



คู่มือผู้ใช้

HP Sure Recover

© Copyright 2020 HP Development Company,
L.P.

Microsoft และ Windows เป็นเครื่องหมายการค้าหรือ
เครื่องหมายการค้าจดทะเบียนของ Microsoft
Corporation ในสหรัฐอเมริกาและ/หรือในประเทศอื่นๆ

ซอฟต์แวร์คอมพิวเตอร์ลิขสิทธิ์เฉพาะ ต้องได้รับการอนุญาต
ที่ถูกต้องจาก HP สำหรับการครอบครองใช้ หรือคัดลอก
ตามระเบียบของ FAR มาตรา 12.211 และ 12.212 ได้
ให้การอนุญาตใช้ซอฟต์แวร์คอมพิวเตอร์เพื่อการ
พาณิชย์ เอกสารประกอบซอฟต์แวร์คอมพิวเตอร์ และ
ข้อมูลทางด้านเทคนิคสำหรับรายการเชิงพาณิชย์ กับ
รัฐบาลสหรัฐอเมริกา ภายใต้การอนุญาตใช้เชิงพาณิชย์
ตามมาตรฐานของผู้ค้า

ข้อมูลที่ระบุในที่นี้อาจมีการเปลี่ยนแปลงโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า การรับประกันสำหรับ
ผลิตภัณฑ์และบริการของ HP ระบุไว้อย่างชัดเจนในใบรับ
ประกันที่ ให้มาพร้อมกับผลิตภัณฑ์และบริการดังกล่าว
เท่านั้น ข้อความในที่นี้ไม่ถือเป็นการรับประกันเพิ่มเติม
แต่อย่างใด HP จะไม่รับผิดชอบต่อข้อผิดพลาดทาง
เทคนิคหรือภาษาหรือการละเว้นข้อความในที่นี้

พิมพ์ครั้งที่หนึ่ง: กุมภาพันธ์ 2020

หมายเลขภาคผนวกของเอกสาร: L93434-281

คีย์รูปแบบคำสั่งที่ป้อนเข้าโดยผู้ใช้

จะมีการระบุข้อความที่คุณจะต้องป้อนเข้าในอินเทอร์เน็ตเฟสผู้ใช้ตามแบบตัวอักษรที่มีความกว้างคงที่

ตาราง -1 คีย์รูปแบบคำสั่งที่ป้อนเข้าโดยผู้ใช้

รายการ	คำอธิบาย
ข้อความที่ไม่มีวงเล็บเหลี่ยมหรือวงเล็บปีกกา	รายการที่คุณต้องพิมพ์ให้ตรงตามที่ปรากฏทุกประการ
<ข้อความที่อยู่ในวงเล็บมุม>	พื้นที่ที่สำรองไว้สำหรับค่าที่คุณต้องระบุไม่ต้องใส่วงเล็บเหลี่ยม
[ข้อความที่อยู่ในวงเล็บสี่เหลี่ยม]	รายการที่เป็นตัวเลือกไม่ต้องใส่วงเล็บเหลี่ยม
{ข้อความที่อยู่ในวงเล็บปีกกา}	ชุดรายการที่คุณต้องเลือกเพียงรายการเดียวไม่ต้องใส่วงเล็บปีกกา
	ตัวคั่นระหว่างรายการที่คุณต้องเลือกเพียงรายการเดียวไม่ต้องใส่แถบแนวตั้ง
...	รายการที่สามารถหรือต้องทำซ้ำไม่ต้องใส่จุดไข่ปลา

สารบัญ

1 การเริ่มต้นใช้งาน	1
การดำเนินการกู้คืนระบบเครือข่าย	1
การดำเนินการกู้คืนไดรฟ์แบบโลคัล	1
2 การสร้างอิมเมจของบริษัท	3
ข้อกำหนด	3
การสร้างอิมเมจ	3
ตัวอย่างที่ 1: การสร้างอิมเมจโดยใช้อิมเมจการติดตั้งของ Microsoft Windows	3
ตัวอย่างที่ 2: การสร้างอิมเมจจากระบบอ้างอิง	6
การแยกอิมเมจ	6
การสร้างไฟล์กำกับ	6
การสร้างไฟล์กำกับ	7
การสร้างลายเซ็นไฟล์กำกับ	8
การโฮสต์ไฟล์	9
การจัดเตรียมระบบเป้าหมายของคุณ	9
การแก้ไขปัญหา	10
3 การใช้งานเอเจนต์ HP Sure Recover ภายในไฟร์วอลล์บริษัท	11
การติดตั้งเอเจนต์ HP Sure Recover	11
4 การใช้งานพร้อม HP Client Management Script Library (CMSL)	13
การสร้างคีย์ตัวอย่างโดยใช้ OpenSSL	16
ภาคผนวก A การแก้ไขปัญหา	18
การจัดพาร์ติชันไดรฟ์ล้มเหลว	18
ข้อมูลบันทึกการตรวจสอบเฟิร์มแวร์	18
ข้อมูลบันทึกเหตุการณ์ของ Windows	18
HP Secure Platform Management (ID ต้นทาง = 84h)	18

1 การเริ่มต้นใช้งาน

HP Sure Recover จะช่วยให้คุณสามารถติดตั้งระบบปฏิบัติการจากเครือข่ายได้อย่างปลอดภัย โดยที่ผู้ใช้แทบไม่ต้องดำเนินการใดๆ เพิ่มเติม ระบบที่ใช้ HP Sure Recover ร่วมกับ Embedded Reimaging จะรองรับการติดตั้งจากอุปกรณ์จัดเก็บข้อมูลแบบโลคัลด้วย

 **สิ่งสำคัญ:** สำรองข้อมูลของคุณก่อนที่จะใช้ HP Sure Recover เนื่องจากกระบวนการสร้างอิมเมจ จะทำการฟอร์แมตไดรฟ์ใหม่ จึงเกิดการสูญเสียข้อมูลขึ้น

อิมเมจการกู้คืนที่ HP เตรียมให้ จะมีตัวติดตั้ง Windows 10[®] พื้นฐานรวมอยู่ด้วย หรืออีกทางหนึ่ง HP Sure Recover สามารถติดตั้งไดรเวอร์ที่เหมาะสมกับอุปกรณ์ HP ได้ อิมเมจการกู้คืนของ HP จะรวมเฉพาะเอเจนต์การกู้คืนข้อมูลที่รวมอยู่ใน Windows 10 เช่น OneDrive เท่านั้น บริษัทสามารถสร้างอิมเมจเฉพาะของตัวเอง เพื่อเพิ่มการตั้งค่าบริษัท แอปพลิเคชัน ไดรเวอร์ และเอเจนต์กู้คืนข้อมูลได้

เอเจนต์การกู้คืนระบบปฏิบัติการ (OS) จะดำเนินการตามขั้นตอนที่จำเป็น เพื่อติดตั้งอิมเมจการกู้คืน เอเจนต์การกู้คืนที่จัดเตรียมโดย HP จะดำเนินการตามขั้นตอนทั่วไป เช่น การจัดพาร์ติชัน การฟอร์แมต และการแยกอิมเมจการกู้คืนไปยังอุปกรณ์เป้าหมาย เนื่องจากเอเจนต์การกู้คืนของ HP จะอยู่บน hp.com คุณจึงต้องเข้าใช้งานอินเทอร์เน็ตเพื่อเรียกใช้ ยกเว้นกรณีที่ในระบบมี embedded reimaging อยู่ นอกจากนี้ บริษัทยังสามารถโฮสต์เอเจนต์การกู้คืนของ HP ภายในไฟร์วอลล์ของตนเอง หรือสร้างเอเจนต์การกู้คืนแบบกำหนดเองเพื่อใช้ในสภาพแวดล้อมการกู้คืนที่ซับซ้อนมากขึ้น

คุณสามารถเริ่มต้น HP Sure Recovery ได้เมื่อไม่พบระบบปฏิบัติการ นอกจากนี้ คุณยังสามารถสั่งรัน HP Sure Recover ตามกำหนดเวลาได้ เช่น เพื่อช่วยให้มั่นใจว่าจะมีการลบมัลแวร์ออก ดำเนินการกำหนดค่าการตั้งค่าเหล่านั้นผ่านทาง HP Client Security Manager (CSM), Manageability Integration Kit (MIK) หรือ HP Client Management Script Library

การดำเนินการกู้คืนระบบเครือข่าย

 **หมายเหตุ:** ในการดำเนินการกู้คืนระบบเครือข่าย คุณจะต้องใช้การเชื่อมต่อแบบใช้สาย HP ขอแนะนำให้คุณสำรองไฟล์ ข้อมูล ภาพถ่าย วิดีโอ และอื่นๆ ที่สำคัญ ก่อนที่จะใช้ HP Sure Recover เพื่อหลีกเลี่ยงการสูญเสียข้อมูล

1. เชื่อมต่อระบบไคลเอนต์เข้ากับเครือข่ายที่สามารถเข้าใช้งานจุดกระจายข้อมูล HTTP หรือ FTP ได้
2. รีสตาร์ทระบบไคลเอนต์ และเมื่อโลโก้ HP ปรากฏขึ้น ให้กด **F11**
3. เลือก **คืนค่าจากเครือข่าย**.

การดำเนินการกู้คืนไดรฟ์แบบโลคัล

หากระบบไคลเอนต์รองรับ embedded reimaging และมีการเปิดใช้งานตัวเลือกการดาวน์โหลดอิมเมจตามกำหนดเวลาไว้ในนโยบายที่ปรับใช้ ระบบจะทำการดาวน์โหลดอิมเมจไปยังระบบไคลเอนต์ตามเวลาที่กำหนด หลังจากดาวน์โหลดอิมเมจสำหรับระบบไคลเอนต์แล้ว ให้รีสตาร์ทเพื่อคัดลอกอิมเมจไปยังอุปกรณ์จัดเก็บข้อมูล Embedded Reimaging

หากต้องการกู้คืนแบบโลคัลโดยใช้อิมเมจบนอุปกรณ์จัดเก็บข้อมูล Embedded Reimaging:

1. รีสตาร์ทระบบไคลเอนต์ และเมื่อโลโก้ HP ปรากฏขึ้น ให้กด **F11**
2. เลือก **คืนค่าจากไดรฟ์แบบโลคัล**

ระบบที่ใช้ Embedded Reimaging จะต้องกำหนดค่าการกำหนดเวลาดาวนโหลด และใช้เอเจนต์การดาวนโหลดเพื่อตรวจสอบการอัปเดต จะมีการรวมเอเจนต์การดาวนโหลดไว้ใน HP Sure Recover Plug-in for HP Client Security Manager และยังสามารถกำหนดค่าใน MIK ได้อีกด้วย ดูที่ <https://www.hp.com/go/clientmanagement> สำหรับคำแนะนำในการใช้งาน MIK

นอกจากนี้ คุณยังสามารถสร้างงานตามกำหนดเวลา เพื่อตัดออกเอเจนต์ไปยังพาร์ติชัน SR_AED และตัดออกอิมเมจไปยังพาร์ติชัน SR_IMAGE จากนั้น คุณสามารถใช้ HP Client Management Script Library เพื่อส่งเหตุการณ์การบริการ ที่แจ้งให้ BIOS ทราบว่าควรตรวจสอบเนื้อหา และตัดออกไปยังอุปกรณ์จัดเก็บข้อมูล embedded reimaging ในการรีบูตครั้งถัดไป

2 การสร้างอิมเมจของบริษัท

บริษัทส่วนใหญ่จะใช้ Microsoft Deployment Tools, Windows 10 Assessment and Deployment kit หรือทั้งสองอย่างในการสร้างไฟล์ที่มีอิมเมจภายในอาร์คิฟรูปแบบไฟล์ Windows Imaging (WIM)

ข้อกำหนด

- Windows 10 Assessment and Deployment Kit (Windows ADK) เวอร์ชันล่าสุด
- PowerShell
- OpenSSL (หรือวิธีแก้ไขปัญหานั้นๆ สำหรับการสร้างคู่คีย์ส่วนตัว/สาธารณะของ RSA) ใช้เพื่อสร้างคู่คีย์ RSA ที่ใช้เพื่อรักษาความสมบูรณ์ของอิมเมจของบริษัทที่คุณสร้างและโฮสต์
- โซลูชันการโฮสต์บนเซิร์ฟเวอร์ (เช่น Microsoft Internet Information Services [IIS])

การสร้างอิมเมจ

ก่อนที่จะเริ่มกระบวนการสร้างอิมเมจ ให้ตั้งค่าระบบการทำงานหรือสร้างระบบที่คุณติดตั้งเครื่องมือที่จำเป็นไว้ เพื่อเตรียมความพร้อมสำหรับการประมวลผลอิมเมจ ดังที่แสดงไว้ในขั้นตอนต่อไปนี้:

1. ในฐานะผู้ดูแลระบบ ให้เปิดพร้อมท์คำสั่ง Deployment and Imaging Tools Environment (ติดตั้งไว้พร้อมกับ Deployment Tools ของ Windows ADK)
2. สร้างพื้นที่จัดเตรียมสำหรับอิมเมจของคุณ โดยใช้คำสั่งต่อไปนี้:

```
mkdir C:\staging
```

3. สร้างอิมเมจโดยใช้หนึ่งในตัวอย่างต่อไปนี้:

[ตัวอย่างที่ 1: การสร้างอิมเมจโดยใช้อิมเมจการติดตั้งของ Microsoft Windows ในหน้า 3](#)

[ตัวอย่างที่ 2: การสร้างอิมเมจจากระบบอ้างอิงในหน้า 6](#)

ตัวอย่างที่ 1: การสร้างอิมเมจโดยใช้อิมเมจการติดตั้งของ Microsoft Windows

1. เชื่อมต่อหรือเปิดอิมเมจการติดตั้งของ Microsoft Windows (จาก Microsoft ISO หรือจาก HP OSDVD)
2. จากอิมเมจการติดตั้ง Windows ที่เชื่อมต่อไว้ ให้คัดลอกไฟล์ install.wim ไปยังพื้นที่สำหรับการจัดเตรียมของคุณ โดยใช้คำสั่งต่อไปนี้:

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

 **หมายเหตุ:** <M:> หมายถึงไดรฟ์ที่เชื่อมต่อไว้ แทนที่ด้วยตัวอักษรชื่อไดรฟ์ที่ต้องการ

3. เปลี่ยนชื่อ install.wim เป็นชื่อไฟล์อิมเมจ ("my-image" สำหรับตัวอย่างนี้) โดยใช้คำสั่งต่อไปนี้:

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

(ทางเลือก) ใน HP Sure Recover จะมีคุณลักษณะสำหรับกู้คืนรุ่นเฉพาะที่กำหนดจากอิมเมจแบบหลายดัชนี โดยขึ้นอยู่กับรุ่นของ Windows ที่ได้รับใบอนุญาตดั้งเดิมสำหรับระบบเป้าหมายของ HP ในโรงงาน กลไกนี้จะทำงานหากมีการตั้งชื่อดัชนีอย่างถูกต้อง หากอิมเมจการติดตั้งของ Windows ของคุณมาจากอิมเมจ OSDVD ของ HP แสดงว่าคุณอาจมีอิมเมจแบบหลายรุ่น หากคุณไม่ต้องการใช้งานลักษณะการทำงานนี้ และต้องการตรวจสอบให้แน่ใจว่ามีการใช้งานเพียงรุ่นเฉพาะที่กำหนดไว้รุ่นเดียว สำหรับระบบเป้าหมายทั้งหมดของคุณ คุณจะต้องตรวจสอบให้แน่ใจว่ามีเพียงดัชนีเดียวในอิมเมจสำหรับการติดตั้ง

4. ตรวจสอบเนื้อหาของอิมเมจสำหรับการติดตั้ง โดยใช้คำสั่งต่อไปนี้:

```
disk /Get-ImageInfo /ImageFile:C:\staging\
```

เนื้อหาต่อไปนี้จะแสดงเอาท์พุทตัวอย่างจากอิมเมจสำหรับการติดตั้งที่รองรับห้ารุ่น (สำหรับเลือกจับคู่ตาม BIOS ของระบบเป้าหมายแต่ละเครื่อง):

รายละเอียดสำหรับอิมเมจ: my-image.wim

ดัชนี: 1

ชื่อ: CoreSingleLanguage

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

ขนาด: 19,512,500,682 bytes

ดัชนี: 2

ชื่อ: Core

คำอธิบาย: Windows 10 May 2019 Update - Home edition

ขนาด: 19,512,500,682 bytes

ดัชนี: 3

ชื่อ: Professional

คำอธิบาย: Windows 10 May 2019 Update- Professional Update

ขนาด: 19,758,019,520 bytes

ดัชนี: 4

ชื่อ: ProfessionalEducation

คำอธิบาย: Windows 10 May 2019 Update - Professional Education edition


ขนาด: 19,758,019,480 bytes

ดัชนี: 5

ชื่อ: ProfessionalWorkstation

คำอธิบาย: Windows 10 May 2019 Update - Professional Workstation edition

ขนาด: 19,758,023,576 bytes

 **หมายเหตุ:** เมื่อมีเพียงดัชนีเดียว จะใช้ชื่อเมจดังกล่าวในการกู้คืนโดยไม่สนใจชื่อ ขนาดไฟล์อิมเมจของคุณ อาจใหญ่กว่าขนาดไฟล์ก่อนการลบ

5. หากคุณไม่ต้องการใช้งานลักษณะการทำงานแบบหลายรุ่น ให้ลบแต่ละดัชนีที่คุณไม่ต้องการออก

ตามที่แสดงในตัวอย่างต่อไปนี้ หากคุณต้องการใช้งานเฉพาะรุ่น Professional (ในกรณีที่ระบบเป้าหมายทั้งหมดมีใบอนุญาต) ให้ลบดัชนี 5, 4, 2 และ 1 ออก โดยในแต่ละครั้งที่คุณลบดัชนี ระบบจะกำหนดหมายเลขดัชนีใหม่ ดังนั้น คุณควรลบไล่จากหมายเลขดัชนีสูงสุดไปหาต่ำสุด รัน Get-ImageInfo ภายหลังจากการลบแต่ละครั้ง เพื่อยืนยันดัชนีที่คุณจะทำการลบถัดไปด้วยตัวเอง

```
disimg /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:5  
disimg /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:4  
disimg /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:2  
disimg /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:1
```

เลือกเพียงดัชนีเดียวสำหรับรุ่นที่ต้องการ (สำหรับตัวอย่างนี้คือ Professional) เมื่อมีเพียงดัชนีเดียว จะใช้ชื่อเมจดังกล่าวในการกู้คืนโดยไม่สนใจชื่อ โปรดทราบว่า ขนาดไฟล์อิมเมจของคุณ อาจใหญ่กว่าขนาดไฟล์ก่อนการลบ เนื่องจากรูปแบบการปรับเปลี่ยนข้อมูลเมตาของ WIM และการนอร์มาไลเซชันของเนื้อหา

6. (ทางเลือก) หากคุณต้องการรวมไดรเวอร์ไว้ในอิมเมจการกู้คืนสำหรับบริษัทของคุณ ให้ปฏิบัติตามขั้นตอนเหล่านี้:

a. เชื่อมต่ออิมเมจของคุณเข้ากับโฟลเดอร์เปล่า โดยใช้คำสั่งต่อไปนี้:

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

b. เชื่อมต่อ DVD ไดรเวอร์ของ HP Windows 10 (DRDVD) ที่ถูกต้องสำหรับระบบเป้าหมายที่รองรับ จากมีเดียไดรเวอร์ที่เชื่อมต่อไว้ให้คัดลอกโฟลเดอร์ย่อยของไดรเวอร์ไปยังพื้นที่สำหรับการจัดเตรียมของคุณ โดยใช้คำสั่งต่อไปนี้:

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

 **หมายเหตุ:** <M:> หมายถึงไดรฟ์ที่เชื่อมต่อไว้ แทนที่ด้วยตัวอักษรชื่อไดรฟ์ที่ต้องการ

คุณสามารถเพิ่มไดรเวอร์ .inf-style เพิ่มเติมได้ โดยวางไว้ในโฟลเดอร์ C:\staging\mount\SWSETUP\DRV สามารถอ่านคำอธิบายเกี่ยวกับวิธีการที่ HP Sure Recover ใช้ในการประมวลผลเนื้อหาด้วยฟังก์ชัน disimg /Add-Driver /Recurse ได้ที่ “การเพิ่มและลบไดรเวอร์ในอิมเมจ Windows แบบออฟไลน์” ในหัวข้อต่อไปนี้: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image>.

คุณลักษณะนี้ไม่รองรับไดรเวอร์ .exe-style ซึ่งจำเป็นต้องรันแอปพลิเคชัน

c. บันทึกการเปลี่ยนแปลง และยกเลิกการเชื่อมต่ออิมเมจของคุณ โดยใช้คำสั่งต่อไปนี้:

```
disimg /Unmount-Wim /MountDir:C:\staging\mount /Commit  
ไฟล์อิมเมจที่ได้จะอยู่ที่: C:\staging\my-image.wim.
```

d. ไปที่ [การแยกอิมเมจในหน้า 6](#)

ตัวอย่างที่ 2: การสร้างอิมเมจจากระบบอ้างอิง

1. สร้างมีเดีย USB WinPE ที่สามารถใช้ในการบูทระบบได้



หมายเหตุ: สามารถศึกษาวิธีการเพิ่มเติมที่ใช้ในการบันทึกอิมเมจได้จากในเอกสาร ADK

ตรวจสอบให้แน่ใจว่าไดรฟ์ USB มีพื้นที่ว่างเพียงพอสำหรับการบันทึกอิมเมจจากระบบอ้างอิง

2. สร้างอิมเมจจากระบบอ้างอิง

3. บันทึกอิมเมจโดยการบูทระบบอ้างอิงด้วยมีเดีย USB WinPE และจากนั้นใช้ DISM



หมายเหตุ: <U:> หมายถึงไดรฟ์ USB แทนที่ด้วยตัวอักษรชื่อไดรฟ์ที่ถูกต้อง

แก้ไขส่วน “my-image” ของชื่อไฟล์ ตามด้วยคำอธิบาย <my-image> ตามต้องการ

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

4. คัดลอกอิมเมจจาก USB ไปยังพื้นที่สำหรับการจัดเตรียมภายในระบบการทำงานของคุณ โดยใช้คำสั่งต่อไปนี้:

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

คุณควรมีไฟล์อิมเมจต่อไปนี้: C:\staging\my-image.wim.

5. ไปที่ [การแยกอิมเมจ](#) ในหน้า 6

การแยกอิมเมจ

HP ขอแนะนำให้คุณแยกอิมเมจลงเป็นไฟล์ขนาดเล็กหลายๆไฟล์ เพื่อให้สามารถดาวน์โหลดผ่านเครือข่ายได้ดียิ่งขึ้น โดยใช้คำสั่งต่อไปนี้:

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



หมายเหตุ: FileSize จะแสดงผลในหน่วยเมกะไบต์ แก้ไขตามความจำเป็น



หมายเหตุ: เนื่องจากลักษณะทั่วไปของอัลกอริธึมการแยกของ DISM ขนาดของไฟล์ SWM ที่สร้างขึ้น อาจเล็กกว่าหรือใหญ่กว่าขนาดไฟล์ที่ระบุก็ได้

การสร้างไฟล์กำกับ

กำหนดรูปแบบไฟล์กำกับเป็น UTF-8 without Byte Order Mark (BOM)

คุณสามารถเปลี่ยนชื่อไฟล์กำกับ (custom.mft) ที่ใช้ ในขั้นตอนการดำเนินงานต่อไปนี้ได้ แต่จะต้องไม่เปลี่ยนนามสกุล .mft และ .sig และส่วนชื่อไฟล์ของไฟล์กำกับและไฟล์ลายเซ็นจะต้องตรงกัน ตัวอย่างเช่น คุณสามารถเปลี่ยนคู่ (custom.mft, custom.sig) เป็น (myimage.mft, myimage.sig) ได้

mft_version มีไว้เพื่อกำหนดรูปแบบของไฟล์อิมเมจ และจะต้องตั้งค่าไว้เป็น 1 ในขณะนี้

image_version มีไว้เพื่อระบุว่าอิมเมจเวอร์ชันใหม่กว่าที่พร้อมใช้งานอยู่หรือไม่ และเพื่อป้องกันไม่ให้เกิดการติดตั้งเวอร์ชันที่เก่ากว่า

ค่าทั้งสองจะต้องเป็นจำนวนเต็ม 16 บิตแบบไม่ระบุเครื่องหมาย และใช้ '\r\n' (CR + LF) ในการคั่นระหว่างบรรทัดภายในไฟล์กำกับ

การสร้างไฟล์กำกับ

เนื่องจากอาจมีหลายไฟล์ที่เกี่ยวข้องกับอิมเมจแยกของคุณ ให้ใช้สคริปต์ powershell ในการสร้างไฟล์กำกับ

ในการดำเนินการขั้นตอนที่เหลือทั้งหมด คุณจะต้องอยู่ในโฟลเดอร์ C:\staging

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

1. สร้างสคริปต์ powershell โดยใช้ตัวแก้ไขที่สามารถสร้างไฟล์ข้อความในรูปแบบ UTF 8 without BOM ได้ โดยใช้คำสั่งต่อไปนี้: notepad C:\staging\generate-manifest.ps1

สร้างสคริปต์ต่อไปนี้:

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

```
$imageVersion = 1907 (หมายเหตุ: สามารถใช้จำนวนเต็ม 16 บิตใดๆ)
```

```
$header = "mft_version=1, image_version=$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 = $hashObject.Path.Replace($pathToManifest + '\\', '')
$fileSize = (Get-Item $_.FullName).length
$manifestContent = "$fileHash $filePath $fileSize"

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

$current = $current + 1
}

```

 **หมายเหตุ:** ในไฟล์กำกับสำหรับ HP Sure Recover จะต้องไม่มี BOM ดังนั้น คำสั่งต่อไปนี้ จะเขียนทับไฟล์ในรูปแบบ UTF8 without BOM

```

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

```

2. บันทึกสคริปต์
3. เรียกใช้สคริปต์

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

การสร้างลายเซ็นไฟล์กำกับ

Sure Recover จะตรวจสอบเอเจนต์และอิมเมจโดยใช้ลายเซ็นเข้ารหัสลับ ตัวอย่างต่อไปนี้ จะใช้คู่คีย์แบบส่วนตัว/สาธารณะในรูปแบบ X.509 PEM (นามสกุล .PEM) ปรับเปลี่ยนคำสั่งตามความเหมาะสม เพื่อใช้ใบรับรองไบนารี DER (นามสกุล .CER หรือ .CRT) ใบรับรอง PEM ที่เข้ารหัสแบบ BASE-64 (นามสกุล .CER หรือ .CRT) หรือไฟล์ PKCS1 PEM (นามสกุล .PEM) และตัวอย่างนี้ยังใช้ OpenSSL ซึ่งจะสร้างลายเซ็นในรูปแบบ big-endian คุณสามารถใช้ยูลิตีใดก็ได้ในการเซ็นชื่อไฟล์กำกับ แต่ BIOS บางเวอร์ชัน จะรองรับเฉพาะลายเซ็นในรูปแบบ little-endian เท่านั้น

1. สร้างคีย์ส่วนบุคคล RSA แบบ 2048-บิต โดยใช้คำสั่งต่อไปนี้ หากคุณมีคู่คีย์ส่วนบุคคล/สาธารณะ RSA แบบ 2048-บิตในรูปแบบ pem ให้คัดลอกไปวางที่ C:\staging และจากนั้น ข้ามไปขั้นตอนที่ 3

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

2. สร้างคีย์สาธารณะจากคีย์ส่วนบุคคลของคุณ (หากคุณมีคีย์สาธารณะที่ตรงกับคีย์ส่วนบุคคลของคุณในรูปแบบ PEM ให้คัดลอกไปวางที่ C:\staging) โดยใช้คำสั่งต่อไปนี้:

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

3. สร้างไฟล์ลายเซ็น (โดยใช้แฮช sha256-based) ตามคีย์ส่วนตัว RSA แบบ 2048-บิตของคุณจากขั้นตอนที่ 1 โดยใช้คำสั่งต่อไปนี้:

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

4. ตรวจสอบไฟล์ลายเซ็น โดยใช้คีย์สาธารณะของคุณจากขั้นตอนก่อนหน้า โดยใช้คำสั่งต่อไปนี้:

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

หมายเหตุ:

- หากคุณต้องการสร้างเฉพาะไฟล์ลายเซ็น ขั้นตอนที่เหมาะสมได้แก่ 1 และ 3
 - สำหรับ HP Sure Recover ขั้นตอนพื้นฐานที่เหมาะสมได้แก่ 1, 2 และ 3 คุณจะต้องใช้คีย์สาธารณะจากขั้นตอนที่ 2 เพื่อจัดเตรียมระบบเป้าหมายของคุณ
 - ขั้นตอนที่ 4 เป็นเพียงทางเลือก แต่ขอแนะนำให้ดำเนินการ เพื่อให้สามารถตรวจสอบไฟล์ลายเซ็นและไฟล์กำกับได้อย่างถูกต้อง
-

การโฮสต์ไฟล์

โฮสต์ไฟล์ต่อไปนี้บนเซิร์ฟเวอร์ของคุณจากโฟลเดอร์ C:\staging:

- *.swm
- custom.mft (หรือชื่อไฟล์ที่คุณเลือกเองสำหรับไฟล์กำกับ)
- custom.sig (หรือชื่อไฟล์ที่ตรงกันที่คุณเลือกไว้สำหรับไฟล์ลายเซ็น)

 **หมายเหตุ:** หากคุณใช้ IIS เป็นโฮสต์ขั้นการโฮสต์ของคุณ คุณจะต้องกำหนดรายการ MIME ของคุณ โดยรวมนามสกุลต่อไปนี้ไว้ และกำหนดค่าทั้งหมดเป็น "application/octet-stream:"

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

การจัดเตรียมระบบเป้าหมายของคุณ

คุณสามารถจัดเตรียมระบบเป้าหมายของคุณได้ โดยใช้ HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover หรือ the Manageability Integration Kit (MIK) (<https://www.hp.com/go/clientmanagement>)

ป้อนข้อมูลต่อไปนี้สำหรับการจัดเตรียมนี้:

1. ที่อยู่ URL ของไฟล์กำกับที่โฮสต์ไว้ในส่วนก่อนหน้า (http://your_server.domain/path/custom.mft)
2. คีย์สาธารณะที่ใช้ในการตรวจสอบไฟล์ลายเซ็นที่สร้างไว้ก่อนหน้านี้ (เช่น C:\staging\my-recovery-public.pem)

การแก้ไขปัญหา

หากคุณได้รับข้อความเกี่ยวกับกระบวนการกู้คืนแบบกำหนดเองไม่ผ่านการตรวจสอบการรักษาความปลอดภัยให้ตรวจสอบรายละเอียดต่อไปนี้:


1. ไฟล์กำกับต้องอยู่ในรูปแบบ UTF-8 without BOM
2. ตรวจสอบแฮชไฟล์
3. ตรวจสอบให้แน่ใจว่าได้ทำการจัดเตรียมระบบด้วยคีย์สาธารณะที่ตรงตามคีย์ส่วนบุคคล ซึ่งใช้ในการเซ็นชื่อไฟล์กำกับ
4. ประเภท mime ของเซิร์ฟเวอร์ IIS ต้องเป็น application/octet-stream
5. พารของไฟล์ภายในไฟล์กำกับ ต้องมีพารแบบเต็มไปยั้งใดเรทหรือรับนสุด ซึ่งมีอิมเมจอยู่ ตามที่สามารถมองเห็นได้จากระบบไคลเอนต์ พารนี้จะไม่ใช่พารแบบเต็มที่ใช้ในการบันทึกไฟล์ไว้ ณ จุดกระจายข้อมูล

3 การใช้งานเอเจนต์ HP Sure Recover ภายใน ไฟร์วอลล์บริษัท


สามารถโฮสต์เอเจนต์ HP Sure Recover ไว้บนอินเทอร์เน็ตบริษัทได้ หลังจากติดตั้ง HP Sure Recover SoftPaq แล้วให้คัดลอกไฟล์เอเจนต์จากไดเรกทอรีของเอเจนต์ HP Sure Recover จากตำแหน่งที่ติดตั้งไปยังจุดกระจายข้อมูล HTTP หรือ FTP จากนั้นจัดเตรียมระบบไคลเอนต์โดยใช้ URL ของจุดกระจายข้อมูลและคีย์สาธารณะของ HP ที่ชื่อ `hpsr_agent_public_key.pem` ซึ่งจะมีการส่งไปพร้อมกับเอเจนต์ HP Sure Recover SoftPaq

การติดตั้งเอเจนต์ HP Sure Recover

1. ดาวน์โหลดเอเจนต์ HP Sure Recover และแยกไฟล์ไปยังจุดกระจายข้อมูล HTTP หรือ FTP ของคุณ
2. ตั้งค่าสิทธิ์ของไฟล์บนจุดกระจายข้อมูลตามความเหมาะสม
3. หากคุณใช้งาน Internet Information Services (IIS) ให้สร้างประเภท MIME application/octet-stream สำหรับรูปแบบไฟล์ต่อไปนี้:
 - .
 - .wim
 - .swm
 - .mft
 - .sig
 - .efi
 - .sdi

 **สิ่งสำคัญ:** ขั้นตอนต่อไปนี้จะอธิบายถึงการจัดเตรียม Sure Recover โดยใช้ SCCM สามารถดูตัวอย่างวิธีการจัดเตรียม Sure Recover โดยใช้ HP Client Management Script Library ได้ที่ [การใช้งานพร้อม HP Client Management Script Library \(CMSL\) ในหน้า 13](#)

4. เริ่มต้น SCCM ไปที่ **HP Client Security Suite** และจากนั้น เลือกหน้า HP Sure Recover

 **หมายเหตุ:** URL ของจุดกระจายข้อมูล จะใช้ ftp หรือ http เป็นโปรโตคอลการขนส่ง และยังมีพารามิเตอร์เพิ่มเติมไปยังไดเรกทอรีบนสุด ซึ่งมีไฟล์กำกับสำหรับเอเจนต์ HP Sure Recover ตามที่มองเห็นได้จากระบบเอเจนต์ด้วย พารามิเตอร์จะไม่ใช้พารามิเตอร์ที่ใช้ในการบันทึกไฟล์ไว้ ณ จุดกระจายข้อมูล

5. ในส่วน **อิมเมจแพลตฟอร์ม** ให้เลือกตัวเลือก **บริษัท** เพื่อคืนค่าอิมเมจ OS ที่ปรับแต่งเองจากจุดกระจายข้อมูลของบริษัท ป้อนค่า URL ที่ได้จากผู้ดูแลระบบ IT ลงในช่อง **URL ตำแหน่งอิมเมจ** ป้อนคีย์สาธารณะ `hpsr_agent_public_key.pem` ลงในช่อง **การตรวจสอบอิมเมจ**

 **หมายเหตุ:** URL ของอิมเมจแบบกำหนดเอง จะต้องมียชื่อไฟล์กำกับอิมเมจอยู่ด้วย

6. ในส่วน **เอเจนต์การกู้คืน** ให้เลือกตัวเลือก **บริษัท** เพื่อใช้เอเจนต์การกู้คืนแบบกำหนดเอง หรือเอเจนต์การกู้คืนของ HP จากจุดกระจายข้อมูลของบริษัท ป้อน URL ที่ได้จากผู้ดูแลระบบ IT ลงในช่อง **URL ตำแหน่งเอเจนต์** ป้อนคีย์สาธารณะ `hpsr_agent_public_key.pem` ลงในช่อง **คีย์การตรวจสอบของเอเจนต์**

 **หมายเหตุ:** ห้ามใส่ชื่อไฟล์สำหรับไฟล์กำกับเอเจนต์ลงใน URL เนื่องจาก BIOS กำหนดให้ต้องใช้ชื่อ `recovery.mft`


7. หลังจากปรับใช้นโยบายกับระบบไคลเอนต์แล้ว ให้ทำการรีสตาร์ท
8. ในระหว่างการจัดเตรียมเบื้องต้น จะมีข้อความแจ้งให้คุณป้อนรหัสรักษาความปลอดภัย 4 ตัว เพื่อทำการเปิดใช้งาน HP Sure Recover หากต้องการดูรายละเอียดเพิ่มเติม ให้ไปที่ hp.com และค้นหาเอกสารรายงานเป็นทางการของบริษัท HP Manageability Integration Kit (MIK) for Microsoft System Center Manager

หลังจากเปิดใช้งาน HP Sure Recover เป็นที่สำเร็จแล้ว URL ที่กำหนดเองซึ่งได้รับการปรับใช้โดยนโยบาย จะปรากฏขึ้นในเมนูการตั้งค่า BIOS ของ HP Sure Recover

เพื่อยืนยันว่าการเปิดใช้งานเป็นที่สำเร็จ ให้รีสตาร์ทคอมพิวเตอร์ และเมื่อโลโก้ HP ปรากฏขึ้น ให้กด **f10** เลือก **ขั้นสูง** เลือก **HP Sure Recover** เลือก **เอเจนต์การกู้คืน** และจากนั้นเลือก **URL**

4 การใช้งานพร้อม HP Client Management Script Library (CMSL)

HP Client Management Script Library ช่วยให้คุณสามารถจัดการการตั้งค่าของ HP Sure Recover โดยใช้ PowerShell ได้ สคริปต์ตัวอย่างต่อไปนี้ จะสาธิตวิธีการจัดเตรียม กำหนดสถานะ เปลี่ยนแปลงการกำหนดค่า และยกเลิกการจัดเตรียม HP Sure Recover

 **หมายเหตุ:** มีหลายคำสั่งที่มีความยาวเกินความยาวของบรรทัดในเอกสารคู่มือนี้ แต่ในการทำงานจริงจะต้องป้อนรวมไว้ในบรรทัดเดียว

```
$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
}

```

การสร้างคีย์ตัวอย่างโดยใช้ OpenSSL

จัดเก็บคีย์ส่วนบุคคลไว้ในที่ปลอดภัย จะมีการใช้คีย์สาธารณะในการตรวจสอบ และจะต้องป้อนในระหว่างการจัดเตรียม คีย์เหล่านี้จะต้องมีความยาว 2048 บิต และใช้เอ็กซ์โพเนน 0x10001 แทนที่หัวข้อในตัวอย่างไม่ด้วยข้อมูลเกี่ยวกับองค์กรของคุณ

ตั้งค่าตัวแปรสภาพแวดล้อมต่อไปนี้ ก่อนดำเนินการต่อ:

```
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:
```

คุณสามารถเซ็นชื่อไฟล์กำกับอิมเมจได้โดยใช้คำสั่งนี้:

```
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:
```

คุณสามารถเซ็นชื่อไฟล์กำกับเอเจนต์ได้โดยใช้คำสั่งนี้:

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

OpenSSL จะสร้างไฟล์ลายเซ็นในรูปแบบ **big-endian** ซึ่งจะไม่สามารถใช้งานร่วมกับ BIOS บางเวอร์ชันได้ ดังนั้น อาจจำเป็นต้อง ย้อนกลับลำดับไบนารีไฟล์ลายเซ็นเอเจนต์ก่อนทำการปรับใช้ BIOS เวอร์ชันที่รองรับการเรียงลำดับไบนารีแบบ **big-endian** จะรองรับการเรียงลำดับแบบ **little-endian** ด้วยเช่นกัน

A การแก้ไขปัญหา

การจัดพาร์ติชันไดรฟ์ล้มเหลว

การจัดพาร์ติชันไดรฟ์ล้มเหลวอาจเกิดขึ้นในกรณีที่พาร์ติชัน SR_AED หรือ SR_IMAGE ได้รับการเข้ารหัสไว้ด้วย BitLocker โดยปกติแล้ว พาร์ติชันเหล่านี้จะได้รับการสร้างขึ้นด้วยแอตทริบิวต์ gpt ที่ป้องกันไม่ให้ BitLocker ทำการเข้ารหัส แต่หากผู้ใช้ลบและสร้างพาร์ติชันใหม่ หรือสร้างขึ้นด้วยตัวเองบนไดรฟ์แบบ bare metal เอเจนต์ Sure Recover จะไม่สามารถลบออกได้ และจะออกจากการทำงานพร้อมแสดงข้อผิดพลาดในขณะจัดพาร์ติชันไดรฟ์ดังกล่าวใหม่ ผู้ใช้จะต้องลบออกด้วยตัวเอง โดยการรัน diskpart เลือกไดรฟ์ และส่งคำสั่งแทนที่ del vol หรือคำสั่งที่คล้ายกัน

ข้อมูลบันทึกการตรวจสอบเฟิร์มแวร์

ข้อมูลตัวแปร EFI จะมีดังต่อไปนี้:


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

มี API อยู่ใน Windows สำหรับการอ่านค่าตัวแปร EFI หรือคุณสามารถสืบเนื้อหาตัวแปรไปยังไฟล์ได้ โดยใช้ยูทิลิตี้ UEFI Shell dmpstore

คุณสามารถสืบข้อมูลบันทึกเหตุการณ์การตรวจสอบได้โดยใช้คำสั่ง Get-HPFirmwareAuditLog ซึ่งจัดเตรียมโดย HP Client Management Script Library

ข้อมูลบันทึกเหตุการณ์ของ Windows

Sure Recover จะเริ่มต้นและหยุดเหตุการณ์ที่มีการส่งจากข้อมูลบันทึกเหตุการณ์การตรวจสอบ BIOS ซึ่งคุณสามารถดูได้ใน Windows Event Viewer ในข้อมูลบันทึกเหตุการณ์ Sure Start หากมีการติดตั้ง HP Notifications ไว้ เหตุการณ์เหล่านี้จะประกอบไปด้วยวันที่และเวลา ID ต้นทาง ID เหตุการณ์ และรหัสเฉพาะเหตุการณ์ เช่น [fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3] ซึ่งจะระบุว่าการกู้คืนล้มเหลว เนื่องจากไม่สามารถรับรองความถูกต้องไฟล์กำกับด้วยรหัสระบุเหตุการณ์ c3f 23000 ที่มีการบันทึกไว้เมื่อเวลา 2:26:40 ในวันที่ 6/27/18

 **หมายเหตุ:** ข้อมูลบันทึกเหตุการณ์เหล่านี้ จะใช้รูปแบบเดือน/วัน/ปี ตามวันที่สหรัฐอเมริกา

HP Secure Platform Management (ID ต้นทาง = 84h)

ตาราง A-1 HP Secure Platform Management

ID เหตุการณ์	จำนวนอุปกรณ์ (ทั้งหมด/DaaS)	จำนวนเหตุการณ์ (ทั้งหมด/DaaS)	คำอธิบาย	หมายเหตุ
40	256/178	943/552	เริ่มต้นกระบวนการกู้คืนแพลตฟอร์ม OS โดยเฟิร์มแวร์	เริ่มต้นการกู้คืนแพลตฟอร์มแล้ว

ตาราง A-1 HP Secure Platform Management (ต่อ)

ID เหตุการณ์	จำนวนอุปกรณ์ (ทั้งหมด/DaaS)	จำนวนเหตุการณ์ (ทั้งหมด/DaaS)	คำอธิบาย	หมายเหตุ
41	221/147	588/332	กระบวนการกู้คืนแพลตฟอร์ม OS เสร็จสมบูรณ์แล้ว	การกู้คืนแพลตฟอร์มเสร็จสมบูรณ์แล้ว
42	54/42	252/156	กระบวนการกู้คืนแพลตฟอร์ม OS ไม่เสร็จสมบูรณ์	การกู้คืนแพลตฟอร์มล้มเหลว

คุณสามารถเรียกใช้งานข้อมูลบันทึกเหตุการณ์การตรวจสอบเฟิร์มแวร์ได้โดยใช้ Get-HPFirmwareAuditLog ใน HP Client Management Script Library ซึ่งสามารถโหลดได้ที่ <http://www.hp.com/go/clientmanagement> ID เหตุการณ์ 40, 41 และ 42 ของ HP Secure Platform Management จะส่งคืนรหัสระบุเหตุการณ์ในช่องข้อมูล ซึ่งจะระบุผลการทำงานของ Sure Recover เช่น รายการข้อมูลบันทึกเหตุการณ์ต่อไปนี้ จะระบุว่า Sure Recover ล้มเหลวในการดาวน์โหลดไฟล์กำกับหรือไฟล์ลายเซ็น โดยมีข้อผิดพลาด event_id 42 และข้อมูล: 00:30:f1:c3 ซึ่งควรแปลเป็นค่า 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
```

การกู้คืนสำเร็จจะปรากฏในรูปแบบ event_id = 41 และข้อมูล: 00:00:00:00 เช่น:

```
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 จะใช้รหัสระบุเหตุการณ์ต่อไปนี้

ตาราง A-2 รหัสระบุเหตุการณ์

คำอธิบายเหตุการณ์	รหัสเหตุการณ์
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

ตาราง A-2 รหัสระบุเหตุการณ์ (ต่อ)

คำอธิบายเหตุการณ์	รหัสเหตุการณ์
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000