשק משתמש מצוין על-ידי גופן בעל רוחב קבוע.

טבלה 1- מקש תחביר של קלט משתמש

פריט	תיאור
טקסט ללא סוגריים מרובעים או מסולסלים	פריטים שעליך להקליד בדיוק כפי שמוצג
<טקסט בתוך סוגריים זוויתיים>	מציין מיקום עבור ערך שעליך לספק; השמטת הסוגריים
[טקסט בתוך סוגריים מרובעים]	פריטים אופציונליים; השמטת הסוגריים
{טקסט בתוך סוגריים מסולסלים}	סדרה של פריטים שמהם עליך לבחור פריט אחד בלבד; השמטת הסוגריים המסולסלים
	מפריד עבור פריטים שמהם עליך לבחור פריט אחד בלבד; השמטת הקו האנכי
...	פריטים שיכולים או חייבים לחזור על עצמם; השמטת שלוש הנקודות

תוכן העניינים

1	1 צעדים ראשוניים	1
1	ביצוע שחזור רשת	1
1	ביצוע שחזור מכונן מקומי	1
2	2 יצירת תמונה ארגונית	2
2	דרישות	2
2	יצירת התמונה	2
2	דוגמה 1: יצירת תמונה בהתאם לתמונת ההתקנה של Microsoft Windows	2
4	דוגמה 2: יצירת תמונה בהתבסס על מערכת ייחוס	4
5	פיצול התמונה	5
5	יצירת מניפסט	5
5	הפקת המניפסט	5
6	יצירת חתימה למניפסט	6
7	אירוח הקבצים	7
7	הקצאת מערכת היעד	7
8	פתרון בעיות	8
9	3 שימוש בסוכן HP Sure Recover הסוכן בתוך חומת אש ארגונית	9
9	התקנת הסוכן של HP Sure Recover	9
11	4 עבודה עם ספריית הסקריפטים (CMSL) HP Client Management	11
13	יצירת מפתחות דוגמה באמצעות OpenSSL	13
15	נספח א פתרון בעיות	15
15	החלוקה למחיצות של כונן נכשלה	15
15	יומן ביקורת קושחה	15
15	יומן אירועים של Windows	15
15	HP Secure Platform Management (מזהה מקור = 84h)	15

1 צעדים ראשונים

HP Sure Recover מסייע לך להתקין את מערכת ההפעלה מהרשת באופן מאובטח תוך התערבות מינימלית של המשתמש. מערכות התומכות ב-HP Sure Recover עם Embedded Reimaging תומכות גם בהתקנה מהתקן אחסון מקומי.

חשוב: גבה את הנתונים שלך לפני השימוש ב-HP Sure Recover. מאחר שתהליך ההדמיה מאתחל מחדש את הכונן, הדבר כרוך באובדן נתונים.

תמונות השחזור ש-HP מספקת כוללות את תוכנית ההתקנה הבסיסית של Windows 10®. במידת הצורך, HP Sure Recover יכול להתקין מנהלי התקן ממוטבים עבור התקני HP. תמונות השחזור של HP כוללות רק גורמי שחזור נתונים הכלולים במערכת ההפעלה Windows 10, כגון OneDrive. ארגונים יכולים ליצור תמונות מותאמות אישית משלהם כדי להוסיף הגדרות, יישומים, מנהלי התקן וגורמי שחזור נתונים של הארגון.

סוכן שחזור של מערכת ההפעלה (OS) מבצע את הפעולות הנדרשות כדי להתקין את תמונת השחזור. סוכן השחזור המסופק על-ידי HP מבצע פעולות שכיחות כגון חלוקה למחיצות, אתחול וחילוץ תמונת השחזור אל התקן היעד. מאחר שסוכן השחזור של HP נמצא ב-hp.com, נדרשת גישה לאינטרנט כדי לאחזר אותו, אלא אם כן המערכת מכילה תמונת שחזור מובנית. ארגונים יכולים גם לארח את סוכן השחזור של HP בתוך חומת האש שלהם או ליצור גורמי שחזור מותאמים אישית לסביבות שחזור מורכבות יותר.

באפשרותך להפעיל את HP Sure Recover כאשר לא נמצאה מערכת הפעלה. כמו כן, באפשרותך להפעיל את HP Sure Recover לפי לוח זמנים, למשל כדי להבטיח הסרת תוכנות זדוניות. הגדר את התצורה של הגדרות אלה באמצעות HP Client Security Manager (CSM), ערכת (MIK) Manageability Integration Kit, או ספריית הסקריפטים HP Client Management.

ביצוע שחזור רשת

הערה: כדי לבצע שחזור רשת, עליך להשתמש בחיבור קווי. HP ממליצה לגבות קבצים חשובים, נתונים, תמונות, סרטוני וידאו וכדומה לפני השימוש ב-HP Sure Recover כדי למנוע אובדן נתונים.

1. חבר את מערכת הלקוח לרשת שבה יש גישה לנקודת ההפצה באמצעות HTTP או FTP.
2. הפעל מחדש את מערכת הלקוח, ועם הופעת הלוגו של HP, הקש על f11.
3. בחר **שחזור רשת**.

ביצוע שחזור מכונן מקומי

אם מערכת לקוח תומכת בתמונת שחזור מובנית והאפשרות להורדת תמונה מתוזמנת נבחרה במדיניות הפעילה, תתבצע הורדה של התמונה למערכת הלקוח במועד שנקבע. לאחר הורדת התמונה למערכת הלקוח, הפעל אותה מחדש כדי להעתיק את התמונה להתקן האחסון של תמונת השחזור המובנית.

כדי לבצע שחזור מקומי באמצעות התמונה שבהתקן האחסון של תמונת השחזור המובנית:

1. הפעל מחדש את מערכת הלקוח, ועם הופעת הלוגו של HP, הקש על f11.
2. בחר **שחזור מכונן מקומי**.

מערכות עם תמונת שחזור מובנית חייבות להגדיר את לוח זמנים להורדה ולהשתמש בסוכן ההורדה כדי לבדוק אם קיימים עדכונים. סוכן ההורדה מצורף ליישום ה-Plug-in של HP Sure Recover עבור HP Client Security Manager, וביתן להגדיר את תצורתו גם ב-MIK. ראה <https://www.hp.com/go/clientmanagement> לקבלת הוראות לשימוש ב-MIK.

בנוסף, באפשרותך ליצור משימה מתוזמנת כדי להעתיק את הסוכן אל מחיצת SR_AED ואת התמונה אל מחיצת SR_IMAGE. לאחר מכן, באפשרותך להשתמש בספריית הסקריפטים HP Client Management כדי לשלוח אירוע שירות שיוזע ל-BIOS שעליו לאמת את התוכן ולהעתיק אותו להתקן האחסון של תמונת השחזור המובנית באתחול הבא.

2 יצירת תמונה ארגונית

רוב החברות משתמשות בכלי הפריסה של Microsoft, בערכת ההערכה והפריסה של Windows 10, או בשניהם להפקת קבצים הכוללים תמונה בתוך ארכיון בתבנית Windows Imaging (WIM).

דרישות

- גרסה עדכנית של ערכת ההערכה והפריסה של Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (או פתרון אחר ליצירה של צמד מפתחות RSA פרטי/ציבורי)
- השתמש בהם כדי ליצור צמד מפתחות RSA שישמש להבטחת התקינות של התמונה הארגונית שאתה יוצר ומארח.
- פתרון אירוח בשרת (כגון Internet Information Services [IIS] של Microsoft)

יצירת התמונה

לפני שתתחיל בתהליך יצירת התמונה, הגדר את מערכת העבודה או את מערכת הבנייה שבה התקנת את הכלים הדורשים להכנה לעיבוד התמונה, כמודגם בשלבים הבאים:

1. כמנהל מערכת, פתח את שורת הפקודה Deployment and Imaging Tools Environment (סביבת פריסה וכלי תמונת שחזור - מותקנת עם כלי הפריסה ADK של Windows).
2. צור אזור אחסון זמני (staging) עבור התמונה שלך, באמצעות הפקודה הבאה:
`mkdir C:\staging`
3. צור את התמונה באמצעות אחת הדוגמאות הבאות:


[דוגמה 1: יצירת תמונה בהתאם לתמונת ההתקנה של Microsoft Windows בעמוד 2](#)

[דוגמה 2: יצירת תמונה בהתבסס על מערכת ייחוס בעמוד 4](#)

דוגמה 1: יצירת תמונה בהתאם לתמונת ההתקנה של Microsoft Windows

1. טען או פתח את תמונת ההתקנה של Microsoft Windows (מקובץ ISO של Microsoft, או מ-HP OSDVD).
2. מתמונת ההתקנה הטעונה של Windows, העתק את הקובץ `install.wim` לאזור האחסון הזמני שלך, באמצעות הפקודה הבאה:

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

הערה: <M:> מתייחס לכונן הנטען. החלף באות הכונן הנכונה. 

3. שנה את שם הקובץ `install.wim` לשם קובץ תמונה ("my-image" בדוגמה זו), באמצעות הפקודה הבאה:

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

(אופציונלי) HP Sure Recover כולל מאפיין שנועד לשחזר מהדורה מסוימת מתמונה עם multi-index (מספר אינדקסים), בהתבסס על מהדורת Windows שהורשתה במקור למערכת היעד של HP במפעל. מנגנון זה יפעל בתנאי שלאינדקסים ניתנו השמות הנכונים. אם תמונת ההתקנה של Windows מגיעה מתמונת HP OSDVD, יש להניח שברשותך תמונת multiedition (מספר מהדורות). אם אינך מעוניין בהתנהגות זו, וברצונך להבטיח שנעשה שימוש במהדורה מסוימת אחת עבור כל מערכות היעד שלך, עליך לוודא שתמונת ההתקנה כוללת אינדקס אחד בלבד.

4. בדוק את תוכן תמונת ההתקנה באמצעות הפקודה הבאה:

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

הקוד הבא מדגים פלט של תמונת התקנה התומכת בחמש מהדורות (להתאמה בהתאם ל-BIOS של כל מערכת יעד):

פרטי התמונה: my-image.wim

אינדקס: 1

שם: CoreSingleLanguage

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

גודל: 19,512,500,682 בתים

אינדקס: 2

שם: Core

תיאור: Windows 10 May 2019 Update - Home edition

גודל: 19,512,500,682 bytes

אינדקס: 3

שם: Professional

תיאור: Windows 10 May 2019 Update- Professional Update

גודל: 19,758,019,520 bytes

אינדקס: 4

שם: ProfessionalEducation

תיאור: Windows 10 May 2019 Update - Professional Education edition

גודל: 19,758,019,480 bytes

אינדקס: 5

שם: ProfessionalWorkstation

תיאור: Windows 10 May 2019 Update - Professional Workstation edition

גודל: 19,758,023,576 bytes

הערה: כאשר קיים אינדקס אחד בלבד, התמונה משמשת לשחזור, בלי קשר לשם. גודל קובץ התמונה עשוי להיות גדול יותר מאשר לפני המחקיקות.

5. אם אינך מעוניין באופן פעולה של ריבוי מהדורות, מחק כל אינדקס שאינך מעוניין בו.

כמודגם להלן, אם אתה מעוניין במהדורה מקצועית בלבד (בהנחה שכל מערכות היעד מורשות), מחק את אינדקסים 5, 4, 2 ו-1. בכל פעם שאתה מוחק אינדקס, מספרי האינדקס מוקצים מחדש. לכן, עליך למחוק ממספרי האינדקסים הגבוהים יותר לנמוכים יותר. הרץ את הפקודה Get-ImageInfo לאחר כל מחיקה כדי לאשר באופן חזותי את האינדקס שתמחק בפעם הבאה.

```
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
```

בחר רק אינדקס אחד של המהדורה (לדוגמה, Professional). כאשר קיים אינדקס אחד בלבד, התמונה משמשת לשחזור, בלי קשר לשם. שים לב שגודל קובץ התמונה שלך עשוי להיות גדול יותר מאשר לפני המחיקות, בשל אופן הפעולה של שינויי המטא-נתונים ונורמליזציית התוכן של WIM.

6. (אופציונלי) אם ברצונך לכלול מנהלי התקן בתמונת השחזור הארגונית שלך, פעל בהתאם לשלבים הבאים:

א. טען את התמונה בתיקייה ריקה, באמצעות הפקודות הבאות:

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

ב. טען את ה-DVD של מנהל ההתקן (DRDVD) המתאים של HP ל-Windows 10 עבור מערכת היעד הנתמכת. מהמדיה הטעונה של מנהל ההתקן, העתק את תיקיות המשנה של מנהל ההתקן לאזור האחסון הזמני באמצעות הפקודה הבאה:

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

הערה: <M:> מתייחס לכונן הנטען. החלף באות הכונן הנכונה.

באפשרותך לכלול מנהלי התקנים נוספים בסגנון של קובצי inf. על-ידי הצבתם בתיקייה C:\staging\mount\SWSETUP\DRV. לקבלת הסבר על אופן העיבוד של תוכן זה על-ידי HP Sure Recover באמצעות הפונקציה "dism/Add-Driver/Recurse", ראה "הוספה והסרה של מנהלי התקן לתמונת Windows לא מקוונת" בסעיף הבא: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

מאפיין זה אינו תומך במנהלי התקנים בסגנון קובצי exe. המחייבים הפעלת יישום.

ג. שמור את השינויים ובטל את טעינת התמונה באמצעות הפקודה הבאה:

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

קובץ התמונה שהתקבל הוא: C:\staging\my-image.wim.

ד. בקר בכתובת [פיצול התמונה בעמוד 5](#).

דוגמה 2: יצירת תמונה בהתבסס על מערכת ייחוס

1. צור מדיה ניתנת לאתחול מסוג USB WinPE.

הערה: ניתן למצוא שיטות נוספות ללכידת תמונה בתיעוד של ADK.

ודא שכונן ה-USB מכיל מספיק שטח פנוי עבור התמונה שנלכדה ממערכת הייחוס.

2. צור תמונה במערכת ייחוס.

3. לכוד את התמונה על-ידי אתחול מערכת הייחוס עם המדיה של USB WinPE, ולאחר מכן השתמש ב-DISM.

הערה: <U:> מתייחס לכונן ה-USB. החלף באות הכונן הנכונה.

ערוך את החלק "my-image" בשם הקובץ, ואת התיאור של <my-image>, לפי הצורך.

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

4. העתק את התמונה מכונן ה-USB לאזור האחסון הזמני של מערכת העבודה באמצעות הפקודה הבאה:

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


אתה אמור לקבל את קובץ התמונה הבא: C:\staging\my-image.wim.


5. בקר בכתובת [פיצול התמונה בעמוד 5](#).

פיצול התמונה

HP ממליצה לך לפצל את התמונה לקבצים קטנים יותר כדי לשפר את המהימנות של הורדות מהרשת, באמצעות הפקודה הבאה:

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

 **הערה:** FileSize (גודל הקובץ) מוצג במגהבייט. ערוך לפי הצורך.

 **הערה:** בשל אופן פעולת האלגוריתם המפצל של DISM, גודל קובצי ה-SWM שייווצרו עשוי להיות קטן או גדול יותר מגודל הקובץ המבוקש.

יצירת מניפסט

צור את קובצי המניפסט בתבנית UTF-8 ללא תו סימן סדר הסיביות (BOM).

באפשרותך לשנות את שם קובץ המניפסט (custom.mft) המופיע בהליכים הבאים, אך אין לשנות את הסימונים mft ו-sig, וחלק שם הקובץ במניפסט ובקובצי החתימה חייב להיות תואם. לדוגמה, באפשרותך לשנות את צמד השמות (custom.mft, custom.sig) לשמות כמו (myimage.mft, myimage.sig).

mft_version משמש לקביעת התבנית של קובץ התמונה ויש להגדירו בשלב זה כ-1.

image_version משמש כדי לקבוע אם קיימת גרסה חדשה יותר של התמונה ולמנוע התקנה של גרסאות ישנות יותר.

שני הערכים חייבים להיות מספרים שלמים של 16 סיביות ללא סימן, ומפריד השורה במניפסט חייב להיות '\r\n' (CR + LF).

הפקת המניפסט

מאחר שהתמונה המפוצלת שלך עשויה לכלול מספר קבצים, השתמש בסקריפט של powershell כדי ליצור מניפסט.

בכל השלבים הנוגעים, עליך להיות בתיקייה C:\staging.

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

1. צור סקריפט של powershell באמצעות עורך שמסוגל ליצור קובץ טקסט בתבנית UTF-8 ללא תו BOM, עם הפקודה הבאה: notepad C:\staging\generate-manifest.ps1

צור את הסקריפט הבא:

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

```
$imageVersion = 1907 (הערה: זה יכול להיות כל מספר שלם של 16 סיביות)
```

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

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

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

```

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

$spathToManifest = (Resolve-Path ".").Path

$total = $swmFiles.count
$current = 1

$swmFiles | Sort-Object $ToNatural | ForEach-Object {
    Write-Progress
    ` "Activity "Generating manifest-
    ` "($_) Status "$current of $total-
    (PercentComplete ($current / $total * 100-

hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName$
    ()fileHash = $hashObject.Hash.ToLower$
('' ,'\ ' + filePath = $hashObject.Path.Replace($spathToManifest$
    fileSize = (Get-Item $_.FullName).length$
    "manifestContent = "$fileHash $filePath $fileSize$

    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
        $manifestContent -Append
    current = $current + 1$
}

```

הערה: מניפסטים עבור HP Sure Recover לא יכולים לכלול תו BOM, והפקודות הבאות משכתבות את הקובץ כקובץ UTF-8 ללא תו BOM.

```

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

```

2. שמור את הסקריפט.

3. הפעל את הסקריפט.

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

יצירת חתימה למניפסט

Sure Recover מאמת את הסוכן ואת התמונה באמצעות חתימות קריפטוגרפיות. הדוגמאות הבאות משתמשות בצמד מפתחות פרטי/ציבורי בתבנית PEM 509 X. (סימנת PEM). התאם את הפקודות לפי העניין לשימוש באישורי DER בינאריים

(סיומת CER או CRT), אישורי PEM בהצפנת BASE-64 (סיומת CER או CRT), או קובצי PEM PKCS1 (סיומת PEM). כמו כן, הדוגמה משתמשת ב-OpenSSL, היוצר חתימות בתבנית big-endian. באפשרותך להשתמש בכל תוכנית שירות כדי לחתום על מניפסטים, אך גרסאות BIOS מסוימות תומכות בחתימות בפורמט little-endian בלבד.

1. צור מפתח RSA פרטי ב-2,048 סיביות באמצעות הפקודה הבאה. אם ברשותך צמד מפתחות RSA פרטי/ציבורי ב-2,048 סיביות בתבנית pem, העתק אותם אל C:\staging, ולאחר מכן דלג לשלב 3.

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

2. צור את המפתח הציבורי מהמפתח הפרטי שלך (אם יש ברשותך מפתח ציבורי המתאים למפתח הפרטי שלך בתבנית PEM, העתק אותו ל-C:\staging), באמצעות הפקודה הבאה:

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

3. צור קובץ חתימה (באמצעות קוד Hash על בסיס sha256) המבוסס על מפתח RSA הפרטי ב-2,048 סיביות משלב 1, באמצעות הפקודה הבאה:

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

4. אמת את קובץ החתימה באמצעות המפתח הציבורי מהשלב הקודם, באמצעות הפקודה הבאה:

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

הערה:

- אם עליך ליצור קובץ חתימה בלבד, השלבים הדרושים הם 1 ו-3.
- עבור HP Sure Recover, צעדי המינימום הנדרשים הם 1, 2 ו-3. תזדקק למפתח הציבורי משלב 2 כדי להכין את מערכת היעד שלך.
- שלב 4 הוא אופציונלי אך מומלץ, כדי שקובצי החתימה והמניפסט שלך יאומתו כראוי.

אירוח הקבצים

ארח את הקבצים הבאים בשרת מהתיקייה C:\staging:

- *.swm
- custom.mft (או שם הקובץ שבחרת עבור קובץ המניפסט)
- custom.sig (או שם הקובץ התואם שבחרת עבור קובץ החתימה)

הערה: אם אתה משתמש ב-IIS כפתרון האחסון שלך, עליך להגדיר את ערכי MIME שלך כך שיכללו את הסיומות הבאות, כשהכל מוגדר כ-"application/octet-stream":

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

הקצאת מערכת היעד

באפשרותך להקצות את מערכות היעד שלך באמצעות ספריית הסקריפטים HP Client Security, HP Client Management Sure Recover/(CSM) Manager או ערכת (MIK) Manageability Integration Kit (<https://www.hp.com/go/clientmanagement>).

ספק את המידע הבא להקצאה זו:

1. כתובת ה-URL של קובץ המניפסט המתארח מהסעיף הקודם (`http://your_server.domain/path/custom.mft`)
2. המפתח הציבורי המשמש לאימות קובץ החתימה שנוצר קודם לכן (לדוגמה, `C:\staging\my-recovery-public.pem`).

פתרון בעיות

אם מופיעה הודעה לפיה תהליך השחזור המותאם אישית כשל באימות האבטחה, בדוק את הפרטים הבאים:

1. המניפסט חייב להיות קובץ UTF-8 ללא BOM.
2. בדוק את קודי ה-Hash של הקבצים.
3. ודא כי המערכת הוקצתה עם המפתח הציבורי המתאים למפתח הפרטי ששימש לחתימה על המניפסט.
4. סוגי ה-MIME של שרת IIS חייבים להיות `application/octet-stream`.
5. נתיבי הקבצים בתוך המניפסט חייבים לכלול את הנתיב המלא אל התיקייה העליונה המכילה את התמונה כפי שהוא נראה ממערכת הלקוח. נתיב זה אינו הנתיב המלא למקום שבו הקבצים נשמרים בנקודת ההפצה.

שימוש בסוכן HP Sure Recover הסוכן בתוך

חומת אש ארגונית

ניתן לארוח את סוכן HP Sure Recover באינטראנט הארגוני. לאחר התקנת חבילת התוכנה של HP Sure Recover, העתק את קובצי הסוכן שבתיקיית הסוכן של HP Sure Recover ממיקום ההתקנה לנקודת הפצה באמצעות HTTP או FTP. לאחר מכן, הקצה את מערכת עם כתובת ה-URL של נקודת ההפצה והמפתח הציבורי של HP בשם `hpsr_agent_public_key.pem`, המופץ יחד עם סוכן חבילת התוכנה של HP Sure Recover.

התקנת הסוכן של HP Sure Recover

1. הורד את הסוכן של HP Sure Recover וחלץ את הקבצים אל נקודת ההפצה שלך באמצעות HTTP או FTP.
2. הגדר את הרשאות הקבצים המתאימות בנקודת ההפצה.
3. אם אתה משתמש ב-Internet Information Services (IIS), צור סוגי MIME של application/octet-stream עבור התבניות הבאות:

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

חשוב: הצעדים הבאים מתארים את הקצאת Sure Recover עם SCCM. לדוגמאות להקצאת Sure Recover עם ספריית הסקריפטים HP Client Management, ראה [עבודה עם ספריית הסקריפטים HP Client Management \(CMSL\)](#) בעמוד 11.

4. הפעל את SCCM, בוט אל **Hp Client Security Suite**, ולאחר מכן בחר את דף HP Sure Recover.

הערה: כתובת ה-URL של נקודת ההפצה כוללת את ftp או http כפרוטוקול ההעברה. היא כוללת גם את הנתיב המלא אל התיקייה העליונה המכילה את המניפסט של סוכן HP Sure Recover כפי שהוא נראה ממערכת לקוח. נתיב זה אינו הנתיב המלא אל המקום שבו נשמרים הקבצים בנקודת ההפצה.

5. במקטע **Platform Image** (תמונת פלטפורמה), בחר את האפשרות **Corporation** (ארגונית) כדי לשחזר תמונת מערכת הפעלה מותאמת אישית מנקודת הפצה ארגונית. הזן את כתובת ה-URL שסופקה על-ידי מנהל ה-IT בתיבה **Image Location URL** (כתובת URL של מיקום התמונה). הזן את המפתח הציבורי `hpsr_agent_public_key.pem` בשדה **Image Verification** (אימות תמונה).

הערה: כתובת ה-URL של התמונה המותאמת אישית חייבת לכלול את שם קובץ המניפסט.

6. במקטע **Recovery Agent** (סוכן שחזור), בחר את האפשרות **Corporation** (ארגונית) כדי להשתמש בסוכן שחזור מותאם אישית או בסוכן שחזור של HP מנקודת הפצה ארגונית. הזן את כתובת ה-URL שסופקה על-ידי מנהל ה-IT בתיבה **Agent Location URL** (כתובת URL של מיקום הסוכן). הזן את המפתח הציבורי `hpsr_agent_public_key.pem` בשדה **Agent Verification Key** (מפתח אימות הסוכן).

7. לאחר החלת המדיניות על מערכת הלקוח, הפעל אותה מחדש.

8. במהלך ההקצאה הראשונית, תופיע הנחיה להזין קוד אבטחה בן 4 ספרות כדי להשלים את הפעלת HP Sure Recover. לקבלת פרטים נוספים, בקר בכתובת hp.com וחפש אחר ערכת HP Manageability Integration Kit (MIK) לקבלת נייר העבודה של Microsoft System Center Manager.

לאחר השלמת ההפעלה של HP Sure Recover בהצלחה, כתובת ה-URL המותאמת אישית שהוחלה על-ידי המדיניות מוצגת בתפריט הגדרות ה-BIOS של HP Sure Recover.

כדי לאמת את הצלחת ההפעלה, הפעל מחדש את המחשב, וכשמופיע הלוגו של HP, הקש על **f10**. בחר **Advanced** (מתקדם), בחר **HP Sure Recover**, בחר **Recovery Agent** (סוכן שחזור), ולאחר מכן בחר **URL**.

4 עבודה עם ספריית הסקריפטים HP Client Management (CMSL)

ספריית הסקריפטים HP Client Management מאפשרת לך לנהל את ההגדרות של HP Sure Recover באמצעות PowerShell. סקריפט הדוגמה להלן מדגים כיצד להקצות, לקבוע את המצב, לשנות את התצורה ולמשוך את ההקצאה של HP Sure Recover.

הערה: חלק מהפקודות חורגות מאורך השורה של מדריך זה, אך יש להזין אותן כשורה אחת.

```
$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
    }

```

יצירת מפתחות דוגמה באמצעות OpenSSL

אחסן את המפתחות הפרטיים במקום בטוח. המפתחות הציבוריים ישמשו לצורך אימות ויש להזין אותם במהלך ההקצאה. מפתחות אלה נדרשים להיות באורך של 2,048 סיביות ולהשתמש במערך של 0x10001. החלף את הנושא בדוגמאות המוצגות במידע על הארגון שלך.

הגדר את משתנה הסביבה הבא לפני שתמשיך:

```

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:
```

באפשרותך לחתום על המניפסט של התמונה באמצעות הפקודה הבאה:

```
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.co"

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:
```

באפשרותך לחתום על המניפסט של הסוכן באמצעות הפקודה הבאה:

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

OpenSSL יוצר קובצי חתימות בפורמט big-endian, שאינם מתאימים לגרסאות BIOS מסוימות, כך שיתכן שתצטרך להפוך את סדר הסיביות של קובץ חתימת הסוכן לפני הפריסה. גרסאות BIOS התומכות בסדר סיביות של big-endian תומכות גם בסדר סיביות של little-endian.

החלוקה למחיצות של כונן נכשלה

מחיצת כונן שנכשלה עלולה לקרות כאשר מחיצת SR_AED או SR_IMAGE מוצפנת באמצעות Bitlocker. מחיצות אלה נוצרות בדרך כלל עם מאפיין gpt המונע מ-Bitlocker להצפין אותן, אך אם משתמש מוחק ויוצר מחדש את המחיצות או יוצר אותן באופן ידני על-גבי כונן קשיח ריק, הסוכן של Sure Recover לא מסוגל למחוק אותן והוא יוצא מהפעולה בהודעת שגיאה בעת החלוקה למחיצות. המשתמש חייב למחוק אותן באופן ידני על-ידי הפעלת diskpart, בחירת אמצעי האחסון והרצה של הפקודה העוקפת del vol או פקודה דומה.

יומן ביקורת קושחה

מידע משתני EFI הוא כדלהלן:

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


- שם: OsRecoveryInfoLog

קיימים ממשקי API במערכת ההפעלה Windows לקריאת משתני EFI, או שבאפשרותן להוריד את תוכן המשתנים לקובץ באמצעות תוכנית השירות UEFI Shell dmpstore.

באפשרותן להוריד את יומן הביקורת באמצעות הפקודה Get-HPFirmwareAuditLog המסופקת על-ידי ספריית הסקריפטים HP Client Management.

יומן אירועים של Windows

אירועי התחלה ועצירה של Sure Recover נשלחים ליומן הביקורת של ה-BIOS, אותו ניתן להציג ב-Windows Event Viewer (מציג האירועים של Windows) ביומן של Sure Start אם הותקן HP Notifications. אירועים אלה כוללים את התאריך והשעה, מזהה המקור, מזהה האירוע וקוד ספציפי לאירוע. לדוגמה, [fe 00 40 26 02 27 06 18 84 2a 02, 01 00 30 f2 c3] מציין כי השחזור נכשל מאחר שלא ניתן היה לאמת את המניפסט באמצעות הקוד הספציפי לאירוע c3f 23000 שנרשם בשעה 2:26:40 בתאריך 27/06/18.

 **הערה:** יומנים אלה מובאים בתבנית התאריך האמריקאית של MM/DD/YY.

HP Secure Platform Management (מזהה מקור = 84h)

טבלה א-1 HP Secure Platform Management

מזהה אירוע	מונה התקנים (All/DaaS)	מונה אירועים (All/DaaS)	תיאור	הערות
40	256/178	943/552	תהליך שחזור מערכת ההפעלה של הפלטפורמה הותחל על-ידי הקושחה.	שחזור הפלטפורמה הותחל
41	221/147	588/332	תהליך שחזור מערכת ההפעלה של הפלטפורמה הושלם בהצלחה.	שחזור הפלטפורמה הושלם
42	54/42	252/156	תהליך שחזור מערכת ההפעלה של הפלטפורמה לא הושלם בהצלחה.	שחזור הפלטפורמה נכשל

באפשרותך לאחזר את יומן ביקורת הקושחה על ידי הרצת Get-HPFirmwareAuditLog בספריית הסקריפטים HP Client Management, הזמינה בכתובת <http://www.hp.com/go/clientmanagement>. מזהי האירועים 40, 41 ו-42 של HP Secure Platform Management מחזירים קודים ספציפיים לאירוע בשדה הנתונים, המציינים את תוצאות הפעולות של Sure Recover. לדוגמה, רשומת היום הבאה מציינת כי Sure Recover לא הצליח להוריד את קובץ המניפסט או את קובץ החתימה באמצעות קוד שגיאה 42 event_id עם הנתון: 00:30:f1:c3, אותו יש לפרש כערך ה-dword = 0xC3F13000.

```

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
תיאור: The platform OS recovery process failed to complete successfully.
data: 00:30:f1:c3

```

שחזור מוצלח מצוין בקוד event_id = 41 עם הנתון: 00:00:00:00, לדוגמה:

```

Event Specific Codes
Success = 0x00000000
CatalogDownloadFailed = 0xC3F11000
message_number: 0
severity: Info
system_state_at_event: S0
source_id: HP Secure Platform Management
event_id: 41
timestamp_is_exact: 1
timestamp: 5/27/2019 2:55:41 PM
description: The platform OS recovery process failed to complete
successfully.
data: 00:00:00:00

```

HP Sure Recover משתמש בקודים הספציפיים לאירוע הבאים.

טבלה א-2 קודים ספציפיים לאירוע

קוד האירוע	תיאור האירוע
0xC3F11000	CatalogDownloadFailed
0xC3F12000	SignatureDownloadFailed
0xC3F13000	MftOrSigDownloadFailed
0xC3F14000	FtpHttpDownloadFailed

טבלה א-2 קודים ספציפיים לאירוע (המשך)

קוד האירוע	תיאור האירוע
0xC3F15000	AwsDownloadFailed
0xC3F16000	AwsDownloadUnattendedFailed
0xC3F17000	UnableToConnectToNetwork
0xC3F21000	CatalogNotAuthenticated
0xC3F22000	FtpHttpDownloadHashFailed
0xC3F23000	ManifestDoesNotAuthenticate
0xC3F31000	CatalogVersionMismatch
0xC3F32000	CatalogLoadFailed
0xC3F33000	OsDvdDidNotResolvedToOneComponent
0xC3F34000	DriversDvdDidNotResolvedToOneComponent
0xC3F41000	ManifestFileEmptyOrInvalid
0xC3F42000	ListedFileInManifestNotFound
0xC3F51000	FailedToInstallDrivers
0xC3F52000	FailedToApplyWimImage
0xC3F53000	FailedToRegisterWimCallback
0xC3F54000	FailedToCreateDismProcess
0xC3F55000	BcdbootFailed
0xC3F56000	NoSuitableDiskFound
0xC3F57000	PartitoningFailed
0xC3F58000	DiskLayoutCreationFailed
0xC3FF1000	UnexpectedProblemWithConfigJson
0xC3FF2000	SureRecoverJsonParsingFailed
0xC3FF3000	RebootRequestFailed
0xC3FF4000	UnableToReadConfigFile
0xC3FF5000	FailedToDetectWindowsPE