Käyttöopas

HP Sure Recover

Ensimmäinen painos: helmikuu 2020

Asiakirjan osanumero: L93434-351

Käyttäjän syöttämä syntaksiavain

Käyttöliittymään kirjoitettava teksti on merkitty `kiinteäleveyksisellä fontilla`.

Taulukko -1 Käyttäjän syöttämä syntaksiavain

Kohde	Kuvaus
`Teksti ilman sulkeita tai aaltosulkeita`	Kohteet, jotka on kirjoitettava täsmälleen samalla tavalla kuin kuvassa
`<Kulmasulkeiden sisällä oleva teksti>`	Paikkamerkki, jonka arvo on annettava; jätä sulkeet pois
`[Hakasulkeiden sisällä oleva teksti]`	Valinnaisia kohteita; jätä sulkeet pois
`{Aaltosulkeiden sisällä oleva teksti}`	Kohteiden sarja, joista voit valita vain yhden; jätä aaltosulkeet pois
`|`	Erotin kohteille, joista voit valita vain yhden; jätä pystypalkki pois
`...`	Kohteet, jotka voivat toistua tai joiden täytyy toistua; jätä ellipsi pois

Sisällysluettelo

1 Aloitusopas

HP Sure Recover auttaa sinua asentamaan käyttöjärjestelmän turvallisesti verkosta. Käyttäjän ei tarvitse osallistua suurimpaan osaan asennuksesta. Järjestelmät, joissa on HP Sure Recover ja Embedded Reimaging, tukevat asennusta myös paikalliselta tallennuslaitteelta.

TÄRKEÄÄ: Varmuuskopioi tiedot ennen HP Sure Recover -toiminnon käyttöä. Näköistiedoston luomisprosessi alustaa aseman, joten sen tiedot menetetään.

HP:n palautusnäköistiedostoissa on perustason Windows 10® -asennusohjelma. Vaihtoehtoisesti HP Sure Recover voi asentaa HP-laitteille optimoidut ohjaimet. HP Recovery -näköistiedostot sisältävät vain Windows 10:een sisältyviä tietojenpalautusagentteja. Yritykset voivat luoda omia mukautettuja näköistiedostojaan, joihin voidaan sisällyttää yritysten omia asetuksia, sovelluksia, ohjaimia ja tietojenpalautusagentteja.

Käyttöjärjestelmän palautusagentti suorittaa palautusnäköistiedoston asentamiseen vaadittavat toimenpiteet. HP:n palautusagentti suorittaa tavalliset toimenpiteet, kuten osioinnin, muotoilun ja palautusnäköistiedoston purkamisen kohdelaitteelle. HP:n palautusagentti sijaitsee verkossa osoitteessa hp.com, joten tarvitset Internet-yhteyden sen palauttamiseen, ellei järjestelmässä ole upotettua näköistiedoston uudelleenasentamisominaisuutta. Yritykset voivat myös isännöidä HP:n palautusagenttia yrityksen oman palomuurin sisällä tai luoda mukautettuja palautusagentteja monimutkaisempia palautusympäristöjä varten.

Voit käynnistää HP Sure Recover -palautuksen, kun käyttöjärjestelmää ei ole. Voit myös suorittaa HP Sure Recover -ohjelman ajastetusti, esimerkiksi haittaohjelmien poistamisen varmistamiseksi. Määritä nämä asetukset HP Client Security Managerin (CSM), Manageability Integration Kitin (MIK) tai HP Client Management Script Libraryn kautta.

Palauttaminen verkon kautta

HUOMAUTUS: Jotta voit suorittaa palautuksen verkon kautta, sinun on käytettävä langallista yhteyttä. HP suosittelee, että varmuuskopioit tärkeät tiedostot, tiedot, kuvat, videot ja muut kohteet ennen kuin käytät HP Sure Recover -toimintoa. Näin et menetä tietoja.

1. Liitä asiakasjärjestelmä verkkoon, jossa HTTP- tai FTP-jakelupistettä voidaan käyttää.
2. Käynnistä asiakasjärjestelmä uudelleen, ja kun HP-logo ilmestyy näyttöön, paina F11-näppäintä.
3. Valitse **Palauta verkosta**.

Paikallisen aseman palauttaminen

Näköistiedosto ladataan asiakasjärjestelmään ajastuksen mukaisesti, jos asiakasjärjestelmä tukee upotettua näköistiedoston uudelleenasentamista ja ajastettu näköistiedoston lataaminen -valinta on otettu käyttöön sovellettavassa käytännössä. Kun näköistiedosto on ladattu asiakasjärjestelmään, käynnistä se uudelleen, jotta voit kopioida näköistiedoston Embedded Reimaging -ominaisuudella varustettuun tallennuslaitteeseen.

Voit suorittaa paikallisen palautuksen käyttämällä Embedded Reimaging -ominaisuudella varustetulla tallennuslaitteella olevaa näköistiedostoa:

1. Käynnistä asiakasjärjestelmä uudelleen, ja kun HP-logo ilmestyy näyttöön, paina F11-näppäintä.
2. Valitse **Palautus paikallisesta asemasta**.

Jos käytössä on Embedded Reimaging -ominaisuudella varustettu järjestelmä, latauksia varten on määritettävä ajastus ja päivitykset on tarkistettava latausagentin avulla. Latausagentti sisältyy HP Client Security Managerin Sure Recover -liitännäiseen. Se voidaan määrittää myös Manageability Integration Kitin kautta. Lisätietoja Manageability Integration Kitin käytöstä on osoitteessa https://www.hp.com/go/clientmanagement.

Voit myös luoda ajastetun tehtävän, jossa agentti kopioidaan SR_AED-osioon ja näköistiedosto SR_IMAGE-osioon. Tämän jälkeen voit lähettää HP Client Management Script Libraryn kautta BIOSille palvelutapahtuman. Tällä palvelutapahtumalla ohjataan BIOSia vahvistamaan ja kopioimaan sisältö näköistiedoston uudelleenluomista tukevalle tallennuslaitteelle seuraavan uudelleenkäynnistyksen yhteydessä.

2 Näköistiedoston luominen yrityskäyttöön

Useimmat yritykset käyttävät Microsoft Deployment Tools -työkaluja, Windows 10 Assessment and Deployment Kitiä tai molempia tuottaakseen Windows Imaging (WIM) -muotoisiin arkistoihin sisältyviä tiedostoja, jotka sisältävät näköistiedoston.

Vaatimukset

- Viimeisin Windows 10 Assessment and Deployment Kit (Windows ADK) -versio
- PowerShell
- OpenSSL (tai muu ratkaisu yksityisen ja julkisen avaimen RSA-avainparin luomiseen)

  Tämän avulla voit luoda RSA-avainparin, jota käytetään luomasi ja isännöimäsi yritysnäköistiedoston eheyden suojaamiseen.
- Palvelinten isännöintiratkaisu (kuten Microsoft Internet Information Services [IIS])

Näköistiedoston luominen

Ennen kuin aloitat näköistiedoston luomisen, määritä työjärjestelmä tai koontiversiojärjestelmä, johon asensit tarvittavat työkalut näköistiedoston käsittelemistä varten, kuten seuraavassa on esitetty:

1. Avaa järjestelmänvalvojana `Deployment and Imaging Tools Environment` -komentorivi (asennetaan Windows ADK:n Deployment Tools -työkalujen avulla).
2. Luo näköistiedostolle valmistelualue seuraavan komennon avulla:

   ```
   mkdir C:\staging
   ```
3. Luo näköistiedosto käyttäen jotain seuraavista esimerkeistä:

   Esimerkki 1: Microsoft Windowsin asennusnäköistiedostoon pohjautuvan näköistiedoston luominen sivulla 3

   Esimerkki 2: Viitejärjestelmään perustuvan näköistiedoston luominen sivulla 6

Esimerkki 1: Microsoft Windowsin asennusnäköistiedostoon pohjautuvan näköistiedoston luominen

1. Avaa tai ota käyttöön Microsoft Windowsin asennusnäköistiedosto (Microsoft ISO -tiedostosta tai HP OSDVD -levyltä).
2. Kopioi install.wim-tiedosto käyttöönotetusta Windows-asennusnäköistiedostosta valmistelualueelle seuraavan komennon avulla:

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

   HUOMAUTUS: `<M:>` viittaa käyttöönotettuun asemaan. Korvaa tämä kyseessä olevan aseman kirjaimella.

3. Nimeä install.wim uudelleen näköistiedoston tiedostonimellä (tässä esimerkissä ”my-image”) seuraavan komennon avulla:

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

(Valinnainen) HP Sure Recover sisältää ominaisuuden, jonka avulla voit palauttaa tietyn version usean indeksin näköistiedostosta. Tämä perustuu kyseessä olevalle HP-kohdejärjestelmälle tehtaalla lisensoituun Windows-versioon. Tämä mekanismi toimii, jos indeksit on nimetty oikein. Jos käyttämäsi Windowsin asennusnäköistiedosto on peräisin HP:n OSDVD-levyltä, se on todennäköisesti usean version näköistiedosto. Jos et halua käyttää tätä toimintoa ja haluat, että kaikki kohdejärjestelmäsi käyttävät tiettyä samaa versiota, varmista, että näköistiedostoon sisältyy vain yksi indeksi.

4. Tarkastele asennusnäköistiedoston sisältöä seuraavan komennon avulla:

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

Alla on näyte tuloksista asennusnäköistiedostosta, joka tukee viittä versiota (jotka sovitetaan kunkin kohdejärjestelmän BIOSin perusteella):

Näköistiedoston tiedot: `my-image.wim`

Indeksi: `1`

Nimi: `CoreSingleLanguage`

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

Koko: `19 512 500 682 tavua`

Indeksi: `2`

Nimi: `Ydin`

Kuvaus: `Windows 10 May 2019 Update - Home Edition`

Koko: `19 512 500 682 tavua`

Indeksi: `3`

Nimi: `Professional`

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

Koko: `19 758 019 520 tavua`

Indeksi: `4`

Nimi: `ProfessionalEducation`

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

Koko: `19 758 019 480 tavua`

Indeksi: `5`

Nimi: `ProfessionalWorkstation`

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

Koko: `19 758 023 576 tavua`

HUOMAUTUS: Kun indeksejä on vain yksi, näköistiedostoa käytetään nimestä riippumatta. Näköistiedoston koko voi olla suurempi kuin ennen poistoja.

5. Jos et halua käyttää useamman version toimintoa, poista indeksit, joita et halua käyttää.

   Kuten seuraavasta esimerkistä näkyy, jos haluat vain Professional-version (olettaen, että kaikki kohdejärjestelmät on lisensoitu), poista indeksit 5, 4, 2 ja 1. Indeksinumerot määritetään uudelleen aina, kun poistat indeksin. Tästä johtuen indeksit on poistettava järjestyksessä suurimmasta indeksinumerosta pienimpään. Suorita `Get-ImageInfo` jokaisen poiston jälkeen, niin voit varmuuden vuoksi katsoa, mikä indeksi sinun on poistettava seuraavaksi.

   ```
   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
   ```

   Valitse vain yksi version indeksi (tässä esimerkissä Professional). Kun indeksejä on vain yksi, näköistiedostoa käytetään nimestä riippumatta. Huomaa, että näköistiedoston koko voi olla suurempi kuin ennen poistoja. Tämä johtuu WIM-metatietojen muokkausten ja sisällön normalisoinnin toimintamallista.

6. (Valinnainen) Jos haluat sisällyttää ohjaimet yrityksen palautusnäköistiedostoon, toimi seuraavasti:

   a. Ota näköistiedosto käyttöön tyhjässä kansiossa seuraavien komentojen avulla:

   ```
   mkdir C:\staging\mount
   ```

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

   b. Ota käyttöön tuetulle kohdejärjestelmälle kuuluva HP Windows 10 Driver DVD (DRDVD) -ohjain-DVD-levy. Kopioi ohjaimen alikansiot käyttöön otetulta ohjaimen asennusmedialta valmistelualueelle seuraavan komennon avulla:

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

   HUOMAUTUS: `<M:>` viittaa käyttöön otettuun asemaan. Korvaa tämä kyseessä olevan aseman kirjaimella.

   Voit sisällyttää lisää .inf-tyylisiä ohjaimia sijoittamalla ne C:\staging\mount\SWSETUP\DRV -kansioon. Lisätietoja siitä, kuinka tämä sisältö käsitellään HP Sure Recover -ohjelmalla käyttämällä `dism /Add-Driver /Recurse` -funktiota, löydät kohdasta Add and Remove Drivers to an Offline Windows image (Lisää ja poista ohjaimia Windowsin Offline-näköistiedostosta), joka sisältyy seuraavaan artikkeliin: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Tämä ominaisuus ei tue .exe-tyylisiä ohjaimia, jotka vaativat sovelluksen suorittamista.

   c. Tallenna muutokset ja poista näköistiedosto käytöstä seuraavan komennon avulla:

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

   Tuloksena saatava näköistiedosto on C:\staging\my-image.wim.

   d. Siirry kohtaan Näköistiedoston jakaminen sivulla 6.

Esimerkki 2: Viitejärjestelmään perustuvan näköistiedoston luominen

1. Luo käynnistystä tukeva USB WinPE -tietoväline.

   HUOMAUTUS: Lisämenetelmiä näköistiedoston sieppaamiseen löytyy ADK:n ohjeista.

   Varmista, että USB-muistitikulla on riittävästi vapaata tilaa, jotta viitejärjestelmästä siepattu näköistiedosto voidaan säilyttää.

2. Luo näköistiedosto viitejärjestelmään.
3. Sieppaa näköistiedosto käyttöön käynnistämällä viitejärjestelmä USB WinPE -tietovälineeltä ja käyttämällä sitten DISM-työkalua.

   HUOMAUTUS: `<U:>` viittaa USB-asemaan. Korvaa tämä kyseessä olevan aseman kirjaimella.

   Muokkaa tiedostonimen “my-image”-osaa ja kuvausta `<my-image>` tarvittaessa.

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

4. Kopioi näköistiedosto USB-muistitikulta työjärjestelmäsi valmistelualueelle seuraavan komennon avulla:

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

   Sinun pitäisi saada seuraava näköistiedosto: C:\staging\my-image.wim.

5. Siirry kohtaan Näköistiedoston jakaminen sivulla 6.

Näköistiedoston jakaminen

HP suosittelee, että jaat näköistiedoston pienemmiksi tiedostoiksi, jotta voit parantaa verkkolatausten luotettavuutta. Voit tehdä näin seuraavan komennon avulla:

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

HUOMAUTUS: FileSize (tiedostokoko) näytetään megatavuina. Muokkaa tarvittaessa.

HUOMAUTUS: DISM-työkalun jakoalgoritmin luonteen vuoksi luotujen SWM-tiedostojen koot voivat olla joko pienempiä tai suurempia kuin ilmoitettu tiedostokoko.

Kokoonpanotietojen luominen

Muotoile luettelotiedostot UTF-8-koodattuun muotoon ilman tavujärjestysmerkkiä (BOM).

Voit muuttaa seuraavissa toimissa käytettävää luettelotiedoston nimeä (custom.mft), mutta tiedostopäätteitä .mft ja .sig ei tule muokata. Tämän lisäksi luettelotiedoston ja allekirjoitustiedoston tiedostonimien on vastattava toisiaan. Voit esimerkiksi muuttaa parin (custom.mft, custom.sig) muotoon (myimage.mft, myimage.sig).

Muuttujaa `mft_version` käytetään määrittämään kuvatiedoston muoto, ja sen arvon on tässä vaiheessa oltava 1.

Muuttujan `image_version` avulla voidaan määrittää, onko näköistiedostosta saatavilla uudempaa versiota. Sen avulla voidaan myös estää vanhojen versioiden asentaminen.

Molempien arvojen on oltava etumerkittömiä 16-bittisiä kokonaislukuja, minkä lisäksi kokoonpanotietojen rivin erottimen on oltava `'\r\n' (CR + LF)`.

Kokoonpanotietojen muodostaminen

Koska jaetussa näköistiedostossa voi olla useita tiedostoja, voit luoda kokoonpanotiedot PowerShell-komentosarjalla.

Sinun on oltava kansiossa C:\staging kaikkia seuraavia vaiheita varten.

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

1. Käytä PowerShell-komentosarjan luomiseen editoria, joka pystyy tuottamaan UTF-8-tekstitiedoston ilman tavujärjestysmerkkiä. Luo komentosarja seuraavan komennon avulla: `notepad C:\staging\generate-manifest.ps1`

   Luo seuraava komentosarja:

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

   `$imageVersion = 1907` (Huomaa: tämä voi olla mikä tahansa 16-bittinen kokonaisluku)

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

}
```

HUOMAUTUS: HP Sure Recoverin kanssa käytettävissä kokoonpanotiedoissa ei saa olla tavujärjestysmerkkiä. Seuraavat komennot kirjoittavat tiedoston uudelleen UTF-8-koodattuna ilman tavujärjestysmerkkiä.

```
$content = Get-Content $mftFilename

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

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

2. Tallenna komentosarja.
3. Suorita komentosarja.

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

Kokoonpanotietojen tunnisteen muodostaminen

Sure Recover vahvistaa agentin ja näköistiedoston salausallekirjoitusten avulla. Seuraavissa esimerkeissä käytetään yksityisestä ja julkisesta avaimesta koostuvaa avainparia X.509 PEM -muodossa (.PEM-tiedostopääte). Säädä komennot tilannekohtaisesti käyttämään joko DER-binäärivarmenteita (.CER- tai .CRT-tiedostopääte), BASE-64-koodattuja PEM-varmenteita (.CER- tai .CRT-tiedostopääte) tai PKCS1 PEM -tiedostoja (.PEM-tiedostopääte). Esimerkissä käytetään myös OpenSSL-toteutusta, joka luo allekirjoitukset big endian -muodossa. Voit käyttää mitä tahansa apuohjelmaa allekirjoittamiseen, mutta jotkin BIOS-versiot tukevat vain little endian -muotoisia allekirjoituksia.

1. Muodosta 2048-bittinen yksityinen RSA-avain seuraavan komennon avulla. Jos sinulla on 2048-bittinen yksityisen ja julkisen avaimen RSA-avainpari PEM-muodossa, kopioi ne kohteeseen C:\staging ja siirry sitten suoraan vaiheeseen 3.

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

2. Muodosta julkinen avain yksityisen avaimen pohjalta (jos sinulla on yksityistä avaintasi vastaava PEM-muotoinen julkinen avain, kopioi se kohteeseen C:\staging) seuraavan komennon avulla:

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

3. Luo ensimmäisen vaiheen 2048-bittiseen RSA-avaimeen pohjautuva allekirjoitustiedosto (käyttäen sha256-pohjaista hajautusarvoa) seuraavan komennon avulla:

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

4. Tarkista allekirjoitustiedosto edellisen vaiheen julkisella avaimella seuraavan komennon avulla:

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

HUOMAUTUS:

- Jos haluat luoda pelkän allekirjoitustiedoston, sinun tarvitsee suorittaa vain vaiheet 1 ja 3.
- Vähimmäisvaiheet HP Sure Recoveria varten ovat 1, 2 ja 3. Tarvitset julkisen avaimen vaiheesta 2, jotta voit valmistella kohdejärjestelmän.
- Vaiheen 4 suorittaminen on vapaaehtoista. Sen suorittaminen on kuitenkin suositeltavaa, jotta allekirjoitustiedosto ja luettelotiedosto tarkistetaan oikein.

Tiedostojen isännöinti

Isännöi seuraavia palvelimessa olevia tiedostoja kansiosta C:\staging käsin:

- *.swm
- custom.mft (tai luettelotiedostolle valitsemasi tiedostonimi)
- custom.sig (tai valitsemasi allekirjoitustiedoston nimeä vastaava nimi)

HUOMAUTUS: Jos käytät isännöintiin IIS-ohjelmistoa, sinun on määritettävä MIME-merkintäsi sisältämään seuraavat laajennukset, määriteltynä seuraavasti: "application/octet-stream:"

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

Kohdejärjestelmien valmisteleminen

Voit valmistella kohdejärjestelmät käyttämällä HP Client Management Script Librarya, HP Client Security Manageria (CSM) / Sure Recoveria tai Manageability Integration Kitiä (MIK) (https://www.hp.com/go/clientmanagement).

Anna seuraavat tiedot tätä valmistelua varten:

1. Edellisessä osassa isännöidyn luettelotiedoston URL-osoite (http://oman_palvelimesi_nimi.domain/path/custom.mft)
2. Aiemmin luodun allekirjoitustiedoston tarkistamiseen käytetty julkinen avain (esimerkiksi C:\staging\my-recovery-public.pem).

Vianmääritys

Jos saat ilmoituksen mukautetun palautusprosessin turvatarkistuksen epäonnistumisesta, varmista seuraavat asiat:

1. Kokoonpanotietojen on oltava UTF-8-koodattuja, eikä niissä saa olla tavujärjestysmerkkiä.
2. Tarkista tiedostojen hajautusarvot.
3. Varmista, että järjestelmä on valmisteltu julkisella avaimella, joka vastaa kokoonpanotietojen allekirjoitukseen käytettyä yksityistä avainta.

4. IIS-palvelimen MIME-tyyppien on oltava `application/octet-stream`.
5. Kokoonpanotietojen tiedostopolkujen täytyy sisältää koko polku asiakasjärjestelmästä katsottuna ylimpään hakemistoon, joka sisältää näköistiedoston. Tämä polku ei ole se koko polku, johon tiedostot tallennetaan jakelupisteessä.

3 HP Sure Recover Agent -agentin käyttäminen yrityksen palomuurin sisällä

HP Sure Recover Agent -agenttia voidaan isännöidä yrityksen intranetissä. Kun olet asentanut HP Sure Recover SoftPaq -tiedostot, kopioi agenttitiedostot asennussijainnin HP Sure Recover -agenttihakemistosta HTTP- tai FTP-jakelupisteeseen. Valmistele tämän jälkeen asiakasjärjestelmä käyttämällä jakelupisteen URL-osoitetta ja HP:n julkista avainta nimeltä `hpsr_agent_public_key.pem`. Avain toimitetaan HP Sure Recover -agentin Softpaqin mukana.

HP Sure Recover -agentin asentaminen

1. Lataa HP Sure Recover -agentti ja pura tiedostot HTTP- tai FTP-jakelupisteellesi.
2. Aseta jakelupisteelle asiaankuuluvat tiedosto-oikeudet.
3. Jos käytät IIS-palvelua (Internet Information Services), luo application/octet-stream-MIME-tyypit seuraaville tiedostomuodoille:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   TÄRKEÄÄ: Seuraavat vaiheet käsittelevät Sure Recoverin valmistelua SCCM:llä. Esimerkkejä Sure Recoverin valmistelusta HP Client Management Script Libraryn avulla löydät kohdasta HP Client Management Script Libraryn (CMSL) käyttö sivulla 13.
4. Käynnistä SCCM, siirry kohteeseen **HP Client Security Suite** ja valitse HP Sure Recover -sivu.

   HUOMAUTUS: Jakelupisteen URL-osoitteen siirtoprotokollana toimii joko FTP tai HTTP. Se sisältää myös koko polun asiakasjärjestelmästä katsottuna ylimpään hakemistoon, joka sisältää HP Sure Recover -agentin kokoonpanotiedot. Tämä polku ei ole se koko polku, johon tiedostot tallennetaan jakelupisteessä.
5. Palauta mukautettu käyttöjärjestelmän näköistiedosto yrityksen jakelupisteestä valitsemalla **Alustan näköistiedosto** -osiossa **Yritys**. Syötä IT-järjestelmänvalvojan toimittama URL-osoite **Kuvan sijainnin URL** -tekstikenttään. Syötä julkinen avain `hpsr_agent_public_key.pem` **Näköistiedoston tarkistus** -kenttään.

   HUOMAUTUS: Mukautetun näköistiedoston URL-osoitteen pitää sisältää näköistiedoston luettelotiedoston tiedostonimi.
6. Käytä mukautettua palautusagenttia tai HP:n palautusagenttia yrityksen jakelupisteeltä valitsemalla **Palautusagentti**-osiossa **Yritys**. Syötä IT-järjestelmänvalvojan toimittama URL-osoite **Agentin**

sijainnin URL -tekstikenttään. Syötä julkinen avain `hpsr_agent_public_key.pem` **Agentin tarkistusavain** -tekstikenttään.

HUOMAUTUS: Älä sisällytä kokoonpanotietojen tiedostonimeä URL-osoitteeseen. Toimiakseen BIOSin kanssa sen nimen on oltava recovery.mft.

7. Kun käytäntö on otettu käyttöön asiakasjärjestelmässä, käynnistä järjestelmä uudelleen.
8. Alkuvalmistelun aikana näyttöön tulee kehote, jossa pyydetään syöttämään nelinumeroinen turvakoodi HP Sure Recoverin aktivoinnin viimeistelemiseksi. Lisätietoja (englanniksi) löydät osoitteesta hp.com tekemällä haun HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

Kun HP Sure Recoverin aktivointi on onnistunut, käytännön käyttöön ottama mukautettu URL-osoite näkyy HP Sure Recoverin BIOS-asetusvalikossa.

Vahvista aktivoinnin onnistuminen käynnistämällä tietokone uudelleen. Kun HP-logo tulee näyttöön, paina F10. Valitse **Lisäasetukset**, valitse **HP Sure Recover**, valitse **Palautusagentti** ja valitse sitten **URL**.

4 HP Client Management Script Libraryn (CMSL) käyttö

HP Client Management Script Librarylla voit hallita HP Sure Recover -asetuksia PowerShellin kautta. Seuraavassa komentosarjaesimerkissä neuvotaan HP Sure Recoverin valmistelu, sen tilan selvittäminen, sen määrityksen muuttaminen sekä sen valmistelun poistaminen.

HUOMAUTUS: Useat näistä komennoista ylittävät tämän oppaan rivikohtaisen enimmäispituuden, mutta ne on todellisuudessa kirjoitettava yhdelle riville.

```
$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
}
```

Näyteavaimen muodostaminen OpenSSL:n avulla

Säilytä yksityisiä avaimia turvallisessa sijainnissa. Julkisia avaimia käytetään vahvistamiseen, ja ne on annettava valmisteluprosessin aikana. Näiden avainten on oltava 2048 bitin pituisia ja käytettävä eksponenttina arvoa 0x10001. Korvaa esimerkkien sisältökentät yrityksesi tiedoilla.

Aseta seuraava ympäristömuuttuja ennen kuin jatkat:

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


# Luo itse allekirjoitettu päämyöntäjän varmenne testausta varten
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=FI/ST=Maakunta/L=Kaupunki/O=Yritys/OU=Org/CN=www.example.com"


# Luo avaimen hyväksyntävarmenne
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
"/C=FI/ST=Maakunta/L=Kaupunki/O=Yritys/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:


# Luo komennon allekirjoitusnäppäin

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=/ST=Maakunta/L=Kaupunki/O=Yritys/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:


# Luo näköistiedoston allekirjoituspainike

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=FI/ST=Maakunta/L=Kaupunki/O=Yritys/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:
```

Voit myös allekirjoittaa näköistiedoston kokoonpanotiedot tämän komennon avulla:

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


# Luo agentin allekirjoituspainike

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=Fi/ST=Maakunta/L=Kaupunki/O=Yritys/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:
```

Voit allekirjoittaa agentin kokoonpanotiedot tämän komennon avulla:

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

OpenSSL luo allekirjoitustiedostot big endian -muodossa, joka ei ole yhteensopiva joidenkin BIOS-versioiden kanssa. Tästä johtuen agentin allekirjoitustiedoston tavujärjestys voidaan joutua muuttamaan päinvastaiseksi ennen käyttöönottoa. Big endian -tavujärjestystä tukevat BIOS-versiot tukevat myös little endian -tavujärjestystä.

A Vianmääritys

Aseman osiointi epäonnistui

Aseman osiointi voi epäonnistua, jos SR_AED-tai SR_IMAGE-osio salataan BitLockerilla. Nämä osiot luodaan yleensä GPT-määritteellä, joka estää BitLockeria salaamasta niitä, mutta jos käyttäjä poistaa osiot ja luo ne uudelleen tai luo ne manuaalisesti vain tärkeimmät tiedot sisältävällä asemalla, Sure Recover -agentti ei voi poistaa niitä ja ilmoittaa virheestä osioidessaan asemaa uudelleen. Käyttäjän on poistettava ne manuaalisesti suorittamalla DiskPart-apuohjelma, valitsemalla kyseessä oleva asema ja syöttämällä `del vol` -ohituskomento tai sitä vastaava komento.

Laiteohjelmiston valvontaloki

EFI-muuttujien tiedot ovat seuraavat:

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

EFI-muuttujien lukemiseen voi käyttää Windowsiin sisältyviä ohjelmointirajapintoja, tai muuttujasisällön voi vaihtoehtoisesti vedostaa tiedostoon UEFI Shell dmpstore -apuohjelmaa käyttäen.

Voit vedostaa valvontalokin käyttämällä HP Client Management Script Libraryyn kuuluvaa `Get-HPFirmwareAuditLog`-komentoa.

Windows-tapahtumaloki

Sure Recoverin alku- ja pysähdystapahtumat kirjataan BIOSin valvontalokiin. Voit tarkastella sitä Windowsin tapahtumienvalvonnan kautta Sure Start -lokissa, jos HP Notifications -ilmoitukset ovat asennettuina. Näihin tapahtumiin kuuluvat aika ja päivämäärä, lähteen tunnus, tapahtuman tunnus sekä tapahtumakohtainen koodi. Esimerkiksi `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` ilmaisee, että palautus epäonnistui, koska kokoonpanotietoja ei voitu vahvistaa tapahtumakohtaisella koodilla c3f 23000, joka kirjattiin 27.6.2018 kello 2.26.40.

HUOMAUTUS: Nämä lokit noudattavat Yhdysvaltojen päivämäärämuotoilua: kuukausi/päivämäärä/vuosi.

HP Secure Platform Management (lähteen tunniste = 84h)

Taulukko A-1 HP Secure Platform Management

Tapahtuman tunnus	Laitteiden lukumäärä (Kaikki/DaaS)	Tapahtumien lukumäärä (Kaikki/DaaS)	Kuvaus	Huomautukset
40	256/178	943/552	Alustan käyttöjärjestelmän palautusprosessi käynnistettiin laiteohjelmistossa.	Alustan palautus aloitettu

Taulukko A-1 HP Secure Platform Management (jatkoa)

Tapahtuman tunnus	Laitteiden lukumäärä (Kaikki/DaaS)	Tapahtumien lukumäärä (Kaikki/DaaS)	Kuvaus	Huomautukset
41	221/147	588/332	Alustan käyttöjärjestelmän palautusprosessi on suoritettu loppuun.	Alustan palautus suoritettu
42	54/42	252/156	Alustan käyttöjärjestelmän palautusprosessin suorittaminen loppuun epäonnistui.	Alustan palautus epäonnistui

Voit hakea laiteohjelmiston valvontalokin käyttämällä komentoa Get-HPFirmwareAuditLog HP Client Management Script Libraryssa. Se on saatavilla osoitteesta http://www.hp.com/go/clientmanagement. HP Secure Platform Managementin tapahtumatunnukset 40, 41 ja 42 palauttavat tietokenttään tapahtumakohtaiset koodit. Tämä ilmaisee Sure Recover -toimintojen tuloksen. Esimerkiksi seuraava lokimerkintä ilmaisee, että Sure Recover ei onnistunut lataamaan kokoonpanotietoja tai allekirjoitustiedostoa virhetapahtumatunnuksella event_id 42 ja tiedoilla: 00:30:f1:c3, jotka tulee tulkita dword-arvona 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: Alustan käyttöjärjestelmän palautusprosessin suorittaminen
loppuun epäonnistui.

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

Onnistunut palautus näkyy merkintänä event_id = 41 ja sen tiedot ovat: 00:00:00:00, esimerkiksi:

```
Tapahtumakohtaiset koodit

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: Alustan käyttöjärjestelmän palautusprosessin suorittaminen
loppuun epäonnistui.
data: 00:00:00:00
```

HP Sure Recover käyttää seuraavia tapahtumakohtaisia koodeja.

Taulukko A-2 Tapahtumakohtaiset koodit

Tapahtuman kuvaus	Tapahtumakoodi
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